

สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ
Office of the National Land Policy Board

แผนบริหารจัดการ

ความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

โครงการจัดทำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศ
และการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

โครงการจัดทำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำนำ

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ฉบับนี้ จัดทำขึ้นเพื่อให้ผู้ดูแลระบบสารสนเทศและผู้ปฏิบัติงานได้ทราบถึงหน้าที่และความรับผิดชอบในการใช้งานระบบเครือข่ายและระบบสารสนเทศต่าง ๆ มีความเข้าใจและสามารถปฏิบัติตามแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ สคทช. ได้อย่างเหมาะสม เป็นไปตามกฎหมาย กฎระเบียบ และมาตรฐานสากลที่เกี่ยวข้อง เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลมาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565 ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ 2562 และมาตรฐาน ISO/IEC27001:2022 เป็นต้น เพื่อป้องกันและลดความเสี่ยงจากการหยุดชะงักที่อาจเกิดขึ้นกับข้อมูลสารสนเทศ อุปกรณ์สารสนเทศ กระบวนการ บุคคล และธุรกิจของ สคทช. อันเนื่องมาจากภัยคุกคามหรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

สารบัญ

1. บทนำ 13
1.1 คำนิยาม 14
1.1.1 คำนิยามทั่วไป 14
1.1.2 คำนิยามเหตุการณ์ (Event Definition) 20
1.2 องค์ประกอบของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ 21
1.3 ยุทธศาสตร์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568 - 2570 22
1.3.1 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) 25
1.3.2 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) 34
1.3.3 ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard) 39
2. นโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร 42
2.1 บทนำนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร 42
2.1.1 ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร 44
2.1.2 วัตถุประสงค์ของนโยบาย 46
2.1.3 บทบาทและความรับผิดชอบ 46
2.1.4 การปฏิบัติตามกฎหมายและมาตรฐาน 46
2.1.5 แนวทางการปรับปรุงและพัฒนา 47
2.1.6 ผลลัพธ์ที่คาดหวัง 47
2.1.7 องค์ประกอบของนโยบาย 47
2.2 มาตรการที่ 1 มาตรการควบคุมด้านองค์กร (Organizational controls) 48
2.2.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security) 48
2.2.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities) 48
2.2.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties) 49
2.2.4 หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities) 49
2.2.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities) 50
2.2.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups) 50
2.2.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence) 50
2.2.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management) 51
2.2.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Inventory of information and other associated assets) 51

2.2.10 การใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)....52
2.2.11 การคืนทรัพย์สิน (Return of assets)....52
2.2.12 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification of information)....53
2.2.13 การทำป้ายบ่งชี้สารสนเทศ (Labelling of information)....53
2.2.14 การถ่ายโอนสารสนเทศ (Information transfer)....53
2.2.15 การควบคุมการเข้าถึง (Access control)....54
2.2.16 การบริหารจัดการพิสูจน์ตัวตน (Identity management)....54
2.2.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)....54
2.2.18 การควบคุมสิทธิ์และการเข้าถึงระบบสารสนเทศ (Access rights)....56
2.2.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)....56
2.2.20 การระบุถึงความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงกับผู้ให้บริการภายนอก (Addressing Information security within supplier agreements)....56
2.2.21 การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและ การสื่อสาร (Managing information security in the ICT supply chain)....57
2.2.22 การติดตาม ทบทวน และการจัดการ การเปลี่ยนแปลงสำหรับบริการของผู้ให้บริการภายนอก (Monitoring, Review and change management of supplier services)....57
2.2.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)....57
2.2.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)....58
2.2.25 การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)....58
2.2.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)....59
2.2.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)....59
2.2.28 การรวบรวมหลักฐาน (Collection of evidence)....60
2.2.29 ความมั่นคงปลอดภัยสารสนเทศในช่วงภาวะหยุดชะงัก (Information security during disruption)....60
2.2.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)60
2.2.31 ความมั่นคงปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด (Legal, Statutory, Regulatory and Contractual requirements)....61
2.2.32 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)....62
2.2.33 การป้องกันบันทึก (Protection of records)....62
2.2.34 การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล (Privacy and protection of PII)62
2.2.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)....63

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานสำหรับความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security).....64
2.2.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures) 64
2.3 มาตรการที่ 2 มาตรการควบคุมด้านบุคลากร (People controls).....65
2.3.1 การคัดกรอง (Screening).....65
2.3.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment).....65
2.3.3 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศข้อกำหนด (Information security awareness, education and training) 66
2.3.4 กระบวนการทางวินัย (Disciplinary Process).....66
2.3.5 ความรับผิดชอบหลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment).....67
2.3.6 ข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (NDA) (Confidentiality or non-disclosure agreements).....67
2.3.7 การปฏิบัติงานจากระยะไกล (Remote Working).....67
2.3.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting).....68
2.4 มาตรการที่ 3 มาตรการควบคุมด้านกายภาพ (Physical Controls) 68
2.4.1 ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters) 68
2.4.2 การเข้า - ออกพื้นที่ทางกายภาพ (Physical entry).....68
2.4.3 การรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities).....69
2.4.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring).....69
2.4.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats) 70
2.4.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas).....70
2.4.7 การจัดเก็บโต๊ะทำงาน และการจัดการหน้าจอ (Clear desk and clear screen) 71
2.4.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection).....71
2.4.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสถานที่ (Security of assets off-premises) 71
2.4.10 สื่อบันทึกข้อมูล (Storage Media) 72
2.4.11 ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities).....72
2.4.12 การรักษาความมั่นคงปลอดภัยของการเดินสาย (Cabling Security).....73
2.4.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance) 73
2.4.14 การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment) 74
2.5 มาตรการที่ 4 มาตรการควบคุมด้านเทคโนโลยี (Technological Controls) 74
2.5.1 อุปกรณ์ของผู้ใช้งาน (User endpoint devices) 74
2.5.2 สิทธิพิเศษในการเข้าถึงสารสนเทศ (Privileged access rights) 75
2.5.3 การจำกัดการเข้าถึงระบบสารสนเทศ (Information access restriction).....75

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.5.4 การเข้าถึงโปรแกรมต้นฉบับ (Access to source code) 76
2.5.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication) 76
2.5.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity management) 76
2.5.7 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection against malware) 76
2.5.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities) 77
2.5.9 การบริหารจัดการ การกำหนดค่า (Configuration management) 78
2.5.10 การลบข้อมูล (Information deletion) 78
2.5.11 การซ่อนข้อมูล (Data masking) 79
2.5.12 การป้องกันการรั่วไหลของข้อมูล (Data leakage prevention) 80
2.5.13 การสำรองข้อมูล (Information backup) 80
2.5.14 ระบบทดแทน (Redundancy of information processing facilities) 81
2.5.15 การลงบันทึกเหตุการณ์ (Logging) 81
2.5.16 กิจกรรมการเฝ้าติดตาม (Monitoring activities) 82
2.5.17 การตั้งค่านาฬิกาและเวลาให้ตรงกัน (Clock synchronization) 82
2.5.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs) 82
2.5.19 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of software on operational systems) 83
2.5.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security) 83
2.5.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services) 84
2.5.22 การแบ่งแยกเครือข่าย (Segregation of networks) 85
2.5.23 การกรองเว็บ (Web filtering) 85
2.5.24 การเข้ารหัสข้อมูล (Use of cryptography) 86
2.5.25 วงจรการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure development life cycle) 87
2.5.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements) 88
2.5.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles) 88
2.5.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure coding) 90
2.5.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาระบบและการยอมรับ (Security testing in development and acceptance) 90
2.5.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development) 90
2.5.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง (Separation of development, test and production environments) 91
2.5.32 การบริหารจัดการ การเปลี่ยนแปลง (Change management) 91
2.5.33 ข้อมูลในการทดสอบ (Test information) 92
2.5.34 การป้องกันระบบสารสนเทศระหว่างทดสอบในการตรวจประเมิน (Protection of information systems during audit testing) 92
3. แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร 92

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.1 บทนำแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร....94
3.1.1 ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร....94
3.1.2 ข้อมูลติดต่อและการยกระดับการดำเนินการ (Contact Information and Escalation Level) 95
3.1.3 หน้าที่และความรับผิดชอบ (Roles and Responsibilities)....96
3.2 กรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Framework)....100
3.2.1 ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation)....103
3.2.2 ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)....104
3.2.3 ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)....111
3.2.4 ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (After-Action Review Process)....118
3.3 การแจ้งเตือนและการสื่อสาร (Notification and Communication)....120
3.3.1 การปฏิสัมพันธ์กับการบังคับใช้กฎหมาย (InterAction with Law Enforcement)....121
3.3.2 หน่วยงานควบคุมหรือกำกับดูแล (Regulatory Authorities)....121
3.3.3 ผู้รับบริการ (Customers)....122
3.3.4 การจัดการสื่อสาธารณะ (Public Media Handling)....122
3.4 แผนการทดสอบและทบทวน (Plan Testing and Review)....122
3.5 รายละเอียดการซ้อมแผนบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์....123
3.6 ภาคผนวกแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร....124
3.6.1 ภาคผนวก 1 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการ เฝ้าระวัง (Monitoring)....124
3.6.2 ภาคผนวก 2 การอ้างอิงการประเมินเหตุการณ์สองนาที (Two Minute Incident Assessment Reference)....125
3.6.3 ภาคผนวก 3 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist) 126
3.6.4 ภาคผนวก 4 ข้อกำหนดการแจ้งเตือน (Notification Requirements)....127
3.6.5 ภาคผนวก 5 แถลงการณ์ของสื่อ....129
3.6.6 ภาคผนวก 6 เทมเพลตจดหมายผู้รับบริการ (Customer Letter Template)....134
3.6.7 ภาคผนวก 7 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Organizations)....135
3.6.8 ภาคผนวก 8 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)....135
3.6.9 ภาคผนวก 9 ข้อตกลงการประกันภัยทางไซเบอร์และการบริการบุคคลที่สาม (Cyber Insurance and Third-Party Service Agreements)....138
3.6.10 ภาคผนวก 10 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด .. 139
4. แผนการตรวจสอบและประเมินผลการปฏิบัติงาน 140
4.1 แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์....140
4.1.1 บทนำแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์....141
4.1.2 การอนุมัติผู้ตรวจสอบ....142
4.1.3 ความคาดหวังในการตรวจสอบ....142

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4.1.4 ขั้นตอนการปฏิบัติในการตรวจสอบ 150
4.1.5 การจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ 151
4.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 153
4.2.1 บทนำการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ 153
4.2.2 สร้างบริบทความเสี่ยง 156
4.2.3 ดำเนินการประเมินความเสี่ยง 160
4.2.4 ตอบสนองต่อความเสี่ยง 164
5. แผนที่นำทาง (Road Map) ในการนำแผนฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรม 165
5.1 บทนำของแผนที่นำทาง (Road Map) 165
5.1.1 ตัวชี้วัดของแผนที่นำทาง (Road Map) 165
5.1.2 การจัดลำดับความสำคัญของการดำเนินงาน 169
5.2 แผนที่นำทาง (Road Map) ในระยะ 3 ปี (พ.ศ. 2568-2570) 171
5.3 แนวทางการดำเนินงานและแผนพัฒนาสำหรับสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ในระยะถัดไป (ปี พ.ศ. 2571-2575 และ 2576-2580) 173
5.3.1 แผนปี พ.ศ. 2571 - 2575: "บูรณาการความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการที่ดิน" (Integrating Cybersecurity and Land Management) 174
5.3.2 แผนปี พ.ศ. 2576 - 2580: "การบริหารจัดการที่ดินอย่างยั่งยืนด้วย Blockchain และนวัตกรรม" (Blockchain-Driven Land Management for Sustainability) 174
5.3.3 แนวทางการพัฒนาทั้งสองช่วง (พ.ศ. 2571 - 2580) 175
6. กลไกการดำเนินงาน 176
6.1 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) 189
6.2 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) 198
6.3 ยุทธศาสตร์ที่ 3 การขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดี (Driving Security with Good Governance) 201
7. ข้อเสนอเพื่อเพิ่มแผนเร่งด่วนในแผนแม่บทของสำนักงานคณะกรรมการ นโยบายที่ดินแห่งชาติ (สคทช.) 203
8. ภาคผนวกความเชื่อมโยงของแผนฯ และการตอบสนองของแผนฯ ต่อการประเมินต่าง ๆ 205
8.1 ความเชื่อมโยงระหว่างนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรฐานสากล ISO 27002 : 2022 205
8.2 ความเชื่อมโยงระหว่างกลุ่มผู้รับผิดชอบและแนวปฏิบัติ 209
8.3 ความเชื่อมโยงระหว่างแนวปฏิบัติ และยุทธศาสตร์ในแผนที่นำทาง (Road Map) 220
8.4 การตอบสนองของแผนฯ ต่อการประเมินการปรับเปลี่ยนหน่วยงานไปสู่ความเป็นดิจิทัลในระบบการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร. 228
8.5 การตอบสนองของแผนฯ ต่อการสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. 230
8.6 แบบฟอร์มการวัดผลตัวชี้วัด 234

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

สารบัญตาราง

ตารางที่ 1-1 คำนิยามทั่วไป 20
ตารางที่ 1-2 ยุทธศาสตร์และกลยุทธ์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร 23
ตารางที่ 1-3 ความสอดคล้องของยุทธศาสตร์ 24
ตารางที่ 1-4 ตัวชี้วัดยุทธศาสตร์ที่ 1 และค่าเป้าหมาย 27
ตารางที่ 1-5 ตัวชี้วัดยุทธศาสตร์ที่ 1 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง 28
ตารางที่ 1-6 ตัวชี้วัดและค่าเป้าหมาย 1.1 29
ตารางที่ 1-7 คำอธิบายตัวชี้วัด 1.1 29
ตารางที่ 1-8 ตัวชี้วัดและค่าเป้าหมาย 1.2 30
ตารางที่ 1-9 คำอธิบายตัวชี้วัด 1.2 30
ตารางที่ 1-10 ตัวชี้วัดและค่าเป้าหมาย 1.3 32
ตารางที่ 1-11 คำอธิบายตัวชี้วัด 1.3 32
ตารางที่ 1-12 ตัวชี้วัดและค่าเป้าหมาย 1.4 33
ตารางที่ 1-13 คำอธิบายตัวชี้วัด 1.4 34
ตารางที่ 1-14 ตัวชี้วัดยุทธศาสตร์ที่ 2 และค่าเป้าหมาย 35
ตารางที่ 1-15 ตัวชี้วัดยุทธศาสตร์ที่ 2 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง 35
ตารางที่ 1-16 ตัวชี้วัดและค่าเป้าหมาย 2.1 36
ตารางที่ 1-17 คำอธิบายตัวชี้วัด 2.1 37
ตารางที่ 1-18 ตัวชี้วัดและค่าเป้าหมาย 2.2 38
ตารางที่ 1-19 คำอธิบายตัวชี้วัด 2.2 39
ตารางที่ 1-20 ตัวชี้วัดยุทธศาสตร์ที่ 3 และค่าเป้าหมาย 40
ตารางที่ 1-21 ตัวชี้วัดยุทธศาสตร์ที่ 3 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง 40
ตารางที่ 1-22 ตัวชี้วัดและค่าเป้าหมาย 3.1 41
ตารางที่ 1-23 คำอธิบายตัวชี้วัด 3.1 41
ตารางที่ 2-1 ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร 45

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตารางที่ 2-2 การควบคุมการจัดวางอุปกรณ์สารสนเทศตามระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ 69
ตารางที่ 3-1 ข้อมูลติดต่อและการยกระดับการดำเนินการ 96
ตารางที่ 3-2 ข้อมูลสมาชิกทีม CIRT (CIRT Team Members) 100
ตารางที่ 3-3 เปรียบเทียบแนวทางปฏิบัติและประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 102
ตารางที่ 3-4 แนวทางการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Guide) 104
ตารางที่ 3-5 การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization) 106
ตารางที่ 3-6 ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ 106
ตารางที่ 3-7 ตัวอย่างเกณฑ์ผลกระทบการทำงาน (Functional Impact) 108
ตารางที่ 3-8 ตัวอย่างเกณฑ์ผลกระทบต่อสารสนเทศ (Informational Impact) 109
ตารางที่ 3-9 การจำแนกระดับการตอบสนอง 110
ตารางที่ 3-10 ระดับความรุนแรงและการตอบสนองตาม SLA 110
ตารางที่ 3-11 ตัวเลือกการใช้ทรัพยากรตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์ 113
ตารางที่ 3-12 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring) จัดเตรียมโดย (Prepared by) วันที่ปรับปรุง (Date updated) 124
ตารางที่ 3-13 การประเมินผลกระทบ/ผลกระทบที่อาจเกิดขึ้น และแนวทางการตอบสนอง 126
ตารางที่ 3-14 แนวทางการสื่อสาร 126
ตารางที่ 3-15 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist) 127
ตารางที่ 3-16 ตัวอย่างการระบุข้อกำหนดทั้งหมดที่ใช้กับหน่วยงาน 127
ตารางที่ 3-17 ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์ 128
ตารางที่ 3-18 ตัวอย่างการกำหนดช่องทางสื่อสารและวิธีการเผยแพร่ข้อมูล 129
ตารางที่ 3-19 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ 135
ตารางที่ 3-20 เกณฑ์ Service Level Agreement 138
ตารางที่ 3-21 การสนับสนุนและการตอบสนองของบุคคลที่สาม 139
ตารางที่ 3-22 ความคุ้มครองประกันภัยและข้อมูลการติดต่อ 139
ตารางที่ 3-23 ตัวอย่างการกำหนดการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ 140

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตารางที่ 4-1 ขอบเขตการตรวจสอบ (Audit Scope)..... 145
ตารางที่ 4-2 แบบฟอร์มข้อค้นพบการตรวจสอบ..... 149
ตารางที่ 4-3 รายงานการตรวจสอบ..... 150
ตารางที่ 4-4 แบบฟอร์มการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)..... 153
ตารางที่ 4-5 ระดับที่โอกาสความเสี่ยงที่จะเกิดขึ้น (Likelihood)..... 157
ตารางที่ 4-6 ระดับผลกระทบ (Impact)..... 158
ตารางที่ 4-7 ตารางระดับความเสี่ยง..... 158
ตารางที่ 4-8 ตารางการยอมรับความเสี่ยง..... 159
ตารางที่ 5-1 ความสอดคล้องของตัวชี้วัดยุทธศาสตร์ของแผนฯ กับตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators) ของแผนที่นำทาง (Road Map)..... 166
ตารางที่ 6-1 การจัดลำดับความสำคัญโดยพิจารณาจากความเกี่ยวข้องกับกฎหมายและแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ..... 179
ตารางที่ 6-2 สรุปผลการจัดลำดับความสำคัญโดยพิจารณาจากความเกี่ยวข้องกับกฎหมายและแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ..... 180
ตารางที่ 6-3 เหตุผลประกอบการพิจารณาระดับความสำคัญของโครงการ..... 184
ตารางที่ 6-4 สรุปผลการเรียงลำดับความสำคัญและความเร่งด่วนของโครงการ..... 185
ตารางที่ 6-5 รายละเอียดความสอดคล้องของโครงการตามยุทธศาสตร์ กลยุทธ์ และความสอดคล้องกับตัวชี้วัดต่าง ๆ..... 188
ตารางที่ 6-6 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)..... 197
ตารางที่ 6-7 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)..... 200
ตารางที่ 6-8 ยุทธศาสตร์ที่ 3 การขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดี (Driving Security with Good Governance)..... 202
ตารางที่ 8-1 ความเชื่อมโยงระหว่างนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรฐานสากล ISO 27002 : 2022..... 209
ตารางที่ 8-2 ความเชื่อมโยงระหว่างกลุ่มผู้รับผิดชอบและแนวปฏิบัติ..... 219
ตารางที่ 8-3 ความเชื่อมโยงระหว่างแนวปฏิบัติ และยุทธศาสตร์ในแผนที่นำทาง (Road Map)..... 227

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตารางที่ 8-4 ความสอดคล้องของแผนกับการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร. 229

ตารางที่ 8-5 การตอบสนองของแผนฯ ต่อการสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. 233

ตารางที่ 8-6 แบบฟอร์มการวัดผลตัวชี้วัด 234

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

สารบัญรูปภาพ

รูปที่ 1-1: ยุทธศาสตร์ของบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ 25

รูปที่ 2-1: 4 มาตรการ สำหรับนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านไซเบอร์ 42

รูปที่ 3-1: แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร 92

รูปที่ 4-1: หลักการตรวจสอบ (Principles of Auditing) 143

รูปที่ 5-1: แผนที่นำทาง (Road Map) 171

รูปที่ 8-1: กรอบแนวทางการประเมินส่วนราชการฯ ประจำปีงบประมาณ 2567 228

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

1. บทนำ

ในยุคดิจิทัลที่เทคโนโลยีสารสนเทศและการสื่อสารมีบทบาทสำคัญต่อการดำเนินงานของทุกองค์กร ความมั่นคงปลอดภัยทางไซเบอร์ถือเป็นปัจจัยสำคัญที่ต้องให้ความสำคัญอย่างสูงสุด โดยเฉพาะสำหรับสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ซึ่งมีภารกิจหลักในการบริหารจัดการข้อมูลที่ดินและทรัพยากรดินที่มีความสำคัญต่อประเทศ การจัดทำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารฉบับนี้ ได้รับการพัฒนาโดยอาศัยข้อมูลและผลการศึกษา เพื่อให้แผนดังกล่าวมีความครอบคลุมและตอบสนองต่อความต้องการที่แท้จริงขององค์กร

จากผลการศึกษาและการประเมินสถานการณ์ภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร ได้ชี้ให้เห็นถึงรูปแบบภัยคุกคามทางไซเบอร์ที่สำคัญทั้งในระดับประเทศและสากล เช่น การโจมตีด้วยมัลแวร์ (Malware) แรนซัมแวร์ (Ransomware) และการละเมิดข้อมูล (Data Breach) ซึ่งล้วนส่งผลกระทบต่อความน่าเชื่อถือและการดำเนินงานของหน่วยงาน นอกจากนี้ในการศึกษาทบทวนและวิเคราะห์แผนระดับชาติ นโยบาย กฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง ได้ให้กรอบแนวทางที่สำคัญในการพัฒนาแผนฯ โดยเฉพาะการอ้างอิงมาตรฐานสากล เช่น ISO/IEC 27001 และ NIST Cybersecurity Framework รวมถึงข้อกำหนดในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และ การศึกษาบริบทและสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสารของ สคทช. ยังช่วยเสริมความเข้าใจเกี่ยวกับความท้าทายและความต้องการเฉพาะขององค์กร ซึ่งเป็นพื้นฐานสำคัญในการออกแบบแผนฯ ที่ตอบสนองต่อภัยคุกคามและส่งเสริมการดำเนินงานในระยะยาว ในแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ จึงเป็นการรวบรวมและบูรณาการผลการศึกษาทั้งหมด เพื่อนำไปสู่การพัฒนาแผนบริหารจัดการความปลอดภัยไซเบอร์ที่ครบถ้วนและครอบคลุม ประกอบด้วยแนวทางที่เป็นรูปธรรมในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากภัยคุกคาม โดยคำนึงถึงความยั่งยืนและการบูรณาการความร่วมมือในระดับองค์กรและระดับประเทศ

ก่อนการเข้าสู่เนื้อหาหลักของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ มีการระบุรายละเอียดเบื้องต้นเกี่ยวกับองค์ประกอบของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ยุทธศาสตร์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568-2570 และคำนิยามของคำศัพท์ที่เกี่ยวข้องกับแผนฯ ดังกล่าว ซึ่งมีรายละเอียด ดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

1.1 คำนิยาม

1.1.1 คำนิยามทั่วไป

คำนิยามในส่วนนี้เป็นการให้คำจำกัดความสำหรับศัพท์ที่ใช้งานในแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติฉบับนี้ เพื่อให้มีความหมายที่ชัดเจนและเข้าใจตรงกัน

คำศัพท์	ความหมาย
การกู้คืน (Recovery)	การนำข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบสารสนเทศที่เกิดความเสียหายกลับมาใช้งานได้อย่างถูกต้องครบถ้วน
การเข้าถึง (Access)	การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ
การพิสูจน์และยืนยันตัวตน (Identification and Authentication)	กระบวนการพิสูจน์และยืนยันความถูกต้องของตัวบุคคล (อ้างอิงจาก พ.ร.บ. ว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2562)
การสำรองข้อมูล (Backup)	การเก็บรักษาข้อมูลคอมพิวเตอร์ลงในสื่อที่ได้เตรียมการไว้แล้ว และจะถูกนำมาใช้งานแทนในกรณีที่ข้อมูลหลักที่กำลังถูกใช้ในการปฏิบัติงานอยู่เกิดความเสียหาย
ความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศ (Cyber and Information Security)	มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกหน่วยงาน
เครือข่าย (Network)	ระบบที่เกิดจากการนำเครื่องคอมพิวเตอร์ตั้งแต่ 2 เครื่องขึ้นไปมาต่อเชื่อมโยงเข้าด้วยกัน เพื่อแลกเปลี่ยนข้อมูลข่าวสาร หรือใช้ทรัพยากรต่าง ๆ
ซอฟต์แวร์ (Software)	โปรแกรมคอมพิวเตอร์หรือโปรแกรมประยุกต์ประเภทใด ๆ ก็ได้ ตั้งแต่ระบบปฏิบัติการเช่น ดอส (Dos) โปรแกรมอำนวยประโยชน์ระบบงาน จนกระทั่งโปรแกรมที่เก็บอยู่ในรอม (Rom)
ไซเบอร์ (Cyber)	ข้อมูลและการสื่อสารที่เกิดจากการให้บริการหรือการประยุกต์ใช้เครือข่ายคอมพิวเตอร์ ระบบอินเทอร์เน็ต หรือโครงข่ายโทรคมนาคม รวมทั้งการให้บริการโดยปกติของดาวเทียมและระบบเครือข่ายที่คล้ายคลึงกันที่เชื่อมต่อกันเป็นการทั่วไป (อ้างอิงจาก พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
ทรัพย์สิน (Assets)	สิ่งที่มีมูลค่าต่อ สคทช. และเป็นเจ้าของ เช่น ว่าจ้าง หรือพัฒนาเป็นต้น
ทรัพย์สินสารสนเทศ	1. ระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ 2. ตัวเครื่องคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ เครื่องบันทึกข้อมูล และอุปกรณ์อื่นใด 3. ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์ (อ้างอิงจาก พระราชกฤษฎีกา ว่าด้วย วิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2553)
ผู้ใช้งาน (Users)	ผู้ทดลองงาน พนักงาน และลูกจ้างของ สคทช. รวมถึงหน่วยงานภายนอก บุคลากรของหน่วยงานภายนอกที่ปฏิบัติงานให้ สคทช.

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
	ที่ได้รับสิทธิ์เข้าถึงสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศของ สคทช.
ผู้ดูแลระบบ (Administrator)	ผู้ปฏิบัติงาน (Employee)
ผู้พัฒนาระบบ (Developer)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการพัฒนาและปรับปรุงระบบงานสารสนเทศ
ระบบสารสนเทศ (Information System)	ระบบคอมพิวเตอร์และการเก็บบันทึกข้อมูลซึ่งมีการประมวลผลด้วยระบบคอมพิวเตอร์
สารสนเทศ (Information)	ข้อมูลคอมพิวเตอร์หรือข้อความที่ได้มีการประมวลผล เช่น ทรัพย์สินประเภทฐานข้อมูล (Database) และไฟล์ข้อมูล (Data file) สัญญา (Contract) และข้อตกลง (Agreement) เอกสารและคู่มือระบบงาน (System Document) ข้อมูลวิจัย (Research Document) คู่มือผู้ใช้งาน (User Manual) เอกสารการฝึกอบรม (Training Document) ขั้นตอนการปฏิบัติงาน (Operational or Support Procedure) แผนรองรับความต่อเนื่องทางธุรกิจ (Business Continuity Plan) เอกสาร และข้อมูลจัดเก็บสำรอง (Archived Information) เป็นต้น
สิทธิ์ของผู้ใช้งาน (User Rights)	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์อื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
สิทธิพิเศษ (Privileged Access Right)	สิทธิ์สูงสุดของระบบ หรือสิทธิ์สำหรับผู้ดูแลระบบหรือเทียบเท่า เช่น บัญชีผู้ใช้ Administrators (Windows), Root (Unix) เป็นต้น
เหตุการณ์ (Event Definition)	การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Adverse Events)	เหตุการณ์ที่มีผลเชิงลบ (Events with a Negative Consequence)" หรือ "เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์" หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศ (Cyber and Information Security Event)	เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
ภัยคุกคามทางไซเบอร์ (Incident)	การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือ ข้อมูลอื่นที่เกี่ยวข้อง ภัยคุกคามทางไซเบอร์ อาจมีลักษณะดังต่อไปนี้อย่างน้อยหนึ่งอย่าง ดังนี้: ก. การละเมิด (Violation) นโยบายความมั่นคงปลอดภัยโดยชัดแจ้งหรือโดยนัย ข. ความพยายามในการเข้าถึง (Unauthorized Access) ทรัพยากรสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต ค. การปฏิเสธการให้บริการ (Denial of Service) แก่ทรัพยากรสารสนเทศของหน่วยงาน ง. การใช้ทรัพยากรสารสนเทศ (Unauthorized Use) ของหน่วยงาน โดยไม่ได้รับอนุญาต จ. การแก้ไขข้อมูล (Unauthorized Modification) ของหน่วยงาน โดยไม่ได้รับอนุญาต ฉ. การสูญเสีย (Loss) ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองของหน่วยงาน
อิเล็กทรอนิกส์ (Electronic)	การประยุกต์ใช้วิธีการทางอิเล็กตรอน ไฟฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึงการประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็กหรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ เช่นว่านั้น (อ้างอิงจาก พ.ร.บ. ว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544)
อุปกรณ์สารสนเทศ (Information Processing Facilities)	เครื่องมือ เครื่องใช้ วัสดุ และอุปกรณ์ต่าง ๆ ที่ประมวลผลหรือจัดเก็บสารสนเทศ เช่น คอมพิวเตอร์ กล้องดิจิทัล สื่อบันทึกข้อมูล สแกนเนอร์ เครื่องพิมพ์
การจ้างงาน (Employment)	การว่าจ้างผู้ปฏิบัติงาน หรือหน่วยงานภายนอก เพื่อปฏิบัติงานหรือให้บริการแก่ สคทช.
การปฏิบัติงานจากระยะไกล (Teleworking)	การทำงานที่บ้านหรือสถานที่ตั้งภายนอกองค์กรอื่น ๆ ที่มีการเชื่อมต่อทางอิเล็กทรอนิกส์โดยผ่านทางเครื่องคอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์พกพาหรือเครื่องโทรสาร เป็นต้น ไปยัง สคทช. หรือสถานที่อื่นอันเป็นสถานที่ทำงานหลัก
ข้อมูลส่วนบุคคล (Personal Data)	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ (อ้างอิงจาก พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562)
เปลี่ยนแปลงการจ้างงาน (Change of Employment)	เปลี่ยนแปลงหน้าที่รับผิดชอบของผู้ปฏิบัติงานในหน่วยงานต้นสังกัด หรือเงื่อนไขการว่าจ้างของหน่วยงานภายนอก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
ดัดแปลง (Tamper)	ทำซ้ำโดยเปลี่ยนรูปใหม่ ปรับปรุงแก้ไขเพิ่มเติม หรือจำลองงานต้นฉบับในส่วนอันเป็นสาระสำคัญโดยไม่มีลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน ในส่วนที่เกี่ยวกับโปรแกรมประยุกต์ ให้หมายความรวมถึง ทำซ้ำโดยเปลี่ยนรูปใหม่ ปรับปรุง แก้ไขเพิ่มเติมโปรแกรมประยุกต์ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำขึ้นใหม่ (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2537)
ทำซ้ำ (Copy)	คัดลอกไม่ว่าโดยวิธีใด ๆ เลียนแบบ ทำสำเนา ทำแม่พิมพ์ บันทึกเสียง บันทึกภาพ หรือ บันทึกเสียงและภาพ จากต้นฉบับ หรือจากการโฆษณาในส่วนอันเป็นสาระสำคัญ ทั้งนี้ ไม่ว่าทั้งหมดหรือบางส่วน สำหรับในส่วนที่เกี่ยวกับโปรแกรมประยุกต์ ให้หมายความถึง คัดลอกหรือทำสำเนาโปรแกรมประยุกต์จากสื่อบันทึกใด ๆ ไม่ว่าด้วยวิธีใด ๆ ในส่วนอันเป็นสาระสำคัญ โดยไม่มีลักษณะเป็นการจัดทำงานขึ้นใหม่ ทั้งนี้ไม่ว่าทั้งหมดหรือบางส่วน (อ้างอิงจาก พระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537)
ลิขสิทธิ์ (Copyright)	สิทธิ์แต่ผู้เดียวที่จะทำการใด ๆ ตามพระราชบัญญัติลิขสิทธิ์ พ.ศ. 2537 เกี่ยวกับงานที่ผู้สร้างสรรค์ได้ทำขึ้น (อ้างอิงจาก พ.ร.บ. ลิขสิทธิ์ พ.ศ. 2565)
โปรแกรมประยุกต์ (Program)	คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่ทำไปใช้กับเครื่องคอมพิวเตอร์ เพื่อให้เครื่องคอมพิวเตอร์ทำงานหรือเพื่อให้ได้รับผลอย่างหนึ่งอย่างใด ทั้งนี้ ไม่ว่าจะเป็นภาษาโปรแกรมในลักษณะใด
โปรแกรมไม่พึงประสงค์ (Malicious Software)/ มัลแวร์ (Malware)	โปรแกรมหรือชุดโปรแกรมที่ทำให้สารสนเทศ หรือระบบสารสนเทศเกิดความเสียหายโดยตั้งใจ เช่น ไวรัส (Virus) เวิร์ม (Worm) โทรจัน (Trojan) แอดแวร์ (Adware) หรือสปายแวร์ (Spyware) เป็นต้น
ผู้ปฏิบัติงาน (Employee)	ผู้ทดลองงาน พนักงาน พนักงานสัญญาจ้างพิเศษ ลูกจ้างทดลองงาน และลูกจ้างของ สคทช.
ผู้ดูแลห้องคอมพิวเตอร์ (Computer Room Administrator)	ผู้ที่ได้รับมอบหมายให้มีหน้าที่ดูแลรับผิดชอบห้องคอมพิวเตอร์
ระบบคอมพิวเตอร์ (Computer System)	อุปกรณ์คอมพิวเตอร์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ (อ้างอิงจากพ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550)
ศูนย์คอมพิวเตอร์ (Data Center)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์ประมวลผลสารสนเทศ ที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”
สื่อบันทึกข้อมูล (Removable Media Device)	เอกสารที่เป็นกระดาษ หรืออุปกรณ์ที่ใช้ในการบันทึกข้อมูลอิเล็กทรอนิกส์ เช่น เทป ดิสก์ CD DVD Thumb drive เป็นต้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
ห้องคอมพิวเตอร์ (Computer Room)	สถานที่ที่ใช้ในการจัดวางอุปกรณ์ประมวลผลสารสนเทศ ที่ประมวลผลหรือจัดเก็บสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “ปานกลาง”
หัวหน้าศูนย์คอมพิวเตอร์ (Data Center Manager)	หัวหน้างานของศูนย์คอมพิวเตอร์
อุปกรณ์คอมพิวเตอร์พกพา (Mobile Device)	อุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารที่สะดวกในการพกพา เช่น คอมพิวเตอร์โน้ตบุ๊ค (Notebook/Laptop) โทรศัพท์มือถือ (Smartphone) เป็นต้น
อุปกรณ์ประมวลผลสารสนเทศ (Information Processing Facilities)	ระบบสารสนเทศ ระบบเครือข่าย สถานที่ตั้งทางกายภาพของระบบสารสนเทศและระบบเครือข่าย ตลอดจนอุปกรณ์และระบบสนับสนุนต่าง ๆ เช่น ระบบไฟฟ้า ระบบการสื่อสาร ระบบแหล่งจ่ายน้ำแก๊ส ระบบบำบัด ระบบระบายอากาศ ระบบทำความเย็น ระบบปรับอากาศ ระบบควบคุมอุณหภูมิและความชื้น เป็นต้น
แอปพลิเคชัน (Application)	โปรแกรมประยุกต์หรือกลุ่มของโปรแกรม ซึ่งทำหน้าที่เพื่อจุดประสงค์อย่างใดอย่างหนึ่ง เช่น เวิร์ดโปรเซสเซอร์ (Word Processor) สเปรดชีต (Spreadsheet) ฐานข้อมูล (Database) เป็นต้น
บล็อกเชน (blockchain)	วิธีการเก็บข้อมูลรายการเปลี่ยนแปลงตามหลักการทางบัญชี โดยการเข้ารหัสและจัดเรียงข้อมูลเหล่านี้ต่อกันตามลำดับเวลาที่ข้อมูลเข้ามา กลุ่มข้อมูลดังกล่าวจะเผยแพร่ไปให้ผู้ใช้ในเครือข่ายที่กำหนดได้ทราบทั่วกัน ทั้งนี้ ผู้ใช้ทุกคนจะทราบการแก้ไขเพิ่มเติมรายการเปลี่ยนแปลงในบล็อกเชนทุกรายการตลอดเวลา
ปัญญาประดิษฐ์ (เอไอ) (artificial intelligence (AI))	สาขาหนึ่งของวิทยาการคอมพิวเตอร์ ซึ่งเน้นเรื่องที่จะทำให้คอมพิวเตอร์ทำงานได้ใกล้เคียงมนุษย์มากขึ้น แบ่งย่อยออกเป็นสาขาต่าง ๆ เช่น การแปลภาษาด้วยเครื่อง ระบบผู้เชี่ยวชาญ วิทยาการหุ่นยนต์ การรู้จำแบบ การรับรู้เยี่ยงมนุษย์ (human perception) ฯลฯ
การละเมิดข้อมูลส่วนบุคคล	การละเมิดมาตรการรักษาความมั่นคงปลอดภัย ที่ทำให้เกิดการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ ไม่ว่าจะเกิดจากเจตนา ความจงใจ ความประมาทเลินเล่อ การกระทำโดยปราศจากอำนาจหรือโดยมิชอบ การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ภัยคุกคามทางไซเบอร์ ข้อผิดพลาดบกพร่องหรืออุบัติเหตุ หรือเหตุอื่นใด
การละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)	มีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล โดยปราศจากอำนาจหรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่อง หรืออุบัติเหตุ
การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)	มีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วนโดยปราศจากอำนาจ หรือโดยมิชอบ หรือเกิดจากข้อผิดพลาดบกพร่องหรืออุบัติเหตุ
การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)	ทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ
ฝาแฝดดิจิทัล (Digital Twin)	แบบโมเดลจำลองเสมือนจากวัตถุทางกายภาพ ทำให้สามารถทำงานได้เหมือนกับวัตถุจริง ซึ่งวัตถุในที่นี้อาจจะเป็น รถยนต์ ตึก หรือแม้กระทั่งเมืองหนึ่งในโลก มีการติดตั้งตัวเซนเซอร์บนวัตถุจริง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
	หลายตัว ทำหน้าที่เป็นกลไกเชื่อมต่อกันระหว่างตัววัตถุทางกายภาพกับวัตถุเสมือนเชื่อมต่อกันแบบ Real-time ข้อมูลที่เชื่อมเป็นข้อมูลในมุมมองต่าง ๆ ของวัตถุกายภาพเช่น ข้อมูลการใช้พลังงาน อุณหภูมิ สภาพอากาศ ข้อมูลพวกนี้ก็จะถูกนำมาใช้ให้กับตัวแบบโมเดลจำลองนี้ที่อยู่ในรูปแบบของดิจิทัล จะถูกใช้ในการสร้างแบบจำลอง ศึกษาประสิทธิภาพ หรือทดลองการพัฒนา ทำให้สามารถนำกลับไปปรับใช้ในการพัฒนาของวัตถุทางกายภาพได้ ทั้งนี้ตัว Digital Twin จะต่างกับการทำ Simulation ตรงที่ตัว Digital Twin จะมีการแลกเปลี่ยนข้อมูลของสภาพแวดล้อมจริง และแลกเปลี่ยนข้อมูลไปกลับระหว่างวัตถุจริงกับวัตถุเสมือนแบบ Real-time
ข้อมูลส่วนบุคคล	ข้อมูลเกี่ยวกับบุคคลซึ่งทำให้สามารถระบุตัวบุคคลนั้นได้ ไม่ว่าทางตรงหรือทางอ้อม แต่ไม่รวมถึงข้อมูลของผู้ถึงแก่กรรมโดยเฉพาะ
ข้อมูลส่วนบุคคลอ่อนไหว	ข้อมูลส่วนบุคคลเกี่ยวกับเชื้อชาติ เผ่าพันธุ์ ความคิดเห็นทางการเมือง ความเชื่อในลัทธิ ศาสนาหรือปรัชญา พฤติกรรมทางเพศ ประวัติอาชญากรรม ข้อมูลสุขภาพ ความพิการ ข้อมูลสหภาพแรงงาน ข้อมูลพันธุกรรม ข้อมูลชีวภาพ หรือข้อมูลอื่นใด ซึ่งกระทบต่อเจ้าของข้อมูลส่วนบุคคลในทำนองเดียวกันตามที่คณะกรรมการประกาศกำหนด
ผู้ควบคุมข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งมีอำนาจหน้าที่ตัดสินใจ เกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล
ผู้ประมวลผลข้อมูลส่วนบุคคล	บุคคลหรือนิติบุคคลซึ่งดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ หรือเปิดเผยข้อมูลส่วนบุคคลตามคำสั่งหรือในนามของผู้ควบคุมข้อมูลส่วนบุคคล ทั้งนี้ บุคคลหรือนิติบุคคลซึ่งดำเนินการดังกล่าวไม่เป็นผู้ควบคุมข้อมูลส่วนบุคคล
มาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์	การแก้ไขปัญหาความมั่นคงปลอดภัยไซเบอร์โดยใช้บุคลากร กระบวนการ และเทคโนโลยี โดยผ่านคอมพิวเตอร์ ระบบคอมพิวเตอร์ โปรแกรมคอมพิวเตอร์ หรือบริการที่เกี่ยวกับคอมพิวเตอร์ใด ๆ เพื่อสร้างความมั่นใจ และเสริมสร้างความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชนใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	หน่วยงานของรัฐหรือ หน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ข้อมูลคอมพิวเตอร์	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย
ข้อมูลจราจรทางคอมพิวเตอร์	ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำศัพท์	ความหมาย
	ระยะเวลา ชนิดของบริการ หรืออื่นๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น
Managed Security Service Provider: MSSP	บริษัทหรือผู้ที่ให้บริการดูแลรักษาความปลอดภัยข้อมูลองค์กรและป้องกันภัยจากอินเทอร์เน็ต โดยมีหน้าที่ให้บริการคอยเป็นยามตรวจสอบระบบและป้องกันภัยอันตรายที่อาจเกิดขึ้นกับข้อมูล ไม่ว่าจะเป็นการแฮกข้อมูลจากผู้บุกรุก การตรวจสอบและเตือนภัยจากไวรัสในอินเทอร์เน็ต การคัดกรองเว็บไซต์ (Content Filtering) และอีกหลาย ๆ หน้าที่ที่เกี่ยวข้องกับระบบการรักษาความมั่นคงปลอดภัยสารสนเทศ
Security Operation Center: SOC	ศูนย์ปฏิบัติการเฝ้าระวังความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ที่ทำหน้าที่เฝ้าระวังและป้องกันระบบหรืออุปกรณ์สำคัญขององค์กรจากการถูกบุกรุกหรือการเข้าถึงโดยไม่ได้รับอนุญาต ซึ่งหากมีเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Incident) เกิดขึ้น เช่น ระบบถูกบุกรุก หรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต SOC จะทำหน้าที่ประเมิน ตรวจสอบและแก้ไขเหตุการณ์ที่เกิดขึ้น เพื่อลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับองค์กรให้อยู่ในระดับที่ไม่รุนแรง
Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
แผนดำเนินธุรกิจอย่างต่อเนื่อง (Business Continuity Plan: BCP)	แผนที่กำหนดแนวทางการดำเนินการของหน่วยงานเมื่อเกิดสภาวะวิกฤตหรือภัยต่าง ๆ ที่ส่งผลให้กระบวนการทำงานของหน่วยงานหยุดชะงัก เพื่อให้สามารถกลับมาดำเนินการได้อย่างต่อเนื่อง โดยเฉพาะงานบริการภาครัฐที่สำคัญต่อประชาชน

ตารางที่ 1-1 คำนิยามทั่วไป

1.1.2 คำนิยามเหตุการณ์ (Event Definition)

การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable Occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

1.1.2.1 คำนิยามเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ *(Adverse Events Definition)*

“เหตุการณ์ที่มีผลเชิงลบ (Events with a Negative Consequence)” หรือ “เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์” หมายความว่า เหตุการณ์ที่เกิดจากการกระทำหรือการดำเนินการใด ๆ ที่มิชอบซึ่งกระทำการผ่านทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ซึ่งอาจเกิดความเสียหายหรือผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความมั่นคงปลอดภัยไซเบอร์ของคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์นี้ไม่ใช้กับเหตุการณ์ที่เกิดจากภัยธรรมชาติ ไฟฟ้าขัดข้อง ฯลฯ

1.1.2.2 นิยามภัยคุกคามทางไซเบอร์ (*Incident Definition*)

“เหตุภัยคุกคามทางไซเบอร์” หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์[1] อาจมีลักษณะดังต่อไปนี้อย่างน้อยหนึ่งอย่าง ดังนี้:

ก. การละเมิด (Violation) นโยบายความมั่นคงปลอดภัยโดยชัดแจ้งหรือโดยนัย

ข. ความพยายามในการเข้าถึง (Unauthorized Access) ทรัพยากรสารสนเทศของหน่วยงานโดยไม่ได้รับอนุญาต

ค. การปฏิเสธการให้บริการ (Denial of Service) แก่ทรัพยากรสารสนเทศของหน่วยงาน

ง. การใช้ทรัพยากรสารสนเทศ (Unauthorized Use) ของหน่วยงาน โดยไม่ได้รับอนุญาต

จ. การแก้ไขข้อมูล (Unauthorized Modification) ของหน่วยงาน โดยไม่ได้รับอนุญาต

ฉ. การสูญเสีย (Loss) ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองของหน่วยงาน

1.2 องค์ประกอบของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ **พัฒนาขึ้นจากผลการศึกษาต่าง ๆ เช่น การศึกษาและประเมินสถานการณ์ภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร การศึกษา ทบทวน และวิเคราะห์นโยบาย กฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง รวมไปถึงการศึกษาบริบทและสภาพแวดล้อมด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ** ทั้งจากการรวบรวมข้อมูลด้วยการสัมภาษณ์หรือจัดประชุมกับผู้บริหารและผู้มีส่วนเกี่ยวข้องในหน่วยงาน ตลอดจนการศึกษาข้อมูลจากเอกสารที่เกี่ยวข้อง เช่น ประกาศคณะกรรมการนโยบายที่ดินแห่งชาติ เรื่อง นโยบายและแผนการบริหารจัดการที่ดินและทรัพยากรดินของประเทศ (พ.ศ. 2566 – 2580) แผนปฏิบัติการด้านการบริหารจัดการที่ดินและทรัพยากรดินของประเทศ (พ.ศ. 2566 – 2570) แผนปฏิบัติราชการระยะ 5 ปี (พ.ศ. 2566 – 2570) ฉบับปรับปรุง ธันวาคม 2566 และแผนพัฒนาศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน พ.ศ. 2566 – 2570 เป็นต้น นำไปสู่ผลการศึกษาการวิเคราะห์จุดแข็ง จุดอ่อน โอกาส และภัยคุกคามทางไซเบอร์ โดยกรอบการวิเคราะห์ SWOT และ TOWS Matrix ในการบริหารจัดการเทคโนโลยีและการสื่อสาร รวมทั้งวิเคราะห์ช่องว่าง (Gap analysis) ซึ่ง**แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ครอบคลุมประเด็นสำคัญ** ได้แก่

1. **นโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร**

[1] Blue Team Handbook: Incident Response Edition, Don Murdoch และ NIST SP800-61r2: Computer Security Incident Handling Guide

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2. **แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร**
3. **แผนการตรวจสอบและประเมินผลการปฏิบัติงาน**
4. **แผนที่นำทาง (Road Map) ในการนำแผนฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรม**

นอกจากนี้เพื่อให้เกิดการดำเนินงานที่สอดคล้องกับแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ จึงมีการระบุ**กลไกการดำเนินงาน**ด้วยโครงการสำคัญต่าง ๆ ที่มีความสอดคล้องกับตัวชี้วัดและยุทธศาสตร์ของแผนฯ ซึ่งมีการระบุรายละเอียดโครงการสำคัญ กลไกและวิธีการปฏิบัติ กรอบระยะเวลา และผู้รับผิดชอบ อีกทั้งในภาคผนวกมีรายละเอียดด้านความเชื่อมโยงของแผนฯ กับกรอบหรือมาตรฐานที่เกี่ยวข้อง ได้แก่

- ความเชื่อมโยงระหว่างนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรฐานสากล ISO 27002:2022
- ความเชื่อมโยงระหว่างกลุ่มผู้รับผิดชอบและแนวปฏิบัติ
- ความสอดคล้องของแผนฯ กับแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
- การตอบสนองของแผนฯ ต่อการประเมินการปรับเปลี่ยนหน่วยงานไปสู่ความเป็นดิจิทัลในระบบการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร.
- การตอบสนองของแผนฯ ต่อการสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร.

1.3 ยุทธศาสตร์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568 - 2570

จากผลการศึกษาการประเมินสถานะปัจจุบันของการรักษาความมั่นคงปลอดภัย พบว่ามีประเด็นการขาดการพัฒนาบุคลากรด้านไซเบอร์ที่เพียงพอ และต้องเสริมสร้างองค์ความรู้ผ่านการฝึกอบรม รวมถึงการศึกษาแนวปฏิบัติด้านมาตรฐาน เช่น ISO/IEC 27001 แนะนำให้เพิ่มศักยภาพบุคลากรและปรับปรุงการใช้เทคโนโลยีในระบบสารสนเทศ ในแผนฯ จึงเน้นการสร้างความเชี่ยวชาญด้านเทคโนโลยีผ่านการวางแผนฝึกอบรมและการใช้นวัตกรรมเพื่อเพิ่มความปลอดภัยในองค์กร ซึ่งเป็นที่มาของ**ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)** โดยประกอบด้วย**กลยุทธ์ที่ 1.1 : เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ** เนื่องจากผลการศึกษามีการระบุความสำคัญของการเฝ้าระวังระบบที่สำคัญ เช่น ระบบที่เก็บข้อมูลที่ดินของประเทศ จำเป็นต้องใช้บริการ Managed Security Service Provider (MSSP) เพื่อเฝ้าระวังและตอบสนองต่อภัยคุกคามอย่างมีประสิทธิภาพ อีกทั้งผลการศึกษาชี้ให้เห็นว่าภัยคุกคามทางไซเบอร์ในประเทศไทยมุ่งเป้าหมายไปยังโครงสร้างพื้นฐานสำคัญ การปรับปรุงโครงสร้างพื้นฐาน เช่น Firewall, IDS/IPS และการเข้ารหัสข้อมูลจึงเป็นสิ่งจำเป็นจึงเป็นที่มาของ**กลยุทธ์ที่ 1.2: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย** สำหรับ**กลยุทธ์ที่ 1.3: พัฒนาทักษะความมั่นคงปลอดภัย** สืบเนื่องจากการวิเคราะห์ความต้องการในการพัฒนาทักษะบุคลากรเพื่อเพิ่มความสามารถในการจัดการภัยคุกคามพบว่า ควรเพิ่มทักษะต่าง ๆ เช่น การอบรมเกี่ยวกับ NIST Cybersecurity Framework และ ISO 27001 และเนื่องจาก e-Learning Platforms มีบทบาทสำคัญในการเพิ่มทักษะและการเรียนรู้ของบุคลากรเพื่อให้ทันกับการเปลี่ยนแปลงของภัยคุกคามไซเบอร์จึงมีการกำหนด**กลยุทธ์ที่ 1.4: บูรณาการหลักสูตรการเรียนรู้ผ่าน Platform ออนไลน์**

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การวิเคราะห์ภัยคุกคามทั้งในและต่างประเทศ พบว่าความร่วมมือระหว่างองค์กรเป็นกุญแจสำคัญในการตอบสนองต่อเหตุการณ์ภัยคุกคาม อีกทั้งข้อมูลจากกรณีศึกษาของสิงคโปร์และสหรัฐฯ ชี้ให้เห็นถึงประโยชน์ของความร่วมมือระหว่างหน่วยงานในการป้องกันภัยไซเบอร์ จึงมีการกำหนด**ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)** เป็นหนึ่งในยุทธศาสตร์ที่สำคัญของแผนฯ ซึ่งยุทธศาสตร์นี้ประกอบด้วย **กลยุทธ์ที่ 2.1: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร**[2] เนื่องจากการแบ่งปันข้อมูลจะช่วยให้องค์กรสามารถปรับตัวและเตรียมการรับมือภัยคุกคามทางไซเบอร์ได้ และ **กลยุทธ์ที่ 2.2: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน** มีที่มาเนื่องจากการวางแผน Business Continuity Plan (BCP) สำหรับระบบสำคัญและการใช้ Cloud Solutions เป็นแนวทางที่เหมาะสมในการลดผลกระทบจากเหตุการณ์ภัยคุกคามทางไซเบอร์

ผลการศึกษาแสดงให้เห็นถึงความสำคัญของการปฏิบัติตามกฎหมายไซเบอร์ เช่น พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ และมาตรฐานสากล เช่น NIST Framework เพื่อยกระดับการจัดการความปลอดภัย การวิเคราะห์มาตรฐานเทคโนโลยีพบว่า การออกแบบระบบจะช่วยยกระดับคุณภาพระบบความปลอดภัยขององค์กร จึงเป็นที่มาของ**ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)** และ**กลยุทธ์ที่ 3.1: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ** ในการนำมาตรฐาน ISO/IEC 27001 และ NIST Framework มาใช้เพื่อเพิ่มความมั่นคงปลอดภัยของข้อมูลและสร้างความน่าเชื่อถือให้กับระบบของหน่วยงาน

จากการศึกษาและวิเคราะห์สามารถกำหนด วิสัยทัศน์ (Vision) ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568-2570 ดังนี้ “การบริหารจัดการที่ดินและทรัพยากรดินของประเทศอย่างมีมาตรฐานและมั่นคงปลอดภัย บนฐานความร่วมมือที่เป็นหนึ่งเดียว”

ยุทธศาสตร์และกลยุทธ์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568-2570 สามารถสรุปได้ ดังนี้

ยุทธศาสตร์	กลยุทธ์
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	กลยุทธ์ที่ 1.1 : เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ
	กลยุทธ์ที่ 1.2: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย
	กลยุทธ์ที่ 1.3: พัฒนาทักษะความมั่นคงปลอดภัย
	กลยุทธ์ที่ 1.4: บูรณาการหลักสูตรการเรียนรู้ผ่าน Platform ออนไลน์
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	กลยุทธ์ที่ 2.1: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร กลยุทธ์ที่ 2.2: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	กลยุทธ์ที่ 3.1: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

ตารางที่ 1-2 ยุทธศาสตร์และกลยุทธ์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

[2] หน่วยงานพันธมิตร หมายถึง หน่วยงานส่วนกลางและภาคีเครือข่ายที่เกี่ยวข้อง รวม 12 หน่วยงาน เช่น กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม กระทรวงเกษตรและสหกรณ์ กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ กระทรวงการคลัง กระทรวงกลาโหม กระทรวงคมนาคม ตลอดจนหน่วยงานอิสระ เช่น สำนักงานผู้ตรวจการแผ่นดิน เป็นต้น ซึ่งปัจจุบันอยู่ระหว่างการเชื่อมโยงข้อมูลภาครัฐเข้าหากัน เพื่อให้เป็นไปตามนโยบายของรัฐบาลในการแก้ไขปัญหาที่ดินอย่างเป็นระบบและเป็นรูปธรรม สร้างศูนย์ราชการเบ็ดเสร็จจุดเดียว รวมถึงการเตรียมพร้อมเข้าสู่รัฐบาลดิจิทัล และรวมถึงหน่วยงานอื่น ๆ ที่จะมีการทำงานร่วมกันในอนาคตด้วย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยิ่งไปกว่านั้น ยุทธศาสตร์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ ปี พ.ศ. 2568-2570 ยังมีความสอดคล้องกับแผนพัฒนาศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน พ.ศ. 2565-2570 และนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570) ตามตารางด้านล่าง

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ	แผนพัฒนาศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน พ.ศ. 2565-2570	นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	**ยุทธศาสตร์ 1** การบูรณาการแบบรวมศูนย์ (Digital Centralization) **ยุทธศาสตร์ 2** การพัฒนานวัตกรรมและบุคลากรดิจิทัล (Digital Innovation & Human Capital) **ยุทธศาสตร์ 3** การสร้างความร่วมมือและเครือข่าย (Digital Collaboration) **ยุทธศาสตร์ 4** การพัฒนาและวางรากฐานเทคโนโลยี (Digital Footing)	**ยุทธศาสตร์ 1** สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity) **ยุทธศาสตร์ 3** สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และ ฟื้นคืนสู่สภาพปกติได้ (Resilience)
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	**ยุทธศาสตร์ 1** การบูรณาการแบบรวมศูนย์ (Digital Centralization) **ยุทธศาสตร์ 3** การสร้างความร่วมมือและเครือข่าย (Digital Collaboration)	**ยุทธศาสตร์ 2** บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) **ยุทธศาสตร์ 3** สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และ ฟื้นคืนสู่สภาพปกติได้ (Resilience)
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	**ยุทธศาสตร์ 5** การขับเคลื่อนธรรมาภิบาลดิจิทัลที่ดี (Digital Good Governance)	**ยุทธศาสตร์ 4** สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

ตารางที่ 1-3 ความสอดคล้องของยุทธศาสตร์

หมายเหตุ เนื่องจากแผนพัฒนาศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน พ.ศ. 2565-2570 ได้มีการพิจารณาความเชื่อมโยงกับแผนระดับที่ 1 ระดับที่ 2 และระดับที่ 3 อื่น ๆ ที่มีก่อนหน้านี้อยู่แล้ว ดังนั้นในการแสดงความสัมพันธ์ในแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ จึงแสดงเฉพาะความสัมพันธ์กับนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ซึ่งยังไม่ได้มีการพิจารณาในขณะที่มีการดำเนินการแผนพัฒนาฯ ดังกล่าว

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน



รูปที่ 1-1: ยุทธศาสตร์ของบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ กำหนดวิสัยทัศน์ (Vision) ดังนี้ “การบริหารจัดการที่ดินและทรัพยากรดินของประเทศอย่างมีมาตรฐานและมั่นคงปลอดภัย บนฐานความร่วมมือที่เป็นหนึ่งเดียว” ประกอบด้วย 3 ยุทธศาสตร์ ได้แก่

- ยุทธศาสตร์ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้และเทคโนโลยี) (Integrating cybersecurity capabilities)
- ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)
- ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพของหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)

รายละเอียดของยุทธศาสตร์ต่าง ๆ ทั้งวัตถุประสงค์ กลยุทธ์ ตัวชี้วัด แผนงาน/โครงการ และ ปัจจัยแห่งความสำเร็จ มีดังนี้

การเปรียบเทียบอื่น ๆ ดูได้ที่ภาคผนวกความเชื่อมโยงของแผนฯ และการตอบสนองของแผนฯ ต่อการประเมินต่าง ๆ

1.3.1 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)

วัตถุประสงค์

พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้และเทคโนโลยี) (Integrating cybersecurity capabilities) ภายใต้แนวคิดการขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดี มีดังนี้:

1. **เพิ่มประสิทธิภาพในการจัดการความมั่นคงปลอดภัย :**
    - เพื่อให้การจัดการด้านความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพและรวดเร็ว โดยการรวมศูนย์ข้อมูลและกระบวนการต่าง ๆ ที่เกี่ยวข้อง
2. **ลดความซ้ำซ้อนและเพิ่มความสอดคล้องในการดำเนินงาน :**

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- เพื่อขจัดความซ้ำซ้อนในการดำเนินงานและเพิ่มความสอดคล้องในการจัดการความมั่นคงปลอดภัยระหว่างหน่วยงานต่างๆ ภายในองค์กร

3. **เสริมสร้างการควบคุมและการตรวจสอบที่มีประสิทธิภาพ:**
   - เพื่อให้สามารถควบคุมและตรวจสอบการดำเนินงานด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและโปร่งใส
4. **เพิ่มความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์:**
   - เพื่อให้สามารถตอบสนองต่อภัยคุกคามและเหตุการณ์ที่ไม่คาดคิดได้อย่างรวดเร็วและมีประสิทธิภาพ โดยการใช้ข้อมูลและทรัพยากรที่รวมศูนย์
5. **ส่งเสริมการใช้ทรัพยากรอย่างมีประสิทธิภาพ:**
   - เพื่อให้การใช้ทรัพยากรด้านความมั่นคงปลอดภัยเป็นไปอย่างคุ้มค่าและมีประสิทธิภาพสูงสุดผ่านการจัดการแบบรวมศูนย์
6. **เสริมสร้างความรู้และทักษะของบุคลากร:**
   - เพื่อพัฒนาความรู้และทักษะของบุคลากรในการจัดการและรักษาความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง โดยการฝึกอบรมและการพัฒนาวิชาชีพอย่างต่อเนื่อง

การบูรณาการแบบรวมศูนย์จะช่วยให้สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติสามารถจัดการความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและสอดคล้องกับหลักธรรมาภิบาลที่ดี ซึ่งจะนำไปสู่การสร้างความมั่นคงและความยั่งยืนในระยะยาว

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดยุทธศาสตร์ที่ 1 และค่าเป้าหมาย:

ตัวชี้วัดยุทธศาสตร์ที่ 1	ค่าเป้าหมาย		
	2568	2569	2570
ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์	มีระบบเฝ้าระวังครอบคลุมระบบสำคัญ 1 ระบบ	ครอบคลุมระบบสำคัญ 2 ระบบ พร้อมบูรณาการ AI ในการตรวจจับภัยคุกคาม	ครอบคลุมระบบสำคัญ 3 ระบบ พร้อมปรับใช้ระบบแจ้งเตือนแบบเรียลไทม์
การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง	จัดทำแผนการลดความเสี่ยงที่เป็นระบบ	ขยายแผนการลดความเสี่ยงให้ครอบคลุมภัยคุกคามในระดับเครือข่าย พร้อมทดสอบระบบ Incident Response Plan	สามารถลดความเสี่ยงในทุกประเภทภัยคุกคามที่สำคัญ พร้อมสร้างกลไกแจ้งเตือนล่วงหน้า
การพัฒนาทักษะบุคลากรด้านไซเบอร์	จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ	จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ และจัดอบรมเชิงปฏิบัติการสำหรับผู้เชี่ยวชาญ	จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ และจัดอบรมเชิงปฏิบัติการสำหรับผู้เชี่ยวชาญร่วมกับหน่วยงานพันธมิตร

ตารางที่ 1-4 ตัวชี้วัดยุทธศาสตร์ที่ 1 และค่าเป้าหมาย

ตัวชี้วัดยุทธศาสตร์ที่ 1 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง:

ตัวชี้วัดยุทธศาสตร์ที่ 1	ตัวชี้วัดรายกลยุทธ์			
	กลยุทธ์ที่ 1.1	กลยุทธ์ที่ 1.2	กลยุทธ์ที่ 1.3	กลยุทธ์ที่ 1.4
ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์	➢ เวลาตอบสนองต่อภัยคุกคามนับตั้งแต่ตรวจพบ ➢ อัตราการปฏิบัติตามข้อตกลงระดับการให้บริการ (SLA) ที่ MSSP ตกลงไว้			
การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง	➢ เวลาตอบสนองต่อภัยคุกคานับตั้งแต่ตรวจพบ	➢ อุปกรณ์สำคัญในการรักษาความมั่นคงปลอดภัยต้องได้รับการบำรุงรักษาอย่างต่อเนื่อง ➢ การปฏิบัติตามนโยบายอุปกรณ์ ➢ การลดปัญหาด้านการใช้งานอุปกรณ์ ➢ การจัดทำ EA ครบวงจร ➢ การอัปเดต EA ตามเป้าหมายองค์กร		

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัด ยุทธศาสตร์ที่ 1	ตัวชี้วัดรายกลยุทธ์			
	กลยุทธ์ที่ 1.1	กลยุทธ์ที่ 1.2	กลยุทธ์ที่ 1.3	กลยุทธ์ที่ 1.4
การพัฒนาทักษะบุคลากรด้านไซเบอร์			➢ อัตราการเข้าร่วมฝึกอบรมความมั่นคงปลอดภัยเบื้องต้น ➢ การเพิ่มระดับความตระหนักรู้ด้านความมั่นคงปลอดภัย: ประเมินจากแบบสอบถาม ➢ จำนวนพนักงานที่ได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย: เพิ่มขึ้น	➢ อัตราการเข้าใช้งานแพลตฟอร์ม (Platform) การเรียนรู้ออนไลน์ ➢ ความหลากหลายของเนื้อหาบน (Platform) แพลตฟอร์ม: เพิ่มขึ้นทุกปี ➢ คะแนนทดสอบหลังเข้ารับการอบรมของบุคลากรตามสมรรถนะ

ตารางที่ 1-5 ตัวชี้วัดยุทธศาสตร์ที่ 1 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง

ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) ประกอบด้วยกลยุทธ ดังนี้

กลยุทธ์ที่ 1.1: เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ

วัตถุประสงค์:

1. เพิ่มความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคาม – เพื่อให้สามารถระบุความผิดปกติหรือความเสี่ยงที่อาจเกิดขึ้นในระบบที่สำคัญได้อย่างรวดเร็วและแม่นยำ ลดความเสียหายที่อาจเกิดขึ้นต่อองค์กรหรือระบบ
2. เสริมสร้างความมั่นคงและความน่าเชื่อถือของระบบ - เพื่อให้ระบบที่สำคัญสามารถดำเนินงานได้อย่างต่อเนื่องและมีเสถียรภาพ ลดความเสี่ยงจากการหยุดชะงักหรือการทำงานผิดพลาด
3. ปรับปรุงกระบวนการเฝ้าระวังให้มีประสิทธิภาพสูงสุด - เพื่อใช้ทรัพยากรในการเฝ้าระวังอย่างคุ้มค่าโดยการนำเทคโนโลยีหรือเครื่องมือที่ทันสมัยมาใช้ในการตรวจสอบและวิเคราะห์ข้อมูล

แนวทางการดำเนินการ:

1. การเลือกและทำสัญญากับผู้ที่ให้บริการดูแลรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กรและป้องกันภัยจากอินเทอร์เน็ต (Managed Security Service Provider: MSSP) ที่เชื่อถือได้:
    - ประเมินและเลือกผู้ให้บริการ MSSP ที่มีชื่อเสียงและประสบการณ์
    - ทำสัญญาบริการที่ได้กำหนด SLA ชัดเจน
2. การปรับปรุงกระบวนการเฝ้าระวังและตอบสนอง:
    - กำหนดขั้นตอนการทำงานร่วมกับ MSSP เพื่อติดตามและตอบสนองต่อเหตุการณ์
3. การตรวจสอบประสิทธิภาพของการเฝ้าระวัง:
    - จัดการประชุมรายเดือนเพื่อตรวจสอบการให้บริการและพัฒนาแนวทางแก้ไข

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดและค่าเป้าหมาย:

ตัวชี้วัดกลยุทธ์ที่ 1.1	ค่าเป้าหมาย		
	2568	2569	2570
เวลาตอบสนองต่อภัยคุกคามนับตั้งแต่ตรวจพบ	< 1 ชั่วโมง	< 1 ชั่วโมง	< 1 ชั่วโมง
อัตราการปฏิบัติตามข้อตกลงระดับการให้บริการ (SLA) ที่ MSSP ตกลงไว้	100%	100%	100%

ตารางที่ 1-6 ตัวชี้วัดและค่าเป้าหมาย 1.1

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
เวลาตอบสนองต่อภัยคุกคามนับตั้งแต่ตรวจพบ	เฉพาะระบบที่ได้มีจัดจ้างให้มีการเฝ้าระวัง	➢ เวลาที่ตรวจพบ ➢ เวลาที่เริ่มตอบสนองนับตั้งแต่ตรวจพบ	เวลาที่เริ่มตอบสนองนับตั้งแต่ตรวจพบ – เวลาที่ตรวจพบ
อัตราการปฏิบัติตามข้อตกลงระดับการให้บริการ (SLA) ที่ MSSP ตกลงไว้	เฉพาะระบบที่ได้มีจัดจ้างให้มีการเฝ้าระวัง	➢ SLA ที่ MSSP ตกลงไว้ ➢ การปฏิบัติงานที่เป็นไปตาม SLA ตามรายงานการส่งสอบของ MSSP	(การปฏิบัติงานที่เป็นไปตาม SLA ตามรายงานการส่งสอบของ MSSP/ SLA ที่ MSSP ตกลงไว้) * 100

ตารางที่ 1-7 คำอธิบายตัวชี้วัด 1.1

แผนงาน/โครงการที่เกี่ยวข้อง:

- P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์

ปัจจัยแห่งความสำเร็จ:

- ความแม่นยำและทันเวลาของการแจ้งเตือน
- การร่วมมือที่มีประสิทธิภาพระหว่างทีมภายในและ MSSP

กลยุทธ์ที่ 1.2: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย

วัตถุประสงค์:

1. เสริมสร้างความปลอดภัยของระบบโครงสร้างพื้นฐาน – เพื่อป้องกันการโจมตีทางไซเบอร์และลดความเสี่ยงจากช่องโหว่ที่อาจเกิดขึ้นในระบบโครงสร้างพื้นฐานที่สำคัญ
2. เพิ่มความน่าเชื่อถือและความต่อเนื่องในการดำเนินงาน – เพื่อให้โครงสร้างพื้นฐานสามารถรองรับการทำงานได้อย่างมีเสถียรภาพและลดโอกาสการหยุดชะงักที่อาจส่งผลกระทบต่อองค์กร
3. รองรับการพัฒนาและการเปลี่ยนแปลงในอนาคต - เพื่อให้โครงสร้างพื้นฐานมีความยืดหยุ่นและสามารถปรับตัวให้สอดคล้องกับเทคโนโลยีใหม่ ๆ หรือความต้องการที่เปลี่ยนแปลงไป

แนวทางการดำเนินการ:

1. ตรวจสอบและประเมินความเสี่ยงด้านโครงสร้างพื้นฐาน:
    - ดำเนินการประเมินความเสี่ยงเจาะลึกเพื่อระบุจุดอ่อนและโอกาสในการปรับปรุง
2. ปรับปรุงและอัพเกรดระบบรักษาความมั่นคงปลอดภัย:
    - ปรับปรุงระบบไฟร์วอลล์ (Firewall) การจัดการสิทธิ์ และระบบเครือข่ายให้ทันสมัย
    - ดำเนินการอัพเกรดอุปกรณ์ที่ล้าสมัยเพื่อเพิ่มความมั่นคงปลอดภัย
3. การคัดเลือกและติดตั้งระบบ Enterprise Device Management (EDM):

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ประเมินและเลือกแพลตฟอร์ม (Platform) ที่เหมาะสมสำหรับจัดการ Client และ Mobile Device

4. การกำหนดนโยบายการใช้งานอุปกรณ์:
   - สร้างและบังคับใช้นโยบายด้านความมั่นคงปลอดภัยของอุปกรณ์
5. วิเคราะห์และออกแบบโครงสร้าง Enterprise Architecture (EA):
   - การประเมินสถานภาพปัจจุบันของเทคโนโลยีและโครงสร้างความมั่นคงปลอดภัย
   - ออกแบบ EA โดยเน้นด้านการบูรณาการและความมั่นคงปลอดภัย
6. นำ EA เข้าสู่องค์กรและบูรณาการกับแผนกลยุทธ์:
   - บูรณาการ EA กับแผนธุรกิจและกระบวนการขององค์กร
   - มีการประชุมและกิจกรรมเพื่อประสานงานกับทุกส่วนที่เกี่ยวข้อง

ตัวชี้วัดและค่าเป้าหมาย:

ตัวชี้วัดกลยุทธ์ที่ 1.2	ค่าเป้าหมาย		
	2568	2569	2570
อุปกรณ์สำคัญในการรักษาความมั่นคงปลอดภัยต้องได้รับการบำรุงรักษาอย่างต่อเนื่อง	100%	100%	100%
การปฏิบัติตามนโยบายอุปกรณ์	> 80%	> 90%	> 98%
การลดปัญหาด้านการใช้งานอุปกรณ์		> 30%	> 50%
การจัดทำ EA ครบวงจร		100%	
การอัปเดต EA ตามเป้าหมายองค์กร		ทุก 6 เดือน	ทุก 6 เดือน

ตารางที่ 1-8 ตัวชี้วัดและค่าเป้าหมาย 1.2

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
อุปกรณ์สำคัญในการรักษาความมั่นคงปลอดภัยต้องได้รับการบำรุงรักษาอย่างต่อเนื่อง	เฉพาะระบบที่ได้มีจัดจ้างให้มีการเฝ้าระวัง	➢ เวลาที่ตรวจพบ ➢ เวลาที่เริ่มตอบสนองนับตั้งแต่ตรวจพบ	เวลาที่เริ่มตอบสนองนับตั้งแต่ตรวจพบ – เวลาที่ตรวจพบ
การปฏิบัติตามนโยบายอุปกรณ์	เฉพาะระบบที่ได้มีจัดจ้างให้มีการเฝ้าระวัง	➢ SLA ที่ MSSP ตกลงไว้ ➢ การปฏิบัติงานที่เป็นไปตาม SLA ตามรายงานการส่งสอบของ MSSP	(การปฏิบัติงานที่เป็นไปตาม SLA ตามรายงานการส่งสอบของ MSSP/ SLA ที่ MSSP ตกลงไว้) * 100
การจัดทำ EA ครบวงจร	ภายใน สคทช. เท่านั้น	➢ EA ที่ผ่านการเห็นชอบจากผู้บริหารของ สคทช.	EA ที่ผ่านการเห็นชอบจากผู้บริหารของ สคทช. และได้รับการอนุมัติ
การอัปเดต EA ตามเป้าหมายองค์กร	ภายใน สคทช. เท่านั้น	➢ จำนวนการอัปเดต EA ตามเป้าหมายองค์กรในแต่ละปี	การอัปเดต EA ตามเป้าหมายองค์กร

ตารางที่ 1-9 คำอธิบายตัวชี้วัด 1.2

แผนงาน/โครงการที่เกี่ยวข้อง:

- P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน
- P4: โครงการจัดซื้อระบบ EDM (Enterprise Device Management)
- P5: โครงการวิเคราะห์และออกแบบ EA (Enterprise Architecture)

ปัจจัยแห่งความสำเร็จ:

- การยอมรับและความเข้าใจจากบุคลากร
- การใช้งานเครื่องมือในการตรวจสอบที่มีประสิทธิภาพ
- งบประมาณและการสนับสนุนอย่างต่อเนื่องสำหรับการพัฒนาโครงสร้างพื้นฐาน
- การมีส่วนร่วมของทุกฝ่ายในองค์กร
- การสนับสนุนอย่างต่อเนื่องจากผู้บริหาร

กลยุทธ์ที่ 1.3: พัฒนาทักษะความมั่นคงปลอดภัย

วัตถุประสงค์

1. เพิ่มขีดความสามารถของบุคลากรด้านความมั่นคงปลอดภัย - เพื่อให้บุคลากรมีความรู้ ความเชี่ยวชาญและทักษะที่ทันสมัยในการป้องกันและรับมือกับภัยคุกคามทางไซเบอร์
2. สร้างความตระหนักรู้และวัฒนธรรมด้านความมั่นคงปลอดภัยในองค์กร – เพื่อให้บุคลากรทุกระดับเข้าใจถึงความสำคัญของความมั่นคงปลอดภัยและปฏิบัติตามแนวทางที่เหมาะสม
3. พัฒนากระบวนการเรียนรู้และฝึกอบรมอย่างต่อเนื่อง - เพื่อให้บุคลากรสามารถปรับตัวและรับมือกับภัยคุกคามใหม่ ๆ ได้อย่างมีประสิทธิภาพในระยะยาว

แนวทางการดำเนินการ:

1. จัดทำโปรแกรมฝึกอบรมความมั่นคงปลอดภัยทางไซเบอร์พื้นฐาน:
    - พัฒนาเนื้อหาและหลักสูตรที่ครอบคลุมพื้นฐานด้านความมั่นคงปลอดภัย
    - จัดฝึกอบรมให้กับบุคลากรทุกคน
2. ระบุทักษะที่จำเป็นและออกแบบหลักสูตรการพัฒนา:
    - วิเคราะห์ทักษะที่จำเป็นในปัจจุบันและอนาคต
    - พัฒนาหลักสูตรเชิงลึกสำหรับทักษะเฉพาะทาง
3. จัดโปรแกรมพัฒนาทักษะเฉพาะทาง:
    - การทำเวิร์คช็อปการพัฒนาทักษะเฉพาะด้าน เช่น การวิเคราะห์ภัยคุกคาม
    - จัดการร่วมมือกับผู้เชี่ยวชาญจากภายนอกในการจัดอบรม
4. การถอดองค์ความรู้ และพัฒนาความรู้ใหม่ ๆ จากประสบการณ์ในองค์กร
    - การหาบทเรียนจากความผิดพลาด หรือแนวทางการแก้ไขปัญหาเมื่อเกิดเหตุ (Reactive)
    - การพัฒนาความรู้ใหม่ ๆ จากประสบการณ์ในองค์กรเพื่อป้องกันข้อผิดพลาดที่จะเกิดขึ้นหรือเกิดซ้ำ (Proactive)

ตัวชี้วัดและค่าเป้าหมาย:

ตัวชี้วัดกลยุทธ์ที่ 1.3	ค่าเป้าหมาย		
	2568	2569	2570
อัตราการเข้าร่วมฝึกอบรมความมั่นคงปลอดภัยเบื้องต้น	> 80%	> 80%	> 85%
การเพิ่มระดับความตระหนักรู้ด้านความมั่นคงปลอดภัย : ประเมินจากแบบสอบถาม	> 80%	> 80%	> 80%

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดกลยุทธ์ที่ 1.3	ค่าเป้าหมาย		
	2568	2569	2570
จำนวนบุคลากรได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย : เพิ่มขึ้น		> 20%	> 30%

ตารางที่ 1-10 ตัวชี้วัดและค่าเป้าหมาย 1.3

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
อัตราการเข้าร่วมฝึกอบรมความมั่นคงปลอดภัยเบื้องต้น	เฉพาะบุคลากรภายใน สคทช. เท่านั้น	➢ จำนวนบุคลากรที่เข้าร่วมฝึกอบรม ➢ จำนวนบุคลากรภายใน สคทช. ทั้งหมด	(จำนวนบุคลากรที่เข้าร่วมฝึกอบรม/จำนวนบุคลากรภายใน สคทช. ทั้งหมด) * 100%
การเพิ่มระดับความตระหนักรู้ด้านความมั่นคงปลอดภัย: ประเมินจากแบบสอบถาม	เฉพาะบุคลากรภายใน สคทช. เท่านั้น	➢ คะแนนที่ได้จากการทำแบบสอบถาม ➢ คะแนนเต็มของแบบสอบถาม	(คะแนนที่ได้จากการทำแบบสอบถาม/คะแนนเต็มของแบบสอบถาม) * 100%
จำนวนพนักงานที่ได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย: เพิ่มขึ้น	เฉพาะบุคลากรภายใน สคทช. ที่ต้องได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย	➢ จำนวนบุคลากรได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย ➢ บุคลากรภายใน สคทช. ที่ต้องได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทั้งหมด	(จำนวนบุคลากรได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย/บุคลากรภายใน สคทช. ที่ต้องได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัยทั้งหมด) * 100%

ตารางที่ 1-11 คำอธิบายตัวชี้วัด 1.3

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนงาน/โครงการที่เกี่ยวข้อง:

- P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน
- P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก

ปัจจัยแห่งความสำเร็จ:

- ความพร้อมในการเรียนรู้จากบุคลากร
- ทรัพยากรและการสนับสนุนจากองค์กร

กลยุทธ์ที่ 1.4: บูรณาการหลักสูตรการเรียนรู้ผ่านแพลตฟอร์ม Platform ออนไลน์

วัตถุประสงค์:

1. เพิ่มการเข้าถึงการเรียนรู้และพัฒนาทักษะอย่างทั่วถึง - เพื่อให้บุคลากรหรือผู้เรียนสามารถเข้าถึงเนื้อหาหลักสูตรได้ทุกที่ทุกเวลา ผ่านแพลตฟอร์ม (Platform) ออนไลน์ที่สะดวกและยืดหยุ่น
2. ส่งเสริมการเรียนรู้แบบต่อเนื่องและพัฒนาตนเอง - เพื่อสร้างโอกาสให้ผู้เรียนสามารถพัฒนาความรู้และทักษะได้อย่างต่อเนื่อง โดยไม่จำกัดด้วยข้อจำกัดด้านเวลาและสถานที่
3. ลดต้นทุนและเพิ่มประสิทธิภาพในการจัดการเรียนการสอน - เพื่อใช้ทรัพยากรอย่างคุ้มค่า ลดค่าใช้จ่ายในการจัดการเรียนการสอนแบบดั้งเดิม และเพิ่มประสิทธิภาพในการบริหารจัดการหลักสูตรผ่านระบบออนไลน์

แนวทางการดำเนินการ:

1. สำรวจและเลือกแพลตฟอร์ม (Platform) การเรียนรู้ออนไลน์ที่เหมาะสม:
    - ทำการประเมินและเลือกแพลตฟอร์ม (Platform) ที่ตรงกับความต้องการขององค์กร
2. ออกแบบและพัฒนาเนื้อหาการเรียนรู้ที่เข้าถึงได้ง่าย:
    - จัดทำเนื้อหาการเรียนรู้อย่างมีระบบและสามารถเข้าถึงได้ผ่าน online platform
3. ส่งเสริมการใช้แพลตฟอร์ม (Platform) ผ่านการยอมรับและโปรแกรมสนับสนุน:
    - มีคู่มือการใช้งานและกิจกรรมสนับสนุนการใช้งานแพลตฟอร์ม (Platform)

ตัวชี้วัดและค่าเป้าหมาย:

ตัวชี้วัดกลยุทธ์ที่ 1.4	ค่าเป้าหมาย		
	2568	2569	2570
อัตราการเข้าใช้งานแพลตฟอร์ม (Platform) การเรียนรู้ออนไลน์		> 70%	> 75%
ความหลากหลายของเนื้อหาบนแพลตฟอร์ม: เพิ่มขึ้นทุกปี			> 20%
คะแนนทดสอบหลังเข้ารับการอบรมของบุคลากรตามสมรรถนะ		> 80%	> 80%

ตารางที่ 1-12 ตัวชี้วัดและค่าเป้าหมาย 1.4

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
อัตราการเข้าใช้งานแพลตฟอร์ม (Platform) การเรียนรู้ออนไลน์	เฉพาะบุคลากรภายใน สคทช. เท่านั้น	➢ จำนวนบุคลากรที่เข้าร่วมฝึกอบรม ➢ จำนวนบุคลากรภายใน สคทช. ทั้งหมด	(จำนวนบุคลากรที่เข้าร่วมฝึกอบรม/จำนวนบุคลากรภายใน สคทช. ทั้งหมด) * 100%
ความหลากหลายของเนื้อหาบนแพลตฟอร์ม (Platform) : เพิ่มขึ้นทุกปี	เฉพาะกรณีมีการใช้งานแพลตฟอร์ม (Platform) ที่ทาง สคทช. กำหนด เท่านั้น	➢ เนื้อหาที่ได้รับการพิจารณาว่าจำเป็นสำหรับบุคลากรบน	(เนื้อหาที่ได้รับการพิจารณาว่าจำเป็นสำหรับบุคลากรบนแพลตฟอร์ม (Platform)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
		แพลตฟอร์ม (Platform) ที่เพิ่มขึ้นในแต่ละปี ➢ เนื้อหาที่ได้รับการพิจารณาว่าจำเป็นสำหรับบุคลากรบนแพลตฟอร์ม (Platform) ที่มีในปีที่ผ่านมา	ที่เพิ่มขึ้นในแต่ละปี/เนื้อหาที่ได้รับการพิจารณาว่าจำเป็นสำหรับบุคลากรบนแพลตฟอร์ม (Platform) ที่มีในปีที่ผ่านมา) * 100%
คะแนนทดสอบหลังเข้ารับการอบรมของบุคลากรตามสมรรถนะ	เฉพาะบุคลากรภายใน สคทช. เท่านั้น	➢ คะแนนทดสอบหลังเข้ารับการอบรม ➢ คะแนนเต็มของการอบรมของบุคลากรตามสมรรถนะ	(คะแนนทดสอบหลังเข้ารับการอบรม/คะแนนเต็มของการอบรมของบุคลากรตามสมรรถนะ) * 100%

ตารางที่ 1-13 คำอธิบายตัวชี้วัด 1.4

แผนงาน/โครงการที่เกี่ยวข้อง:

- P8: โครงการจัดหาแพลตฟอร์ม (Platform) การเรียนรู้ออนไลน์
- P9: โครงการสนับสนุนการใช้งานแพลตฟอร์ม (Platform) การเรียนรู้

ปัจจัยแห่งความสำเร็จ:

- การเลือกใช้ technology ที่สอดคล้องกับความต้องการของบุคลากร
- การสนับสนุนจากฝ่ายบริหาร

1.3.2 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

วัตถุประสงค์

1. **เสริมสร้างการแลกเปลี่ยนข้อมูลและประสบการณ์:**
   - เพื่อส่งเสริมการเชื่อมโยงข้อมูล OneMap ระหว่างหน่วยงานให้มีความมั่นคงปลอดภัย แลกเปลี่ยนข้อมูล ข่าวสาร และประสบการณ์ระหว่างหน่วยงานต่าง ๆ ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เพื่อเพิ่มประสิทธิภาพในการป้องกันและตอบสนองต่อภัยคุกคาม
2. **สร้างมาตรฐานและแนวทางปฏิบัติร่วมกัน:**
   - เพื่อพัฒนามาตรฐานและแนวทางปฏิบัติที่เป็นที่ยอมรับร่วมกันในการรักษาความมั่นคงปลอดภัย เพื่อให้การดำเนินงานเป็นไปในทิศทางเดียวกัน
3. **เพิ่มขีดความสามารถในการตอบสนองต่อภัยคุกคาม:**
   - เพื่อเพิ่มความสามารถในการตรวจจับและตอบสนองต่อภัยคุกคามผ่านการทำงานร่วมกันและการใช้ทรัพยากรร่วมกัน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4. **ป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์:**
    - เพื่อป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อข้อมูลและระบบสารสนเทศขององค์กร

การสร้างความร่วมมือและเครือข่ายด้านการรักษาความมั่นคงปลอดภัยจะช่วยให้สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติสามารถจัดการกับภัยคุกคามได้อย่างมีประสิทธิภาพและยั่งยืน โดยอาศัยการทำงานร่วมกันและการสนับสนุนจากเครือข่ายที่กว้างขวาง

ตัวชี้วัดยุทธศาสตร์ที่ 2 และค่าเป้าหมาย:

ตัวชี้วัดยุทธศาสตร์ที่ 2	ค่าเป้าหมาย		
	2568	2569	2570
การพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน		จัดทำร่างมาตรฐานและเริ่มทดลองใช้กับ 3 หน่วยงาน	ขยายการทดลองใช้งานให้ครอบคลุม 70% ของหน่วยงานที่เกี่ยวข้อง
การดำเนินแผน BCP สำหรับระบบสำคัญ	มีแผน BCP ครอบคลุมระบบสำคัญ 1 ระบบ และจัดการทดสอบแผน 1 ครั้ง	ขยายการจัดทำแผน BCP ให้ครอบคลุมระบบสำคัญ 2 ระบบ พร้อมทดสอบแผน 1 ครั้ง	ครอบคลุมระบบสำคัญ 100% พร้อมบูรณาการแผน BCP ข้ามหน่วยงาน
ระดับความพึงพอใจของหน่วยงานพันธมิตร		จัดตั้งกลไกการประชุมเชิงปฏิบัติการร่วมกับพันธมิตรและจัดเวิร์กชอป 2 ครั้งต่อปี	ความพึงพอใจเฉลี่ย 85% จากการจัดประชุมและเวิร์กชอป 2 ครั้งต่อปี พร้อมจัดทำแผนความร่วมมือระยะยาว

ตารางที่ 1-14 ตัวชี้วัดยุทธศาสตร์ที่ 2 และค่าเป้าหมาย

ตัวชี้วัดยุทธศาสตร์ที่ 2 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง:

ตัวชี้วัดยุทธศาสตร์ที่ 2	ตัวชี้วัดรายกลยุทธ์	
	กลยุทธ์ที่ 2.1	กลยุทธ์ที่ 2.2
การพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน	➢ การพัฒนามาตรฐานแลกเปลี่ยนข้อมูล ➢ การจัดประชุมและสัมมนา ➢ จำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล: เพิ่มขึ้น	
การดำเนินแผน BCP สำหรับระบบสำคัญ		➢ การจัดทำ BCP สำหรับทุกระบบสำคัญ ➢ การฝึกซ้อมแผน BCP ➢ อัตราความสำเร็จในการทดสอบกู้คืนระบบ ➢ อัตราการใช้คลาวด์(Cloud) สำหรับระบบที่ต้องการปรับตัวสูง
ระดับความพึงพอใจของหน่วยงานพันธมิตร	➢ การจัดประชุมและสัมมนา ➢ จำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล: เพิ่มขึ้น	➢ อัตราความสำเร็จในการทดสอบกู้คืนระบบ

ตารางที่ 1-15 ตัวชี้วัดยุทธศาสตร์ที่ 2 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง

ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) ประกอบด้วยกลยุทธ ดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

กลยุทธ์ที่ 2.1: แบ่งปันข้อมูลกับหน่วยงานด้านความมั่นคงปลอดภัย

วัตถุประสงค์:

1. เสริมสร้างความร่วมมือในการป้องกันและรับมือภัยคุกคาม - เพื่อเพิ่มประสิทธิภาพในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ผ่านการแลกเปลี่ยนข้อมูลที่สำคัญระหว่างหน่วยงาน
2. เพิ่มความรวดเร็วและแม่นยำในการจัดการความเสี่ยง – เพื่อให้หน่วยงานที่เกี่ยวข้องสามารถใช้ข้อมูลที่แบ่งปันในการวางแผนและดำเนินการป้องกันภัยคุกคามได้อย่างทันท่วงที
3. สร้างเครือข่ายความร่วมมือด้านความมั่นคงปลอดภัย - เพื่อพัฒนาความสัมพันธ์และความไว้วางใจระหว่างหน่วยงานต่าง ๆ ในการทำงานร่วมกันเพื่อเสริมสร้างความมั่นคงปลอดภัยในระดับองค์กรและระดับประเทศ

แนวทางการดำเนินการ:

1. พัฒนามาตรฐานการแลกเปลี่ยนข้อมูลร่วมกับหน่วยงานต่างๆ:
    - พิจารณามาตรฐานสากลที่ใช้ในอุตสาหกรรม
    - จัดทำคู่มือและเกณฑ์การแลกเปลี่ยนข้อมูลร่วมกัน
2. สร้างความเข้าใจร่วมกันในเรื่องการแบ่งปันข้อมูล:
    - การจัดประชุม สัมมนาหรือเวิร์คช็อปเพื่อสร้างความเข้าใจถึงเป้าหมายและประโยชน์ของการแบ่งปันข้อมูล
    - รวบรวมข้อเสนอแนะและตกลงแนวทางร่วมกันในการแบ่งปันข้อมูล
3. พัฒนาระบบสำหรับการแบ่งปันข้อมูลอย่างปลอดภัย:
    - พัฒนาและปรับใช้อินเตอร์เฟซสำหรับการแลกเปลี่ยนข้อมูลอย่างปลอดภัยระหว่างหน่วยงานต่าง ๆ
    - จัดทำข้อตกลงการแบ่งปันข้อมูลกับหน่วยงานที่เกี่ยวข้อง
4. ส่งเสริมการสนับสนุนและการมีส่วนร่วมจากหน่วยงานอื่น:
    - สร้างเครือข่ายและกลุ่มทำงานร่วมเพื่อประสานงานและเพิ่มการแลกเปลี่ยนข้อมูล

ตัวชี้วัดและค่าเป้าหมาย :

ตัวชี้วัดกลยุทธ์ที่ 2.1	ค่าเป้าหมาย		
	2568	2569	2570
การพัฒนามาตรฐานแลกเปลี่ยนข้อมูล		ร่างมาตรฐานแลกเปลี่ยนข้อมูล	มาตรฐานแลกเปลี่ยนข้อมูลอย่างเป็นทางการ
การจัดประชุมและสัมมนา		อย่างน้อย 3 ครั้งต่อปี	อย่างน้อย 3 ครั้งต่อปี
จำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล : เพิ่มขึ้น		3 หน่วยงาน	6 หน่วยงาน

ตารางที่ 1-16 ตัวชี้วัดและค่าเป้าหมาย 2.1

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
การพัฒนามาตรฐานแลกเปลี่ยนข้อมูล	เฉพาะมาตรฐานแลกเปลี่ยนข้อมูลที่ทาง สคทช. เป็นผู้กำหนดหรือนำมาใช้งานเท่านั้น	➢ จำนวนมาตรฐานแลกเปลี่ยนข้อมูลที่ทาง สคทช. เป็นผู้กำหนดหรือนำมาใช้งานอย่างเป็นทางการ	นับจำนวนมาตรฐานแลกเปลี่ยนข้อมูลที่ทาง สคทช. เป็นผู้กำหนดหรือนำมาใช้งานอย่างเป็นทางการ
การจัดประชุมและสัมมนา	เฉพาะกรณีการจัดประชุมและสัมมนาที่ทาง สคทช. เป็นผู้ดำเนินการหลักเท่านั้น	➢ จำนวนการจัดประชุมและสัมมนา	นับจำนวนการจัดประชุมและสัมมนา
จำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล: เพิ่มขึ้น	เฉพาะกรณี สคทช. เป็นผู้ดำเนินการหลักเท่านั้น	➢ จำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล	นับจำนวนหน่วยงานที่เข้าร่วมแบ่งปันข้อมูล

ตารางที่ 1-17 คำอธิบายตัวชี้วัด 2.1

แผนงาน/โครงการที่เกี่ยวข้อง:

- P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล
- P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล

ปัจจัยแห่งความสำเร็จ:

- การมีส่วนร่วมและความสม่ำเสมอในการสื่อสารกับหน่วยงานต่างๆ
- การสนับสนุนจากผู้บริหารระดับสูง

กลยุทธ์ที่ 2.2: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน

วัตถุประสงค์:

1. ลดผลกระทบจากเหตุการณ์ที่อาจรบกวนการดำเนินงาน - เพื่อให้หน่วยงานสามารถรับมือและฟื้นตัวจากเหตุการณ์ที่ไม่คาดคิด เช่น ภัยพิบัติหรือการโจมตีทางไซเบอร์ ได้อย่างรวดเร็วและมีประสิทธิภาพ
2. รักษาความต่อเนื่องของการดำเนินงานที่สำคัญ – เพื่อให้ภารกิจหลักของหน่วยงานสามารถดำเนินการได้อย่างต่อเนื่องโดยไม่มีการหยุดชะงักที่ส่งผลกระทบต่อเป้าหมายหรือบริการที่สำคัญ
3. พัฒนากระบวนการบริหารจัดการความเสี่ยงและแผนสำรอง – เพื่อเตรียมความพร้อมและสร้างความยืดหยุ่นในการจัดการกับสถานการณ์ฉุกเฉินหรือความท้าทายที่อาจเกิดขึ้นในอนาคต

แนวทางการดำเนินการ:

1. จัดทำแผน Business Continuity Plan (BCP):
    - รวบรวมข้อมูลและระบุความเสี่ยงสำหรับระบบที่สำคัญ
    - สร้าง BCP ที่พร้อมใช้งานในสถานการณ์ฉุกเฉิน
2. ประเมินและเลือกใช้เทคโนโลยีคลาวด์ (Cloud):
    - สำรวจความเหมาะสมของการใช้คลาวด์ (Cloud) ภาครัฐและ Public Cloud สำหรับระบบต่างๆ
    - จัดหาและใช้งานคลาวด์ (Cloud) ที่เหมาะสมเพื่อสนับสนุน BCP

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3. ทดสอบและปรับปรุงแผน BCP:
    - ดำเนินการฝึกซ้อมแผน BCP เพื่อทดสอบประสิทธิภาพ
    - เก็บรวบรวมข้อมูลเพื่อปรับปรุงแผน

ตัวชี้วัดและค่าเป้าหมาย:

ตัวชี้วัดกลยุทธที่ 2.2	ค่าเป้าหมาย		
	2568	2569	2570
การจัดทำ BCP สำหรับทุกระบบสำคัญ	1 ระบบ	2 ระบบ	3 ระบบ
การฝึกซ้อมแผน BCP	ปีละ 1 ครั้ง	ปีละ 1 ครั้ง	ปีละ 1 ครั้ง ทดสอบร่วมกับพันธมิตร
อัตราความสำเร็จในการทดสอบกู้คืนระบบ		100 %	100 %
อัตราการใช้คลาวด์ (Cloud) สำหรับระบบที่ต้องการปรับตัวสูง			> 50%

ตารางที่ 1-18 ตัวชี้วัดและค่าเป้าหมาย 2.2

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
การจัดทำ BCP สำหรับทุกระบบสำคัญ	เฉพาะระบบสำคัญที่มีการวิเคราะห์ตามการวิเคราะห์ผลกระทบธุรกิจ (Business Impact Analysis: BIA) ตามที่ทาง สคทช. ระบุว่ามีความสำคัญ	➢ แผน BCP ➢ ระบบสำคัญที่มีการวิเคราะห์ตามการวิเคราะห์ผลกระทบธุรกิจ (Business Impact Analysis: BIA) ตามที่ทาง สคทช. ระบุว่ามีความสำคัญ	นับจำนวนแผน BCP ระบบสำคัญที่มีการวิเคราะห์ตามการวิเคราะห์ผลกระทบธุรกิจ (Business Impact Analysis: BIA) ตามที่ทาง สคทช. ระบุว่ามีความสำคัญ
การฝึกซ้อมแผน BCP	เฉพาะแผน BCP ที่ได้รับการอนุมัติอย่างเป็นทางการจากทาง สคทช.	➢ จำนวนการฝึกซ้อมแผน BCP ➢ แผน BCP ที่ได้รับการอนุมัติอย่างเป็นทางการจากทาง สคทช.	จำนวนการฝึกซ้อมแผน BCP ที่ได้รับการอนุมัติอย่างเป็นทางการจากทาง สคทช. หรือ จำนวนการฝึกซ้อมแผน BCP ที่ได้รับการอนุมัติอย่างเป็นทางการจากทาง สคทช.ที่ได้ฝึกซ้อมร่วมกับพันธมิตร
อัตราความสำเร็จในการทดสอบกู้คืนระบบ	เฉพาะระบบที่ สคทช. พิจารณาว่ามีความสำคัญและกำหนดให้มีการ Backup	➢ จำนวนระบบที่ได้มีการทดสอบการกู้คืน ➢ จำนวนระบบที่ สคทช. พิจารณาว่ามีความสำคัญและกำหนดให้มีการ Backup	(จำนวนระบบที่ได้มีการทดสอบการกู้คืน/จำนวนระบบที่ สคทช. พิจารณาว่ามีความสำคัญ และกำหนดให้มีการ Backup) * 100%
อัตราการใช้คลาวด์ (Cloud) สำหรับระบบที่ต้องการปรับตัวสูง	เฉพาะระบบ/เทคโนโลยีที่มีการพิจารณาจากทาง สคทช. แล้วว่าเหมาะสมกับการใช้งานบนบริการคลาวด์ (Cloud)	➢ จำนวนระบบ/เทคโนโลยีที่มีการพิจารณาจากทาง สคทช. แล้วว่าเหมาะสมกับการใช้งานบนบริการ	(จำนวนระบบ/เทคโนโลยีที่มีการพิจารณาจากทาง สคทช. แล้วว่าเหมาะสมกับการใช้งานบนบริการคลาวด์ (Cloud) ที่มีการใช้บริการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
		คลาวด์ (Cloud) ที่มีการใช้บริการคลาวด์ (Cloud) ➢ จำนวนระบบ/เทคโนโลยีที่มีการพิจารณาจากทาง สคทช. แล้วว่าเหมาะสมกับการใช้งานบนบริการคลาวด์ (Cloud)	คลาวด์ Cloud /จำนวนระบบ/เทคโนโลยีที่มีการพิจารณาจากทาง สคทช. แล้วว่าเหมาะสมกับการใช้งานบนบริการคลาวด์ (Cloud) * 100 %

ตารางที่ 1-19 คำอธิบายตัวชี้วัด 2.2

แผนงาน/โครงการที่เกี่ยวข้อง:

- P12: โครงการจัดทำและทดสอบ BCP
- P13: โครงการประเมินและจัดหาเทคโนโลยีคลาวด์ (Cloud)

ปัจจัยแห่งความสำเร็จ:

- ความพร้อมของทีมงานและทรัพยากรที่เกี่ยวข้อง
- การเลือกใช้เทคโนโลยีคลาวด์ (Cloud) ที่เหมาะสม

การดำเนินการตามยุทธศาสตร์นี้ตั้งอยู่บนการสร้างความเข้าใจและการมีส่วนร่วมอย่างเข้มข้นจากทุกหน่วยงานที่เกี่ยวข้อง รวมถึงการเลือกใช้เทคโนโลยีและมาตรฐานที่สอดคล้องกับเป้าหมายและวิสัยทัศน์ขององค์กร

1.3.3 ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)

วัตถุประสงค์

1. **เสริมสร้างความโปร่งใสและความรับผิดชอบในการจัดการความมั่นคงปลอดภัย:**
   - เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยเป็นไปอย่างโปร่งใสและมีความรับผิดชอบโดยการกำหนดนโยบายและแนวทางปฏิบัติที่ชัดเจน
2. **พัฒนากรอบการบริหารจัดการที่มีประสิทธิภาพและได้มาตรฐาน:**
   - เพื่อพัฒนากรอบการบริหารจัดการที่สามารถรองรับการเปลี่ยนแปลงและความท้าทายด้านความมั่นคงปลอดภัยได้อย่างมีประสิทธิภาพและได้มาตรฐาน
3. **เพิ่มประสิทธิภาพในการตรวจสอบและประเมินผล:**
   - เพื่อเพิ่มประสิทธิภาพในการตรวจสอบและประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัย โดยการใช้เครื่องมือและกระบวนการที่ทันสมัย
4. **สร้างวัฒนธรรมองค์กรที่เน้นธรรมาภิบาล:**
   - เพื่อสร้างวัฒนธรรมองค์กรที่ให้ความสำคัญกับธรรมาภิบาลและการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัย

การขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดีจะช่วยให้สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติสามารถดำเนินงานได้อย่างมีประสิทธิภาพและยั่งยืน โดยการสร้างความเชื่อมั่นและความไว้วางใจจากผู้มีส่วนได้ส่วนเสีย

ตัวชี้วัดยุทธศาสตร์ที่ 3 และค่าเป้าหมาย:

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดยุทธศาสตร์ที่ 3	ค่าเป้าหมาย		
	2568	2569	2570
การได้รับการรับรองมาตรฐาน ISO/IEC 27001		พัฒนากระบวนการและระบบตามข้อกำหนดของมาตรฐาน พร้อมดำเนินการตรวจสอบภายใน	ดำเนินการตรวจรับรองจากหน่วยงานภายนอกและได้รับการรับรองมาตรฐาน

ตารางที่ 1-20 ตัวชี้วัดยุทธศาสตร์ที่ 3 และค่าเป้าหมาย

ตัวชี้วัดยุทธศาสตร์ที่ 3 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง:

ตัวชี้วัดยุทธศาสตร์ที่ 3	ตัวชี้วัดกลยุทธ์
	กลยุทธ์ที่ 3.1
การได้รับการรับรองมาตรฐาน ISO/IEC 27001	➢ ระดับความรู้เกี่ยวกับมาตรฐานสากลภายในองค์กร: ➢ การได้รับการรับรองมาตรฐาน ➢ ประสิทธิภาพของการปฏิบัติตามมาตรฐาน

ตารางที่ 1-21 ตัวชี้วัดยุทธศาสตร์ที่ 3 และตัวชี้วัดรายกลยุทธ์ที่สอดคล้อง

ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard) วัตถุประสงค์ประกอบด้วยกลยุทธ ดังนี้

กลยุทธ์ที่ 3.1: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ

วัตถุประสงค์:

1. ยกระดับความน่าเชื่อถือและความมั่นคงปลอดภัยของระบบสารสนเทศ - เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยสารสนเทศเป็นไปตามมาตรฐานสากล สร้างความเชื่อมั่นให้กับผู้ใช้งานและหน่วยงานที่เกี่ยวข้อง
2. ลดความเสี่ยงและช่องโหว่ในระบบสารสนเทศ - เพื่อให้กระบวนการบริหารจัดการความมั่นคงปลอดภัยมีประสิทธิภาพและสามารถป้องกันภัยคุกคามทางไซเบอร์ได้อย่างเป็นระบบ
3. เพิ่มขีดความสามารถในการแข่งขันและการยอมรับในระดับสากล - เพื่อให้หน่วยงานสามารถดำเนินงานได้ตามมาตรฐานที่ได้รับการยอมรับในระดับโลก และสร้างโอกาสในการทำงานร่วมกับองค์กรหรือหน่วยงานระหว่างประเทศ

แนวทางการดำเนินการ:

1. ศึกษาและวิเคราะห์มาตรฐานสากลที่เกี่ยวข้อง:
    - ทำการศึกษามาตรฐานสากล เช่น ISO/IEC 27001 และอื่น ๆ ที่สัมพันธ์กับความมั่นคงปลอดภัยสารสนเทศ
    - ระบุช่องว่างและสิ่งที่จำเป็นต้องปรับปรุงเพื่อให้สอดคล้องกับมาตรฐาน
2. พัฒนาระบบและกระบวนการเพื่อรองรับมาตรฐาน:
    - ปรับปรุงและพัฒนากระบวนการภายในเพื่อให้เป็นไปตามข้อกำหนดของมาตรฐานที่ต้องการ
    - จัดทำเอกสารและบันทึกที่จำเป็นสำหรับการรับรองมาตรฐาน
3. ดำเนินการรับรองมาตรฐาน:
    - ติดต่อและดำเนินการร่วมกับองค์กรที่ได้รับอนุญาตในการประเมินและรับรองมาตรฐาน
    - เตรียมความพร้อมสำหรับการตรวจสอบและปรับปรุงตามคำแนะนำ

ตัวชี้วัดและค่าเป้าหมาย:

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดกลยุทธ์ที่ 3.1	ค่าเป้าหมาย		
	2568	2569	2570
ระดับความรู้เกี่ยวกับมาตรฐานสากลภายในองค์กร:		> 80% ของบุคลากรที่เกี่ยวข้อง	> 90% ของบุคลากรที่เกี่ยวข้อง
การได้รับการรับรองมาตรฐาน		เตรียมความพร้อม	ได้รับการรับรองมาตรฐาน
ประสิทธิภาพของการปฏิบัติตามมาตรฐาน		ตรวจสอบภายในประจำปีและไม่มีข้อผิดพลาดร้ายแรง	ตรวจสอบภายในประจำปีและไม่มีข้อผิดพลาดร้ายแรง

ตารางที่ 1-22 ตัวชี้วัดและค่าเป้าหมาย 3.1

คำอธิบายตัวชี้วัด:

ชื่อตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ
ระดับความรู้เกี่ยวกับมาตรฐานสากลภายในองค์กร:	เฉพาะบุคลากรภายใต้ขอบเขตการขอรับรองมาตรฐาน	➢ ผลการทดสอบหลังอบรมจากแบบทดสอบ ➢ คะแนนเต็มของแบบทดสอบ	(ผลการทดสอบหลังอบรมจากแบบทดสอบ/คะแนนเต็มของแบบทดสอบ) * 100%
การได้รับการรับรองมาตรฐาน	เฉพาะขอบเขตการขอรับรองมาตรฐานที่ทาง สคทช. กำหนด	➢ การได้รับรองมาตรฐานสากล	การได้รับรองมาตรฐานสากล
ประสิทธิภาพของการปฏิบัติตามมาตรฐาน	เฉพาะขอบเขตการขอรับรองมาตรฐานที่ทาง สคทช. กำหนด	➢ ตรวจสอบภายในประจำปีและไม่มีข้อผิดพลาดร้ายแรง จากรายงานของผู้ตรวจสอบภายใน	ตรวจสอบภายในประจำปีและไม่มีข้อผิดพลาดร้ายแรง

ตารางที่ 1-23 คำอธิบายตัวชี้วัด 3.1

แผนงาน/โครงการที่เกี่ยวข้อง:

- P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ

ปัจจัยแห่งความสำเร็จ:

- ความเข้าใจและการมีส่วนร่วมจากบุคลากร
- การสนับสนุนทางการเงินและบริหารจากผู้บริหารระดับสูง
- ความชัดเจนและการสื่อสารอย่างมีประสิทธิภาพภายในองค์กร

การใช้ยุทธศาสตร์นี้จะช่วยให้สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติมีความมั่นคงปลอดภัยผ่านการปฏิบัติงานที่เป็นธรรมาภิบาลที่ดี ซึ่งเป็นพื้นฐานในการสร้างความยั่งยืนและความน่าเชื่อถือในระยะยาว

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2. นโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

นโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศของ สคทช. ประกอบด้วย 4 มาตรการ ได้แก่ มาตรการควบคุมด้านองค์กร ด้านบุคลากร ด้านกายภาพ และด้านเทคโนโลยี ดังภาพ



รูปที่ 2-1: 4 มาตรการ สำหรับนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านไซเบอร์

2.1 บทนำนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ภาพรวมของมาตรการ 4 มาตรการ สำหรับนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านไซเบอร์และสารสนเทศของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) มีดังนี้

1. มาตรการเชิงองค์กร (Organizational Measures): มาตรการนี้เกี่ยวข้องกับการกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ในระดับองค์กร โดยเน้นการบริหารจัดการในระดับสูง การกำหนดบทบาทและความรับผิดชอบที่ชัดเจน รวมถึงการประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อรับมือกับภัยคุกคามทางไซเบอร์
2. มาตรการด้านบุคลากร (Personnel Measures): มาตรการนี้ครอบคลุมการบริหารจัดการบุคลากรที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น การตรวจสอบและคัดเลือกบุคลากรก่อนเริ่มปฏิบัติงาน การจัดอบรมให้ความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง รวมถึงการมีแนวทางปฏิบัติเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคาม
3. มาตรการเชิงกายภาพ (Physical Measures): มาตรการนี้มุ่งเน้นการรักษาความมั่นคงปลอดภัยในด้านกายภาพ เช่น การกำหนดขอบเขตการเข้าถึงพื้นที่เฉพาะ การจัดการความปลอดภัยของอาคารและห้องเซิร์ฟเวอร์ รวมถึงการควบคุมการเข้าถึงพื้นที่สำคัญที่เกี่ยวข้องกับการจัดการข้อมูลและระบบ
4. มาตรการด้านเทคโนโลยี (Technological Measures): มาตรการนี้เกี่ยวข้องกับการใช้เทคโนโลยีในการป้องกันภัยคุกคามทางไซเบอร์ เช่น การรักษาความปลอดภัยของเครือข่าย การ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ควบคุมการเข้าถึงระบบ การป้องกันมัลแวร์ การเข้ารหัสข้อมูล และการสำรองข้อมูลเพื่อป้องกันความสูญเสียของข้อมูลในกรณีฉุกเฉิน

มาตรการทั้ง 4 มาตรการดังกล่าว มีความสอดคล้องกับยุทธศาสตร์ของแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ โดยมีรายละเอียดดังนี้

- **ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)**
  1. มาตรการเชิงองค์กร (Organizational Measures) กำหนดนโยบายความมั่นคงปลอดภัยที่ชัดเจน เพื่อรองรับการพัฒนาความสามารถของบุคลากรและเทคโนโลยีให้เหมาะสม
  2. มาตรการด้านบุคลากร (Personnel Measures) พัฒนาทักษะบุคลากรในการจัดการภัยคุกคามไซเบอร์ เช่น การอบรมเกี่ยวกับการจัดการความเสี่ยงและการตอบสนองต่อเหตุการณ์
  3. มาตรการเชิงกายภาพ (Physical Measures) พัฒนามาตรการป้องกันการเข้าถึงพื้นที่เฉพาะ เช่น การใช้ระบบควบคุมการเข้า-ออกด้วยเทคโนโลยีที่ทันสมัย
  4. มาตรการด้านเทคโนโลยี (Technological Measures) ใช้เทคโนโลยีในการป้องกันภัยคุกคาม เช่น ระบบ IDS/IPS การสำรองข้อมูล และการเข้ารหัสข้อมูล
- **ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)**
  1. มาตรการเชิงองค์กร (Organizational Measures) จัดทำกรอบความร่วมมือในการรับมือภัยคุกคาม เช่น การแบ่งปันข้อมูลภัยคุกคามระหว่างองค์กร
  2. มาตรการด้านบุคลากร (Personnel Measures) ส่งเสริมความร่วมมือในการฝึกอบรมและแลกเปลี่ยนองค์ความรู้กับพันธมิตรในภาคส่วนต่าง ๆ
  3. มาตรการเชิงกายภาพ (Physical Measures) ประสานงานกับหน่วยงานพันธมิตรเพื่อเสริมสร้างระบบรักษาความปลอดภัยกายภาพ เช่น ศูนย์ข้อมูลกลาง (Data Center)
  4. มาตรการด้านเทคโนโลยี (Technological Measures) ใช้คลาวด์ (Cloud) ภาครัฐและเครือข่ายความร่วมมือในการป้องกันและตอบสนองภัยคุกคาม เช่น ระบบแจ้งเตือนภัยคุกคาม
- **ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)**
  1. มาตรการเชิงองค์กร (Organizational Measures) นำกรอบมาตรฐานสากล เช่น ISO/IEC 27001 มาใช้เป็นแนวทางในการกำหนดนโยบายและแนวปฏิบัติระดับองค์กร
  2. มาตรการด้านบุคลากร (Personnel Measures) ใช้แนวทางการพัฒนาบุคลากรให้เป็นไปตามมาตรฐาน เช่น การกำหนดเกณฑ์การฝึกอบรมที่สอดคล้องกับ ISO/IEC 27001
  3. มาตรการเชิงกายภาพ (Physical Measures) ปฏิบัติตามมาตรฐาน เช่น ISO/IEC เพื่อควบคุมการเข้าถึงพื้นที่สำคัญอย่างมีประสิทธิภาพ
  4. มาตรการด้านเทคโนโลยี (Technological Measures) ใช้กรอบมาตรฐาน เช่น NIST Cybersecurity Framework และ ISO/IEC เพื่อเพิ่มประสิทธิภาพการใช้เทคโนโลยี

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ทั้งนี้รายละเอียดในมาตรการต่าง ๆ จะถูกกล่าวอย่างละเอียดในบทถัดไป ยิ่งไปกว่านั้น ในตอนท้ายของเอกสารมีการสรุปรายละเอียดความเชื่อมโยงระหว่างแนวปฏิบัติและมาตรฐานสากล ISO 27002:2022 ให้เห็นว่าตามมาตรการดังกล่าวทั้ง 4 มาตรการมีความสอดคล้องกับมาตรฐานสากล ISO 27002:2022 และสามารถยกระดับ สคทช. ให้มีมาตรการทางด้านความมั่นคงปลอดภัยไซเบอร์ที่เชื่อมโยงกับมาตรฐานสากล

ดูรายละเอียดเพิ่มเติมในหัวข้อความเชื่อมโยงระหว่างแนวปฏิบัติ และยุทธศาสตร์ในแผนที่นำทาง (Road Map) ในบทนำนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร ประกอบด้วยรายละเอียดต่าง ๆ ได้แก่ ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร วัตถุประสงค์ของนโยบาย บทบาทและความรับผิดชอบ การปฏิบัติตามกฎหมายและมาตรฐาน แนวทางการปรับปรุงและพัฒนา ผลลัพธ์ที่คาดหวัง และ องค์ประกอบของนโยบาย ดังนี้

2.1.1 ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ยุทธศาสตร์	ตัวชี้ของมาตรการ			
	มาตรการเชิงองค์กร (Organizational Measures)	มาตรการด้านบุคลากร (Personnel Measures)	มาตรการเชิงกายภาพ (Physical Measures)	มาตรการด้านเทคโนโลยี (Technological Measures)
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	1.1 ร้อยละของหน่วยงานหรือพนักงานที่ปฏิบัติตามนโยบายที่กำหนด 1.2 เวลาที่ใช้ในการตอบสนองต่อเหตุการณ์ (Response Time) เมื่อเกิดเหตุด้านความมั่นคงปลอดภัย	2.1 ร้อยละของพนักงานที่เข้าร่วมอบรมด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปี 2.2 อัตราการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย	3.1 อัตราการตรวจสอบอุปกรณ์กายภาพ (Physical Equipment Inspection Rate) 3.2 อัตราการติดตั้งระบบควบคุมการเข้าถึงพื้นที่สำคัญ (Access Control Systems Installation Rate)	4.1 อัตราการแก้ไขช่องโหว่ 4.2 ความพร้อมใช้งานของระบบเครือข่าย
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	1.2 เวลาที่ใช้ในการตอบสนองต่อเหตุการณ์ (Response Time) เมื่อเกิดเหตุด้านความมั่นคงปลอดภัย	2.1 ร้อยละของพนักงานที่เข้าร่วมอบรมด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปี 2.2 อัตราการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย		4.1 อัตราการแก้ไขช่องโหว่ 4.2 ความพร้อมใช้งานของระบบเครือข่าย
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	1.1 ร้อยละของหน่วยงานหรือพนักงานที่ปฏิบัติตามนโยบายที่กำหนด 1.2 เวลาที่ใช้ในการตอบสนองต่อเหตุการณ์	2.1 ร้อยละของพนักงานที่เข้าร่วมอบรมด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปี	3.1 อัตราการตรวจสอบอุปกรณ์กายภาพ (Physical Equipment Inspection Rate) 3.2 อัตราการติดตั้งระบบควบคุมการเข้าถึงพื้นที่สำคัญ (Access	4.1 อัตราการแก้ไขช่องโหว่ 4.2 ความพร้อมใช้งานของระบบเครือข่าย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์	ตัวชี้ของมาตรการ			
	มาตรการเชิงองค์กร (Organizational Measures)	มาตรการด้านบุคลากร (Personnel Measures)	มาตรการเชิงกายภาพ (Physical Measures)	มาตรการด้านเทคโนโลยี (Technological Measures)
	(Response Time) เมื่อเกิดเหตุด้านความมั่นคงปลอดภัย	2.2 อัตราการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย	Control Systems Installation Rate)	

ตารางที่ 2-1 ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ตัวชี้วัดของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารถูกกำหนดขึ้นสำหรับการวัดผลสำเร็จหรือการดำเนินการภายใต้กรอบการดำเนินการของนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีรายละเอียด ดังนี้

1. ตัวชี้วัดมาตรการเชิงองค์กร (Organizational Measures)

1.1 ร้อยละของหน่วยงานหรือพนักงานที่ปฏิบัติตามนโยบายที่กำหนด

- **เป้าหมาย :** พนักงาน 100% ต้องปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ
- **วิธีวัด :** 1) ดำเนินการตรวจสอบ (Audit) การปฏิบัติงานตามนโยบายในทุกส่วนงาน
  2) เก็บข้อมูลจากรายงานการตรวจสอบ (Internal Audit Report)
  3) วิเคราะห์จำนวนข้อบกพร่อง (Non-compliance) และหาค่าเฉลี่ยเปอร์เซ็นต์การปฏิบัติตาม

1.2 เวลาที่ใช้ในการตอบสนองต่อเหตุการณ์ (Response Time) เมื่อเกิดเหตุด้านความมั่นคงปลอดภัย

- **เป้าหมาย** : ตอบสนองภายในระยะเวลา SLA (เช่น 4 ชั่วโมง)
- **วิธีวัด** : 1) เก็บข้อมูลจากบันทึกการจัดการเหตุการณ์ (Incident Logs)
  2) ตรวจสอบรายงานการตอบสนองและเวลาเริ่มต้น-สิ้นสุดการดำเนินการ

2. ตัวชี้วัดมาตรการด้านบุคลากร (Personnel Measures)

2.1 ร้อยละของพนักงานที่เข้าร่วมอบรมด้านความมั่นคงปลอดภัยสารสนเทศในแต่ละปี

- **เป้าหมาย** : พนักงานอย่างน้อย 80% ต้องเข้าร่วมอบรมในปีนั้น
- **วิธีวัด** : 1) ตรวจสอบรายชื่อผู้เข้าร่วมอบรม
  2) เก็บคะแนนความเข้าใจจากแบบทดสอบหลังการอบรม (ไม่น้อยกว่า 80%)

2.2 อัตราการรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

- **เป้าหมาย** : 100% ของเหตุการณ์ที่เกิดขึ้นต้องได้รับการรายงานผ่านช่องทางที่กำหนด
- **วิธีวัด** : รวบรวมข้อมูลจากระบบการจัดการเหตุการณ์ (Incident Management System)

3. ตัวชี้วัดมาตรการเชิงกายภาพ (Physical Measures)

3.1 อัตราการตรวจสอบอุปกรณ์กายภาพ (Physical Equipment Inspection Rate)

- **เป้าหมาย** : ตรวจสอบอุปกรณ์ด้านความมั่นคงปลอดภัย เช่น ประตูล็อก ระบบเซ็นเซอร์ และเครื่องดับเพลิง อย่างน้อย 95% ตามแผนการตรวจสอบ
- **วิธีวัด** : รวบรวมรายงานการตรวจสอบอุปกรณ์ตามแผน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.2 อัตราการติดตั้งระบบควบคุมการเข้าถึงพื้นที่สำคัญ (Access Control Systems Installation Rate)

- **เป้าหมาย** : พื้นที่สำคัญ 100% เช่น ห้องเซิร์ฟเวอร์และห้องเก็บข้อมูลต้องติดตั้งระบบควบคุมการเข้าถึง เช่น ระบบสแกนบัตรหรือสแกนลายนิ้วมือ
- **วิธีวัด** : ตรวจสอบจำนวนพื้นที่สำคัญที่ติดตั้งระบบควบคุมการเข้าถึง

4. ตัวชี้วัดมาตรการด้านเทคโนโลยี (Technological Measures)

4.1 อัตราการแก้ไขช่องโหว่

- **เป้าหมาย** : แก้ไขช่องโหว่ที่ตรวจพบไม่น้อยกว่า 90% ภายในระยะเวลาที่กำหนด (เช่น 30 วัน)
- **วิธีวัด** : ตรวจสอบบันทึกการสแกนช่องโหว่ (Vulnerability Scan Reports) และสถานะการแก้ไข

4.2 ความพร้อมใช้งานของระบบเครือข่าย

- **เป้าหมาย** : ระบบเครือข่ายต้องมีความพร้อมใช้งานไม่น้อยกว่า 99.9% ตลอดเวลา
- **วิธีวัด** : รวบรวมข้อมูลสถานะการทำงานของระบบเครือข่ายจากระบบตรวจสอบเครือข่าย (Network Monitoring System)

2.1.2 วัตถุประสงค์ของนโยบาย

นโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) มีวัตถุประสงค์สำคัญดังนี้:

- **เสริมสร้างความมั่นคงปลอดภัย** ให้แก่ข้อมูลและระบบสารสนเทศที่เกี่ยวข้องกับการจัดการที่ดิน
- **ป้องกันและลดความเสี่ยง** ที่เกิดจากภัยคุกคามทางไซเบอร์ทั้งภายในและภายนอกองค์กร
- **ปฏิบัติตามกฎหมาย** ระเบียบข้อบังคับ และมาตรฐานที่เกี่ยวข้องอย่างเคร่งครัด
- **ส่งเสริมการใช้งานข้อมูล** และระบบอย่างมีประสิทธิภาพและปลอดภัย

2.1.3 บทบาทและความรับผิดชอบ

1. ผู้บริหารระดับสูง

- กำหนดและอนุมัตินโยบาย พร้อมสนับสนุนการดำเนินการให้เกิดผล
- สื่อสารนโยบายให้บุคลากรทุกระดับเข้าใจ และสร้างความตระหนักในความสำคัญของความมั่นคงปลอดภัยไซเบอร์
- จัดสรรทรัพยากรที่เพียงพอทั้งในด้านงบประมาณและบุคลากร
- ทบทวนและประเมินผลการดำเนินงานอย่างต่อเนื่อง

2. ผู้ใช้งานทั่วไป

- ปฏิบัติตามนโยบายและแนวปฏิบัติที่กำหนด
- รักษารหัสผ่านและข้อมูลการเข้าถึงระบบให้ปลอดภัย
- รายงานเหตุการณ์หรือภัยคุกคามที่พบเห็นทันที
- หลีกเลี่ยงการใช้งานทรัพยากรองค์กรในทางที่ไม่เหมาะสม

2.1.4 การปฏิบัติตามกฎหมายและมาตรฐาน

- ปฏิบัติตามข้อกำหนดของ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์, พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล และกฎหมายที่เกี่ยวข้องอื่น ๆ
- ดำเนินการตามมาตรฐานสากล เช่น ISO/IEC 27001 รวมถึงแนวปฏิบัติที่ดีในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- กำหนดระบบตรวจสอบและประเมินผลเพื่อสร้างความสอดคล้องกับกฎหมายและมาตรฐาน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.1.5 แนวทางการปรับปรุงและพัฒนา

- ทบทวนและปรับปรุงนโยบายและมาตรการให้ทันสมัย อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
- ส่งเสริมการเรียนรู้และพัฒนาทักษะของบุคลากรอย่างต่อเนื่อง
- พิจารณาเทคโนโลยีใหม่ ๆ เพื่อเพิ่มประสิทธิภาพการรักษาความมั่นคงปลอดภัย

2.1.6 ผลลัพธ์ที่คาดหวัง

- ความเสี่ยงจากภัยคุกคามทางไซเบอร์ลดลงอย่างมีนัยสำคัญ
- ข้อมูลและทรัพย์สินขององค์กรมีความมั่นคงปลอดภัย
- ความน่าเชื่อถือและความไว้วางใจจากหน่วยงานภายในและภายนอกเพิ่มขึ้น

2.1.7 องค์ประกอบของนโยบาย

นโยบายนี้กำหนดมาตรการครอบคลุมใน 4 ด้านหลัก ดังนี้:

1. มาตรการเชิงองค์กร

- การกำหนดนโยบายและแนวปฏิบัติในการบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ พร้อมสื่อสารให้ผู้เกี่ยวข้องทราบและปฏิบัติตาม
- การจัดตั้งทีมตอบสนองต่อเหตุการณ์ (Cyber Incident Response Team: CIRT) พร้อมกำหนดบทบาทและความรับผิดชอบที่ชัดเจนของผู้บริหารระดับสูง
- การวางแผนและเตรียมความพร้อมในการตอบสนองต่อเหตุการณ์ เช่น การจัดทำแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan)
- การประสานงานและแลกเปลี่ยนข้อมูลกับหน่วยงานภายนอก เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)

2. มาตรการด้านบุคลากร

- การคัดกรองและตรวจสอบประวัติของบุคลากรที่เกี่ยวข้องเพื่อประเมินความเหมาะสม
- การจัดการฝึกอบรมและเสริมสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง
- การสร้างจิตสำนึกในเรื่องความเสี่ยงและภัยคุกคามไซเบอร์ผ่านกิจกรรมเสริมสร้างความเข้าใจ

3. มาตรการเชิงกายภาพ

- การควบคุมการเข้าถึงพื้นที่สำคัญ เช่น ห้องเซิร์ฟเวอร์ อุปกรณ์จัดเก็บข้อมูล และระบบเครือข่าย
- การป้องกันทรัพย์สินและอุปกรณ์ขององค์กรจากการเข้าถึงโดยไม่ได้รับอนุญาต

4. มาตรการด้านเทคโนโลยี

- การนำเทคโนโลยีที่เหมาะสมมาใช้ เช่น การเข้ารหัสข้อมูล การป้องกันมัลแวร์ และระบบตรวจจับภัยคุกคาม
- การสำรองข้อมูลและระบบอย่างสม่ำเสมอเพื่อป้องกันการสูญเสียหรือการถูกโจมตี
- การบริหารจัดการสิทธิ์การเข้าถึงระบบ (Role-Based Access Control: RBAC) ตามบทบาทและหน้าที่ของผู้ใช้งาน

ทั้งนี้รายละเอียดของมาตรการทั้ง 4 มาตรการในส่วนของแนวทางในการปฏิบัติตามด้านต่าง ๆ ที่มีความสอดคล้องกับผลการศึกษาเกี่ยวกับนโยบาย กฎหมาย กฎระเบียบ และมาตรฐานที่เกี่ยวข้อง มีดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2 มาตรการที่ 1 มาตรการควบคุมด้านองค์กร (Organizational controls)

มาตรการเชิงองค์กรถือเป็นหัวใจสำคัญในการจัดการด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยเน้นการวางรากฐานการบริหารจัดการในระดับองค์กร เพื่อให้แน่ใจว่าทุกขั้นตอนของการดำเนินงานเป็นไปตามนโยบายและแผนที่ได้กำหนดไว้ การกำหนดนโยบายที่ชัดเจนและการรับรู้ของผู้บริหารระดับสูงจะช่วยสร้างการบูรณาการในการรับมือกับภัยคุกคามทางไซเบอร์ โดยเฉพาะในหน่วยงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญอย่างสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) การกำหนดบทบาทและความรับผิดชอบที่ชัดเจนให้กับผู้ที่เกี่ยวข้อง เช่น เจ้าหน้าที่ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์หรือทีมงานที่ดูแลด้านความปลอดภัยไซเบอร์ จะทำให้การดำเนินการต่าง ๆ เป็นไปอย่างมีระบบและประสิทธิภาพ นอกจากนี้ มาตรการนี้ยังครอบคลุมถึงการสื่อสารและการประสานงานกับหน่วยงานภายนอก เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) และหน่วยงานที่เกี่ยวข้องอื่น ๆ เพื่อรับมือกับภัยคุกคามไซเบอร์ที่อาจเกิดขึ้น รวมถึงการจัดทำแผนฟื้นฟูเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร การมีมาตรการเชิงองค์กรที่เข้มแข็งจะทำให้องค์กรสามารถรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพและสร้างความมั่นใจในความปลอดภัยของข้อมูลในระยะยาว

2.2.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)

(1) องค์กรต้องมีการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุมแนวทางโดยรวมขององค์กรเกี่ยวกับความมั่นคงปลอดภัยสารสนเทศ และนโยบายนี้ต้องได้รับการอนุมัติจากฝ่ายบริหาร เผยแพร่ สื่อสารไปยังบุคลากรที่เกี่ยวข้องทั้งหมด และมีการทบทวนเป็นประจำ

(2) องค์กรต้องพัฒนานโยบายเพิ่มเติมที่ระบุถึงหัวข้อหรือประเด็นปัญหาเฉพาะด้านความมั่นคงปลอดภัยสารสนเทศ นโยบายเหล่านี้ควรสอดคล้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศโดยรวม และครอบคลุมประเด็นต่าง ๆ เช่น การควบคุมการเข้าถึง การจัดการรหัสผ่าน การตอบสนองต่อเหตุการณ์ การปกป้องข้อมูล และการใช้งานที่ยอมรับได้ เป็นต้น

(3) องค์กรต้องมีการสื่อสารนโยบายความมั่นคงปลอดภัยสารสนเทศทั้งหมดไปยังบุคลากรและผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งหมด ผ่านช่องทางต่าง ๆ เช่น การฝึกอบรม อินทราเน็ต และการแจ้งเตือนทางอีเมล์

(4) นโยบายความมั่นคงปลอดภัยต้องมีภาษาที่ชัดเจน กระชับและเข้าใจได้ง่าย เพื่อหลีกเลี่ยงความคลุมเครือ

(5) นโยบายด้านความมั่นคงปลอดภัยต้องได้รับการทบทวนและปรับปรุงนโยบายความมั่นคงปลอดภัยสารสนเทศเป็นประจำ เพื่อคงไว้ซึ่งประสิทธิภาพในการปฏิบัติงานและสอดคล้องกับการดำเนินการต่าง ๆ ตามที่องค์กรกำหนด

(6) ตรวจสอบการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ และดำเนินการที่เหมาะสมในกรณีที่ไม่ปฏิบัติตาม

2.2.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)

(1) ต้องมีการกำหนดบทบาทและความรับผิดชอบของบุคลากร (Role and responsibility) ด้านความมั่นคงปลอดภัยของข้อมูลโดยแบ่งตามโครงสร้างขององค์กรเพื่อใช้ในการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(2) ต้องมีการจัดทำบันทึกรายชื่อ สำหรับใช้ในการติดต่อหรือประสานงานในการดำเนินการด้านความมั่นคงปลอดภัยตามหน้าที่ที่ได้รับมอบหมายจากหน่วยงาน
(3) ต้องดำเนินการจัดทำเป็นระเบียบและจัดทำเอกสารการจัดสรรบทบาท เช่น ในตารางหรือแผนผังองค์กร
(4) ต้องมีการทบทวนบทบาท หน้าที่ และความรับผิดชอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

2.2.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)

(1) ต้องมีการแบ่งหน้าที่และความรับผิดชอบของบุคลากร (Segregation of Duties) ด้านความมั่นคงปลอดภัยของข้อมูล เพื่อป้องกันความขัดแย้งในการดำเนินงาน โดยแบ่งตามโครงสร้างขององค์กรเพื่อใช้ในการดำเนินการตามหน้าที่ที่ได้รับมอบหมาย
ตัวอย่างการแบ่งแยกหน้าที่ในด้านความมั่นคงปลอดภัยสารสนเทศ:
- การอนุมัติและการดำเนินการ: ผู้ที่อนุมัติการทำธุรกรรม (เช่น การสั่งซื้อ การชำระเงิน) ไม่ควรเป็นผู้เดียวกับที่ดำเนินการธุรกรรมนั้น
- การพัฒนาและการทดสอบระบบ: ผู้ที่พัฒนาซอฟต์แวร์หรือระบบสารสนเทศไม่ควรเป็นผู้เดียวกับที่ทดสอบระบบนั้น
- การดูแลระบบและการตรวจสอบ: ผู้ที่ดูแลระบบสารสนเทศไม่ควรเป็นผู้เดียวกับที่ทำหน้าที่ตรวจสอบความมั่นคงปลอดภัยของระบบ

(2) ต้องดำเนินการจัดทำเป็นระเบียบและจัดทำเอกสารการจัดสรรบทบาท เช่น ในตารางหรือแผนผังองค์กร
(3) ต้องมีการทบทวนบทบาท หน้าที่ และความรับผิดชอบเป็นประจำอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลง

2.2.4 หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities)

(1) ฝ่ายบริหารระดับสูงสุดต้องแสดงให้เห็นถึงความเป็นผู้นำและความมุ่งมั่นในการจัดการความมั่นคงปลอดภัยสารสนเทศ ซึ่งรวมถึงการกำหนดนโยบายและวัตถุประสงค์ด้านความมั่นคงปลอดภัยสารสนเทศ การจัดสรรทรัพยากรที่เพียงพอ และการสื่อสารความสำคัญของความมั่นคงปลอดภัยสารสนเทศไปยังองค์กร
(2) ฝ่ายบริหารต้องรับผิดชอบในการกำหนดนโยบายความมั่นคงปลอดภัยสารสนเทศที่สอดคล้องกับทิศทางเชิงกลยุทธ์ขององค์กร และเป็นไปตามข้อกำหนดทางกฎหมาย กฎระเบียบ และข้อกำหนดอื่น ๆ ที่เกี่ยวข้อง
(3) ฝ่ายบริหารต้องกำหนดบทบาท ความรับผิดชอบ และอำนาจหน้าที่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน โดยเฉพาะอย่างยิ่งสำหรับผู้ที่มีบทบาทสำคัญในการดำเนินงานและดูแล ISMS
(4) ฝ่ายบริหารต้องจัดสรรทรัพยากรที่เพียงพอสำหรับการดำเนินงานและปรับปรุง ISMS อย่างต่อเนื่อง ซึ่งรวมถึงทรัพยากรด้านบุคคล งบประมาณ เทคโนโลยี และโครงสร้างพื้นฐาน
(5) การทบทวนการจัดการ: ฝ่ายบริหารต้องทบทวน ISMS เป็นประจำ เพื่อให้แน่ใจว่ายังคงมีความเหมาะสม เพียงพอ และมีประสิทธิภาพในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)

(1) องค์กรต้องระบุหน่วยงานผู้มีอำนาจที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และสร้างความสัมพันธ์กับหน่วยงานที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.) เป็นต้น

(2) องค์กรต้องมีช่องทางการติดต่อสื่อสารที่ชัดเจนและมีประสิทธิภาพกับหน่วยงานผู้มีอำนาจ

(3) องค์กรต้องรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่สำคัญไปยังหน่วยงานผู้มีอำนาจตามข้อกำหนดที่เกี่ยวข้อง เช่น การละเมิดข้อมูลส่วนบุคคล หรือการโจมตีทางไซเบอร์ เป็นต้น

2.2.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)

(1) องค์กรต้องระบุกลุ่มผลประโยชน์เฉพาะที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศ และสร้างความสัมพันธ์กับกลุ่มเหล่านั้น

(2) องค์กรต้องมีช่องทางการติดต่อสื่อสารที่ชัดเจนและมีประสิทธิภาพกับกลุ่มผลประโยชน์เฉพาะ

(3) องค์กรต้องแลกเปลี่ยนข้อมูลข่าวสารและแนวทางปฏิบัติที่ดีที่สุดด้านความมั่นคงปลอดภัยสารสนเทศกับกลุ่มผลประโยชน์เฉพาะ

(4) องค์กรควรมีส่วนร่วมในกิจกรรมที่จัดโดยกลุ่มผลประโยชน์เฉพาะ เช่น การประชุม การสัมมนา หรือการฝึกอบรม

2.2.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)

(1) ให้มีการเข้าร่วมกลุ่มหรือเป็นสมาชิกในกลุ่มองค์กรที่จัดตั้งขึ้น เพื่อการแลกเปลี่ยนข้อมูลข่าวสารภัยคุกคามทางไซเบอร์ รวมถึงการติดตามข้อมูลข่าวสารจากสื่อสังคมออนไลน์ต่าง ๆ เพื่อให้หน่วยงานมีข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ที่ทันสมัยอยู่ตลอดเวลา และให้มีการเก็บรวบรวมและวิเคราะห์ข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์ (Threat Intelligence) ที่อาจส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานเพื่อแจ้งเตือนให้ผู้ที่เกี่ยวข้องภายในหน่วยงานได้ทราบล่วงหน้าเพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

- แหล่งข้อมูลภายใน
  - อุปกรณ์หรือระบบรักษาความมั่นคงปลอดภัยสารสนเทศเช่น Firewall, IPS, Anti-virus
- แหล่งข้อมูลภายนอก
  - เครื่องมือข่าวกรองภัยคุกคามแบบ Opensource หรือ Commercial license
  - ศูนย์แลกเปลี่ยนข้อมูลภัยคุกคาม
  - กลุ่มหน่วยงานภาครัฐ

(2) กำหนดให้มีการรวบรวมและวิเคราะห์สารสนเทศที่เกี่ยวข้องกับภัยคุกคามต่อการรักษาความมั่นคงปลอดภัยของสารสนเทศเพื่อสร้างข่าวกรองด้านภัยคุกคาม (Threat intelligence) เพื่อให้ความตระหนักถึงสภาพแวดล้อมภัยคุกคามขององค์กรเพื่อให้สามารถดำเนินการบรรเทาที่เหมาะสมได้

(3) การวิเคราะห์ข้อมูล: องค์กรต้องวิเคราะห์ข้อมูลที่รวบรวมได้ เพื่อระบุและประเมินภัยคุกคามที่อาจส่งผลกระทบต่อองค์กร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(4) การใช้ประโยชน์จากข้อมูล: องค์กรต้องใช้ประโยชน์จากข้อมูลการข่าวกรองภัยคุกคามเพื่อปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศ ตัดสินใจเกี่ยวกับการจัดการความเสี่ยง และเพิ่มความสามารถในการตรวจจับและตอบสนองต่อเหตุการณ์

(5) การแบ่งปันข้อมูล: องค์กรควรพิจารณาแบ่งปันข้อมูลการข่าวกรองภัยคุกคามกับองค์กรอื่น ๆ หรือหน่วยงานที่เกี่ยวข้อง เพื่อช่วยเพิ่มความตระหนักรู้และความสามารถในการรับมือกับภัยคุกคามในวงกว้าง

2.2.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)

(1) การวางแผนความมั่นคงปลอดภัยสารสนเทศ: ในระหว่างขั้นตอนการวางแผนโครงการ องค์กรต้องระบุและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น และกำหนดมาตรการควบคุมที่เหมาะสมเพื่อลดความเสี่ยงเหล่านั้น

(2) การออกแบบและการพัฒนา: ในระหว่างขั้นตอนการออกแบบและพัฒนาโครงการ องค์กรต้องพิจารณาและนำข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไปปฏิบัติ เช่น การควบคุมการเข้าถึง การปกป้องข้อมูล การเข้ารหัส และการทดสอบความมั่นคงปลอดภัย

(3) การดำเนินการและการบำรุงรักษา: ในระหว่างขั้นตอนการดำเนินการและบำรุงรักษาโครงการ องค์กรต้องตรวจสอบและทบทวนมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ เพื่อให้แน่ใจว่ายังคงมีความเหมาะสมและมีประสิทธิภาพ

(4) การเปลี่ยนแปลงโครงการ: องค์กรต้องประเมินผลกระทบด้านความมั่นคงปลอดภัยสารสนเทศของการเปลี่ยนแปลงโครงการใด ๆ และปรับปรุงมาตรการควบคุมที่เกี่ยวข้องตามความเหมาะสม

2.2.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ (Inventory of information and other associated assets)

(1) จัดหมวดหมู่ทรัพย์สินสารสนเทศตามข้อกำหนดของกฎหมาย คุณค่า ความสำคัญ และความอ่อนไหวต่อการเปิดเผยหรือการเปลี่ยนแปลงแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

(2) จัดทำป้ายบ่งชี้ทรัพย์สินสารสนเทศ และนำไปปฏิบัติให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

(3) จัดทำขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สิน และนำไปปฏิบัติให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

(4) ทรัพย์สินสารสนเทศแต่ละประเภท ต้องมีการระบุผู้ดูแลทรัพย์สินอย่างชัดเจน

(5) ระบุและตรวจสอบ “ทะเบียนทรัพย์สินสารสนเทศ” ของหน่วยงาน โดยรายการทรัพย์สินสารสนเทศ ประกอบไปด้วย สารสนเทศและอุปกรณ์สารสนเทศ ซึ่งจัดแบ่งตามประเภท ดังนี้

- สารสนเทศ (Information) เช่น ข้อมูลในฐานข้อมูล ไฟล์ข้อมูล สัญญา เอกสาร/คู่มือระบบ ข้อมูลการวิจัย คู่มือผู้ใช้งาน ทรัพยากรในการฝึกอบรม ขั้นตอนการปฏิบัติงานหรือสนับสนุนแผนความต่อเนื่องทางธุรกิจ แผนการกู้คืนสภาพ ประวัติการตรวจสอบ สารสนเทศที่สำคัญอื่น ๆ
- ทรัพย์สินทางซอฟต์แวร์ (Software Assets) เช่น ซอฟต์แวร์สำเร็จรูป โปรแกรมระบบเครื่องมือสำหรับพัฒนา โปรแกรมประเภทยูทิลิตี้ (System Utilities)
- ทรัพย์สินทางฮาร์ดแวร์ (Hardware Assets) เช่น อุปกรณ์สารสนเทศ อุปกรณ์ติดต่อสื่อสาร อุปกรณ์เครือข่าย สื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(6) ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญของ สคทช. และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบันโดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

- ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ สคทช. ทรัพย์สินทางซอฟต์แวร์ (Software Assets) เช่น ซอฟต์แวร์สำเร็จรูป โปรแกรมระบบ เครื่องมือสำหรับพัฒนาโปรแกรมประเภทยูทิลิตี้ (System Utilities)
- ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ สคทช.
- การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญของ สคทช.
- เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญ สคทช.
- ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ สคทช. แต่ละรายการ
- การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ สคทช. บนระบบ/เครือข่ายภายใน และ/หรือภายนอก

(7) ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของ สคทช. ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

(8) ควบคุมดูแลให้ผลิตภัณฑ์ที่ได้รับการส่งมอบ ต้องได้รับการลงทะเบียนในทะเบียนรายการทรัพย์สินของหน่วยงาน ก่อนเคลื่อนย้ายไปยังจุดที่ติดตั้งใช้งานจริง

2.2.10 การใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)

(1) จัดทำกฎ ระเบียบ หรือหลักเกณฑ์อย่างเป็นลายลักษณ์อักษรสำหรับการใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศ เพื่อป้องกันความเสียหายต่อทรัพย์สิน

(2) ระบุทรัพย์สินที่เกี่ยวกับสารสนเทศและสถานที่และสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศให้ชัดเจน และจัดทำขั้นตอนปฏิบัติสำหรับการจัดการทรัพย์สินสารสนเทศ รวมทั้งปรับปรุงให้มีความทันสมัย

(3) ทรัพย์สินแต่ละรายการในบัญชีทรัพย์สิน ควรระบุผู้รับผิดชอบ

(4) องค์กรต้องกำหนดนโยบายการใช้งานที่ยอมรับได้ที่ครอบคลุมถึงการใช้งานสารสนเทศ ทรัพย์สิน และบริการต่าง ๆ ขององค์กร โดยนโยบายนี้ควรระบุถึงสิ่งที่อนุญาตและไม่อนุญาตให้ทำ รวมถึงผลที่ตามมาของการละเมิดนโยบาย

(5) องค์กรต้องสื่อสารนโยบายการใช้งานที่ยอมรับได้ให้กับพนักงานและผู้ใช้งานอื่น ๆ อย่างทั่วถึงและเข้าใจง่าย นอกจากนี้ควรจัดให้มีการฝึกอบรมเพื่อให้ความรู้และสร้างความตระหนักเกี่ยวกับนโยบายและความสำคัญของการปฏิบัติตาม

(6) องค์กรต้องมีกลไกในการตรวจสอบการใช้งานสารสนเทศและทรัพย์สินขององค์กร และบังคับใช้นโยบายการใช้งานที่ยอมรับได้อย่างเคร่งครัด

2.2.11 การคืนทรัพย์สิน (Return of assets)

(1) องค์กรต้องกำหนดกระบวนการที่ชัดเจนสำหรับการคืนทรัพย์สิน ซึ่งรวมถึงขั้นตอนการแจ้ง การตรวจสอบ และการบันทึก

(2) องค์กรต้องลบข้อมูลที่เป็นความลับออกจากทรัพย์สินที่ส่งคืนอย่างมั่นคงปลอดภัย ก่อนที่จะนำไปกำจัดหรือนำกลับมาใช้ใหม่

(3) องค์กรต้องจัดเก็บทรัพย์สินที่ส่งคืนอย่างมั่นคงปลอดภัย จนกว่าจะได้รับการตรวจสอบและลบข้อมูลเรียบร้อยแล้ว

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ต้องกำหนดรายการทรัพย์สิน ที่ต้องส่งคืนเมื่อพนักงานออกจากองค์กร เช่น คอมพิวเตอร์ โทรศัพท์มือถือ อุปกรณ์จัดเก็บข้อมูล และบัตรประจำตัวพนักงาน
- จัดทำแบบฟอร์มการคืนทรัพย์สิน เพื่อให้พนักงานกรอกรายละเอียดของทรัพย์สินที่ส่งคืน
- ตรวจสอบทรัพย์สินที่ส่งคืน เพื่อให้แน่ใจว่าครบถ้วนและอยู่ในสภาพดี
- ลบข้อมูลที่เป็นความลับ ออกจากทรัพย์สินที่ส่งคืนโดยใช้ซอฟต์แวร์หรือวิธีการที่ปลอดภัย
- จัดเก็บทรัพย์สินที่ส่งคืน ในสถานที่ที่ปลอดภัยและมีการควบคุมการเข้าถึง

2.2.12 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification of information)

(1) ให้มีการจัดหมวดหมู่ทรัพย์สินสารสนเทศ โดยคำนึงถึงการรักษาความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ของทรัพย์สินสารสนเทศ ซึ่งหมวดหมู่สารสนเทศที่ได้รับการจัดจะแบ่งเป็นระดับการป้องกันความมั่นคงปลอดภัย 4 ระดับ คือ ต่ำ ปานกลาง สูง และ สูงสุด

2.2.13 การทำป้ายบ่งชี้สารสนเทศ (Labelling of information)

(1) พิจารณาจัดทำป้ายบ่งชี้อุปกรณ์สารสนเทศ และสื่อบันทึกข้อมูลแบบอิเล็กทรอนิกส์ เช่น ซีดี เทป แผ่นดิสก์ โดยต้องไม่แสดงวัตถุประสงค์ของอุปกรณ์ดังกล่าวอย่างชัดแจ้ง

(2) ทรัพย์สินสารสนเทศที่อยู่ในระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” ให้มีการจัดทำป้ายบ่งชี้ทรัพย์สินสารสนเทศ โดยจัดทำเป็นรหัสและระบุรหัสลงในทะเบียนทรัพย์สินสารสนเทศ เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตเข้าถึงสารสนเทศดังกล่าวได้

(3) แจ้งให้ผู้เกี่ยวข้องทราบถึงขั้นตอนการทำป้ายบ่งชี้

2.2.14 การถ่ายโอนสารสนเทศ (Information transfer)

(1) องค์กรต้องมีข้อตกลงที่เป็นลายลักษณ์อักษรกับบุคคลภายนอกที่เกี่ยวข้องกับการถ่ายโอนสารสนเทศ ซึ่งระบุถึงความรับผิดชอบของแต่ละฝ่าย ข้อกำหนดด้านความมั่นคงปลอดภัย และมาตรการในการปกป้องสารสนเทศ

(2) องค์กรต้องควบคุมการเข้าถึงสารสนเทศที่ถูกถ่ายโอน โดยจำกัดสิทธิ์การเข้าถึงเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(3) องค์กรต้องใช้มาตรการที่เหมาะสมในการป้องกันสารสนเทศที่ถูกถ่ายโอน เช่น การเข้ารหัส การใช้ช่องทางการสื่อสารที่ปลอดภัย และการตรวจสอบกิจกรรมการถ่ายโอน

(4) องค์กรต้องติดตามและตรวจสอบกิจกรรมการถ่ายโอนสารสนเทศ เพื่อให้แน่ใจว่าเป็นไปตามนโยบายและข้อกำหนดที่เกี่ยวข้อง

- กำหนดข้อตกลงการถ่ายโอนสารสนเทศ กับคู่ค้า ผู้ให้บริการภายนอก หรือบุคคลที่สามอื่น ๆ ที่เกี่ยวข้อง
- ใช้ช่องทางการสื่อสารที่ปลอดภัย เช่น VPN หรือ SFTP สำหรับการถ่ายโอนข้อมูลที่เป็นความลับ
- เข้ารหัสข้อมูล ที่เป็นความลับก่อนทำการถ่ายโอน
- บันทึกและตรวจสอบ กิจกรรมการถ่ายโอนสารสนเทศ
- ให้ความรู้และฝึกอบรม พนักงานเกี่ยวกับความสำคัญของการปกป้องสารสนเทศระหว่างการถ่ายโอน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.15 การควบคุมการเข้าถึง (Access control)

(1) เจ้าของข้อมูลและเจ้าของระบบ ต้องประเมินความเสี่ยง ที่เกิดจากการเข้าถึงข้อมูลและการใช้ระบบสารสนเทศของลูกค้าหรือผู้ใช้บริการโดยต้องคำนึงถึงปัจจัยต่าง ๆ ตามมาตรฐานฯ เพื่อให้เป็นไปตามข้อตกลงระหว่างกัน

(2) ต้องมีการควบคุมบุคลากรในหน่วยงาน ให้เข้าถึงระบบและข้อมูลสารสนเทศโดยได้สิทธิการทำงานตามหน้าที่ความรับผิดชอบ (Roles Based Access Control) สอดคล้องกับความต้องการทางธุรกิจเป็นปัจจุบันอยู่เสมอ และเป็นไปตามมาตรฐานฯ ที่กำหนด

(3) ต้องมีการควบคุมให้ผู้ใช้งานระบบเข้าถึงระบบและข้อมูลสารสนเทศได้โดยได้สิทธิการทำงานตามหน้าที่ความรับผิดชอบ (Roles Based Access Control) สอดคล้องกับความต้องการทางธุรกิจเป็นปัจจุบันอยู่เสมอ และเป็นไปตามมาตรฐานฯ ที่กำหนด

(4) เจ้าของข้อมูล หรือเจ้าของระบบ ต้องสอบทานความเหมาะสมของตารางควบคุมสิทธิ อย่างน้อยปีละ 1 ครั้ง

(5) ต้องมีการควบคุมการเข้าถึงระบบเครือข่ายที่สำคัญและการให้บริการเครือข่าย (Network Service) ให้เข้าได้เฉพาะผู้ได้รับอนุญาตเท่านั้น รวมทั้งควบคุมให้เป็นไปตามมาตรฐานฯ ที่กำหนด

(6) ต้องมีการจำกัดผู้ใช้งานที่เชื่อมต่อระบบเครือข่ายของ สคทช. ให้เป็นไปตามความจำเป็นในการใช้งานและตามความต้องการทางธุรกิจ

2.2.16 การบริหารจัดการพิสูจน์ตัวตน (Identity management)

(1) จัดทำกระบวนการที่เป็นทางการสำหรับการลงทะเบียนและเพิกถอนผู้ใช้งาน เพื่อใช้ในการกำหนดสิทธิการเข้าถึง

(2) จัดทำขั้นตอนปฏิบัติสำหรับการจัดเตรียมการเข้าถึงของผู้ใช้งาน เพื่อกำหนดหรือเพิกถอนสิทธิในการเข้าถึงระบบและบริการทั้งหมดสำหรับผู้ใช้งานทุกประเภท

(3) ควบคุมการจัดสรรข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งานผ่านกระบวนการบริหารจัดการอย่างเป็นทางการ

(4) เพิกถอนสิทธิการเข้าถึงสารสนเทศและสิ่งอำนวยความสะดวกสำหรับการประมวลผลสารสนเทศของผู้ปฏิบัติงานและผู้ใช้งานที่เป็นบุคคลภายนอกทุกคนออก เมื่อสิ้นสุดการจ้างงาน สัญญาหรือข้อตกลง หรือปรับปรุงสิทธิดังกล่าวเมื่อมีการเปลี่ยนแปลง

2.2.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)

(1) หน่วยงานที่รับผิดชอบระบบ ต้องระบุข้อกำหนดสำหรับการควบคุมรหัสผ่านสำหรับการพัฒนาระบบ รวมทั้งต้องพัฒนาและทดสอบระบบสารสนเทศให้มีการควบคุมเรื่องการจัดการรหัสผ่านให้เป็นไปตามมาตรฐานฯ ที่กำหนด

(2) พนักงาน ต้องถือว่ารหัสผ่านเป็นความลับ โดยต้องเก็บรักษาและตั้งรหัสผ่านอย่างปลอดภัย ตามมาตรฐานฯ ที่กำหนด

(3) ผู้ดูแลระบบ ต้องระบุข้อกำหนดสำหรับการควบคุมรหัสผ่านสำหรับการติดตั้งและใช้งานระบบ รวมทั้งการกำหนดค่าพารามิเตอร์ในระบบเพื่อควบคุมระบบสารสนเทศ ให้เป็นไปตามมาตรฐานฯ ที่กำหนด

(4) ผู้ดูแลบัญชีรหัสผู้ใช้งานระบบ ต้องแจกจ่ายรหัสผ่านให้แก่ผู้ใช้งานระบบสารสนเทศอย่างปลอดภัย เพื่อป้องกันการรั่วไหลของรหัสผ่านระหว่างการแจกจ่าย และกำหนดให้ผู้ใช้งานลงนามรับทราบข้อปฏิบัติในการใช้และเก็บรักษารหัสผ่าน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(5) ผู้ใช้งานต้องปฏิบัติตามระเบียบปฏิบัติในการใช้ข้อมูลความลับสำหรับการพิสูจน์ตัวตน

(6) แนวปฏิบัติสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

- รักษารหัสผ่านไว้เป็นความลับเฉพาะบุคคล ไม่เปิดเผยให้ผู้อื่นรับทราบ รวมถึงผู้ดูแลระบบ
- ไม่พิมพ์รหัสผ่านในลักษณะเปิดเผย เช่น พิมพ์รหัสผ่านต่อหน้าผู้ปฏิบัติงานคนอื่น
- ไม่บันทึกรหัสผ่านไว้ในโปรแกรมประยุกต์หรือแอปพลิเคชัน เพื่อช่วยในการจำรหัสผ่านของตน
- ไม่เก็บรหัสผ่านในที่ที่เปิดเผย เช่น บันทึกรหัสผ่านบนกระดาษหรือในไฟล์ที่อ่านได้โดยง่าย
- ไม่ใช้บัญชีชื่อผู้ใช้งานและรหัสผ่านของผู้อื่น แม้ว่าบัญชีชื่อผู้ใช้งานจะได้รับการอนุญาตจากเจ้าของชื่อผู้ใช้งานบุคคลนั้นก็ตาม
- เปลี่ยนแปลงรหัสผ่านอย่างเป็นประจำหรือเมื่อมีเหตุการณ์ที่มีนัยสำคัญสมควรจะต้องเปลี่ยนแปลงรหัสผ่าน เช่น เมื่อสงสัยว่ารหัสผ่านล่วงรู้โดยบุคคลอื่น เมื่อมีการแจ้งเตือนจากระบบหรือผู้ดูแลระบบ
- กำหนดรหัสผ่านที่ใช้สำหรับระบบสารสนเทศภายใน สคทช. ให้มีความแตกต่างกับระบบสารสนเทศอื่นๆ ที่ให้บริการโดยหน่วยงานภายนอก สคทช.
- ไม่กำหนดรหัสผ่านที่สามารถคาดเดาได้ง่าย ได้แก่
- ข้อมูลส่วนตัว เช่น ชื่อ วันเดือนปีเกิด เลขบัตรประชาชน ชื่อเล่น
- ตัวเลขหรือตัวอักษรเรียงต่อเนื่องกัน หรือเป็นตัวเลขหรือตัวอักษรทั้งหมด เช่น 12345678 password qwerty 111111
- ในกรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เพื่อให้สามารถปฏิบัติงานแทนตนเองได้ หลังจากที่ทำงานนั้นเสร็จแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
- ในกรณีที่มีการใช้งานบัญชีผู้ใช้งานร่วมกัน ต้องมีความตระหนักว่าหากมีความเสียหายเกิดขึ้น ผู้ใช้งานร่วมกันนั้นจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(7) กำหนดคุณสมบัติของรหัสผ่านอย่างน้อย ดังนี้

- รหัสผ่านต้องมีความยาวอย่างน้อย 8 หลัก
- รหัสผ่านต้องประกอบด้วย ตัวอักษร ตัวเลข และอักขระพิเศษ หรือสัญลักษณ์ เช่น (a-Z) (0-9) (@ , # , & , “ , ‘ , *, =, < , > , % , $, + , ?)
- รหัสผ่านต้องไม่ตรงกับชื่อผู้ใช้งานระบบ (User Logon) และชื่อผู้ใช้งานจริง (User Name)

(8) สำหรับระบบที่มีการสร้างรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ต้องบังคับให้มีการเปลี่ยนแปลงรหัสผ่านชั่วคราว (Temporary Password) ในครั้งแรกของการเข้าสู่ระบบ

(9) มีฟังก์ชันการทำงานให้ผู้ใช้งานสามารถเปลี่ยนแปลงรหัสผ่านของตนเอง พร้อมทั้งมีขั้นตอนในการยืนยันรหัสผ่านเดิม และการตั้งรหัสผ่านใหม่

(10) กำหนดให้มีการเปลี่ยนแปลงรหัสผ่านในการเข้าถึงระบบทุก 90 วัน สำหรับระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด”

(11) กำหนดให้มีการระงับการใช้งานชั่วคราวตามความเหมาะสมของหมวดหมู่ทรัพย์สินสารสนเทศสำหรับบัญชีผู้ใช้ที่ใส่รหัสผ่านผิดเกิน 5 ครั้ง

(12) ไม่แสดงรหัสผ่านที่ผู้ใช้งานพิมพ์ในขณะเข้าสู่ระบบ โดยอาจมีการแสดงสัญลักษณ์แทนรหัสผ่านจริงในขณะที่ผู้ใช้งานพิมพ์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.18 การควบคุมสิทธิ์และการเข้าถึงระบบสารสนเทศ (Access rights)

(1) จำกัดการเข้าถึงสารสนเทศและฟังก์ชันของระบบหรือโปรแกรมประยุกต์ให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

(2) ควบคุมการเข้าถึงระบบงานและโปรแกรมประยุกต์ต่าง ๆ ผ่านขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบอย่างมั่นคงปลอดภัยตามที่กำหนดไว้ในนโยบายควบคุมการเข้าถึง

(3) ต้องสรุปรายชื่อพนักงานที่มีการเปลี่ยนแปลงสถานะ/ตำแหน่ง หรือหน้าที่งาน ที่มีผลต่อสิทธิ์การใช้งานระบบสารสนเทศ และส่งให้หน่วยงานที่เกี่ยวข้อง ทำการปรับปรุงสิทธิ์ให้เป็นปัจจุบัน ทันทีที่มีการเปลี่ยนแปลง

(4) ผู้ดูแลระบบ ต้องจัดให้มีการทบทวนสิทธิ์การใช้งานบนระบบสารสนเทศตามมาตรฐานฯ ที่กำหนดโดยทบทวนสิทธิ์ตามรอบระยะเวลา และเมื่อมีการเปลี่ยนแปลงที่สำคัญ รวมทั้งปรับปรุงสิทธิ์ให้เป็นปัจจุบันเพื่อให้มั่นใจว่าไม่มีการกำหนดสิทธิ์เกินกว่าความจำเป็น

(5) หน่วยงานทรัพยากรบุคคล ต้องดำเนินการแจ้งหน่วยงานที่ดูแลระบบทำการถอดถอนหรือเปลี่ยนแปลงสิทธิ์ของพนักงาน พนักงานชั่วคราว และคู่สัญญา (บุคคล) เมื่อสิ้นสุดการจ้างงาน หรือปรับเปลี่ยน/เปลี่ยนแปลงหน้าที่ความรับผิดชอบ

(6) ระบบสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ต้องควบคุมให้มีการพิสูจน์และยืนยันตัวตนโดยการใช้วิธีการพิสูจน์และยืนยันตัวตนแบบ 2 Factors

(7) แจ้งฝ่ายงานที่เกี่ยวข้องเมื่อตรวจพบการละเมิดมาตรการควบคุมการเข้าสู่ระบบ หรือสงสัยว่าอาจเป็นเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

2.2.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

(1) องค์กรต้องปฏิบัติตาม คู่มือปฏิบัติตามระดับมาตรการควบคุมการจัดซื้อจัดจ้างสำหรับผู้ส่งมอบ

(2) องค์กรต้องกำหนดเกณฑ์การคัดเลือกผู้ให้บริการภายนอก ที่คำนึงถึงความสามารถด้านความมั่นคงปลอดภัยสารสนเทศ

(3) องค์กรต้องประเมินความเสี่ยงที่เกิดจากการเข้าถึงข้อมูลและการเข้าถึงระบบสารสนเทศของหน่วยงานภายนอก ซึ่งรวมถึงระบบสาธารณูปโภค ระบบเครือข่าย และอาคารสถานที่ โดยต้องคำนึงถึงปัจจัยต่าง ๆ ตามมาตรฐานฯ เพื่อให้มีการควบคุมที่เหมาะสมรัดกุม

(4) องค์กรต้องมีข้อตกลงที่เป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอก ซึ่งระบุถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการภายนอกต้องปฏิบัติตาม เช่น การควบคุมการเข้าถึง การปกป้องข้อมูล การตอบสนองต่อเหตุการณ์ และการรายงานเหตุการณ์

2.2.20 การระบุถึงความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงกับผู้ให้บริการภายนอก (Addressing Information security within supplier agreements)

(1) องค์กรต้องระบุข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการภายนอก เช่น ข้อกำหนดเกี่ยวกับการควบคุมการเข้าถึง การปกป้องข้อมูล การตอบสนองต่อเหตุการณ์ และการรายงานเหตุการณ์

(2) องค์กรต้องรวมข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่ระบุไว้ในข้อ 1 เข้าไปในข้อตกลงกับผู้ให้บริการภายนอกอย่างชัดเจน

(3) องค์กรต้องมีกลไกในการตรวจสอบและบังคับใช้ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศที่ระบุไว้ในข้อตกลงกับผู้ให้บริการภายนอก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.21 การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (Managing information security in the ICT supply chain)

(1) องค์กรต้องจัดทำข้อตกลงที่เป็นลายลักษณ์อักษรกับผู้ให้บริการภายนอก ที่มีการเข้าถึง ประมวลผล สื่อสารข้อมูล บริหารจัดการข้อมูลและระบบสารสนเทศ ซึ่งระบุเกี่ยวกับความรับผิดชอบของผู้ให้บริการภายนอกอย่างเต็มจำนวน ในทุกกรณี เมื่อผู้ให้บริการภายนอกทำการจ้างช่วงงานต่อไปยังผู้ให้บริการรายอื่น ๆ (Supply chain)

2.2.22 การติดตาม ทบทวน และการจัดการ การเปลี่ยนแปลงสำหรับบริการของผู้ให้บริการภายนอก (Monitoring, Review and change management of supplier services)

(1) องค์กรต้องติดตามประสิทธิภาพและความมั่นคงปลอดภัยของบริการที่ได้รับจากผู้ให้บริการภายนอกอย่างสม่ำเสมอ ซึ่งอาจรวมถึงการตรวจสอบบันทึก การทบทวนรายงาน และการประเมินผลการปฏิบัติงานของผู้ให้บริการภายนอก

(2) องค์กรต้องทบทวนบริการที่ได้รับจากผู้ให้บริการภายนอกเป็นประจำ เพื่อให้แน่ใจว่ายังคงสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร และเพื่อระบุโอกาสในการปรับปรุง

(3) องค์กรต้องมีกระบวนการที่ชัดเจนในการจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก ซึ่งรวมถึงการประเมินผลกระทบ การอนุมัติ และการสื่อสาร

(4) จัดให้มีการประชุมทบทวน กับผู้ให้บริการภายนอกเป็นประจำ เพื่อหารือเกี่ยวกับประสิทธิภาพของบริการและปัญหาที่อาจเกิดขึ้น

(5) กำหนดกระบวนการจัดการ การเปลี่ยนแปลง ที่ชัดเจนและมีประสิทธิภาพ

(6) สื่อสารการเปลี่ยนแปลง ที่เกี่ยวข้องกับบริการของผู้ให้บริการภายนอกให้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทราบ

2.2.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)

(1) การประเมินความเสี่ยง: องค์กรต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้องกับการใช้บริการคลาวด์ โดยพิจารณาจากปัจจัยต่างๆ เช่น ประเภทของข้อมูลที่จัดเก็บหรือประมวลผลในคลาวด์ ความสำคัญของข้อมูล และความสามารถของผู้ให้บริการคลาวด์ในการรักษาความมั่นคงปลอดภัย

(2) ข้อตกลงกับผู้ให้บริการคลาวด์: องค์กรต้องมีข้อตกลงที่ชัดเจนและครอบคลุมกับผู้ให้บริการคลาวด์ ซึ่งระบุถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ เช่น การควบคุมการเข้าถึง การปกป้องข้อมูล การสำรองข้อมูล การกู้คืนระบบ และการรายงานเหตุการณ์

(3) การตรวจสอบและการทบทวน: องค์กรต้องตรวจสอบและทบทวนการปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการคลาวด์อย่างสม่ำเสมอ เช่น

- ทำการประเมินความเสี่ยง ก่อนตัดสินใจใช้บริการคลาวด์ โดยพิจารณาถึงความเสี่ยงที่อาจเกิดขึ้นกับข้อมูลและระบบสารสนเทศขององค์กร
- เลือกผู้ให้บริการคลาวด์ ที่มีมาตรฐานความมั่นคงปลอดภัยสูง และมีการรับรองมาตรฐานที่เกี่ยวข้อง เช่น ISO 27001, ISO 27017, หรือ ISO 27018
- ทำข้อตกลงการให้บริการ (SLA) ที่ครอบคลุมและชัดเจนกับผู้ให้บริการคลาวด์ โดยระบุถึงข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอย่างละเอียด

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ตรวจสอบการปฏิบัติตามข้อตกลง ของผู้ให้บริการคลาวด์เป็นประจำ เช่น การตรวจสอบบันทึกกิจกรรม การทดสอบระบบ และการตรวจสอบความมั่นคงปลอดภัย
- จัดให้มีการฝึกอบรม ให้กับพนักงานเกี่ยวกับการใช้งานบริการคลาวด์อย่างมั่นคปลอดภัย

2.2.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)

(1) องค์กรต้องกำหนดกระบวนการจัดการเหตุการณ์ที่ครอบคลุมขั้นตอนการรายงาน การประเมิน การตอบสนอง การสื่อสาร และการเรียนรู้จากเหตุการณ์

(2) องค์กรต้องจัดทำแผนการตอบสนองต่อเหตุการณ์ที่กำหนดบทบาทและความรับผิดชอบของทีมรับมือเหตุการณ์ ขั้นตอนการดำเนินการ และทรัพยากรที่จำเป็น

(3) องค์กรต้องจัดให้มีการฝึกอบรมและการทดสอบแผนการตอบสนองต่อเหตุการณ์เป็นประจำ เพื่อให้แน่ใจว่าทีมรับมือเหตุการณ์มีความพร้อมและสามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ

(4) องค์กรต้องทบทวนและปรับปรุงกระบวนการจัดการเหตุการณ์และแผนการตอบสนองต่อเหตุการณ์อย่างสม่ำเสมอ เพื่อให้สอดคล้องกับภัยคุกคามและความเสี่ยงที่เปลี่ยนแปลงไป

2.2.25 การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)

(1) เหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้นนั้นต้องมีการจัดเก็บเป็นหลักฐานการดำเนินการที่เกี่ยวข้องกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

(2) องค์กรต้องมีกลไกในการตรวจจับและรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจเกิดขึ้น ซึ่งรวมถึงการกำหนดเกณฑ์ในการระบุเหตุการณ์ ช่องทางการรายงาน และผู้รับผิดชอบในการตรวจสอบและประเมินเหตุการณ์

(3) องค์กรต้องประเมินเหตุการณ์ที่ได้รับรายงาน เพื่อพิจารณาว่าเป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศหรือไม่ และประเมินความรุนแรงและผลกระทบที่อาจเกิดขึ้น

(4) องค์กรต้องตัดสินใจว่าจะดำเนินการอย่างไรกับเหตุการณ์ที่ได้รับการยืนยันว่าเป็นเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ โดยพิจารณาจากความรุนแรง ผลกระทบ และทรัพยากรที่มีอยู่ เช่น

- กำหนดเกณฑ์ในการระบุเหตุการณ์ เช่น การตรวจพบการเข้าถึงระบบโดยไม่ได้รับอนุญาต การสูญหายของข้อมูล หรือการหยุดชะงักของบริการ
- จัดให้มีช่องทางการรายงานเหตุการณ์ ที่สะดวกและเข้าถึงง่าย เช่น สายด่วน หรือระบบแจ้งเตือนออนไลน์
- แต่งตั้งผู้รับผิดชอบ ในการตรวจสอบและประเมินเหตุการณ์
- จัดทำขั้นตอนการประเมินเหตุการณ์ ที่ชัดเจนและครอบคลุม
- กำหนดเกณฑ์ความรุนแรงของเหตุการณ์ และแผนการตอบสนองต่อเหตุการณ์แต่ละระดับ
- ทบทวนและปรับปรุง กระบวนการประเมินและตัดสินใจเกี่ยวกับเหตุการณ์เป็นประจำ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

(1) องค์กรต้องจัดทำแผนการตอบสนองต่อเหตุการณ์ที่กำหนดบทบาทและความรับผิดชอบของทีมรับมือเหตุการณ์ ขั้นตอนการดำเนินการ และทรัพยากรที่จำเป็น

(2) องค์กรต้องมีช่องทางการสื่อสารที่ชัดเจนและมีประสิทธิภาพในการรายงานและแจ้งเตือนเกี่ยวกับเหตุการณ์

(3) องค์กรต้องดำเนินการเพื่อบรรเทาผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ เช่น การหยุดการแพร่กระจายของมัลแวร์ การปิดกั้นการเข้าถึงระบบที่ได้รับผลกระทบ หรือการกู้คืนข้อมูลจากแหล่งสำรอง

(4) องค์กรต้องหาสาเหตุของเหตุการณ์ เพื่อระบุจุดอ่อนและดำเนินการแก้ไข

(5) องค์กรต้องเรียนรู้จากเหตุการณ์ที่เกิดขึ้น และนำบทเรียนที่ได้ไปปรับปรุงกระบวนการจัดการเหตุการณ์และมาตรการควบคุมความมั่นคงปลอดภัยสารสนเทศตัวอย่างเช่น

- จัดตั้งทีมรับมือเหตุการณ์ (CSIRT หรือ CIRT) ที่มีความรู้ความสามารถและประสบการณ์ในการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- จัดทำแผนการตอบสนองต่อเหตุการณ์ ที่ครอบคลุมทุกประเภทของเหตุการณ์ที่อาจเกิดขึ้น และกำหนดขั้นตอนการดำเนินการที่ชัดเจน
- จัดให้มีการฝึกอบรมและการทดสอบ แผนการตอบสนองต่อเหตุการณ์เป็นประจำ เช่น การฝึกซ้อมจำลองสถานการณ์ (Tabletop Exercise) หรือ การฝึกซ้อมเต็มรูปแบบ (Full-Scale Exercise)
- ใช้เครื่องมือและเทคโนโลยี ที่เหมาะสมในการตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุการณ์
- รายงานเหตุการณ์ที่สำคัญ ไปยังผู้บริหารระดับสูงและหน่วยงานที่เกี่ยวข้องตามข้อกำหนด

2.2.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)

(1) องค์กรต้องวิเคราะห์สาเหตุที่แท้จริงของเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดขึ้น โดยพิจารณาถึงปัจจัยทางเทคนิค กระบวนการ และบุคคลที่เกี่ยวข้อง

(2) องค์กรต้องระบุบทเรียนที่ได้รับจากเหตุการณ์ และนำบทเรียนเหล่านั้นไปปรับปรุง ISMS และมาตรการควบคุมต่าง ๆ

(3) องค์กรต้องดำเนินการแก้ไขเพื่อสาเหตุที่แท้จริงของเหตุการณ์ และป้องกันไม่ให้เหตุการณ์เกิดขึ้นซ้ำ

(4) องค์กรต้องสื่อสารบทเรียนที่ได้รับและการดำเนินการแก้ไขไปยังผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้อง ตัวอย่างเช่น

- จัดทำรายงานการวิเคราะห์สาเหตุของเหตุการณ์: รายงานนี้ควรระบุถึงลำดับเหตุการณ์ สาเหตุที่แท้จริง ผลกระทบ และข้อเสนอแนะในการปรับปรุง
- จัดประชุมเพื่อสรุปบทเรียนที่ได้รับ: เชิญผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องเข้าร่วมประชุมเพื่อหารือเกี่ยวกับบทเรียนที่ได้รับและวิธีการนำไปปรับใช้
- ปรับปรุงนโยบาย ขั้นตอน และมาตรการควบคุม: นำบทเรียนที่ได้รับไปปรับปรุงเอกสารและกระบวนการที่เกี่ยวข้อง เพื่อป้องกันไม่ให้เหตุการณ์เกิดขึ้นซ้ำ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- จัดให้มีการฝึกอบรมและการสร้างความตระหนัก: ให้ความรู้แก่พนักงานเกี่ยวกับเหตุการณ์ที่เกิดขึ้น บทเรียนที่ได้รับ และวิธีการป้องกัน
- ติดตามและประเมินผลการดำเนินการแก้ไข: ตรวจสอบให้แน่ใจว่าการดำเนินการแก้ไขมีประสิทธิภาพและสามารถป้องกันเหตุการณ์ในอนาคตได้

2.2.28 การรวบรวมหลักฐาน (Collection of evidence)

(1) กระบวนการรวบรวมหลักฐาน: องค์กรต้องมีกระบวนการที่ชัดเจนในการรวบรวมหลักฐาน ซึ่งรวมถึงการระบุประเภทของหลักฐานที่ต้องรวบรวม วิธีการรวบรวม และผู้รับผิดชอบในการรวบรวม

(2) การจัดเก็บหลักฐาน: องค์กรต้องจัดเก็บหลักฐานอย่างมั่นคงปลอดภัย เพื่อให้แน่ใจว่าหลักฐานมีความสมบูรณ์ ถูกต้อง และเชื่อถือได้

(3) การเข้าถึงหลักฐาน: องค์กรต้องควบคุมการเข้าถึงหลักฐาน โดยจำกัดเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(4) การทำลายหลักฐาน: องค์กรต้องมีนโยบายและขั้นตอนในการทำลายหลักฐานที่ไม่จำเป็นต้องเก็บรักษาไว้อีกต่อไป ตัวอย่างเช่น

- กำหนดประเภทของหลักฐาน ที่ต้องรวบรวม เช่น บันทึกการเข้าถึงระบบ ภาพจากกล้องวงจรปิด อีเมล และไฟล์ข้อมูล
- ใช้เครื่องมือและเทคนิค ที่เหมาะสมในการรวบรวมหลักฐาน เช่น ซอฟต์แวร์ฟอร์เรนสิก หรือการทำสำเนาข้อมูล
- จัดเก็บหลักฐานในรูปแบบที่ปลอดภัย เช่น การเข้ารหัส หรือการใช้ระบบจัดเก็บข้อมูลที่ปลอดภัย
- จำกัดการเข้าถึงหลักฐาน เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น เช่น เจ้าหน้าที่ผู้รับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ หรือเจ้าหน้าที่ผู้มีอำนาจสืบสวน
- ทำลายหลักฐานที่ไม่จำเป็น ตามนโยบายและขั้นตอนที่กำหนด

2.2.29 ความมั่นคงปลอดภัยสารสนเทศในช่วงภาวะหยุดชะงัก (Information security during disruption)

(1) องค์กรต้องมีแผน BCP ที่ครอบคลุมการจัดการความเสี่ยง การระบุทรัพยากรที่สำคัญ และขั้นตอนการกู้คืนระบบและบริการในกรณีที่เกิดภาวะหยุดชะงัก

(2) องค์กรต้องสำรองข้อมูลและระบบสารสนเทศที่สำคัญอย่างสม่ำเสมอ และเก็บรักษาข้อมูลสำรองไว้ในสถานที่ที่ปลอดภัยและสามารถเข้าถึงได้ง่าย

(3) องค์กรต้องมีขั้นตอนการกู้คืนระบบและบริการสารสนเทศที่ชัดเจนและมีประสิทธิภาพ เพื่อให้สามารถกลับมาดำเนินงานได้อย่างรวดเร็วหลังจากเกิดภาวะหยุดชะงัก

(4) องค์กรต้องมีแผนการสื่อสารในภาวะวิกฤต เพื่อให้แน่ใจว่าสามารถสื่อสารกับพนักงาน ลูกค้า คู่ค้า และผู้มีส่วนได้ส่วนเสียอื่น ๆ ได้อย่างมีประสิทธิภาพในช่วงภาวะหยุดชะงัก

2.2.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)

(1) องค์กรต้องทำการวิเคราะห์ BIA เพื่อระบุและประเมินผลกระทบที่อาจเกิดขึ้นจากการหยุดชะงักของระบบและบริการ ICT ต่อการดำเนินธุรกิจ

(2) องค์กรต้องจัดทำ BCP ที่ครอบคลุมถึงการระบุทรัพยากรที่สำคัญ การกำหนดกลยุทธ์การกู้คืน และขั้นตอนการดำเนินการในกรณีที่เกิดภาวะหยุดชะงัก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(3) องค์กรต้องทดสอบ BCP เป็นประจำ เพื่อให้แน่ใจว่าแผนมีความทันสมัยและสามารถนำไปใช้ได้จริง นอกจากนี้ องค์กรต้องจัดให้มีการฝึกอบรมพนักงานเกี่ยวกับ BCP เพื่อให้พนักงานมีความรู้ความเข้าใจและสามารถปฏิบัติตามแผนได้อย่างมีประสิทธิภาพ

(4) ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

- เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ: Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด
- ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ 1 ครั้งเพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- จัดให้มีการรายงานผลการดำเนินการทดสอบแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

2.2.31 ความมั่นคงปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด (Legal, Statutory, Regulatory and Contractual requirements)

(1) องค์กรต้องรวบรวมข้อกำหนดทางกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้องให้เป็นปัจจุบัน และต้องสร้างความตระหนักรู้ ให้ทุกหน่วยงานรับทราบกฎระเบียบที่เกี่ยวข้องกับงานของตนเอง

(2) บุคลากรมีหน้าที่ต้องทำความเข้าใจ และปฏิบัติตามนโยบาย กฎระเบียบ ข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศที่กำหนดขึ้นอย่างเคร่งครัด ทั้งนี้ รวมถึงแต่ไม่จำกัดเฉพาะ

- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ 2550
- พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 (ฉบับที่ 2)
- พ.ร.บ. ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ 2544
- พ.ร.บ. ลิขสิทธิ์ พ.ศ 2537
- พ.ร.บ. ลิขสิทธิ์ (ฉบับที่ 2) พ.ศ. 2558
- พ.ร.บ. ลิขสิทธิ์ (ฉบับที่ 3) พ.ศ. 2558
- พ.ร.บ. ลิขสิทธิ์ (ฉบับที่ 4) พ.ศ. 2561
- พ.ร.บ. ลิขสิทธิ์ (ฉบับที่ 5) พ.ศ. 2565
- พ.ร.บ. เครื่องหมายการค้า พ.ศ 2534
- พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ 2562
- ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวทางการใช้บริการคลาวด์ พ.ศ. 2562

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- Cloud Computing Practice, สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ พฤศจิกายน 2562

(3) ต้องกำหนดให้มีการป้องกันข้อมูล ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและแนวปฏิบัติข้อกำหนดที่ปรากฏในสัญญา และข้อกำหนดทางธุรกิจ รวมถึงต้องมีมาตรการป้องกันข้อมูลส่วนตัวตามที่ระบุไว้ในกฎหมาย แนวปฏิบัติและสัญญาที่เกี่ยวข้อง

(4) ต้องกำหนดให้มีการป้องกัน สารสนเทศ ระบบสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่ายและคอมพิวเตอร์แม่ข่าย ไม่ให้ใช้งานไปในทางที่ผิดหรือโดยไม่มีสิทธิ์ และต้องกำหนดให้ใช้มาตรการเข้ารหัสข้อมูลโดยให้ยึดถือตามหรือสอดคล้องกับข้อตกลงทางกฎหมาย

(5) ทบทวนและพิจารณาข้อกำหนดต่าง ๆ ที่มีผลทางกฎหมายซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ สคทช. เช่น พระราชบัญญัติ ข้อกำหนดทางกฎหมาย ข้อกำหนดในสัญญา และข้อกำหนดทางด้านความมั่นคงปลอดภัยอื่น ๆ

2.2.32 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)

(1) มาตรการ/ แนวปฏิบัติ

- ไม่ทำซ้ำหรือดัดแปลงซอฟต์แวร์ที่ สคทช. เป็นเจ้าของ ไปยังสื่อบันทึกข้อมูล
- ไม่โอนย้ายซอฟต์แวร์ที่ สคทช. เป็นเจ้าของ ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น
- ไม่เปิดเผยซอร์สโค้ด (Source Code) ของระบบสารสนเทศที่ สคทช. เป็นเจ้าของโดยไม่ได้รับอนุญาต
- ไม่ดำเนินการหรือมีส่วนร่วมในการทำซ้ำ ดัดแปลง เผยแพร่ โอนย้าย หรือแลกเปลี่ยนเอกสารสารสนเทศ ซอฟต์แวร์ หรือเครื่องมือใด ๆ อันเป็นการละเมิดลิขสิทธิ์และทรัพย์สินทางปัญญาสารสนเทศหรือระบบสารสนเทศที่สร้างหรือพัฒนาโดยผู้ปฏิบัติงานในระหว่างการว่าจ้าง ถือเป็นทรัพย์สินและลิขสิทธิ์ของ สคทช.

(2) หมายเหตุ

- เมื่อซื้อซอฟต์แวร์ถูกต้องตามกฎหมาย หากทำซ้ำ เพื่อป้องกันการสูญหายหรือเสียหาย (Backup) ไม่ถือว่า เป็นการละเมิดลิขสิทธิ์

2.2.33 การป้องกันบันทึก (Protection of records)

(1) ข้อมูลบันทึกเหตุการณ์ที่สำคัญขององค์กร ที่เกี่ยวข้องกับข้อกำหนดทางกฎหมายและข้อกำหนดทางธุรกิจ ต้องมีการจัดการ จัดเก็บ และการทำลายข้อมูล รวมถึงการป้องกันข้อมูลสารสนเทศจากการสูญหาย ถูกทำลาย การปลอมแปลง และนำไปใช้ผิดวัตถุประสงค์

(2) ควบคุมดูแลให้เอกสารระบบถูกจัดเก็บในที่ปลอดภัยตามความเหมาะสม

2.2.34 การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล (Privacy and protection of PII)

(1) ข้อมูลส่วนบุคคลทั้งในรูปแบบเอกสารและข้อมูลอิเล็กทรอนิกส์ ถือเป็นความลับ การเปิดเผยต้องได้รับอนุญาตจากเจ้าของข้อมูลเท่านั้น

(2) ในกรณีที่ได้รับการร้องขอข้อมูลส่วนบุคคลเพื่อปฏิบัติตามกฎหมาย ต้องดำเนินการแจ้งเจ้าของข้อมูลส่วนบุคคลเพื่อทราบ เว้นแต่การร้องขอตามกฎหมายนั้นมีข้อกำหนดในการห้ามแจ้งเจ้าของข้อมูลส่วนบุคคล

(3) ให้มีมาตรการรักษาความมั่นคงปลอดภัยที่เหมาะสม เพื่อป้องกันการสูญหาย เข้าถึง ใช้ เปลี่ยนแปลง แก้ไข หรือเปิดเผยข้อมูลส่วนบุคคลโดยปราศจากอำนาจหรือโดยมิชอบ โดยมาตรการรักษาความมั่นคงปลอดภัยดังกล่าว อย่างน้อยต้องมีการดำเนินการ ดังต่อไปนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตามกฎหมายว่าด้วยการคุ้มครองข้อมูลส่วนบุคคล ไม่ว่าข้อมูลส่วนบุคคลดังกล่าวจะอยู่ในรูปแบบเอกสารหรือในรูปแบบอิเล็กทรอนิกส์ หรือรูปแบบอื่นใดก็ตาม
- มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล
- มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็น เหมาะสม และเป็นไปได้ตามระดับความเสี่ยง
- สำหรับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องครอบคลุมส่วนประกอบต่าง ๆ ของระบบสารสนเทศที่เกี่ยวข้องกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล เช่น ระบบและอุปกรณ์จัดเก็บข้อมูลส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (servers) เครื่องคอมพิวเตอร์ลูกข่าย (clients) และอุปกรณ์ต่าง ๆ ที่ใช้ ระบบเครือข่าย ซอฟต์แวร์ และแอปพลิเคชัน อย่างเหมาะสมตามระดับความเสี่ยง โดยคำนึงถึงหลักการป้องกันเชิงลึก (defense in depth) ที่ควรประกอบด้วยมาตรการป้องกันหลายชั้น (multiple layers of security controls) เพื่อลดความเสี่ยงในกรณีที่มาตรการบางมาตรการมีข้อจำกัดในการป้องกันความมั่นคงปลอดภัยในบางสถานการณ์

2.2.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Independent review of information security)

(1) องค์กรต้องมีการทบทวนต้องดำเนินการโดยบุคคลหรือหน่วยงานที่เป็นอิสระจาก ISMS ที่ได้รับการทบทวน เพื่อให้มั่นใจว่าการทบทวนมีความเป็นกลางและปราศจากอคติ

(2) องค์กรต้องมีขอบเขตของการทบทวนต้องครอบคลุมองค์ประกอบทั้งหมดของ ISMS รวมถึงนโยบาย ขั้นตอน มาตรการควบคุม และการดำเนินงาน

(3) องค์กรต้องมีการทบทวนซึ่งสามารถดำเนินการได้หลายวิธี เช่น การสัมภาษณ์ การตรวจสอบเอกสาร การสังเกตการณ์ และการทดสอบ

(4) องค์กรต้องมีผลการทบทวนต้องถูกรายงานต่อฝ่ายบริหาร โดยระบุถึงจุดแข็ง จุดอ่อน และข้อเสนอแนะในการปรับปรุง ISMS ตัวอย่างเช่น

- องค์กรสามารถว่าจ้างผู้ตรวจสอบภายนอกที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยสารสนเทศมาทำการทบทวน ISMS

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- องค์กรสามารถจัดตั้งทีมตรวจสอบภายในที่ประกอบด้วยบุคคลจากหน่วยงานต่าง ๆ ที่ไม่เกี่ยวข้องกับ ISMS โดยตรง
- องค์กรสามารถใช้แนวทางการตรวจสอบที่เป็นที่ยอมรับ เช่น ISO 27001 เป็นต้น
- รายงานการทบทวนควรมีรายละเอียดที่ชัดเจนและครอบคลุม เพื่อให้ฝ่ายบริหารสามารถเข้าใจและนำไปใช้ในการปรับปรุง ISMS ได้

2.2.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานสำหรับความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)

(1) องค์กรต้องมีกระบวนการในการตรวจสอบการปฏิบัติตามนโยบาย กฎ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอาจรวมถึงการตรวจสอบบันทึก การสัมภาษณ์ การสังเกตการณ์ และการทดสอบ

(2) องค์กรต้องประเมินผลการปฏิบัติตามข้อกำหนดเป็นประจำ เพื่อระบุจุดอ่อนและช่องโหว่ที่อาจเกิดขึ้น

(3) องค์กรต้องดำเนินการแก้ไขปัญหาการไม่ปฏิบัติตามข้อกำหนดที่พบในการตรวจสอบและประเมินผล

(4) องค์กรต้องรายงานผลการตรวจสอบ การประเมินผล และการดำเนินการแก้ไขต่อฝ่ายบริหาร ตัวอย่างเช่น:

- กำหนดตัวชี้วัดการปฏิบัติตาม (Compliance Metrics): กำหนดตัวชี้วัดที่สามารถวัดได้เพื่อประเมินระดับการปฏิบัติตามนโยบาย กฎ และมาตรฐาน เช่น เปอร์เซ็นต์ของบุคลากรที่ผ่านการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ หรือจำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยที่รายงาน
- ใช้เครื่องมือตรวจสอบ: ใช้ซอฟต์แวร์หรือระบบอื่น ๆ เพื่อช่วยในการตรวจสอบการปฏิบัติตาม เช่น ซอฟต์แวร์ตรวจสอบการเข้าถึงระบบ หรือซอฟต์แวร์ป้องกันไวรัส
- จัดให้มีการฝึกอบรม: จัดให้มีการฝึกอบรมบุคลากรเกี่ยวกับนโยบาย กฎ และมาตรฐานด้านความมั่นคงปลอดภัยสารสนเทศอย่างสม่ำเสมอ
- สื่อสารและสร้างความตระหนัก: สื่อสารความสำคัญของการปฏิบัติตามข้อกำหนดให้กับบุคลากรและผู้ใช้งานอื่น ๆ ทราบ
- ทบทวนและปรับปรุง: ทบทวนและปรับปรุงนโยบาย กฎ และมาตรฐานให้ทันสมัยอยู่เสมอ

2.2.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)

(1) จัดทำขั้นตอนปฏิบัติสำหรับการดำเนินงานไว้เป็นลายลักษณ์อักษร และพร้อมให้ผู้ใช้งานทุกคนที่ต้องการนำไปใช้งานได้

(2) องค์กรต้องระบุขั้นตอนปฏิบัติงานที่สำคัญทั้งหมดที่เกี่ยวข้องกับการดำเนินงานของระบบสารสนเทศและการสื่อสาร ซึ่งอาจรวมถึงขั้นตอนการเปิดและปิดระบบ การสำรองข้อมูล การบำรุงรักษาอุปกรณ์ การจัดการสื่อบันทึกข้อมูล การจัดการห้องคอมพิวเตอร์ การจัดการจดหมาย และความมั่นคงปลอดภัย

(3) องค์กรต้องจัดทำเอกสารสำหรับขั้นตอนปฏิบัติงานที่ระบุไว้ในข้อ 1 โดยเอกสารควรมีความชัดเจน ครบถ้วน เข้าใจง่าย และสามารถเข้าถึงได้ง่ายสำหรับผู้ที่เกี่ยวข้อง

(4) องค์กรต้องทบทวนและปรับปรุงขั้นตอนปฏิบัติงานและเอกสารที่เกี่ยวข้องเป็นประจำ เพื่อให้มั่นใจว่ายังคงมีความทันสมัยและสอดคล้องกับการเปลี่ยนแปลงของระบบและเทคโนโลยี

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.3 มาตรการที่ 2 มาตรการควบคุมด้านบุคลากร (People controls)

บุคลากรถือเป็นปัจจัยที่สำคัญที่สุดในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ การมีบุคลากรที่มีความรู้และความเข้าใจในการจัดการข้อมูลและระบบไซเบอร์อย่างถูกต้องเป็นสิ่งจำเป็นต่อการป้องกันและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ มาตรการด้านบุคลากรครอบคลุมถึงกระบวนการตรวจสอบคัดเลือก และแต่งตั้งบุคลากรที่มีความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศขององค์กร เช่น การคัดกรองบุคลากรใหม่ที่มีทักษะและความรู้ด้านไซเบอร์เพื่อให้แน่ใจว่าบุคคลเหล่านี้มีคุณสมบัติเหมาะสมในการทำงานในตำแหน่งที่เกี่ยวข้อง นอกจากนี้ มาตรการนี้ยังเน้นการจัดฝึกอบรมบุคลากรอย่างต่อเนื่อง เพื่อให้ทุกคนตระหนักถึงความเสี่ยงและภัยคุกคามที่อาจเกิดขึ้นในระบบไซเบอร์ รวมถึงการรายงานเหตุการณ์ที่ผิดปกติและการปฏิบัติตามนโยบายและกฎระเบียบด้านไซเบอร์ขององค์กรอย่างเคร่งครัด โดยเฉพาะหน่วยงานที่จัดการข้อมูลสำคัญและมีความเกี่ยวข้องกับการรักษาความมั่นคงปลอดภัย เช่น สคทช. การจัดการด้านบุคลากรที่ดีจะช่วยเสริมสร้างความเชื่อมั่นในความมั่นคงปลอดภัยของข้อมูล และป้องกันการเกิดความผิดพลาดหรือการละเมิดข้อมูลที่อาจเกิดขึ้นจากการกระทำโดยบุคลากรภายในองค์กรเอง

2.3.1 การคัดกรอง (Screening)

(1) องค์กรต้องดำเนินการตรวจสอบประวัติของผู้สมัครงานก่อนการจ้างงาน ซึ่งอาจรวมถึงการตรวจสอบประวัติการทำงาน ประวัติอาชญากรรม และข้อมูลอื่น ๆ ที่เกี่ยวข้อง

(2) ขอบเขตและระดับความเข้มข้นของการตรวจสอบประวัติต้องมีความเหมาะสมกับความเสี่ยงที่เกี่ยวข้องกับตำแหน่งงานหรือบทบาทของบุคคลนั้น ๆ

(3) องค์กรต้องปฏิบัติตามกฎหมายและข้อบังคับที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคลและการจ้างงานในการดำเนินการตรวจสอบประวัติ

(4) ก่อนดำเนินการจ้างงาน ต้องดำเนินการ ดังนี้

- กำหนดหน้าที่ความรับผิดชอบเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศในคุณสมบัติของบุคลากรตามหนาที่งานที่ได้รับมอบหมาย
- ตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนกอนที่จะบรรจุเป็นบุคลากรของหน่วยงานจะต้องมีการตรวจสอบตามพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551
- การกำหนดเงื่อนไขการจ้างงาน (Terms and Conditions of Employment) ตามพระราชบัญญัติระเบียบข้าราชการพลเรือน พ.ศ. 2551 โดยรวมถึงหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน
- เตรียมข้อมูลที่เกี่ยวข้องกับนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงานเพื่อให้บุคลากรและผู้ใช้งานที่เข้ามาใหม่ได้ศึกษาและลงนามรับทราบรวมถึงยอมรับสัญญาในการปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศในส่วนที่เกี่ยวข้องกับตำแหน่งหน้าที่ความรับผิดชอบตามนโยบายของหน่วยงานที่กำหนดขึ้น

2.3.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)

(1) องค์กรต้องรวมข้อกำหนดและเงื่อนไขที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศไว้ในข้อตกลงการจ้างงานของบุคลากร

(2) ข้อตกลงการจ้างงานต้องระบุความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรและองค์กรอย่างชัดเจน เช่น การปฏิบัติตามนโยบาย การรายงานเหตุการณ์ และการรักษาความลับของข้อมูล

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(3) องค์กรต้องให้การฝึกอบรมและการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศแก่บุคลากรและผู้ที่เกี่ยวข้องอย่างสม่ำเสมอ

(4) การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกหรือการสิ้นสุดการเป็นบุคลากรของหน่วยงาน
- การโอนย้ายหน่วยงาน
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

(5) บุคลากรที่เข้ามาปฏิบัติงาน ตองลงนามรับทราบและยินยอมปฏิบัติตามสัญญา การรักษาข้อมูลที่เป็นความลับ และเอกสารอื่น ๆ ที่เกี่ยวข้อง กอนอนุญาตใหเริ่มงานหรือเข่าถึงและใช่งานข้อมูลสารสนเทศ

(6) ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

(7) การยุติการจ้างงาน: องค์กรต้องมีกระบวนการที่ชัดเจนในการจัดการกับความมั่นคงปลอดภัยสารสนเทศเมื่อมีการยุติการจ้างงาน เช่น การเพิกถอนสิทธิ์การเข้าถึง การส่งคืนทรัพย์สินขององค์กร และการทำข้อตกลงการรักษาความลับ

2.3.3 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ ข้อกำหนด (Information security awareness, education and training)

(1) ระหว่างดำเนินการจ้างงาน หน่วยงานต้องดำเนินการ ดังนี้ บุคลากรใหม่ต่องได้รับการอบรมเกี่ยวกับนโยบายความมั่นคงปลอดภัยสารสนเทศ

(2) จัดใหมีการอบรมใหความรู และสร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร แก่ผู้ใชงาน อย่างสม่ำเสมอ

2.3.4 กระบวนการทางวินัย (Disciplinary Process)

(1) องค์กรต้องกำหนดนโยบายและขั้นตอนที่ชัดเจนเกี่ยวกับกระบวนการทางวินัย ซึ่งรวมถึง:

(2) ประเภทของพฤติกรรมที่ถือว่าเป็นการละเมิด

(3) ขั้นตอนการสอบสวนและรวบรวมหลักฐาน

(4) ระดับของการลงโทษที่เหมาะสมกับความร้ายแรงของการละเมิด

(5) สิทธิ์ในการอุทธรณ์ของผู้ถูกกล่าวหา

(6) ความเป็นธรรมและความโปร่งใส: กระบวนการทางวินัยต้องเป็นไปอย่างเป็นธรรมและโปร่งใส โดยให้โอกาสผู้ถูกกล่าวหาในการชี้แจงและให้ข้อมูล

(7) การบันทึก: องค์กรต้องบันทึกการดำเนินการทางวินัยทั้งหมด รวมถึงเหตุผลในการลงโทษ เพื่อใช้เป็นหลักฐานอ้างอิงในอนาคต

(8) มีมาตรการดำเนินการกับผู้ฝาฝืน หรือละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงานที่เป็นความผิดตามกฎหมายที่เกี่ยวข้อง เช่น พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ(ฉบับที่ 2) พ.ศ. 2560 พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 เป็นต้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.3.5 ความรับผิดชอบหลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)

การเปลี่ยนตำแหน่งหรือสิ้นสุดการจ้างงาน หน่วยงานต้องดำเนินการ ดังนี้

(1) ต่องดำเนินการเปลี่ยนแปลง/เพิกถอน/ยกเลิก/ระงับ สิทธิ์ของผู้ใช่งานที่เกี่ยวกับการใช่งานระบบสารสนเทศเพื่อให่สอดคล่องกับการเปลี่ยนแปลงสถานะของการวาจ้าง โดยต่องเก็บข้อมูลให่สามารถตรวจสอบ ประวัติการเปลี่ยนแปลงสิทธิ์ในระบบสารสนเทศที่เกิดขึ้นเหล่านั้นได้

(2) เมื่อสิ้นสุดการจ้างงานหรือเปลี่ยนลักษณะการจ้างงาน ผู้ใช้งานจะต่องคืนสินทรัพย์อันเกี่ยวข่องกับการปฏิบัติหน่าที่ของตนที่เป็นของหน่วยงาน ได้แก อุปกรณ์ระบบสารสนเทศ ข้อมูลและสำเนาของข้อมูล กุญแจ บัตรประจำตัว ยกเลิกข้อมูลในระบบบันทึกลายนิ้วมือ ฯลฯ

2.3.6 ข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (NDA) (Confidentiality or non-disclosure agreements)

(1) องค์กรต้องระบุข้อมูลที่ถือว่าเป็นความลับและต้องได้รับการคุ้มครอง ซึ่งอาจรวมถึงข้อมูลทางการเงิน ข้อมูลลูกค้า ข้อมูลบุคลากร แผนธุรกิจ รหัสต้นฉบับซอฟต์แวร์ และข้อมูลอื่น ๆ ที่มีมูลค่าทางธุรกิจ

(2) องค์กรต้องทำข้อตกลง NDA กับบุคลากร ที่จำเป็นต้องเข้าถึงข้อมูลที่เป็นความลับ โดยข้อตกลง NDA ควรกำหนดขอบเขตของข้อมูลที่เป็นความลับ ระยะเวลาที่ต้องรักษาความลับ และผลที่ตามมาของการละเมิดข้อตกลง

(3) องค์กรต้องมีกลไกในการบังคับใช้ข้อตกลง NDA และดำเนินการทางกฎหมายกับผู้ที่ละเมิดข้อตกลง

2.3.7 การปฏิบัติงานจากระยะไกล (Remote Working)

(1) ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของ สคทช. มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

(2) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของ สคทช. ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

- ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น
- ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
- ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น HTTPS, SSH เป็นต้น
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของ สคทช. เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.3.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)

(1) บุคคลมีหน้าที่รายงานเหตุการณ์ด้านความมั่นคงปลอดภัย หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่สังเกตพบหรือต้องสงสัยผ่านช่องทางที่หน่วยงานกำหนดไว้โดยเร็วที่สุด

2.4 มาตรการที่ 3 มาตรการควบคุมด้านกายภาพ (Physical Controls)

มาตรการเชิงกายภาพเป็นมาตรการที่มุ่งเน้นการป้องกันการเข้าถึงระบบสารสนเทศหรืออุปกรณ์ทางกายภาพที่อาจเกิดการรั่วไหลของข้อมูลหรือการเข้าถึงโดยไม่ได้รับอนุญาต ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญมักจะต้องอาศัยการจัดการด้านกายภาพที่เข้มงวดเพื่อให้มั่นใจว่าข้อมูลและอุปกรณ์ที่สำคัญถูกเก็บรักษาอย่างปลอดภัย มาตรการนี้รวมถึงการควบคุมการเข้าถึงอาคาร สำนักงานห้องคอมพิวเตอร์หรือห้องที่มีการจัดเก็บข้อมูลที่มีความสำคัญ การกำหนดมาตรการรักษาความปลอดภัย เช่น การใช้ระบบรักษาความปลอดภัยแบบรหัสผ่าน การใช้บัตรผ่านเข้า-ออก และระบบกล้องวงจรปิด เพื่อป้องกันการบุกรุกจากภายนอกหรือจากผู้ที่ไม่มีสิทธิ์ นอกจากนี้ยังครอบคลุมถึงการจัดการและการเก็บรักษาอุปกรณ์สารสนเทศ เช่น เครื่องคอมพิวเตอร์ เซิร์ฟเวอร์ และอุปกรณ์เครือข่าย เพื่อให้แน่ใจว่าอุปกรณ์เหล่านี้จะไม่ถูกขโมยหรือเสียหายจากภัยธรรมชาติหรืออุบัติเหตุอื่น ๆ การมีมาตรการเชิงกายภาพที่เข้มแข็งจะช่วยเพิ่มความปลอดภัยในการดำเนินงานและป้องกันการสูญเสียข้อมูลหรือความเสียหายที่อาจเกิดขึ้นจากการละเมิดระบบกายภาพ

2.4.1 ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters)

(1) องค์กรต้องกำหนดขอบเขตความมั่นคงปลอดภัยทางกายภาพที่ชัดเจน ซึ่งอาจรวมถึงอาคาร สำนักงาน ศูนย์ข้อมูล และพื้นที่อื่น ๆ ที่จัดเก็บหรือประมวลผลข้อมูลที่สำคัญ

(2) องค์กรต้องมีมาตรการควบคุมการเข้าถึงขอบเขตความมั่นคงปลอดภัยทางกายภาพ เช่น การใช้รั้วกำแพง ประตูรักษาความมั่นคงปลอดภัย ระบบควบคุมการเข้าออก กล้องวงจรปิด และเจ้าหน้าที่รักษาความมั่นคงปลอดภัย

2.4.2 การเข้า - ออกพื้นที่ทางกายภาพ (Physical entry)

(1) ให้มีการดูแลพื้นที่ควบคุมพิเศษ ต้องควบคุมการเข้า-ออกบริเวณหรือพื้นที่ที่กำหนดให้เป็นพื้นที่ควบคุมพิเศษ ให้เป็นไปตามมาตรฐานฯ ที่กำหนด โดยอนุญาตให้ผ่านเข้า – ออกได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(2) ต้องควบคุมให้บุคคลภายนอกอยู่ในบริเวณที่จัดสำหรับบุคคลภายนอกติดต่อหรือรับ - ส่งของ และควรแยกพื้นที่สำหรับการติดต่อ หรือการรับ-ส่งของออกจากบริเวณที่มีทรัพย์สินสารสนเทศ รวมทั้งควรมีผนัง และ/หรือประตูป้องกันเพื่อไม่ให้สามารถผ่านไปยังส่วนงานอื่นได้

(3) ในกรณีที่ต้องมีการรับ - ส่งของ หรือติดต่อกับพนักงานซึ่งต้องมีการเข้าไปภายในพื้นที่อื่น หน่วยงานที่ดูแลพื้นที่ ต้องแจ้งพนักงานที่เกี่ยวข้อง และต้องรอให้พนักงานหรือตัวแทนมารับผู้ที่มารับ-ส่งของหรือมารับผู้ติดต่อเข้าไปภายในพื้นที่

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.4.3 การรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)

(1) ให้มีการออกแบบและติดตั้งระบบรักษาความมั่นคงปลอดภัยทางกายภาพ เพื่อป องกันความเสียหาย และถูกเข าถึงพื้นที่ปฏิบัติงานและพื้นที่ซึ่งมีทรัพย สินสารสนเทศหรือ อุปกรณ ประมวลผลสารสนเทศที่มีความสำคัญโดยไม่ได้รับอนุญาต

(2) สำหรับพื้นที่ควบคุม ศูนย์คอมพิวเตอร์ และห้องคอมพิวเตอร์ ต้องได้รับการอนุญาตตามข้อกำหนดของแต่ละสถานที่ และปฏิบัติตามกฎระเบียบการเข้าพื้นที่ควบคุมอย่างเคร่งครัด

(3) ควบคุมดูแลอุปกรณ์สารสนเทศสำนักงาน โดยจัดวางอยู่ในพื้นที่ตามหน่วยงานที่ได้รับการจัดสรรและอนุญาตให้เข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(4) ควบคุมให้มีการจัดวางอุปกรณ์สารสนเทศในพื้นที่ ให้สอดคล้องกับระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ ดังตารางต่อไปนี้

การควบคุมการจัดวางอุปกรณ์สารสนเทศ ตามระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ	
ระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ	**พื้นที่จัดวาง**
สูงสุด	ศูนย์คอมพิวเตอร์ หรือพื้นที่ควบคุม
สูง	ศูนย์คอมพิวเตอร์ หรือพื้นที่ควบคุม
ปานกลาง	ศูนย์คอมพิวเตอร์ ห้องคอมพิวเตอร์ หรือพื้นที่ควบคุม
ต่ำ	ห้องคอมพิวเตอร์หรือสำนักงาน

ตารางที่ 2-2 การควบคุมการจัดวางอุปกรณ์สารสนเทศตามระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

- อุปกรณ์สารสนเทศที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ “สูง” และ “สูงสุด” ต้องจัดวางอยู่ในศูนย์คอมพิวเตอร์ หรือพื้นที่ควบคุม หรือมีมาตรการควบคุมการเข้าถึงอุปกรณ์สารสนเทศตามความเหมาะสม เช่น ให้มีการพิสูจน์และยืนยันตัวตนโดยใช้วิธีการพิสูจน์และยืนยันตัวตนแบบ 2 Factors
- อุปกรณ์สารสนเทศที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ “ปานกลาง” ให้จัดวางอยู่ในศูนย์คอมพิวเตอร์ ห้องคอมพิวเตอร์ หรือพื้นที่ควบคุม
- อุปกรณ์สารสนเทศที่ถูกจัดไว้ในระดับการป้องกันความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ “ต่ำ” ควรจัดวางอยู่ในห้องคอมพิวเตอร์ หรือ สำนักงาน

2.4.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)

(1) องค์กรต้องออกแบบระบบเฝ้าระวังความมั่นคงปลอดภัยทางกายภาพที่เหมาะสมกับความเสี่ยงและความต้องการขององค์กร ซึ่งอาจรวมถึง:

- กล้องวงจรปิด (CCTV): ติดตั้งกล้องวงจรปิดในบริเวณที่เหมาะสม เช่น ทางเข้า - ออก พื้นที่จัดเก็บข้อมูลสำคัญ และบริเวณโดยรอบอาคาร
- ระบบเตือนภัย: ติดตั้งระบบเตือนภัย เช่น ระบบตรวจจับการเคลื่อนไหว ระบบตรวจจับควัน ระบบตรวจจับความร้อน และระบบตรวจจับการบุกรุก
- ระบบควบคุมการเข้าออก: ใช้ระบบควบคุมการเข้าออก เช่น คีย์การ์ด หรือรหัสผ่าน เพื่อจำกัดการเข้าถึงพื้นที่สำคัญ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- เจ้าหน้าที่รักษาความมั่นคงปลอดภัย: จัดให้มีเจ้าหน้าที่รักษาความมั่นคงปลอดภัยเพื่อตรวจตราและเฝ้าระวังพื้นที่

(2) องค์กรต้องดำเนินการและบำรุงรักษาระบบเฝ้าระวังให้มีประสิทธิภาพ โดย:

- ตรวจสอบและบำรุงรักษาอุปกรณ์เฝ้าระวังอย่างสม่ำเสมอ
- ทบทวนบันทึกเหตุการณ์จากระบบเฝ้าระวังเป็นประจำ
- ฝึกอบรมเจ้าหน้าที่รักษาความมั่นคงปลอดภัยให้มีความรู้และทักษะในการใช้งานระบบเฝ้าระวัง

2.4.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats)

(1) การประเมินความเสี่ยง: องค์กรต้องประเมินความเสี่ยงจากภัยคุกคามทางกายภาพและสิ่งแวดล้อมที่อาจส่งผลกระทบต่อข้อมูลและทรัพย์สินขององค์กร โดยพิจารณาจากปัจจัยต่าง ๆ เช่น สถานที่ตั้งขององค์กร ประเภทของข้อมูลและทรัพย์สิน และประวัติการเกิดภัยพิบัติในพื้นที่

(2) มาตรการป้องกัน: องค์กรต้องกำหนดและดำเนินการตามมาตรการป้องกันที่เหมาะสมกับความเสี่ยงที่ประเมินได้ เช่น:

- ไฟไหม้: ติดตั้งระบบตรวจจับควันและความร้อน ระบบดับเพลิง และจัดให้มีทางหนีไฟที่ชัดเจน
- น้ำท่วม: ยกระดับพื้นที่สำคัญ ป้องกันการรั่วซึมของน้ำ และจัดเตรียมกระสอบทรายหรืออุปกรณ์ป้องกันน้ำท่วมอื่น ๆ
- แผ่นดินไหว: ออกแบบอาคารให้ทนต่อแรงสั่นสะเทือน และจัดเตรียมอุปกรณ์ยังชีพสำหรับบุคลากร
- การโจรกรรม: ติดตั้งระบบรักษาความมั่นคงปลอดภัย เช่น กล้องวงจรปิด ระบบเตือนภัย และระบบควบคุมการเข้าออก

(3) แผนการรับมือเหตุฉุกเฉิน: องค์กรต้องจัดทำแผนการรับมือเหตุฉุกเฉินที่ครอบคลุมถึงขั้นตอนการอพยพ การแจ้งเตือน การสื่อสาร และการกู้คืนระบบและข้อมูล

(4) การฝึกอบรมและการทดสอบ: องค์กรต้องจัดให้มีการฝึกอบรมบุคลากรเกี่ยวกับแผนการรับมือเหตุฉุกเฉิน และทดสอบแผนเป็นประจำเพื่อให้มั่นใจว่าสามารถนำไปใช้ได้จริงในสถานการณ์จริง

2.4.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)

(1) องค์กรต้องมีมาตรการควบคุมการเข้าถึงพื้นที่ปลอดภัยที่เหมาะสม เช่น:

- ใช้ระบบควบคุมการเข้าออก (Access Control System) เช่น คีย์การ์ด รหัสผ่าน หรือข้อมูลชีวภาพ
- จัดให้มีเจ้าหน้าที่รักษาความมั่นคงปลอดภัยประจำการในพื้นที่ปลอดภัย
- ติดตั้งกล้องวงจรปิดเพื่อตรวจสอบและบันทึกกิจกรรม
- จำกัดการเข้าถึงเฉพาะบุคลากรที่ได้รับอนุญาตและมีความจำเป็นต้องเข้าพื้นที่

(2) องค์กรต้องกำหนดกฎระเบียบและขั้นตอนที่ชัดเจนสำหรับการทำงานในพื้นที่ปลอดภัย เช่น:

- ห้ามนำอุปกรณ์ส่วนตัว เช่น โทรศัพท์มือถือ หรือกล้องถ่ายรูป เข้าไปในพื้นที่ปลอดภัย
- ห้ามนำอาหารและเครื่องดื่มเข้าไปในพื้นที่ปลอดภัย
- ห้ามเปิดเผยข้อมูลที่เป็นความลับให้กับบุคคลที่ไม่ได้รับอนุญาต
- รายงานเหตุการณ์ที่น่าสงสัยหรือผิดปกติให้กับผู้รับผิดชอบทันที

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(3) องค์กรต้องดูแลรักษาความสะอาดและเป็นระเบียบเรียบร้อยของพื้นที่ปลอดภัย เพื่อป้องกันอุบัติเหตุและความเสียหายที่อาจเกิดขึ้น

2.4.7 การจัดเก็บโต๊ะทำงาน และการจัดการหน้าจอ (Clear desk and clear screen)

(1) เก็บสารสนเทศที่อยู่ในระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ที่อยู่ในรูปแบบเอกสารหรือสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ โดยใส่กุญแจ (วิธีที่ดีที่สุด คือ เก็บไว้ในตู้นิรภัย หรือตู้ใส่ของหรือครุภัณฑ์ รูปแบบอื่น ๆ ที่รักษาความมั่นคงปลอดภัยได้)

(2) ข้อปฏิบัติในการเข้าถึงพื้นที่ควบคุม สำนักงาน และทรัพย์สินต่าง ๆ

- แนวปฏิบัติสำหรับผู้ปฏิบัติงาน
  - ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์ที่ตนเองรับผิดชอบให้มีการล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า 10 นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์
  - ห้องทำงานส่วนตัว ต้องมีการปิดใส่กุญแจ (Lock) เมื่อไม่อยู่ภายในห้องทำงาน
  - ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า 1 ชั่วโมง
- การป้องกันอุปกรณ์ที่ไม่มีผู้รับผิดชอบโดยตรง
  - ปลดการเชื่อมต่อ (Log-off) จากโปรแกรมหรือบริการเครือข่ายเมื่อไม่มีการใช้งาน
  - ล็อคหน้าจอ เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์

2.4.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)

(1) ต้องควบคุมดูแลให้อุปกรณ์สารสนเทศที่สำคัญ ถูกติดตั้งอยู่ในสถานที่ที่สามารถป้องกันการเข้าถึงจากผู้ไม่มีสิทธิ์

(2) ต้องควบคุมดูแลให้อุปกรณ์สารสนเทศที่สำคัญ ถูกติดตั้งอยู่ในสถานะที่ป้องกันความเสียหายจากภัยธรรมชาติ การถูกขโมย ไฟฟ้าดับ ไฟไหม้ และภัยจากมนุษย์

2.4.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสถานที่ (Security of assets off-premises)

(1) แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

- การนำทรัพย์สินขององค์กรออกนอกพื้นที่ สคทช.
  - นำเอกสารแบบฟอร์มใบนำสิ่งของออกนอกบริเวณ สคทช. (สคทช. -นอ.11) นำเสนอผู้บังคับบัญชา เพื่อขออนุมัติและให้หน่วยงานเก็บเป็นหลักฐาน
  - นำสำเนาเอกสารแบบฟอร์มใบนำสิ่งของออกนอกบริเวณ สคทช. (สคทช. -นอ.11) ที่ผ่านการอนุมัติ ให้เจ้าหน้าที่รักษาความมั่นคงปลอดภัยตรวจสอบลักษณะของทรัพย์สินของ สคทช. ให้ตรงตามรายการในแบบฟอร์ม
- การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกสำนักงาน
  - ขณะเคลื่อนย้ายหรือเดินทาง ต้องจัดเตรียมอุปกรณ์ให้อยู่ในสัมภาระที่ปกปิดมิดชิดและห่อหุ้มในขณะเดินทาง เพื่อป้องกันความเสียหายต่ออุปกรณ์
  - ปฏิบัติตามคำแนะนำจากผู้ผลิตของอุปกรณ์อย่างเคร่งครัด เพื่อป้องกันไม่ให้เกิดความเสียหายของอุปกรณ์ เช่น ไม่วางอุปกรณ์ไว้ใกล้กับอุปกรณ์อื่น ๆ ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง ไม่เก็บอุปกรณ์ไว้ในที่ที่มีอุณหภูมิสูง
  - ทำการสำรองข้อมูลในอุปกรณ์อย่างสม่ำเสมอ
  - ไม่วางอุปกรณ์ทิ้งไว้ในที่สาธารณะ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ในกรณีที่มีความจำเป็นต้องวางอุปกรณ์ในที่สาธารณะ อุปกรณ์ดังกล่าวต้องสามารถใช้สายเข้ากุญแจล็อคกับอุปกรณ์สำนักงานหรืออุปกรณ์อื่น ๆ ที่ไม่สามารถเคลื่อนย้ายได้ หรือมีมาตรการป้องกันการสูญหาย
- จดบันทึกการแลกเปลี่ยนหรือการครอบครองอุปกรณ์ โดยระบุรายละเอียดของผู้รับผิดชอบ ขณะมีการใช้งานนอกสถานที่

➢ การป้องกันอุปกรณ์ที่ไม่มีผู้รับผิดชอบโดยตรง
- ปลดการเชื่อมต่อ (Log-off) จากโปรแกรมหรือบริการเครือข่ายเมื่อไม่มีการใช้งาน
- ล็อคหน้าจอ เมื่อมีความจำเป็นต้องละทิ้งเครื่องคอมพิวเตอร์

2.4.10 สื่อบันทึกข้อมูล (Storage Media)

(1) มาตรการ/ แนวปฏิบัติ

➢ ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของ สคทช. โดยใช้มาตรการอย่างน้อย ดังนี้

➢ ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

➢ ใช้สื่อบันทึกข้อมูล อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น

➢ ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของของ สคทช.

➢ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของ สคทช. บนสื่อบันทึกข้อมูลแบบถอดได้

2.4.11 ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities)

(1) องค์กรต้องประเมินความเสี่ยงที่เกี่ยวข้องกับสาธารณูปโภคที่สนับสนุน เช่น ความเสี่ยงของไฟฟ้าดับ น้ำท่วม หรือความขัดข้องของระบบปรับอากาศ

(2) องค์กรต้องกำหนดและดำเนินการตามมาตรการป้องกันที่เหมาะสม เพื่อลดความเสี่ยงที่ระบุไว้ในข้อ 1 เช่น การติดตั้งเครื่องสำรองไฟ (UPS) การทำระบบป้องกันน้ำท่วม หรือ การทำสัญญาบริการบำรุงรักษาเครื่องปรับอากาศ

(3) องค์กรต้องตรวจสอบและบำรุงรักษาสาธารณูปโภคที่สนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าอยู่ในสภาพพร้อมใช้งานและมีประสิทธิภาพ เช่น

➢ ไฟฟ้า: ติดตั้งเครื่องสำรองไฟ (UPS) สำหรับอุปกรณ์สำคัญ เช่น เซิร์ฟเวอร์ และจัดให้มีระบบจ่ายไฟสำรอง เช่น เครื่องปั่นไฟ

➢ ระบบปรับอากาศ: ทำสัญญาบริการบำรุงรักษาเครื่องปรับอากาศ และตรวจสอบอุณหภูมิและความชื้นในห้องที่ติดตั้งอุปกรณ์สำคัญเป็นประจำ

➢ ระบบสื่อสาร: จัดให้มีระบบสื่อสารสำรอง เช่น สายโทรศัพท์สำรอง หรืออินเทอร์เน็ตสำรอง เพื่อให้สามารถติดต่อสื่อสารได้ในกรณีที่ระบบหลักล่ม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.4.12 การรักษาความมั่นคงปลอดภัยของการเดินสาย (Cabling Security)

(1) บริหารจัดการสายสื่อสาร สายเคเบิ้ลอื่น ๆ และการเดินสายไฟ ดังต่อไปนี้

- สายไฟฟ้าและสายสื่อสารสำหรับอุปกรณ์ต่าง ๆ ต้องวางสายภายในท่อรางร้อยสาย หรือได้รับการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อหลีกเลี่ยงจากการเกิดความเสียหาย หรือการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต
- สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ
- สายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ ต้องได้รับการทำสัญลักษณ์อย่างชัดเจน เพื่อป้องกัน ความสับสน
- ในกรณีที่มีความจำเป็นต้องวางสายไฟฟ้าและสายสื่อสารสำหรับอุปกรณ์ต่าง ๆ ไว้ใต้ดิน ต้องมีป้ายบ่งชี้ถึงแนวสาย เพื่อป้องกับความเสียหายที่เกิดจากการขุดเจาะ
- จัดทำเอกสารรายการ การเข้าสาย (Patch List) เพื่อป้องกันความสับสน

(2) บริหารจัดการระบบและอุปกรณ์ที่มีความสำคัญ (Sensitive or Critical Systems) ดังต่อไปนี้

- ใช้สายสัญญาณที่มีคุณสมบัติป้องกันสนามแม่เหล็กไฟฟ้า หรือ ใช้สายใยแก้วนำแสง (Fiber Optic)
- ติดตั้งท่อหุ้มสายชนิดพิเศษ (Armored Conduit) โดยจุดเชื่อมต่อของสายสัญญาณต่าง ๆ ต้องอยู่ภายในห้องหรือกล่องที่ใส่กุญแจได้
- ควบคุมการเข้าถึงแผงพักปลายสาย (Patch Panel) และห้องพักสาย (Cable Room)
- มีการตรวจสอบระบบสาย เพื่อตรวจจับอุปกรณ์แปลกปลอม

2.4.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)

(1) องค์กรต้องจัดทำแผนการบำรุงรักษาอุปกรณ์ที่ครอบคลุมและเป็นระบบ โดยระบุถึง:

- ประเภทของอุปกรณ์ที่ต้องบำรุงรักษา
- ความถี่ในการบำรุงรักษา
- ขั้นตอนการบำรุงรักษา
- ผู้รับผิดชอบในการบำรุงรักษา

(2) องค์กรต้องดำเนินการบำรุงรักษาเชิงป้องกัน (Preventive Maintenance) เพื่อป้องกันความผิดพลาดและความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์

(3) องค์กรต้องมีขั้นตอนการบำรุงรักษาเชิงแก้ไข (Corrective Maintenance) ที่มีประสิทธิภาพ เพื่อแก้ไขปัญหาที่เกิดขึ้นกับอุปกรณ์ได้อย่างรวดเร็ว

(4) องค์กรต้องบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ทั้งหมด รวมถึงวันที่ เวลา รายละเอียดของปัญหา และการดำเนินการแก้ไข

(5) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญา เท่านั้น

(6) ทบทวนแผนการบำรุงรักษาทรัพย์สินสารสนเทศของหน่วยงานอย่างน้อยปีละ 1 ครั้ง

(7) ทบทวนสัญญาบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ เป็นประจำอย่างน้อยปีละ 1 ครั้ง

(8) จัดให้มีการบันทึกประวัติการบำรุงรักษาอุปกรณ์และระบบสนับสนุนการทำงานต่าง ๆ อย่างเป็นลายลักษณ์อักษร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.4.14 การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment)

(1) องค์กรต้องมีกระบวนการที่ชัดเจนสำหรับการกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย โดยระบุถึง:

- ประเภทของอุปกรณ์ที่ต้องได้รับการกำจัดหรือนำกลับมาใช้ใหม่
- วิธีการลบหรือทำลายข้อมูลที่เหมาะสมสำหรับอุปกรณ์แต่ละประเภท
- ผู้รับผิดชอบในการดำเนินการ
- การบันทึกและการตรวจสอบ

(2) องค์กรต้องลบข้อมูลที่จัดเก็บอยู่ในอุปกรณ์อย่างมั่นคงปลอดภัย โดยใช้วิธีการที่เหมาะสมกับประเภทของอุปกรณ์และความอ่อนไหวของข้อมูล เช่น การเขียนทับข้อมูล (Overwriting) การล้างข้อมูล (Degaussing) หรือการทำลายทางกายภาพ

- ในกรณีที่ไม่สามารถลบข้อมูลได้อย่างมั่นคงปลอดภัย องค์กรต้องทำลายอุปกรณ์ทางกายภาพ เพื่อป้องกันการกู้คืนข้อมูล
- กำหนดนโยบายและขั้นตอน ที่ชัดเจนสำหรับการกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย
- ใช้ซอฟต์แวร์ลบข้อมูล ที่เชื่อถือได้ในการลบข้อมูลออกจากฮาร์ดดิสก์ไดรฟ์และสื่อบันทึกข้อมูลอื่นๆ
- ทำลายอุปกรณ์ที่ไม่สามารถลบข้อมูลได้ เช่น การเผา การบด หรือการทำลายด้วยวิธีการทางกายภาพอื่นๆ
- บันทึกข้อมูลการกำจัดหรือการนำกลับมาใช้ใหม่ ของอุปกรณ์ทุกเครื่อง รวมถึงวิธีการที่ใช้ในการลบหรือทำลายข้อมูล
- พิจารณาใช้บริการของผู้เชี่ยวชาญ ในการกำจัดหรือทำลายอุปกรณ์ที่มีข้อมูลที่อ่อนไหวสูง

2.5 มาตรการที่ 4 มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)

มาตรการด้านเทคโนโลยีเป็นหัวใจหลักในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ในยุคดิจิทัลที่มีการพัฒนาระบบและเทคโนโลยีสารสนเทศอย่างต่อเนื่อง มาตรการนี้ครอบคลุมถึงการป้องกันภัยคุกคามไซเบอร์ที่อาจเกิดขึ้นในรูปแบบต่าง ๆ ผ่านการใช้เทคโนโลยีที่ทันสมัย เช่น การรักษาความปลอดภัยของเครือข่าย การควบคุมการเข้าถึงระบบสารสนเทศ การป้องกันมัลแวร์ (Malware) และการเข้ารหัสข้อมูลที่มีความสำคัญเพื่อป้องกันการโจรกรรมข้อมูล มาตรการนี้ยังรวมถึงการสำรองข้อมูล (Backup) อย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่เกิดความเสียหายหรือการโจมตี นอกจากนี้การตรวจสอบและการตรวจจับภัยคุกคามทางไซเบอร์ เช่น การติดตั้งระบบเฝ้าระวังหรือโปรแกรมตรวจจับไวรัสยังถือเป็นส่วนสำคัญของมาตรการด้านเทคโนโลยี ทั้งนี้ มาตรการด้านเทคโนโลยีที่มีประสิทธิภาพจะช่วยปกป้องข้อมูลและระบบสารสนเทศที่สำคัญขององค์กรจากภัยคุกคามที่เพิ่มขึ้นในโลกไซเบอร์

2.5.1 อุปกรณ์ของผู้ใช้งาน (User endpoint devices)

(1) องค์กรต้องกำหนดนโยบายการใช้อุปกรณ์ปลายทางที่ชัดเจน ครอบคลุมถึง:

- ประเภทของอุปกรณ์ที่อนุญาตให้ใช้
- ข้อกำหนดด้านความมั่นคงปลอดภัย เช่น การใช้รหัสผ่าน การเข้ารหัส และการติดตั้งซอฟต์แวร์ป้องกันไวรัส

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ข้อจำกัดในการใช้งาน เช่น การห้ามเข้าเว็บไซต์ที่ไม่เหมาะสม หรือการห้ามดาวน์โหลดไฟล์จากแหล่งที่ไม่น่าเชื่อถือ

(2) องค์กรควรมีการจัดการและควบคุมอุปกรณ์โดยกำหนดและบังคับใช้นโยบาย การติดตั้งซอฟต์แวร์ การตรวจสอบการใช้งาน และการลบข้อมูลจากระยะไกล เป็นต้น

(3) องค์กรต้องเข้ารหัสข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ปลายทาง เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตในกรณีที่อุปกรณ์สูญหายหรือถูกโจรกรรม

(4) องค์กรต้องสำรองข้อมูลที่จัดเก็บอยู่ในอุปกรณ์ปลายทางอย่างสม่ำเสมอ เพื่อให้สามารถกู้คืนข้อมูลได้ในกรณีที่อุปกรณ์เสียหายหรือสูญหาย

(5) องค์กรต้องปรับปรุงซอฟต์แวร์และระบบปฏิบัติการของอุปกรณ์ปลายทางให้เป็นปัจจุบันอยู่เสมอ เพื่อป้องกันช่องโหว่ด้านความมั่นคงปลอดภัย

2.5.2 สิทธิพิเศษในการเข้าถึงสารสนเทศ (Privileged access rights)

(1) จัดทำกระบวนการที่เป็นทางการสำหรับการลงทะเบียนและเพิกถอนผู้ใช้งาน เพื่อใช้ในการกำหนดสิทธิ์การเข้าถึง

(2) องค์กรต้องระบุบัญชีผู้ใช้ทั้งหมดที่มีสิทธิพิเศษ เช่น บัญชีผู้ดูแลระบบ (Administrator) และบัญชีรูท (Root) และควบคุมการเข้าถึงบัญชีเหล่านี้อย่างเข้มงวด

(3) การจัดการรหัสผ่าน: องค์กรต้องกำหนดและบังคับใช้นโยบายรหัสผ่านที่เข้มงวดสำหรับบัญชีที่มีสิทธิพิเศษ เช่น การใช้รหัสผ่านที่ยาวและซับซ้อน การเปลี่ยนรหัสผ่านเป็นประจำ และการห้ามใช้รหัสผ่านซ้ำ

(4) ควบคุมไม่ให้ผู้ปฏิบัติงานที่มีสิทธิพิเศษเปิดเผยรหัสผ่านของผู้ใช้งาน

(5) จัดทำ “ทะเบียนรายชื่อบัญชีผู้ใช้งานร่วมกัน” โดยลงทะเบียนชื่อผู้ใช้งานเหล่านั้นทั้งหมดที่มีการใช้งานบัญชีเดียวกัน

(6) ควบคุมการใช้บัญชีผู้ใช้งานร่วมกัน โดยจัดทำบันทึกการเข้าใช้งาน ระบุผู้เข้าใช้ วัน/เวลา และการเข้าใช้งาน

(7) ควบคุมดูแลให้มีการเพิกถอนสิทธิ์ในการเข้าถึงบัญชีผู้ใช้งานร่วมกัน เมื่อบุคคลนั้น สิ้นสุดหรือเปลี่ยนแปลงตำแหน่ง/การจ้างงาน และต้องเปลี่ยนรหัสผ่านทันที

(8) แจ้งสมาชิกที่เหลือของผู้ใช้บัญชีผู้ใช้งานร่วมกัน เพื่อให้ทราบถึงจำนวนสมาชิกที่เหลือและรหัสผ่านใหม่ โดยต้องไม่ให้ผู้ที่ถูกเพิกถอนสิทธิ์รับทราบรหัสผ่านใหม่และเข้าถึงบัญชีผู้ใช้งานได้อีก

(9) ทบทวนตารางแสดงสิทธิ์ อย่างน้อยปีละ 1 ครั้ง สำหรับระบบงานที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” ให้ทบทวนตารางแสดงสิทธิ์ทุก 3 เดือน

(10) การจำกัดสิทธิ์การใช้งาน: องค์กรต้องจำกัดสิทธิ์การใช้งานบัญชีที่มีสิทธิ์พิเศษเฉพาะเมื่อจำเป็นจริง ๆ และเพิกถอนสิทธิ์ทันทีเมื่อไม่จำเป็นต้องใช้งานอีกต่อไป

2.5.3 การจำกัดการเข้าถึงระบบสารสนเทศ (Information access restriction)

(1) ต้องควบคุมและกำหนดสิทธิ์ในการเข้าถึงข้อมูลสารสนเทศ ให้เป็นไปตามที่เจ้าของข้อมูลกำหนด โดยพิจารณาตามความจำเป็นสำหรับการใช้งานในบทบาทและหน้าที่ความรับผิดชอบ

(2) จัดทำแนวปฏิบัติในการขออนุมัติและเพิกถอนสิทธิ์การใช้งานแต่ละระบบสารสนเทศ

(3) จัดทำทะเบียนควบคุมสิทธิ์ที่เหมาะสม รวมถึงรายชื่อหรือกลุ่มผู้มีสิทธิ์ใช้งานทั้งที่ต้องขออนุมัติและไม่ต้องขออนุมัติก่อนเริ่มใช้งานอย่างเป็นลายลักษณ์อักษรในแต่ละระบบสารสนเทศ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โดยการเข้าถึงของผู้ใช้งานทั้งหมดต้องสอดคล้องกับการดำเนินงานของ สคทช. และหน้าที่ความรับผิดชอบของผู้ใช้งาน

(4) ดูแลกำกับ สิทธิ์การเข้าถึง ไฟล์ (File) และ โฟลเดอร์ (Folder) ที่สร้างขึ้น

(5) ควบคุมให้จำกัดจำนวนผู้ปฏิบัติงานที่มีสิทธิพิเศษทำหน้าที่เป็นผู้ให้สิทธิ์กับผู้ใช้งานไม่เกิน 3 คนต่อระบบงาน

(6) จำกัดการเข้าถึงสารสนเทศและฟังก์ชันของระบบหรือโปรแกรมประยุกต์ให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

2.5.4 การเข้าถึงโปรแกรมต้นฉบับ (Access to source code)

(1) องค์กรต้องกำหนดสิทธิ์ในการเข้าถึงโปรแกรมต้นฉบับ (Source code) ให้เข้าถึงได้เท่าที่จำเป็นสำหรับผู้ที่มีหน้าที่ในการปฏิบัติงานเท่านั้น รวมถึงปรับปรุงรายชื่อผู้ใช้งานและสิทธิ์การใช้งานให้เป็นปัจจุบันอยู่เสมอ

(2) องค์กรต้องจัดให้มีการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging record) แสดงการเข้าถึงโปรแกรมต้นฉบับให้เพียงพอในการตรวจสอบ การเข้าถึง เปลี่ยนแปลง และแก้ไขโปรแกรมต้นฉบับ

2.5.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)

(1) องค์กรต้องติดตั้งและกำหนดค่าพารามิเตอร์ของระบบปฏิบัติการตาม Baseline Configuration รวมถึงจัดให้มีการพิสูจน์ตัวตน ควบคุมการเข้าถึงให้เป็นไปตามมาตรฐานฯ ที่กำหนด เพื่อป้องกันการเข้าถึงโดยผู้ไม่ได้รับอนุญาต

(2) การกำหนดระยะเวลาในการใช้งานระบบสารสนเทศ (Session time-out) หน่วยงานที่รับผิดชอบระบบ ควรกำหนดให้ระบบยกเลิกการเชื่อมต่อโดยอัตโนมัติเมื่อไม่มีการใช้งานระบบนานเกิน ตามมาตรฐานฯ ที่กำหนด

(3) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) หน่วยงานที่ดูแลระบบ ควรกำหนดและควบคุมช่วงเวลาสำหรับการเชื่อมต่อระบบงานที่มีความเสี่ยงสูง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

2.5.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity management)

(1) องค์กรต้องติดตามการใช้ทรัพยากรของระบบในปัจจุบัน และวิเคราะห์แนวโน้มการขยายการดำเนินธุรกิจในอนาคต เพื่อนำมาจัดทำแผนการขยายทรัพยากรของระบบ ให้รองรับการขยายตัวของธุรกิจ

(2) องค์กรต้องปรับแต่งค่าพารามิเตอร์ของระบบให้ใช้ทรัพยากรสารสนเทศ อย่างมีประสิทธิภาพสูงสุดและใช้เท่าที่จำเป็น

(3) เจ้าหน้าที่ต้องเข้ามาตรวจสอบประสิทธิภาพเป็นประจำทุกสิ้นสัปดาห์

(4) เจ้าหน้าที่ต้องบันทึกลงแบบฟอร์มการตรวจเช็คความพร้อมใช้ทรัพยากรของระบบเป็นประจำทุกสิ้นสัปดาห์ให้เจ้าของระบบทราบ

2.5.7 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection against malware)

(1) หน่วยงานที่ดูแลระบบ และหน่วยงานที่ดูแลเครื่องคอมพิวเตอร์ผู้ใช้งาน ต้องดำเนินการตรวจสอบ ป้องกัน และกู้คืนระบบ จากโปรแกรมไม่ประสงค์ดีตามมาตรฐานฯ ที่กำหนด รวมถึงการสร้างความตระหนักให้ผู้ใช้งานร่วมปฏิบัติตามขั้นตอนที่เหมาะสม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(2) แนวปฏิบัติสำหรับหน่วยงาน

- เตรียมแผนความต่อเนื่องทางธุรกิจที่เหมาะสม เพื่อรับมือกับการถูกโจมตีโดยไวรัสคอมพิวเตอร์ มัลแวร์ โปรแกรมไม่พึงประสงค์อื่น ๆ ทั้งนี้รวมถึงกระบวนการในการสำรองและกู้คืนข้อมูล
- ควบคุมให้ปฏิบัติตามกระบวนการที่กำหนดโดย ฝ่ายที่เกี่ยวข้อง เมื่อตรวจพบโปรแกรมไม่พึงประสงค์ ซึ่งรวมถึงการรายงาน และการกู้ข้อมูลจากการถูกโจมตีโดยโปรแกรมไม่พึงประสงค์

(3) แนวปฏิบัติสำหรับ ฝ่ายที่เกี่ยวข้อง

- จัดทำแนวปฏิบัติ เมื่อตรวจพบไวรัสคอมพิวเตอร์ มัลแวร์ โปรแกรมไม่พึงประสงค์อื่น ๆ ซึ่งรวมถึงการรายงานและการกู้ข้อมูลจากการถูกโจมตีโดยโปรแกรมไม่พึงประสงค์
- ตรวจสอบข้อมูลเกี่ยวกับไวรัสคอมพิวเตอร์ มัลแวร์ โปรแกรมไม่พึงประสงค์อื่น ๆ โดยตรวจสอบให้มั่นใจว่า ประกาศเตือนเป็นข้อมูลที่ถูกต้องและเป็นประโยชน์ ทั้งนี้ต้องตรวจสอบให้มั่นใจว่า แหล่งที่มามีคุณสมบัติเหมาะสม เช่น การใช้วารสารที่มีชื่อเสียง เว็บไซต์ที่เชื่อถือได้ จากผู้ส่งมอบที่ผลิตซอฟต์แวร์ป้องกันโปรแกรมไม่พึงประสงค์

(4) แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

- ตรวจสอบและปรับปรุงโปรแกรมที่ตรวจจับและแก้ไขโปรแกรมไม่พึงประสงค์บนอุปกรณ์ประมวลผลสารสนเทศที่รับผิดชอบให้ทันสมัยอยู่เสมอ โดยให้ทำการตรวจสอบอย่างน้อยสัปดาห์ละ 1 ครั้ง หากพบว่าอุปกรณ์ประมวลผลสารสนเทศทำงานผิดปกติ ให้รีบแจ้งหน่วยงานที่เกี่ยวข้อง เช่น Help Desk เพื่อดำเนินการแก้ไขโดยทันที
- ตรวจสอบไฟล์ที่อยู่ในอุปกรณ์ประมวลผลสารสนเทศและไฟล์ที่ได้รับผ่านเครือข่าย เพื่อตรวจหาโปรแกรมไม่พึงประสงค์ก่อนเปิดใช้งาน
- ตรวจสิ่งแนบที่ส่งมากับจดหมายอิเล็กทรอนิกส์ เพื่อตรวจหาโปรแกรมไม่พึงประสงค์ก่อนเปิดใช้
- ไม่เปิดสิ่งแนบที่ส่งมากับจดหมายอิเล็กทรอนิกส์จากผู้ส่งที่ไม่รู้จัก
- หลีกเลี่ยงการเข้าถึงเว็บไซต์ที่ไม่ปลอดภัย
- ไม่สร้าง เก็บ หรือเผยแพร่โปรแกรมไม่พึงประสงค์เข้าสู่ระบบคอมพิวเตอร์
- ไม่ขัดขวาง หรือรบกวนการทำงานของโปรแกรมป้องกันไวรัส
- ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

2.5.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)

(1) ต้องควบคุมการตรวจสอบช่องโหว่ในระบบสารสนเทศ และติดตามการแก้ไขช่องโหว่ทางเทคนิค โดยมีการจัดลำดับความสำคัญในการแก้ไขช่องโหว่ทางเทคนิคให้เหมาะสมกับระดับความเสี่ยง เพื่อป้องกันการโจมตีโดยอาศัยช่องโหว่ทางเทคนิค

(2) ต้องตรวจสอบข่าวสารด้านความปลอดภัยของระบบที่รับผิดชอบ หากมีการพบช่องโหว่ในระบบที่รับผิดชอบต้องหาแนวทางแก้ไขความเสี่ยงที่เกิดขึ้นให้อยู่ในระดับที่ยอมรับได้

(3) ต้องสุ่มสอบทานการปฏิบัติตามข้อกำหนดทางเทคนิค และช่องโหว่ของระบบสารสนเทศ เพื่อให้มีการปฏิบัติตามนโยบาย และมาตรฐานฯ

(4) เครื่องมือ (Software Tools) ที่ใช้ในการตรวจสอบหรือทดสอบ การปฏิบัติตามข้อกำหนดทางเทคนิค และช่องโหว่ของระบบสารสนเทศ จะต้องถูกจำกัดสิทธิ์ ให้ใช้ได้เฉพาะผู้มีหน้าที่ตรวจสอบหรือทดสอบที่ได้รับอนุญาตเท่านั้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.5.9 การบริหารจัดการ การกำหนดค่า (Configuration management)

(1) จัดทำการกำหนดค่า รวมถึงการกำหนดค่าด้านการรักษาความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ บริการและเครือข่ายและจัดทำเป็นเอกสาร นำไปปฏิบัติ เฝ้าติดตามและทบทวน

(2) แนวปฏิบัติสำหรับหน่วยงาน

- กำหนดเทมเพลต (Template) มาตรฐานสำหรับการกำหนดค่าฮาร์ดแวร์ ซอฟต์แวร์ บริการ และเครือข่ายที่ปลอดภัย
- การใช้แนวทางปฏิบัติที่เปิดเผยต่อสาธารณะ (เช่น เทมเพลต (Template) ที่ผู้ขายและองค์กรการรักษาความมั่นคงปลอดภัยอิสระกำหนดไว้ล่วงหน้า)
- พิจารณาระดับการป้องกันที่จำเป็นเพื่อกำหนดระดับการรักษาความมั่นคงปลอดภัยที่เพียงพอ
- สนับสนุนนโยบายการรักษาความมั่นคงปลอดภัยของสารสนเทศขององค์กร นโยบายเฉพาะหัวข้อ มาตรฐาน และข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยอื่น ๆ
- พิจารณาความเป็นไปได้และการบังคับใช้การกำหนดค่าการรักษาความมั่นคงปลอดภัยในบริบทขององค์กร

2.5.10 การลบข้อมูล (Information deletion)

(1) จัดทำขั้นตอนปฏิบัติสำหรับการบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ให้สอดคล้องกับรูปแบบการจัดหมวดหมู่ทรัพย์สินสารสนเทศ

(2) สื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีกต่อไป ควรกำจัดด้วยวิธีที่ปลอดภัยตามขั้นตอนปฏิบัติที่เป็นทางการ

(3) สื่อบันทึกข้อมูลควรได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้งานผิดวัตถุประสงค์ หรือการเกิดความเสียหายในระหว่างการขนส่ง

(4) แนวปฏิบัติการจัดการสื่อบันทึกข้อมูลสำหรับหน่วยงาน

- จัดทำทะเบียนสื่อบันทึกข้อมูล โดยระบุชนิด วันที่ได้มา ข้อมูลที่จัดเก็บ และชื่อผู้รับผิดชอบ
- อนุญาตให้ใช้สื่อบันทึกข้อมูลกับระบบงานที่เกี่ยวข้องเท่านั้น
- กรณีมีความจำเป็นต้องมีการแลกเปลี่ยนข้อมูลที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” ให้ส่งผ่านช่องทางระบบบริการจัดส่งข้อมูล หรือระบบจดหมายอิเล็กทรอนิกส์ของ สคทช.
- ตรวจสอบอายุของสื่อบันทึกข้อมูลสารสนเทศอย่างน้อยปีละ 1 ครั้ง เพื่อให้คงสภาพความสามารถในการจัดเก็บข้อมูลบนอุปกรณ์
- ลงบันทึกวันที่ทำลายสื่อบันทึกข้อมูลลงใน “ทะเบียนสื่อบันทึกข้อมูล” เพื่อใช้เป็นหลักฐานอ้างอิงสำหรับการตรวจสอบในภายหลัง
- ควบคุมและตรวจสอบการถอดถอนหรือทำลายสารสนเทศของ สคทช. ออกจากอุปกรณ์ดังกล่าวเมื่อเลิกใช้งานสื่อบันทึกข้อมูล หรือโอนให้หน่วยงานอื่น หรือจำหน่ายออกจากองค์กร
  - สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่ใช้บันทึกสารสนเทศ ซึ่งหมดอายุการใช้งานแล้วต้องได้รับการทำลายทางกายภาพ หรือทำลาย ลบ เขียนทับข้อมูลโดยใช้หลักการทางเทคนิคที่มั่นใจได้ว่า จะไม่สามารถนำสารสนเทศเดิมกลับมาได้ (Non-Retrievable)
  - สื่อบันทึกข้อมูลอิเล็กทรอนิกส์ที่ใช้บันทึกสารสนเทศ ซึ่งต้องการนำกลับมาใช้ใหม่ต้องได้รับการลบ เขียนทับข้อมูลโดยใช้หลักการทางเทคนิคที่มั่นใจได้ว่าจะไม่สามารถ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

นำสารสนเทศเดิมกลับมาได้ (Non-Retrievable) โดยพิจารณาตามระดับการป้องกันความมั่นคงปลอดภัยของสารสนเทศ

(5) เอกสารที่เป็นกระดาษซึ่งใช้บันทึกสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” เมื่อไม่มีความจำเป็นต้องใช้งานแล้ว ต้องได้รับการทำลายทางกายภาพผ่านทางเครื่องทำลายกระดาษหรือวิธีการอื่นใดที่ทำให้ไม่สามารถเข้าถึงสารสนเทศนั้นได้

(6) ในกรณีที่มีการใช้บริการจากหน่วยงานภายนอกในการทำลายเอกสาร อุปกรณ์สารสนเทศหรือสื่อบันทึกข้อมูล ต้องกำกับดูแลให้หน่วยงานภายนอกปฏิบัติตามข้อตกลงหรือสัญญาการให้บริการ

(7) เมื่อต้องมีการส่งสื่อบันทึกข้อมูลออกไปนอก สคทช. ต้องจัดให้มีการป้องกันข้อมูลที่มีการส่งถึงกันระหว่างสำนักงาน ดังต่อไปนี้

- บรรจุหีบห่ออย่างเหมาะสม และเป็นไปตามคำแนะนำของผู้ผลิต เพื่อป้องกันความเสียหายทางกายภาพที่อาจเกิดขึ้นในช่วงขนส่ง เช่น การถูกความร้อน ความชื้น หรือคลื่นแม่เหล็กไฟฟ้า และอื่น ๆ เป็นต้น
- ป้องกันการเปิดเผยหรือดัดแปลงสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” โดยไม่ได้รับอนุญาต เช่น ใช้บรรจุภัณฑ์ที่มีกุญแจป้องกัน การส่งมอบถึงผู้รับโดยตรง
- ใช้ผู้ส่งที่น่าเชื่อถือ
- กำหนดกระบวนการในการระบุตัวตนของผู้ส่งและจดบันทึกไว้ เช่น แสดงบัตรประจำตัวผู้ปฏิบัติงาน หรือบัตรประจำตัวประชาชน
- จดบันทึกรายละเอียดการจัดส่ง เช่น สิ่งที่จัดส่ง ผู้ส่ง วัน/เวลา หน่วยงานผู้รับ / ผู้รับ / วัน/เวลาที่รับ

(8) แนวปฏิบัติการจัดการสื่อบันทึกข้อมูลสำหรับผู้ปฏิบัติงานและหน่วยงานภายนอก

- ตรวจสอบโปรแกรมไม่พึงประสงค์ก่อนนำสื่อบันทึกข้อมูลมาใช้งาน และตรวจสอบข้อมูลภายในสื่อบันทึกข้อมูลเป็นประจำ
- ใช้สื่อบันทึกข้อมูลกับงานที่เกี่ยวข้องเท่านั้น
- ไม่ใช้สื่อบันทึกข้อมูลกับข้อมูลที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูงสุด” กรณีมีความจำเป็นต้องมีการแลกเปลี่ยนข้อมูล ให้ส่งผ่านช่องทางระบบบริการจัดส่งข้อมูลหรือจดหมายอิเล็กทรอนิกส์ของ สคทช.
- ทำลายข้อมูลภายในสื่อบันทึกข้อมูล เมื่อไม่มีความจำเป็นต้องใช้งานสื่อบันทึกข้อมูลอีกต่อไป

2.5.11 การซ่อนข้อมูล (Data masking)

(1) ให้มีมาตรการการจำกัดการเปิดเผยของข้อมูลที่มีความอ่อนไหว ข้อมูลส่วนบุคคล และเพื่อให้เป็นไปตามกฎหมาย กฎระเบียบ หรือข้อกำหนด และข้อผูกมัดสัญญาที่เกี่ยวข้องกับการลบข้อมูลสารสนเทศ

- ต้องปิดบังข้อมูลเพื่อปกป้องข้อมูลที่มีความอ่อนไหว จากการเข้าถึง และการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต ให้สอดคล้องตามข้อกำหนดทางด้านกฎหมายหรือระเบียบปฏิบัติที่เกี่ยวข้อง
- มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องประกอบด้วยมาตรการเชิงองค์กร (organizational measures) และมาตรการเชิงเทคนิค (technical measures) ที่เหมาะสม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ซึ่งอาจรวมถึงมาตรการทางกายภาพ (physical measures) ที่จำเป็นด้วย โดยคำนึงถึงระดับความเสี่ยงตามลักษณะและวัตถุประสงค์ของการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลส่วนบุคคล ตลอดจนโอกาสเกิดและผลกระทบจากเหตุการณ์ละเมิดข้อมูลส่วนบุคคล

- มาตรการรักษาความมั่นคงปลอดภัยดังกล่าว จะต้องคำนึงถึงการดำเนินการเกี่ยวกับการรักษาความมั่นคงปลอดภัย ตั้งแต่การระบุความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้นกับทรัพย์สินสารสนเทศ (information assets) ที่สำคัญ การป้องกันความเสี่ยงที่สำคัญที่อาจจะเกิดขึ้น การตรวจสอบและเฝ้าระวังภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามและเหตุการละเมิดข้อมูลส่วนบุคคล และการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามหรือเหตุการละเมิดข้อมูลส่วนบุคคลด้วย ทั้งนี้ เท่าที่จำเป็นเหมาะสม และเป็นไปได้ตามระดับความเสี่ยง

2.5.12 การป้องกันการรั่วไหลของข้อมูล (Data leakage prevention)

(1) องค์กรกำหนดนโยบายการรักษาความลับของข้อมูล กำหนดประเภทของข้อมูลที่เป็นความลับและความอ่อนไหว และกำหนดข้อจำกัดในการเข้าถึงและใช้งานข้อมูลเหล่านั้น

(2) องค์กรต้องมีการเข้ารหัสข้อมูลที่เป็นความลับหรือความอ่อนไหวทั้งในระหว่างการจัดเก็บและการส่งผ่าน

(3) องค์กรต้องจัดให้มีการฝึกอบรมพนักงานเกี่ยวกับนโยบายการรักษาความลับของข้อมูลและวิธีการป้องกันการรั่วไหลของข้อมูล

(4) องค์กรต้อง ตรวจสอบและทบทวนมาตรการควบคุม DLP เป็นประจำ เพื่อให้แน่ใจว่ายังคงมีประสิทธิภาพ

2.5.13 การสำรองข้อมูล (Information backup)

(1) สำรองข้อมูล ซอฟต์แวร์ และชุดข้อมูลจำลองระบบ พร้อมทดสอบอย่างสม่ำเสมอตามนโยบายการสำรองข้อมูลที่ตกลงกันไว้

(2) แนวปฏิบัติสำหรับผู้ดูแลระบบ

- จัดทำแผนสำรองข้อมูล ตามความเหมาะสมของระดับการป้องกันความมั่นคงปลอดภัย ดังนี้
  - ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” และ “สูงสุด” ให้จัดทำแผนสำรองข้อมูล และมีการทบทวนแผนทุก 1 ปี
  - ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “ปานกลาง” ให้พิจารณาจัดทำแผนสำรองข้อมูลตามความเหมาะสม
  - ระบบที่มีระดับการป้องกันความมั่นคงปลอดภัย “ต่ำ” ไม่ต้องจัดทำแผนสำรองข้อมูล

(3) จัดทำแผนการทดสอบการสำรองข้อมูลและการกู้คืน เพื่อให้มั่นใจว่าสามารถใช้งานได้ในกรณีฉุกเฉินเมื่อมีความจำเป็น

(4) มีการทดสอบความสามารถในการเรียกคืนข้อมูลที่สำรองไว้บนสื่อบันทึกข้อมูลที่ใช้เฉพาะสำหรับการทดสอบเท่านั้น โดยไม่เขียนทับสื่อบันทึกข้อมูลต้นฉบับ เนื่องจากในกรณีที่กระบวนการสำรองข้อมูลหรือการกลับสู่สภาวะปกติล้มเหลว จะทำให้เกิดความเสียหายหรือสูญหายของข้อมูลที่ไม่สามารถแก้ไขได้

(5) จัดทำขั้นตอนปฏิบัติสำหรับการเฝ้าระวังการสำรองข้อมูลและการจัดการความล้มเหลวของการสำรองข้อมูลตามกำหนดการ เพื่อให้มั่นใจว่าการสำรองข้อมูลเสร็จสมบูรณ์ตามแผนการสำรองข้อมูล

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.5.14 ระบบทดแทน (Redundancy of information processing facilities)

(1) จัดหาและติดตั้งอุปกรณ์ประมวลผลสารสนเทศสำรอง เพื่อบริหารจัดการอุปกรณ์ประมวลผลสารสนเทศให้มีระดับความพร้อมใช้งานที่สอดคล้องกับความต้องการทางธุรกิจ

(2) ทดสอบระบบคู่ขนาน หรือการกู้คืนที่ศูนย์สำรองของระบบที่สำคัญ อย่างน้อยปีละ 1 ครั้ง โดยระบบคู่ขนานหรือระบบที่ศูนย์สำรองสามารถทำหน้าที่แทนระบบหลักได้ตามเป้าหมายในกรณีที่ระบบหลักหยุดทำงาน

2.5.15 การลงบันทึกเหตุการณ์ (Logging)

(1) จัดทำและเก็บรักษาบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ข้อผิดพลาดและเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ และควรทบทวนอย่างสม่ำเสมอ

(2) ป้องกันสิ่งอำนวยความสะดวกในการลงบันทึกเหตุการณ์และข้อมูลบันทึกเหตุการณ์จากการปลอมแปลงและการเข้าถึงโดยไม่ได้รับอนุญาต

(3) ลงบันทึกเหตุการณ์กิจกรรมของผู้ดูแลระบบและผู้ปฏิบัติงาน มีการป้องกันรวมถึงทบทวนอย่างสม่ำเสมอ

(4) กำหนดข้อมูลเวลาของระบบประมวลผลสารสนเทศทั้งหมดให้ตรงกับแหล่งเวลาอ้างอิง

(5) จัดทำและเก็บรักษาบันทึกเหตุการณ์ที่บันทึกกิจกรรมของผู้ใช้งาน ข้อยกเว้น ข้อผิดพลาดและเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยบันทึกเหตุการณ์ (event logs) ประกอบด้วย

- บัญชีผู้ใช้งาน (user IDs)
- วันที่ เวลา และรายละเอียดของเหตุการณ์สำคัญ เช่น เมื่อเข้าสู่ระบบ (Log-on) เมื่อออกจากระบบ (Log-off)
- สิ่งยืนยันตนหรือตำแหน่งของอุปกรณ์ (หากเป็นไปได้) และตัวระบุระบบ
- บันทึกการพยายามเข้าถึงระบบที่ประสบความสำเร็จและถูกปฏิเสธ
- บันทึกการพยายามเข้าถึงข้อมูลและทรัพยากรอื่น ๆ ที่ประสบความสำเร็จและถูกปฏิเสธ
- การเปลี่ยนแปลงการกำหนดค่าระบบ (System Configuration)
- การใช้งานสิทธิพิเศษ
- การเข้าถึงไฟล์และชนิดของการเข้าถึง
- ที่อยู่ของเครือข่าย เช่น IP address, MAC address
- Protocol ที่ใช้งาน
- สัญญาณเตือนภัยที่เกิดขึ้นโดยระบบควบคุมการเข้าถึง
- การเปิดการใช้งาน (Activation) และการระงับการใช้งาน (De-Activation) ของระบบป้องกัน เช่น ระบบป้องกันไวรัส ระบบตรวจจับการบุกรุก (Intrusion Detection System)

(6) กำหนดให้มีรายละเอียดในการบันทึกกิจกรรมการดำเนินงานของเจ้าหน้าที่ที่เกี่ยวข้องกับระบบสารสนเทศ อย่างน้อยดังต่อไปนี้

- เวลาที่เหตุการณ์ได้เกิดขึ้น
- สารสนเทศที่เกี่ยวกับเหตุการณ์ เช่น การจัดการไฟล์ (File) ข้อผิดพลาดอันเกิดจากความผิดพลาดและมีการแก้ไขให้ถูกต้อง
- บัญชีผู้ใช้ ผู้ดูแลระบบ (Administrator) หรือ ผู้ปฏิบัติการ (Operator) ที่เกี่ยวข้อง
- การประมวลผลคอมพิวเตอร์ (Processing) ที่เกี่ยวข้อง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(7) จัดให้มีการป้องกันการเปลี่ยนแปลงแก้ไขข้อมูลบันทึกเหตุการณ์โดยไม่ได้รับอนุญาตและป้องกันปัญหาที่เกิดกับการบันทึกเหตุการณ์ ดังต่อไปนี้

- การเปลี่ยนแปลงแก้ไขประเภทของข้อความ (Message Types) ที่ได้รับการบันทึก
- การแก้ไขหรือลบไฟล์ (File) ข้อมูลบันทึกเหตุการณ์ (Log)
- ข้อผิดพลาดของเหตุการณ์ที่บันทึกหรือการเขียนทับเหตุการณ์ที่บันทึกอันเนื่องมาจากความจุของสื่อที่เก็บไฟล์ (File) บันทึกเหตุการณ์ (Log File) ไม่เพียงพอ

(8) ตรวจสอบและจัดทำรายงานบันทึกเหตุการณ์ อย่างน้อยเดือนละ 1 ครั้ง

(9) เทียบข้อมูลนาฬิกาของระบบประมวลผลสารสนเทศทั้งหมดให้ตรงกับแหล่งเวลาการอ้างอิงโดยใช้ NTP Server ของ สคทช. เพื่อให้เวลาที่ปรากฏในประวัติเหตุการณ์ (Log) ของระบบสารสนเทศถูกต้องตรงกัน และสามารถนำไปใช้ในการตรวจสอบได้

2.5.16 กิจกรรมการเฝ้าติดตาม (Monitoring activities)

(1) เฝ้าติดตามเครือข่าย ระบบ และแอปพลิเคชันเพื่อหาพฤติกรรมที่ผิดปกติและการดำเนินการที่เหมาะสมเพื่อประเมินอุบัติการณ์ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศที่อาจเกิดขึ้น โดยพิจารณาสิ่งต่อไปนี้เพื่อรวมไว้ในระบบเฝ้าติดตาม :

- เครือข่ายขาออกและขาเข้า ระบบและการรับส่งข้อมูลแอปพลิเคชัน
- การเข้าถึงระบบ เซิร์ฟเวอร์ อุปกรณ์เครือข่าย ระบบเฝ้าติดตาม แอปพลิเคชันที่สำคัญ ฯลฯ
- ระบบในระดับวิกฤติหรือระดับผู้ดูแลระบบและไฟล์การกำหนดค่าเครือข่าย
- บันทึกจากเครื่องมือรักษาความปลอดภัย เช่น โปรแกรมป้องกันไวรัส, IDS, ระบบป้องกันการบุกรุก (IPS) ตัวกรองเว็บ ไฟร์วอลล์ การป้องกันข้อมูลรั่วไหล เป็นต้น
- บันทึกเหตุการณ์ที่เกี่ยวข้องกับกิจกรรมของระบบและเครือข่าย
- ตรวจสอบว่ารหัสที่เรียกใช้ได้รับอนุญาตให้เรียกใช้ในระบบและไม่มีการดัดแปลง (เช่น โดยการรวบรวมใหม่เพื่อเพิ่มรหัสที่ไม่ต้องการเพิ่มเติม)
- การใช้ทรัพยากร เช่น CPU ฮาร์ดดิสก์ หน่วยความจำ แบนด์วิดท์ และสมรรถนะ

องค์กรควรกำหนดพื้นฐานของพฤติกรรมปกติและเฝ้าติดตามพื้นฐานนี้เพื่อหาความผิดปกติ เมื่อกำหนดพื้นฐาน ควรพิจารณาสิ่งต่อไปนี้ :

(1) ทบทวนการใช้งานระบบต่าง ๆ ในช่วงเวลาปกติและช่วงพีค

(2) เวลาปกติในการเข้าถึง ตำแหน่งการเข้าถึง ความถี่ในการเข้าถึงสำหรับผู้ใช้แต่ละรายหรือกลุ่มผู้ใช้แต่ละกลุ่ม

2.5.17 การตั้งค่านาฬิกาและเวลาให้ตรงกัน (Clock synchronization)

(1) ต้องควบคุมและดูแลการตั้งเวลาของระบบสารสนเทศให้ตรงกันตามมาตรฐานฯ ที่กำหนดและเป็นไปตามข้อกำหนดทางด้านกฎหมายหรือระเบียบปฏิบัติที่เกี่ยวข้อง

(2) เทียบข้อมูลนาฬิกาของระบบประมวลผลสารสนเทศทั้งหมดให้ตรงกับแหล่งเวลาการอ้างอิงโดยใช้ NTP Server ของ สคทช. เพื่อให้เวลาที่ปรากฏในประวัติเหตุการณ์ (Log) ของระบบสารสนเทศถูกต้องตรงกัน และสามารถนำไปใช้ในการตรวจสอบได้

2.5.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs)

(1) จำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้อย่างเข้มงวด เนื่องจากโปรแกรมประเภทยูทิลิตี้อาจมีความสามารถที่จะเปลี่ยนแปลงแก้ไขมาตรการควบคุมของระบบและโปรแกรมประยุกต์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(2) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

2.5.19 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of software on operational systems)

(1) ควบคุมการติดตั้งซอฟต์แวร์บนระบบให้บริการ

(2) แนวปฏิบัติสำหรับผู้ดูแลระบบ

- ควบคุมการติดตั้งซอฟต์แวร์บนระบบสารสนเทศที่ให้บริการ ให้ดำเนินงานโดยผู้ดูแลระบบที่ได้รับอนุญาต พร้อมทั้งจัดเก็บบันทึกเหตุการณ์ (Audit Log) เพื่อใช้ในการตรวจสอบ

2.5.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)

(1) จัดให้มีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้ หรือกลุ่มของระบบสารสนเทศ เพื่อควบคุมการใช้งานในแต่ละเครือข่ายย่อยได้อย่างเหมาะสม ทั้งนี้การแบ่งแยกเครือข่าย ต้องมีการติดตั้งอุปกรณ์ที่สามารถแบ่งแยกเครือข่ายได้ เช่น Firewall, Switch ที่สามารถแบ่ง VLAN ได้ โดยหลักเกณฑ์การแบ่งแยกเครือข่าย ต้องสอดคล้องกับมาตรฐาน และนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของ สคทช. ในหมวดอื่น ๆ ความต้องการในการเข้าถึงข้อมูล ระดับการป้องกันความมั่นคงปลอดภัยของข้อมูล รวมถึงการพิจารณาด้านราคา ประสิทธิภาพ และผลกระทบทางด้านความปลอดภัย ดังต่อไปนี้

- เครือข่ายที่อนุญาตให้เข้าถึงจากภายนอกกับเครือข่ายที่ใช้ภายใน สคทช. เท่านั้น
- เครือข่ายร่วมกันระหว่างองค์กร
- เครือข่ายแอพพลิเคชัน (Application) ที่มีความสำคัญกับเครือข่ายอื่น ๆ ที่มีความสำคัญน้อยกว่า
- เครือข่ายสำหรับเครื่องให้บริการ (Server Farm) กับเครือข่ายของผู้ใช้งาน
- กำหนดมาตรการควบคุมการใช้งานเครือข่ายไร้สาย ให้สามารถแยกเครื่องคอมพิวเตอร์ดังต่อไปนี้ออกจากกัน
  - เครื่องคอมพิวเตอร์พกพาขององค์กร
  - เครื่องคอมพิวเตอร์พกพาส่วนบุคคล
  - อุปกรณ์ Internet of Things (IoT)

(2) กำหนดหน้าที่ความรับผิดชอบ และขั้นตอนปฏิบัติสำหรับการบริหารจัดการอุปกรณ์เครือข่าย

(3) กำหนดให้มีการแบ่งแยกหน้าที่ความรับผิดชอบของบุคคลในการปฏิบัติงานด้านเครือข่าย

(4) ต้องมีการแบ่งหน้าที่และความรับผิดชอบของด้านการดำเนินงานเครือข่าย ออกจากการดำเนินงานระบบ ICT ที่เหมาะสม (ตามมาตรการข้อ 1.3)

(5) จัดให้มีมาตรการควบคุมพิเศษสำหรับการรักษาความลับ (Confidentiality) และความสมบูรณ์ (Integrity) ของข้อมูลที่ส่งผ่านเครือข่ายสาธารณะหรือเครือข่ายไร้สาย และสำหรับป้องกันระบบและแอปพลิเคชันที่เชื่อมต่อกับเครือข่าย เช่น การเข้ารหัสข้อมูล นอกจากนี้ให้พิจารณานำมาตรการควบคุมพิเศษมาใช้สำหรับดูแลรักษาความพร้อมใช้งาน (Availability) ของการให้บริการเครือข่ายและคอมพิวเตอร์ที่เชื่อมต่อกับเครือข่าย เช่น มีเส้นทางสำรอง

(6) กำหนดให้มีการลงบันทึกเหตุการณ์และมีการเฝ้าระวังอย่างเหมาะสม เพื่อบันทึกและตรวจหาการกระทำที่อาจส่งผลกระทบหรือเกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(7) ติดตามผลอย่างสม่ำเสมอว่า ผู้ให้บริการเครือข่ายสามารถจัดการงานบริการได้อย่างปลอดภัย เป็นไปตามข้อตกลง และมีข้อตกลงที่ให้สิทธิ์กับ สคทช. ในการตรวจประเมินการดำเนินงานของผู้ให้บริการเครือข่าย

(8) ควบคุมดูแลให้ระบบเครือข่ายมีคุณลักษณะด้านความมั่นคงปลอดภัยของการให้บริการเครือข่าย เช่น

- มีเทคโนโลยีที่นำมาใช้รักษาความมั่นคงปลอดภัยของการให้บริการเครือข่าย เช่น การพิสูจน์และยืนยันตัวตน การเข้ารหัสข้อมูล และการควบคุมการเชื่อมต่อเครือข่าย
- การจัดหาอุปกรณ์และการพัฒนาระบบสารสนเทศ ต้องสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยของการให้บริการเครือข่าย
- กำหนดขั้นตอนปฏิบัติในการใช้บริการเครือข่าย สำหรับควบคุมการเข้าถึงการให้บริการเครือข่ายหรือระบบสารสนเทศตามความจำเป็น

(9) มีการจำกัดสิทธิ์การเข้าถึงช่องเชื่อมต่อสำหรับตั้งค่าการทำงาน (Console Port) ด้วยวิธีการพิสูจน์และยืนยันตัวตน

(10) มีการจำกัดช่องทางการเชื่อมต่อโดยอุปกรณ์เครือข่าย เช่น Firewall, Router ไม่ให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉิน ซึ่งต้องได้รับการอนุญาตจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายหรือเทียบเท่าขึ้นไป

(11) ต้องจัดการและควบคุมดูแลให้เครือข่ายปลอดภัยจากภัยคุกคาม และรักษาความปลอดภัยของระบบงานที่ใช้เครือข่าย ตลอดจนข้อมูลสารสนเทศที่ส่งผ่าน ตามมาตรฐานฯ ที่กำหนด

(12) จัดทำข้อกำหนดด้านความมั่นคงปลอดภัยของการให้บริการเครือข่าย และดำเนินงานให้สอดคล้องกับข้อกำหนดดังกล่าว

(13) มีการจำกัดช่องทางการเชื่อมต่อของระบบไปยังเครือข่าย โดยต้องถูกกำหนดให้ใช้เฉพาะที่จำเป็น เช่น การเข้าถึงระบบสารสนเทศที่สำคัญขององค์กร ต้องเข้าถึงได้เฉพาะอินทราเน็ต (Intranet) เท่านั้น

(14) ควรใช้ข้อมูลแสดงตัวตนและรายละเอียดอุปกรณ์เป็นส่วนหนึ่งของการพิสูจน์ตัวตนในการเชื่อมต่อระบบเครือข่าย

(15) ต้องควบคุมการเชื่อมต่อเข้าสู่ระบบ เพื่อการตรวจสอบหรือแก้ไขการติดตั้งค่าพารามิเตอร์ของอุปกรณ์ ให้สามารถเข้าถึงได้เมื่อได้รับการอนุมัติเท่านั้น

(16) ควรมีการควบคุมเส้นทางในระบบเครือข่าย (Network routing) เพื่อให้มั่นใจว่าการเชื่อมต่อผ่านทางระบบเครือข่ายและการรับส่งข้อมูลสารสนเทศไปยังจุดหมายปลายทางถูกต้อง

(17) ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของ สคทช. และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

2.5.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)

(1) ต้องกำหนดคุณสมบัติด้านความปลอดภัย ระดับการให้บริการ และข้อกำหนดการบริหารเครือข่าย ทั้งของหน่วยงานภายในที่ให้บริการเครือข่ายและหน่วยงานภายนอกที่ให้บริการเครือข่าย

(2) เครือข่ายสารสนเทศแบบใช้สาย (Wired LAN) ต้องควบคุมการเชื่อมต่อให้เฉพาะอุปกรณ์ที่ลงทะเบียนเท่านั้น

(3) เครือข่ายสารสนเทศแบบไร้สาย (Wireless LAN) ต้องควบคุมการเชื่อมต่อให้เฉพาะเครื่องที่ผ่านการพิสูจน์และยืนยันตัวตนเท่านั้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(4) ระงับบัญชีผู้ใช้งานเครือข่ายที่ไม่เปลี่ยนรหัสผ่าน ภายในระยะเวลา 3 เดือน
(5) เพิกถอนบัญชีผู้ใช้งานเครือข่าย เมื่อสิ้นสุดระยะเวลาที่ขอใช้งานหรือสิ้นสุดการจ้างงาน
(6) ระบุข้อตกลงด้านความมั่นคงปลอดภัยที่จำเป็นสำหรับแต่ละการให้บริการ ตามคุณลักษณะด้านความมั่นคงปลอดภัย ระดับการให้บริการ และข้อกำหนดของฝ่ายบริหาร เช่น ข้อตกลง Service Level Agreement (SLA)
(7) ตั้งค่าอุปกรณ์เครือข่าย โดยจำกัดสิทธิ์การเข้าถึงช่องเชื่อมต่อสำหรับตั้งค่าการทำงาน (Console Port) ด้วยวิธีการพิสูจน์และยืนยันตัวตน
(8) ตั้งค่า (Configuration) อุปกรณ์เครือข่าย เช่น Firewall, Router ไม่ให้สามารถบริหารจัดการจากภายนอกเครือข่ายได้ เว้นแต่ในกรณีฉุกเฉิน ซึ่งต้องได้รับการอนุญาตจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายหรือเทียบเท่าขึ้นไป

2.5.22 การแบ่งแยกเครือข่าย (Segregation of networks)

(1) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้
- Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
- Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศภายใน

(2) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ 1 ครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
(3) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ไฟล์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

2.5.23 การกรองเว็บ (Web filtering)

(1) กำหนดให้มีการบริหารจัดการควบคุมการเข้าถึงเว็บไซต์ภายนอก ตามความเหมาะสมความจำเป็นทางธุรกิจ และเพื่อป้องกันการเข้าถึงข้อมูลที่มีเนื้อหาที่เป็นอันตราย
(2) แนวปฏิบัติสำหรับหน่วยงาน
- ควรลดความเสี่ยงจากการที่บุคลากรเข้าถึงเว็บไซต์ที่มีสารสนเทศผิดกฎหมาย หรือทราบกันว่ามีไวรัสหรือเนื้อหาสาระฟิชชิ่ง เทคนิคเพื่อให้บรรลุงานนี้โดยการบล็อกที่อยู่ IP หรือโดเมนของเว็บไซต์ต่าง ๆ ที่เกี่ยวข้อง เบราว์เซอร์และเทคโนโลยีป้องกันมัลแวร์บางตัวทำเรื่องนี้โดยอัตโนมัติหรือสามารถกำหนดค่าให้ทำเช่นนั้นได้
- ควรระบุประเภทของเว็บไซต์ที่บุคลากรควรหรือไม่ควรเข้าถึง องค์กรควรพิจารณาบล็อกการเข้าถึงเว็บไซต์ประเภทต่อไปนี้ :
  - เว็บไซต์ที่มีฟังก์ชันอัปโหลดสารสนเทศเว้นแต่จะได้รับอนุญาตเพื่อเหตุผลทางธุรกิจที่ถูกต้อง
  - เว็บไซต์ที่มุ่งร้ายที่ทราบอยู่แล้วหรือน่าสงสัย (เช่น เว็บไซต์ที่กระจายมัลแวร์หรือข้อมูลฟิชชิ่ง)
  - เว็บไซต์มุ่งร้ายที่ได้มาจากข่าวกรองด้านภัยคุกคาม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- เว็บไซต์แบ่งปันข้อมูลที่ผิดกฎหมาย

2.5.24 การเข้ารหัสข้อมูล (Use of cryptography)

(1) จัดทำและนำนโยบายการใช้มาตรการ การเข้ารหัสข้อมูลไปสู่การปฏิบัติ

(2) จัดทำและนำนโยบายการใช้งาน การป้องกัน และอายุการใช้งานของกุญแจสำหรับการเข้ารหัสข้อมูลตลอดวงจรชีวิตของกุญแจดังกล่าวไปสู่การปฏิบัติ

(3) มาตรการ การเข้ารหัสข้อมูล แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

- จัดให้มีการเข้ารหัสข้อมูล โดยพิจารณาตามระดับการป้องกันความมั่นคงปลอดภัย
- จัดทำบัญชีการใช้งานการเข้ารหัส

(4) มาตรการการใช้กุญแจสำหรับการเข้ารหัสข้อมูล แนวปฏิบัติสำหรับผู้ดูแลระบบและผู้พัฒนาระบบ

- ในระบบที่มีความสำคัญ ต้องจัดเก็บกุญแจคู่ (Key Pair) ในการเข้ารหัสแบบอสมมาตร (Asymmetric Encryption) หรือ กุญแจลับ (Secret Keys) ในการเข้ารหัสแบบสมมาตร (Symmetric Encryption) ด้วยวิธีการที่ปลอดภัย เช่น เก็บแยกในเครื่องอื่นหรืออุปกรณ์อื่นที่มีการควบคุมการเข้าถึงที่อย่างแน่นหนา หรือเก็บในสื่อที่เคลื่อนย้ายได้ที่มีกุญแจป้องกันอย่างแน่นหนา
- จัดเก็บกุญแจสาธารณะ (Public Kes) ในเครือข่ายกลาง ซึ่งสามารถเข้าถึงโดยผู้ที่ได้รับอนุญาตเท่านั้น
- จัดเก็บกุญแจหลัก (Master Keys) กุญแจของผู้ดูแลระบบ (Administrators' Keys) หรือกุญแจฉุกเฉิน (Emergency Keys) ในสื่อที่แยกกันและมีการควบคุมการเข้าถึงที่เข้มงวด
- บริหารจัดการกุญแจเข้ารหัสข้อมูล โดยมีการแบ่งแยกหน้าที่ ดังนี้
  - ในการเบิกหรือใช้งานกุญแจหลัก (Master Keys) ต้องกระทำโดยบุคคลตั้งแต่สองคนขึ้นไป
  - บุคคลเดียวกัน ต้องไม่สามารถสร้างและเปิดการใช้งาน (Activate) กุญแจชุดเดียวกัน

(5) ผู้ดูแลระบบหรือผู้พัฒนาระบบทำหน้าที่สร้างกุญแจในการเข้ารหัส และส่งมอบกุญแจเข้ารหัสอย่างมั่นคงปลอดภัยให้กับเจ้าของกุญแจเท่านั้น

(6) เรียกคืนหรือทำลายกุญแจส่วนบุคคล (Private Keys) และกุญแจลับ (Secret Keys) ในกรณีต่อไปนี้

- ผู้ใช้งานพ้นสภาพการเป็นผู้ปฏิบัติงานของ สคทช.
- ผู้ใช้งานไม่มีความจำเป็นต้องใช้กุญแจ
- กุญแจถูกทำลายหรือล้าสมัยแล้ว
- กุญแจถูกล่วงรู้โดยบุคคลอื่น หรือกุญแจสูญหาย

(7) สร้างกุญแจส่วนบุคคล (Private Keys) หรือกุญแจลับ (Secret Keys) ใหม่ ในกรณีต่อไปนี้

- กุญแจถูกทำลายหรือล้าสมัยแล้ว
- กุญแจถูกล่วงรู้โดยบุคคลอื่น หรือกุญแจสูญหาย

(8) กำหนดกระบวนการในการกู้คืนกุญแจ เพื่อลดความเสี่ยงในการสูญหาย หรือเสียหายของกุญแจ

(9) กำหนดอายุการใช้งานของกุญแจ เพื่อให้กุญแจนั้นถูกใช้ในช่วงเวลาที่จำกัด เช่น

- กุญแจหลัก (Master Keys) ควรเปลี่ยนแปลงทุก ๆ 1 ปี หรือเป็นไปตามที่เจ้าของผลิตภัณฑ์แนะนำ
- กุญแจที่ใช้เข้ารหัสกุญแจ เช่น การใช้กุญแจส่วนบุคคล (Private Keys) เข้ารหัสกุญแจลับ (Secret Keys) ควรเปลี่ยนแปลงอย่างน้อยทุก ๆ 6 เดือน หรือเป็นไปตามที่เจ้าของผลิตภัณฑ์แนะนำ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(10) แนวปฏิบัติสำหรับผู้ปฏิบัติงาน

- ผู้ปฏิบัติงานที่เกี่ยวข้องกับระบบการเข้ารหัส (Cryptographic) ต้องไม่ส่งกุญแจส่วนบุคคล (Private Keys) ไปยังผู้อื่น
- พิสูจน์และยืนยันตัวตนของเจ้าของกุญแจสาธารณะ (Public Keys) โดยแบบการยืนยันโดยตรงจากผู้ส่ง หรือการยืนยันในรูปแบบของใบรับรองกุญแจจาก Certification Authority (CA) ที่เชื่อถือได้
- ทดสอบความถูกต้องของกุญแจที่รับผิดชอบก่อนที่จะใช้งานจริง เช่น ทดสอบการส่งข้อความที่มีการเข้ารหัส ทดสอบการเข้ารหัสและการถอดรหัสไฟล์
- เก็บกุญแจส่วนบุคคล (Private Keys) ในสถานที่ที่ปลอดภัย ซึ่งควรจัดเก็บในอุปกรณ์สารสนเทศที่สามารถเคลื่อนย้ายได้ เช่น Token, Smart Card
- ในกรณีที่พบว่ากุญแจถูกล่วงรู้โดยบุคคลอื่น ต้องแจ้ง IT Services หรือ ฝ่ายที่เกี่ยวข้อง ทันที

2.5.25 วงจรการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure development life cycle)

(1) จัดทำขั้นตอนปฏิบัติสำหรับการดำเนินงานไว้เป็นลายลักษณ์อักษร และพร้อมให้ผู้ใช้งานทุกคนที่ต้องการนำไปใช้งานได้

(2) แยกระบบสำหรับการพัฒนา การทดสอบ และให้บริการออกจากกัน เพื่อลดความเสี่ยงในการเข้าถึงหรือเปลี่ยนแปลงแก้ไขต่อระบบสำหรับให้บริการโดยไม่ได้รับอนุญาต

(3) ต้องมีการผนวกการรักษาความมั่นคงปลอดภัยเข้าเป็นส่วนหนึ่งของวงจรการพัฒนาระบบสารสนเทศ (Security embedded into SDLC) โดยกำหนดกิจกรรมด้านการวิเคราะห์ วางแผน หรือสร้างมาตรการรักษาความมั่นคงปลอดภัยในแต่ละระยะ (Phase) ของวงจรการพัฒนาระบบสารสนเทศ และสอดคล้องกับ วงจรการพัฒนาระบบสารสนเทศขององค์กร

(4) ต้องมีการกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศที่ต้องการพัฒนา

- การตรวจสอบความถูกต้องของข้อมูลนำเข้า (Input data validation)
  - ต้องพัฒนาระบบให้มีการตรวจสอบความถูกต้องของข้อมูลนำเข้าตามมาตรฐานฯ ที่กำหนด เพื่อให้มั่นใจว่าข้อมูลมีความถูกต้องก่อนนำเข้าสู่ระบบ
- การตรวจสอบความถูกต้องของการประมวลผล (Control of internal processing)
  - ต้องพัฒนาระบบให้มีการควบคุมการประมวลผล ตามมาตรฐานฯ ที่กำหนดเพื่อป้องกันการแก้ไข หรือเปลี่ยนแปลงข้อมูลจากผู้ไม่ได้รับอนุญาต
- การตรวจสอบความถูกต้องของข้อความ (Message integrity)
  - ต้องพัฒนาระบบให้มีการตรวจสอบความถูกต้องของข้อความที่รับส่งในระบบหรือระหว่างระบบสารสนเทศ เพื่อให้สามารถตรวจสอบได้ว่าเป็นข้อความต้นฉบับที่ถูกต้อง รวมทั้งควบคุม เพื่อป้องกันการเปลี่ยนแปลงหรือแก้ไขข้อความ/ข้อมูลโดยผู้ที่ไม่ได้รับอนุญาต
- การตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ (Output data validation)
  - ต้องพัฒนาระบบให้มีการควบคุม และตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ให้เป็นไปตามมาตรฐานฯ ที่กำหนด เพื่อให้มั่นใจว่าผลลัพธ์ของการประมวลผลมีความถูกต้อง รวมทั้งควรจัดเก็บบันทึกเหตุการณ์ที่มาของข้อมูลผลลัพธ์ (Result logging) อย่างเพียงพอต่อการตรวจสอบ กรณีเกิดเหตุการณ์ที่ส่งผลต่อความปลอดภัยสารสนเทศ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(5) สำหรับระบบสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ (เช่น อินเทอร์เน็ต) ควรทำการประเมินความเสี่ยง
(6) วางแผนแก้ไขความเสี่ยง
(7) ควรใช้หลักการออกแบบระบบสารสนเทศโดยคำนึงถึงความมั่นคงปลอดภัย (Secure Software Development Principles)
(8) การพัฒนาซอฟต์แวร์ และ/หรือการเขียนโปรแกรมต้องใช้วิธีการที่มั่นคงปลอดภัย (Secure Coding)
(9) ในระหว่างการออกแบบการพัฒนาระบบสารสนเทศ ต้องมีการกำหนดจุดตรวจสอบด้านความมั่นคงปลอดภัย (Security Checkpoint) เพื่อตรวจสอบให้มั่นใจว่ามาตรการการรักษาความมั่นคงปลอดภัย (Controls) จะถูกพัฒนาขึ้นเพื่อตอบสนองต่อความต้องการด้านความมั่นคงปลอดภัยที่ได้กำหนดไว้ เช่น ดำเนินการทบทวน Source Code (Security Code Review) ก่อนเข้าสู่กระบวนการทดสอบซอฟต์แวร์
(10) ปัญหาที่พบในขั้นตอนการพัฒนาซึ่งอาจส่งผลต่อความมั่นคงปลอดภัย ต้องถูกแจ้งไปยังผู้จัดการโครงการ หรือหัวหน้างาน และต้องได้รับการแก้ไขและบันทึกไว้ทุกกรณี
(11) ผู้พัฒนาระบบสารสนเทศต้องได้รับการอบรมความรู้ด้านการพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย และ/ หรือความรู้เกี่ยวกับภัยคุกคามด้านความมั่นคงปลอดภัยสารสนเทศเป็นประจำทุกปี

2.5.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements)

(1) กำหนดแนวทางการพัฒนาซอฟต์แวร์ที่ปลอดภัย (Secure Software Development Lifecycle - SSDLC): SSDLC เป็นแนวทางการพัฒนาซอฟต์แวร์ที่ให้ความสำคัญกับความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนา

2.5.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)

(1) ต้องกำหนดหลักการวิศวกรรมระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure System Engineering Principles) ขึ้นเพื่อให้ระบบสารสนเทศมีความน่าเชื่อถือ มีระดับของการรักษาความมั่นคงปลอดภัยที่เหมาะสม และสามารถตอบสนองต่อความต้องการของแผนกลยุทธ์ของหน่วยงานได้ หลักการดังกล่าวต้องได้รับการนำไปใช้งานร่วมกับวงจรการพัฒนาระบบสารสนเทศของหน่วยงาน (SDLC) และประกอบด้วยประเด็นพื้นฐานที่ต้องได้รับการพิจารณาในระหว่างการออกแบบ สร้าง หรือพัฒนาระบบสารสนเทศ ดังต่อไปนี้
   - การออกแบบระบบสารสนเทศให้มีความมั่นคงปลอดภัย (Security by design)
   - มาตรการรักษาความมั่นคงปลอดภัย ต้องได้รับการพิจารณาและกำหนดตั้งแต่ช่วงแรกของการระบุความต้องการในการพัฒนาระบบสารสนเทศ (Requirements Development Phase) และถือเป็นส่วนหนึ่งของการออกแบบระบบในภาพรวม ในกรณีที่มีการปรับเปลี่ยนความต้องการของระบบ ต้องมีการพิจารณาปรับเปลี่ยนหรือเพิ่มเติมมาตรการรักษาความมั่นคงปลอดภัยให้มีความสอดคล้องกับความต้องการที่เปลี่ยนแปลงไปเสมอ
   - การสร้างสมดุลระหว่างความเสี่ยงและมาตรการรักษาความมั่นคงปลอดภัย (Balance risk and control)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- มาตรการรักษาความมั่นคงปลอดภัยที่เลือกใช้ต้องมีระดับความเข้มงวดที่เหมาะสมกับความเสี่ยง ค่าใช้จ่าย วัตถุประสงค์ทางธุรกิจ และประสิทธิผลของการใช้งานระบบสารสนเทศ เพื่อป้องกันปัญหาการเลือกใช้งานมาตรการรักษาความมั่นคงปลอดภัยที่ไม่เหมาะสม (เช่น เข้มงวดน้อยเกินไป หรือเข้มงวดมากเกินไปจนทำให้ค่าใช้จ่ายสูงเกินกว่าประโยชน์ที่ได้รับ)
- ความเหมาะสมในการใช้งานและการบริหารจัดการ (Usability and manageability)
- มาตรการรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบให้ใช้งานง่ายและไม่เป็นภาระต่อผู้ใช้งานมากเกินไป การบริหารจัดการมาตรการรักษาความมั่นคงปลอดภัย (เช่น การแก้ไขค่าการปรับแต่ง) ต้องไม่ซับซ้อนเกินความจำเป็นจนอาจก่อให้เกิดข้อผิดพลาดได้โดยง่าย
- การใช้มาตรการรักษาความมั่นคงปลอดภัยหลายชั้น (Defense-in-depth)
- ต้องมีการวางมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศไว้หลายชั้น (Multi-layered) โดยครอบคลุมมาตรการรักษาความมั่นคงปลอดภัยทางกายภาพ (Physical) และทางตรรกะ (Logical) ทั้งในระดับระบบปฏิบัติการ ฐานข้อมูล แอพลิเคชั่น และระบบเครือข่าย เพื่อให้สามารถทำงานสอดประสานและทดแทนกันได้ ในเวลาที่มาตรการใดมาตรการหนึ่งทำงานผิดพลาดหรือถูกข้ามผ่านได้
- การลดความซับซ้อน (Simplicity)
- ระบบต้องได้รับการออกแบบให้มีความซับซ้อนน้อยที่สุด เพื่อลดองค์ประกอบที่ไม่จำเป็น ข้อผิดพลาดที่อาจเกิดขึ้น และโอกาสในการถูกโจมตีโดยผู้ไม่ประสงค์ดี
- การสร้างความสามารถในการต้านทานภัยคุกคามและการฟื้นสภาพ (Resilience and Recoverability)
- ระบบต้องได้รับการออกแบบให้มีความสามารถในการต้านทานภัยคุกคาม (เช่น เมื่อมาตรการรักษาความมั่นคงปลอดภัยทำงานผิดพลาดหรือถูกข้ามผ่าน ระบบต้องจำกัดหรือปฏิเสธการเข้าใช้งาน ไม่ใช่ยอมให้เข้าใช้งานได้) และมีความสามารถในการฟื้นสภาพ (Recoverability) (โดยอัตโนมัติ หรือโดยการสร้างกระบวนการกู้คืน) ภายในระยะเวลาที่เหมาะสมกับความต้องการทางธุรกิจ
- การปกป้องข้อมูล (Confidentiality and integrity) ต้องมีการสร้างมาตรการรักษาความมั่นคงปลอดภัยเพื่อปกป้องความลับและความถูกต้องและสมบูรณ์ครบถ้วนของข้อมูล ทั้งในระหว่างการประมวลผล การรับ - ส่ง และการจัดเก็บข้อมูล
- การบังคับใช้นโยบาย (Enforced policy)
- มาตรการรักษาความมั่นคงปลอดภัยต้องได้รับการออกแบบเพื่อบังคับใช้นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ ตลอดจนขั้นตอนปฏิบัติงาน มาตรฐาน หรือแนวปฏิบัติด้านความมั่นคงปลอดภัยที่เกี่ยวข้องขององค์กร
- การออกแบบระบบสารสนเทศเพื่อรับมือต่อผู้ไม่ประสงค์ดีหรือการออกแบบระบบสารสนเทศเพื่อรับมือต่อผู้ไม่ประสงค์ดีหรือการใช้งานในสภาพแวดล้อมที่ไม่พึงประสงค์ (Design for malicious actor/environment)
- ต้องมีการออกแบบมาตรการรักษาความมั่นคงปลอดภัยเชิงป้องกัน ตรวจจับ และกู้คืน โดยพิจารณาในมุมมองของผู้ไม่ประสงค์ดีที่ไม่ได้อยู่ภายใต้กรอบของนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศขององค์กร หรือพยายามข้ามผ่านมาตรการรักษา

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ความมั่นคงปลอดภัยที่มีอยู่ และต้องสร้างมาตรการรักษาความมั่นคงปลอดภัยในกรณีที่จำเป็นต้องใช้งานระบบในสภาพแวดล้อมที่ไม่พึงประสงค์ (เช่น การใช้งานระบบในระหว่างเกิดเหตุฉุกเฉินหรือภัยพิบัติ)

- การออกแบบระบบสารสนเทศเพื่อรองรับการใช้งานแบบโมบาย (Mobility)
- ต้องมีการออกแบบหรือปรับแต่งมาตรการรักษาความมั่นคงปลอดภัยให้เหมาะสม สำหรับระบบสารสนเทศที่ให้บริการหรือทำงานร่วมกับอุปกรณ์โมบาย โดยคำนึงถึงความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง (เช่น การควบคุมความมั่นคงปลอดภัยทางกายภาพ การใช้งานอุปกรณ์โมบายที่เป็นทรัพย์สินส่วนบุคคล การใช้งานเครือข่าย การใช้งานโมบายแอพลิเคชัน การแลกเปลี่ยนข้อมูล การใช้งานฟังก์ชันด้านการระบุตำแหน่งที่อยู่)

2.5.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure coding)

(1) หน่วยงานที่ดูแลรับผิดชอบ หรือหน่วยงานที่จ้างหน่วยงานภายนอกพัฒนาซอฟต์แวร์ ต้องกำหนดสิทธิ์ในการเข้าถึง เปลี่ยนแปลง และแก้ไขโปรแกรมต้นฉบับ (Source code) ให้เข้าถึงได้ เท่าที่จำเป็นสำหรับผู้ที่มีหน้าที่ในการปฏิบัติงานเท่านั้น เพื่อควบคุมให้การพัฒนาซอฟต์แวร์เป็นไปตามมาตรฐานฯ ที่กำหนด

(2) หน่วยงานที่ดูแลรับผิดชอบ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัย ระหว่างการออกแบบ และการพัฒนาระบบ เพื่อให้มั่นใจว่าความต้องการด้านความมั่นคงปลอดภัยได้มีการพัฒนาตามที่ได้กำหนดไว้

(3) ให้มีการกำหนดหลักการเขียนโค้ดที่มั่นคงปลอดภัยในการพัฒนาซอฟต์แวร์ (Secure Coding) เพื่อตรวจสอบให้แน่ใจว่ามีการเขียนซอฟต์แวร์อย่างมั่นคงปลอดภัยโดยลดจำนวนช่องโหว่ด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศที่อาจเกิดขึ้น

2.5.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาระบบและการยอมรับ (Security testing in development and acceptance)

(1) ให้มีการกำหนดข้อมูลในการทดสอบระบบ พิจารณาเลือกชุดข้อมูลที่นำมาใช้ในการทดสอบระบบงานอย่างระมัดระวัง และกำหนดมาตรการควบคุมความมั่นคงปลอดภัยของข้อมูลและปกป้องความเป็นส่วนตัวของข้อมูลส่วนบุคคล รวมถึงกำหนดให้มีผู้ตรวจประเมินการทดสอบระบบ เพื่อป้องกันปัญหาที่อาจเกิดขึ้นกับระบบ

(2) ระบบสำหรับการทดสอบต้องจำลองมาจากระบบที่ใช้งานจริง โดยต้องให้มีความคล้ายคลึงกันมากที่สุด

(3) ในการเข้าถึงระบบสำหรับการทดสอบ ผู้ปฏิบัติงานต้องใช้บัญชีผู้ใช้งานที่แตกต่างจากระบบที่ใช้งานจริง และต้องมีข้อความหรือสัญลักษณ์ที่แสดงประเภทของระบบอย่างชัดเจน เพื่อลดความเสี่ยงจากการผิดพลาดในการเข้าถึงระบบ

(4) นำสำเนาของโปรแกรมต้นฉบับ (Source Code) ล่าสุดที่ใช้ในระบบที่ให้บริการจริง มาจำลองบนระบบสำหรับการทดสอบ ก่อนทำการเปลี่ยนแปลงและแก้ไขบนระบบที่ให้บริการจริง

2.5.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)

(1) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(2) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับโปรแกรมต้นฉบับในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(3) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(4) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(5) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

(6) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องลงนามในสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

(7) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(8) ให้มีการระบุรายละเอียดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ ผนวกรวมเข้ากับการบริหารจัดการโครงการที่เกี่ยวข้องกับระบบสารสนเทศ

2.5.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง (Separation of development, test and production environments)

(1) ควบคุมให้มีการแยกระบบสำหรับการพัฒนา และระบบสำหรับการทดสอบ ออกจากระบบที่ใช้งานจริง เพื่อป้องกันปัญหาที่อาจมีผลกระทบกับข้อมูล หรือการประมวลผลของระบบที่ใช้งานจริง โดยต้องจัดให้มีการควบคุม ดังต่อไปนี้

- จัดทำขั้นตอนการปฏิบัติสำหรับการย้ายโปรแกรมคอมพิวเตอร์ จากระบบสำหรับการพัฒนา หรือระบบสำหรับการทดสอบ ไปยังระบบที่ใช้งานจริง
- ในการแยกระบบออกจากกัน ต้องมีการแยกการทำงานแบบกายภาพ (Physical) เช่น การแยกเครื่องคอมพิวเตอร์แม่ข่าย การแยกระบบสำหรับการพัฒนาหรือระบบสำหรับการทดสอบออกจากเครื่องคอมพิวเตอร์แม่ข่ายระบบที่ใช้งานจริง ทั้งนี้ในกรณีที่ไม่สามารถทำได้เนื่องจากมีข้อจำกัด ต้องทำการแยกการทำงานแบบตรรกะ (Logical) เช่น แยก Directories, แยก Logical Partition ออกจากกัน
- ระบบสำหรับการทดสอบต้องจำลองมาจากระบบที่ใช้งานจริง โดยต้องให้มีความคล้ายคลึงกันมากที่สุด

(2) ในการเข้าถึงระบบสำหรับการทดสอบ ผู้ปฏิบัติงานต้องใช้บัญชีผู้ใช้งานที่แตกต่างจากระบบที่ใช้งานจริง และต้องมีข้อความหรือสัญลักษณ์ที่แสดงประเภทของระบบอย่างชัดเจน เพื่อลดความเสี่ยงจากการผิดพลาดในการเข้าถึงระบบ

2.5.32 การบริหารจัดการ การเปลี่ยนแปลง (Change management)

(1) มีมาตรการในการเปลี่ยนแปลงซอฟต์แวร์ ระบบสารสนเทศ ข้อมูลในระบบประมวลผลสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศอย่างเคร่งครัด โดยขั้นตอนในการแจ้งความประสงค์ขอเปลี่ยนแปลงต้องมีการระบุรายละเอียดดังต่อไปนี้

- วัตถุประสงค์ในการเปลี่ยนแปลง
- รายละเอียดการเปลี่ยนแปลง
- ผลกระทบที่อาจเกิดขึ้น รวมทั้งผลกระทบความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศของการเปลี่ยนแปลงนั้น ๆ
- ผู้ขออนุมัติการเปลี่ยนแปลง และผู้อนุมัติการเปลี่ยนแปลง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- (ผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายหรือเทียบเท่าขึ้นไป)
- วันและเวลาที่จะทำการเปลี่ยนแปลง
- การสื่อสารการเปลี่ยนแปลงให้ผู้เกี่ยวข้องรับทราบ
- ขั้นตอนในการถอยกลับ (Fallback Procedure) รวมทั้งหน้าที่ความรับผิดชอบของผู้เกี่ยวข้องในการกู้คืนระบบ ในกรณีที่การเปลี่ยนแปลงไม่เป็นไปตามแผน

(2) ควบคุมให้มีการปรับปรุงเอกสารระบบที่เปลี่ยนแปลงและแก้ไข เช่น เอกสารการออกแบบ คู่มือการปฏิบัติงาน คู่มือการใช้งาน

(3) จัดเก็บข้อมูลบันทึกเหตุการณ์ เมื่อซอฟต์แวร์ ระบบสารสนเทศ ข้อมูลในระบบประมวลผลสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศมีการเปลี่ยนแปลง

2.5.33 ข้อมูลในการทดสอบ (Test information)

(1) การทดสอบจะต้องได้รับอนุมัติจากเจ้าของข้อมูล ก่อนนำข้อมูลในระบบที่ให้บริการจริงมาทดสอบ

(2) ให้มีการแปลงข้อมูลความลับ จากระบบที่ให้บริการจริงก่อนนำมาใช้ทดสอบ และทำลายข้อมูลที่ใช้ทดสอบ หลังสิ้นสุดการทดสอบ เพื่อป้องกันข้อมูลความลับจากระบบที่ให้บริการจริงรั่วไหลระหว่างทดสอบระบบ

(3) ให้มีการควบคุมการเข้าถึงเครื่องทดสอบให้ปลอดภัยเทียบเท่ากับระบบที่ให้บริการจริง

2.5.34 การป้องกันระบบสารสนเทศระหว่างทดสอบในการตรวจประเมิน (Protection of information systems during audit testing)

(1) วางแผนข้อกำหนดและกิจกรรมสำหรับการตรวจสอบระบบให้บริการอย่างรอบคอบ พร้อมทำข้อตกลงเพื่อลดการหยุดชะงักของกระบวนการทางธุรกิจ

(2) การทดสอบในการตรวจประเมินและกิจกรรมการรับประกันอื่น ๆ ที่เกี่ยวข้องกับการตรวจประเมินระบบปฏิบัติการ ต้องมีการวางแผนและตกลงร่วมกันระหว่างผู้ทดสอบและผู้บริหารอย่างเหมาะสม

3. แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร



รูปที่ 3-1: แผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

แผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ มีรายละเอียดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารครอบคลุม 4 ประเด็น ได้แก่

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

1. ป้องกัน (Prevention)

- วัตถุประสงค์ : ลดความเสี่ยงที่จะเกิดเหตุการณ์ภัยคุกคาม
- กิจกรรม :
  - การติดตั้งระบบรักษาความปลอดภัย เช่น ไฟร์วอลล์ ระบบป้องกันไวรัส
  - การสร้างความตระหนักรู้ให้กับบุคลากรเกี่ยวกับภัยคุกคามทางไซเบอร์
  - การทำการสำรวจและทดสอบความปลอดภัยของระบบเป็นประจำ
  - การอัปเดตซอฟต์แวร์และระบบปฏิบัติการให้เป็นปัจจุบันอยู่เสมอ

2. ตรวจจับและวิเคราะห์ (Detection and Analysis)

- วัตถุประสงค์ : ค้นหาและระบุเหตุการณ์ที่ผิดปกติหรือเป็นภัยคุกคาม
- กิจกรรม :
  - การติดตั้งระบบตรวจจับภัยคุกคาม (IDS)
  - การวิเคราะห์ล็อกไฟล์
  - การตรวจสอบกิจกรรมของผู้ใช้ที่ผิดปกติ
  - การตรวจสอบความผิดปกติของระบบเครือข่าย

3. ตอบสนองและควบคุม (Response and Containment)

- วัตถุประสงค์ : ควบคุมสถานการณ์และป้องกันไม่ให้เกิดความเสียหายเพิ่มเติม
- กิจกรรม :
  - การตัดการเชื่อมต่อระบบที่ถูกโจมตี
  - การทำการสำเนาข้อมูลที่เกี่ยวข้อง
  - การวิเคราะห์เชิงลึกเพื่อหาสาเหตุของเหตุการณ์
  - การประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ตำรวจไซเบอร์

4. กู้คืนและปรับปรุง (Recovery and Lessons Learned)

- วัตถุประสงค์ : ฟื้นฟูระบบให้กลับสู่สภาวะปกติและป้องกันไม่ให้เกิดเหตุการณ์ซ้ำ
- กิจกรรม :
  - การกู้คืนข้อมูลที่เสียหาย
  - การแก้ไขช่องโหว่ที่ถูกใช้ในการโจมตี
  - การทบทวนและปรับปรุงแผนรับมือเหตุการณ์
  - การจัดทำรายงานสรุปเหตุการณ์และบทเรียนที่ได้

จากรายละเอียดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสารครอบคลุม 4 ประเด็น ความเชื่อมโยงของแต่ละประเด็น ดังนี้

- ป้องกัน: เป็นขั้นตอนแรกที่สำคัญในการลดความเสี่ยงที่จะเกิดเหตุการณ์
- ตรวจจับและวิเคราะห์: ต่อเนื่องจากขั้นตอนการป้องกัน หากมีเหตุการณ์เกิดขึ้น ระบบตรวจจับจะทำหน้าที่ระบุและวิเคราะห์เหตุการณ์
- ตอบสนองและควบคุม: เมื่อตรวจพบเหตุการณ์แล้ว จะต้องดำเนินการตอบสนองและควบคุมสถานการณ์โดยเร็ว
- กู้คืนและปรับปรุง: เป็นขั้นตอนสุดท้ายที่สำคัญ เพื่อให้มั่นใจว่าองค์กรจะสามารถฟื้นตัวจากเหตุการณ์ได้อย่างรวดเร็ว และป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนการรับมือภัยคุกคามทางไซเบอร์เป็นวงจรที่ต่อเนื่องกัน โดยแต่ละขั้นตอนมีความสำคัญและเชื่อมโยงกัน หากองค์กรมีการวางแผนและปฏิบัติตามขั้นตอนเหล่านี้ จะสามารถลดความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ ทั้งนี้จะมีการจัดการฝึกซ้อมเพื่อจำลองเหตุการณ์ภัยคุกคามจริง เพื่อเตรียมความพร้อมและประเมินความสามารถของทีมในการตอบสนอง

3.1 บทนำแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Management Plan) ได้รับการพัฒนาขึ้นเพื่อให้เกิดทิศทางและเน้นการจัดการภัยคุกคามทางไซเบอร์สารสนเทศที่ส่งผลกระทบต่อหน่วยงาน ทรัพยากรสารสนเทศ (Information Resources) แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน ใช้กับบุคคลหรือนิติบุคคลใด ๆ ที่ประกาศใช้โดยผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงานกับการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศในหน่วยงาน และโดยเฉพาะเหตุการณ์ที่ส่งผลกระทบต่อหน่วยงาน ทรัพยากรสารสนเทศ

วัตถุประสงค์ของแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ คือ เพื่อให้ของหน่วยงานสามารถตอบสนองต่อภัยคุกคามทางไซเบอร์สารสนเทศได้อย่างรวดเร็วและเหมาะสม

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์นี้ไม่ใช้กับเหตุการณ์ที่เกิดจากภัยธรรมชาติไฟฟ้าขัดข้อง ฯลฯ

3.1.1 ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

ตัวชี้วัดของแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร ครอบคลุมเรื่องการทบทวนแผน การฝึกซ้อมแผน ซึ่งมีรายละเอียดของเป้าหมายและวิธีวัดผล ดังนี้

1. ตัวชี้วัดด้านการทบทวนแผน (Plan Review Metrics)

1.1 ความถี่ในการทบทวนแผน (Plan Review Frequency)

- เป้าหมาย : ทบทวนแผนไม่น้อยกว่า 1 ครั้งต่อปี หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
- วิธีวัด : ตรวจสอบจำนวนครั้งที่มีการทบทวนแผนต่อปี และเปรียบเทียบกับเป้าหมายที่กำหนด

1.2 อัตราการปรับปรุงแผนตามข้อเสนอแนะ (Plan Improvement Implementation Rate)

- เป้าหมาย: นำข้อเสนอแนะจากการทบทวนมาปรับปรุงแผนไม่น้อยกว่า 90%
- วิธีวัด: เปรียบเทียบจำนวนข้อเสนอแนะที่นำไปปรับปรุงกับจำนวนข้อเสนอแนะทั้งหมด

1.3 การครอบคลุมความเสี่ยงใหม่ในการทบทวนแผน (Coverage of New Risks)

- เป้าหมาย: รวมความเสี่ยงใหม่ ๆ ที่ระบุได้จากการประเมินความเสี่ยงเข้ามาในแผน 100%
- วิธีวัด: ตรวจสอบรายการความเสี่ยงที่เพิ่มเข้ามาในแผนหลังการทบทวน

1.4 ระดับความสอดคล้องของแผนกับมาตรฐานและกฎหมาย (Compliance Alignment Rate)

- เป้าหมาย: แผนที่ทบทวนต้องสอดคล้องกับกฎหมายและมาตรฐานที่เกี่ยวข้อง 100%
- วิธีวัด: ใช้ผลการตรวจสอบความสอดคล้องกับกฎหมายและมาตรฐาน

2. ตัวชี้วัดด้านการฝึกซ้อมแผน (Plan Drill Metrics)

2.1 ความถี่ในการฝึกซ้อมแผน (Drill Frequency)

- เป้าหมาย: ดำเนินการฝึกซ้อมไม่น้อยกว่า 2 ครั้งต่อปี (อย่างน้อย 1 ครั้งแบบเต็มรูปแบบ)
- วิธีวัด: นับจำนวนครั้งของการฝึกซ้อมแผนต่อปี

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.2 อัตราการเข้าร่วมฝึกซ้อมของบุคลากรที่เกี่ยวข้อง (Participant Attendance Rate)

- เป้าหมาย: บุคลากรที่เกี่ยวข้องเข้าร่วมไม่น้อยกว่า 90%
- วิธีวัด: เปรียบเทียบจำนวนผู้เข้าร่วมกับจำนวนบุคลากรทั้งหมดที่เกี่ยวข้อง

2.3 ระดับความเข้าใจของผู้เข้าร่วมหลังการฝึกซ้อม (Post-Drill Knowledge Level)

- เป้าหมาย: คะแนนการประเมินหลังฝึกซ้อมเฉลี่ยไม่น้อยกว่า 80%
- วิธีวัด: ใช้แบบทดสอบหรือประเมินผลความรู้หลังการฝึกซ้อม

2.4 การแก้ไขจุดอ่อนที่พบจากการฝึกซ้อม (Weakness Resolution Rate)

- เป้าหมาย: แก้ไขจุดอ่อนที่พบจากการฝึกซ้อม 100% ภายในระยะเวลาที่กำหนด
- วิธีวัด: ตรวจสอบจำนวนจุดอ่อนที่แก้ไขสำเร็จเทียบกับจำนวนจุดอ่อนทั้งหมด

2.5 ระยะเวลาที่ใช้ในการดำเนินการฝึกซ้อม (Drill Execution Time)

- เป้าหมาย: การฝึกซ้อมต้องดำเนินการเสร็จสิ้นภายในระยะเวลาที่กำหนด
- วิธีวัด: บันทึกเวลาที่ใช้ในการดำเนินการฝึกซ้อมและเปรียบเทียบกับเป้าหมาย

3.1.2 ข้อมูลติดต่อและการยกระดับการดำเนินการ (Contact Information and Escalation Level)

ชื่อ	ตำแหน่ง	บทบาท	ข้อมูลการติดต่อ	ระดับที่เกี่ยวข้อง (Escalation 1-3)*
นายสกุลยุช ศรุตานนท์	ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน (กลุ่มงานบริหารระบบเทคโนโลยีสารสนเทศและการสื่อสาร, กลุ่มงานพัฒนาเครือข่ายและนวัตกรรม)	IR Commander, CIRT manager, CIRT member		1
ว่าที่ ร.ต. พีรพล มั่นจิตต์	รองผู้อำนวยการสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ	CIO		2
XXXXX XXXXX	ผู้อำนวยการสำนักงานผู้อำนวยการ (กลุ่มงานอำนวยการและประชาสัมพันธ์)	IHT member		3
XXXXX XXXXX	ผู้อำนวยการกองกฎหมาย (กลุ่มงานกฎหมายและระเบียบ)	IHT member		3
XXXXX XXXXX	กลุ่มพัฒนาระบบบริหาร (การควบคุมความเสี่ยงภายใน)	IHT member		3
XXXXX XXXXX	ผู้อำนวยการสำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	IHT member		3
XXXXX XXXXX	ผู้อำนวยการสำนักงานผู้อำนวยการ (กลุ่มงานอำนวยการและประชาสัมพันธ์) ดูแลเรื่องอาคารสถานที่	IHT member		3
XXXXX XXXXX	3rd Party Support สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	CIRT member	XXXXXXX	3
XXXXX XXXXX	Vendor, Supplier	CSIRT member		1

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

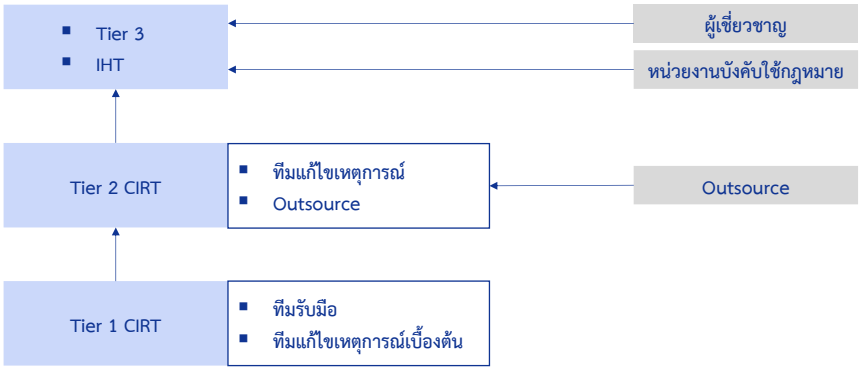
ชื่อ	ตำแหน่ง	บทบาท	ข้อมูลการติดต่อ	ระดับที่เกี่ยวข้อง (Escalation 1-3)*
	บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ			

ตารางที่ 3-1 ข้อมูลติดต่อและการยกระดับการดำเนินการ

การยกระดับการดำเนินการ (Escalation Level) กำหนดลำดับที่การแจ้งเตือนควรเกิดขึ้น:

1. แจ้งก่อน (Notify First) จำเป็นทุกกรณี
2. จำเป็นสำหรับเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือวิกฤตทั้งหมด (Required on all Moderate or High-severity Incidents)
3. มีส่วนร่วมตามความจำเป็น (Involve as Needed)

โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)



รูปที่ 3-2: โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

จากภาพโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) มีการระบุรายละเอียดหน้าที่และความรับผิดชอบ ดังนี้

3.1.3 หน้าที่และความรับผิดชอบ (Roles and Responsibilities)

3.1.3.1 ทีมจัดการเหตุภัยคุกคามทางไซเบอร์ *(Cyber Security Incident Handling Team: IHT)*

- ประกอบด้วยผู้เชี่ยวชาญด้านกฎหมาย ผู้จัดการความเสี่ยง และผู้จัดการแผนกอื่น ๆ ที่อาจให้คำปรึกษาหรือแจ้งในระหว่างการเผชิญเหตุ
- ให้คำแนะนำเกี่ยวกับกิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับความเชี่ยวชาญ
- สร้างความเข้าใจทั่วไปเกี่ยวกับแผนและนโยบายของหน่วยงาน
- ตรวจสอบให้แน่ใจว่ากิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์เป็นไปตามข้อกำหนดทางกฎหมาย สัญญา และข้อบังคับ
- เข้าร่วมในการทดสอบแผนและขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์
- รับผิดชอบในการสื่อสารภายในและภายนอกที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.1.3.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (*Chief Information Officer: CIO* หรือ *CTO)* หรือผู้บริหารระดับสูง ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ *(Chief Information Security Officer : CISO)*

- ขออนุมัติจากผู้บริหารระดับสูง (Executive Management) สำหรับการบริหารชุดโครงการการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Program) ที่เกิดขึ้น
- ประสานงานกิจกรรมตอบสนองกับแผนกเสริมและทรัพยากรภายนอกตามความจำเป็นเพื่อลดความเสียหายต่อทรัพยากรสารสนเทศ
- ให้ข้อมูลเป็นปัจจุบันเกี่ยวกับกิจกรรมรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Handling Team: IHT) และผู้มีส่วนได้ส่วนเสียอื่น ๆ ในระหว่างเหตุการณ์
- ตรวจสอบให้แน่ใจว่าข้อตกลงระดับการบริการกับผู้ให้บริการกำหนดความคาดหวังของหน่วยงานและผู้ให้บริการอย่างชัดเจนเกี่ยวกับการรับมือเหตุภัยคุกคามทางไซเบอร์
- ตรวจสอบให้แน่ใจว่านโยบายที่เกี่ยวข้องกับการรับมือเหตุภัยคุกคามทางไซเบอร์แสดงถึงเป้าหมายของหน่วยงานได้อย่างถูกต้อง
- ทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (“แผน”) เพื่อให้แน่ใจว่าเป็นไปตามวัตถุประสงค์ของนโยบายและสะท้อนเป้าหมายของหน่วยงานได้อย่างถูกต้อง ขออนุมัติแผนจาก IHT
- ทำงานร่วมกับผู้บัญชาการ IR เพื่อประเมินประสิทธิภาพของแผนและ CIRT เป็นระยะ ๆ
- ทบทวนให้แน่ใจว่าผู้จัดการ CIRT ได้รับอำนาจที่จำเป็น (Necessary Authority) ในการยึดทรัพย์สินและหยุดให้บริการอย่างรวดเร็วเพื่อควบคุมเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือระดับวิกฤต (Moderate or Critical-severity Incident) (เทียบเคียงกับ (2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง และ (3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ มาตรา 60 พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)
- อนุมัติการปิดเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงหรือระดับวิกฤต (Moderate or Critical-Severity Incident)
- ตรวจสอบให้แน่ใจว่ามีการรักษา Cyber Insurance ตามความจำเป็นและแจ้งผู้มีส่วนได้ส่วนเสียที่เหมาะสม (ดูภาคผนวก 9)
- ตรวจสอบให้แน่ใจว่าบทเรียนที่เรียนรู้ถูกนำไปใช้/ชั่งน้ำหนักตามความเสี่ยงสำหรับเหตุภัยคุกคามทางไซเบอร์ ความรุนแรงระดับ 1 (Severity 1 Incidents)

หมายเหตุ: อ้างถึงพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 60 การพิจารณาเพื่อใช้อานาจในการป้องกันภัยคุกคามทางไซเบอร์ คณะกรรมการจะกำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็นสามระดับ

(1) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญของประเทศหรือการให้บริการของรัฐด้อยประสิทธิภาพลง

(2) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีโครงสร้างพื้นฐานสำคัญของประเทศและการโจมตีดังกล่าวมีผลทำให้ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศ ความมั่นคงของรัฐ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ความสัมพันธ์ระหว่างประเทศ การป้องกันประเทศ เศรษฐกิจ การสาธารณสุข ความปลอดภัยสาธารณะ หรือความสงบเรียบร้อยของประชาชนเสียหาย จนไม่สามารถทำงานหรือให้บริการได้

(3) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ หมายถึง ภัยคุกคามทางไซเบอร์ในระดับวิกฤติที่มีลักษณะ ดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของหน่วยงานรัฐหรือการให้บริการของโครงสร้างพื้นฐานสำคัญของประเทศที่ให้กับประชาชนล้มเหลวทั้งระบบ จนรัฐไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ของรัฐได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐหรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขตผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุขของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อยหรือประโยชน์ส่วนรวม หรือการป้องปัดหรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

นอกจากนี้ หน่วยงานควรศึกษาดูรายละเอียดเพิ่มเติมเกี่ยวกับลักษณะภัยคุกคามทางไซเบอร์ได้ที่ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

3.1.3.3 ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (*Cyber Incident Response Team: CIRT)*

CIRT ประกอบด้วยการจัดการด้านเทคโนโลยีสารสนเทศและบุคลากรที่มีประสบการณ์ บทบาทของ CIRT คือการจัดการกับเหตุการณ์ในทันที เพื่อให้สามารถกักกัน สืบสวนสอบสวน และกู้คืนได้อย่างรวดเร็ว ในกรณีที่มีการยกระดับบริการของบุคคลที่สาม ตรวจสอบให้แน่ใจว่าพวกเขามีส่วนร่วมตามความจำเป็นบทบาทภายใน CIRT รวมถึง:

3.1.3.3.1 ผู้บัญชาการ IR (IR Commander)

ผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์จะดูแลและจัดลำดับความสำคัญของการดำเนินการระหว่างการตรวจจับ การวิเคราะห์ และการจำกัดขอบเขตเหตุการณ์ และยังมีหน้าที่รับผิดชอบในการถ่ายทอดความต้องการพิเศษของเหตุการณ์ที่มีความรุนแรงสูงไปยังส่วนอื่น ๆ ของหน่วยงาน ตลอดจนการสื่อสารผลกระทบที่อาจเกิดขึ้นกับ CIO นอกจากนี้ ยังมีหน้าที่รับผิดชอบในการทำความเข้าใจข้อตกลงระดับการบริการ (Service Level Agreement: SLA) กับบุคคลที่สาม และบทบาทของบุคคลที่สามอาจมีบทบาทในสถานการณ์การรับมือที่เฉพาะเจาะจง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ความรับผิดชอบเพิ่มเติม:

- ทำหน้าที่เป็นผู้ประสานงานสำหรับการสื่อสารทั้งหมดไปยังและจาก CIO
- รวบรวมทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Incident Response Team: CIRT)
- ตรวจสอบให้แน่ใจว่าบุคลากรที่ได้รับมอบหมายให้รับผิดชอบในการรับมือเหตุภัยคุกคามทางไซเบอร์ได้รับการฝึกอบรมและมีความรู้เกี่ยวกับวิธีการรับมือเหตุภัยคุกคามทางไซเบอร์
- ปรับปรุงข้อมูลที่เป็นปัจจุบันของแผนและขั้นตอนตามความจำเป็นตามผลการทดสอบ บทเรียนการรับมือเหตุภัยคุกคามทางไซเบอร์ที่ได้เรียนรู้ การพัฒนาอุตสาหกรรม และแนวปฏิบัติที่ดีที่สุด
- ทบทวนแผนและขั้นตอนปฏิบัติอย่างน้อยปีละครั้ง
- เริ่มการทดสอบแผนและขั้นตอนอย่างน้อยปีละครั้ง
- ตรวจสอบให้แน่ใจว่ากิจกรรมของทีมเป็นไปตามข้อกำหนดทางกฎหมายและของอุตสาหกรรมสำหรับขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์
- ทำหน้าที่เป็นผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์หลัก รับผิดชอบในการประกาศภัยคุกคามทางไซเบอร์ จัดการกิจกรรมการรับมือของทีม และอนุมัติการปิดภัยคุกคามทางไซเบอร์ระดับความรุนแรง 2 และ 3 (Severity 2 and Severity 3 Incidents)
- ตระหนักถึงนโยบายการประกันภัยทางไซเบอร์ (Cyber Insurance Policies) กลไกการติดต่อและเมื่อใดที่จะรวมผู้ให้บริการ (ดูภาคผนวก 9)

3.1.3.3.2 สมาชิกทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Response Team Members)

Incident Response Manager ได้รับการสนับสนุนโดยทีมเจ้าหน้าที่ด้านเทคนิคที่ทำงานโดยตรงกับระบบข้อมูลที่ได้รับผลกระทบ เพื่อค้นหาเวลา สถานที่ และรายละเอียดของเหตุการณ์ สมาชิกในทีมมักประกอบด้วยผู้เชี่ยวชาญเฉพาะด้าน (Subject Matter Experts: SMEs) เจ้าหน้าที่เทคโนโลยีสารสนเทศระดับอาวุโส บุคคลภายนอก การรักษาความมั่นคงปลอดภัยจากภายนอก หรือพันธมิตรทางนิติวิทยาศาสตร์

ความรับผิดชอบเพิ่มเติม:

- ช่วยเหลือในการรับมือเหตุภัยคุกคามทางไซเบอร์ตามที่ร้องขอ ความรับผิดชอบของ CIRT ควรมีความสำคัญมากกว่าหน้าที่ปกติ
- ทำความเข้าใจของหน่วยงาน แผนรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนในการรับมือเหตุภัยคุกคามทางไซเบอร์อย่างเหมาะสม
- พัฒนาทักษะต่อไปสำหรับการจัดการการรับมือเหตุภัยคุกคามทางไซเบอร์
- ตรวจสอบให้แน่ใจว่าเครื่องมือได้รับการกำหนดค่าและจัดการอย่างเหมาะสมเพื่อแจ้งเตือนเหตุการณ์/ภัยคุกคามทางไซเบอร์ (Incidents/events)
- วิเคราะห์การรับส่งข้อมูลเครือข่ายเพื่อหาสัญญาณของการปฏิเสธบริการ (Denial of Service) การปฏิเสธบริการแบบกระจาย (Distributed Denial of Service) หรือการโจมตีภายนอกอื่น ๆ
- ตรวจทานล็อกไฟล์ของระบบที่สำคัญสำหรับกิจกรรมที่ผิดปกติ
- สังเกตการณ์แอปพลิเคชันและบริการทางธุรกิจสำหรับการหาสัญญาณการโจมตี (Signs of Attack)
- รวบรวมข้อมูลที่เกี่ยวข้องเกี่ยวกับภัยคุกคามทางไซเบอร์ตามคำร้องขอของผู้บัญชาการ IR
- ปรึกษากับเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศที่มีคุณสมบัติเหมาะสมเพื่อขอคำแนะนำเมื่อจำเป็น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ตรวจสอบให้แน่ใจว่าการรวบรวมหลักฐาน ห่วงโซ่การอารักขา (Chain of Custody) และการเก็บรักษามีความเหมาะสม
- เข้าร่วมในการทดสอบแผนและขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์
- มีความรู้เกี่ยวกับข้อตกลงระดับการให้บริการกับผู้ให้บริการเกี่ยวกับการรับมือเหตุภัยคุกคามทางไซเบอร์

3.1.3.3.3 ผู้บันทึก (Recorder)

ผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์อาจมอบหมายให้สมาชิกในทีมเริ่มกระบวนการทางเอกสารอย่างเป็นทางการของภัยคุกคามทางไซเบอร์

ลำดับที่	สมาชิก CIRT	บทบาท
1	XXXXX XXXXX	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน (Information Security Manager)
2	XXXXX XXXXX	บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.) บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ
3	หัวหน้ากลุ่มงานบริหารระบบเทคโนโลยีสารสนเทศและการสื่อสาร	ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร
5	หัวหน้ากลุ่มงานพัฒนาเครือข่ายและนวัตกรรม	ดูแลงานพัฒนาเครือข่ายและนวัตกรรม
6	XXXXX XXXXX	Vendor, Supplier บำรุงรักษา, สำรองข้อมูล, กู้คืนระบบ
7	XXXXX XXXXX	บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.) ใช้บริการที่อาคารไทยซัมมิท ทาวเวอร์ ที่วาง Server สำรองข้อมูลใส่ Hard Disk และเก็บรักษาไว้สำหรับการกู้คืน (ระบบ DR Site)

ตารางที่ 3-2 ข้อมูลสมาชิกทีม CIRT (CIRT Team Members)

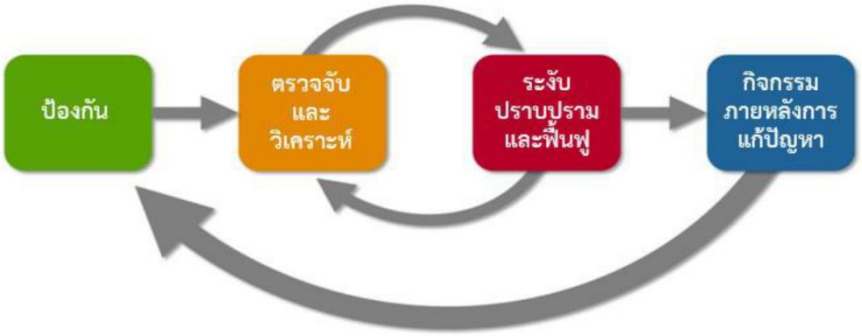
3.2 กรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Framework)

หน่วยงานตระหนักดีว่าถึงแม้จะมีความพยายามและมีความสามารถในการปกป้องทรัพยากรสารสนเทศ แต่อาจมีการละเมิดหรือการสูญเสียข้อมูลอื่น ๆ หน่วยงานต้องใช้การดำเนินการอย่างเหมาะสมเพื่อรับมือเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในลักษณะที่ลดการสูญหายของข้อมูลและความเสียหายที่อาจเกิดขึ้นกับลูกค้า คู่ค้า และหน่วยงานเอง

การพัฒนากรอบการรับมือเหตุภัยคุกคามทางไซเบอร์ที่กำหนดไว้อย่างชัดเจนมีความสำคัญต่อแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ที่มีประสิทธิผล กรอบงานการรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน ประกอบด้วย 4 ขั้นตอนเพื่อให้แน่ใจว่ามีแนวทางที่สอดคล้องกันและเป็นระบบ (Consistent and Systematic Approach)

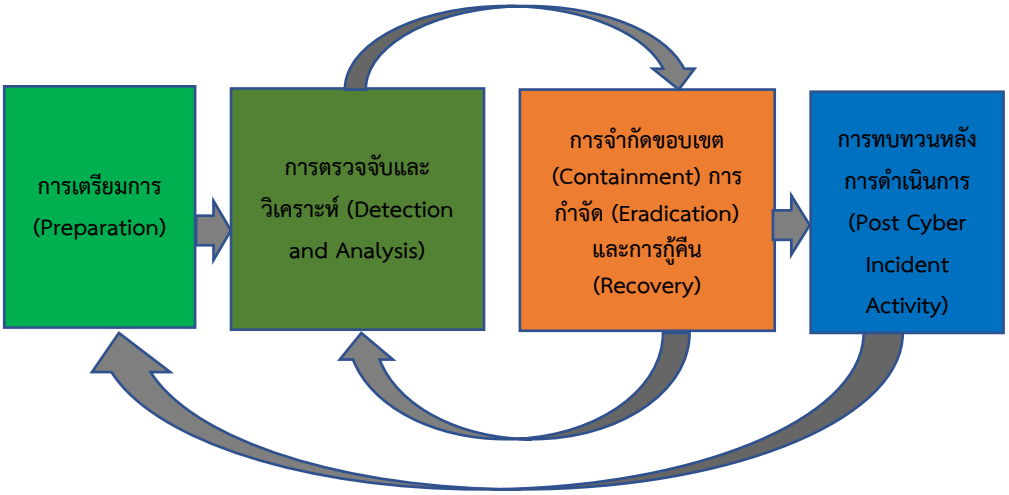
โดยเทียบเคียงกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 ได้ดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน



รูปที่ 3-3: ขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์(Incident Handling Cycle)

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564



รูปที่ 3-4: วงจรชีวิตของการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Life Cycle)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ดังนั้น จึงเปรียบเทียบคำศัพท์ที่มีการใช้งานระหว่างเอกสารทั้งสองฉบับ เพื่อให้ผู้อ่านนำไปใช้งานสามารถเข้าใจได้ง่ายขึ้นดังนี้

แนวทางปฏิบัติในเอกสารนี้	ขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 1 การเตรียมการ (Preparation)	**ขั้นตอนที่ 1**: การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)	**ขั้นตอนที่ 2**: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์
ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)	**ขั้นตอนที่ 3**: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ
ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)	**ขั้นตอนที่ 4**: การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

ตารางที่ 3-3 เปรียบเทียบแนวทางปฏิบัติและประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

จากตารางข้างต้นสามารถอธิบายรายละเอียดของขั้นตอนต่าง ๆ ตั้งแต่การเตรียมการ (Preparation) จนถึงการทบทวนหลังการดำเนินการ (Post Cyber Incident Activity) พอสังเขปได้ดังนี้

ขั้นตอนที่ 1 การเตรียมการ (Preparation)

จำเป็นอย่างยิ่งที่จะต้องจัดตั้งทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team (CIRT)) กำหนดแนวทางการสื่อสารที่เหมาะสม สื่อสารการบริการที่จำเป็นเพื่อสนับสนุนกิจกรรมการรับมือและจัดหาเครื่องมือที่จำเป็น (ดูหัวข้อ 4 ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation))

ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)

การตรวจจับและระบุเหตุการณ์และการดำเนินการประเมินควรดำเนินการเพื่อยืนยันการมีอยู่ของภัยคุกคามทางไซเบอร์ การประเมินควรรวมถึงการกำหนดขอบเขต ผลกระทบ และขอบเขตของความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ ในกรณีที่อาจมีการดำเนินการทางกฎหมาย หลักฐานดิจิทัลจะได้รับการเก็บรักษาไว้ และการวิเคราะห์ทางนิติวิทยาศาสตร์อาจดำเนินการตามข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง (ดูหัวข้อ 5 ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis))

ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

ประกอบไปด้วย 3 ขั้นตอนย่อย (ดูหัวข้อ 6 ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)) ดังนี้

ขั้นตอนที่ 3.1 การจำกัดขอบเขต (Containment))

การจำกัดขอบเขตเหตุการณ์เป็นสิ่งจำเป็นเพื่อลดและแยกความเสียหายที่เกิดขึ้น ต้องดำเนินการตามขั้นตอนเพื่อให้แน่ใจว่าขอบเขตของเหตุการณ์ไม่กระจายไปถึงระบบอื่น ๆ และทรัพยากรสารสนเทศ จำเป็นต้องมีการวิเคราะห์สาเหตุที่แท้จริง (Root Cause Analysis) ก่อนที่จะก้าวข้ามขั้นตอนการจำกัขอบเขต และอาจต้องใช้ผู้เชี่ยวชาญจากบุคคลภายนอก

ขั้นตอนที่ 3.2 การกำจัด (Eradication)

การกำจัดต้องมีการลบ (Removal) หรือจัดการ (Addressing) ส่วนประกอบและอาการของภัยคุกคามทางไซเบอร์ทั้งหมด นอกจากนี้ ต้องดำเนินการตรวจสอบความถูกต้อง (Validation) เพื่อให้แน่ใจว่าภัยคุกคามทางไซเบอร์จะไม่เกิดขึ้นอีก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ขั้นตอนที่ 3.3 การกู้คืน (Recovery)

การกู้คืนเกี่ยวข้องกับขั้นตอนที่จำเป็นในการกู้คืนข้อมูลและระบบให้อยู่ในสถานะการทำงานที่ดีซึ่งช่วยให้การดำเนินธุรกิจสามารถกลับมาดำเนินการได้

ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (Post Cyber Incident Activity)

การทบทวนหลังการดำเนินการเกี่ยวข้องกับการทบทวนบทเรียนที่เรียนรู้รวมถึงการวิเคราะห์หลังเหตุการณ์เกี่ยวกับระบบที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์และระบบอื่น ๆ ที่อาจมีความเสี่ยง บทเรียนที่เรียนรู้จากภัยคุกคามทางไซเบอร์นั้นจะถูกสื่อสารไปยังผู้บริหารระดับสูงและแผนปฏิบัติการที่พัฒนาขึ้นเพื่อปรับปรุงแนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์ในอนาคตและลดความเสี่ยง (ดูขั้นตอนที่ 4 – การทบทวนหลังการดำเนินการ (After-Action Review Process))

ในการดำเนินการตามขั้นตอนต่าง ๆ ในมีการระบุรายละเอียดตามข้อมูลด้านล่าง เพื่อเป็นแนวทางการปฏิบัติจริงสำหรับ สคทช. ดังนี้

3.2.1 ขั้นตอนที่ 1 รายละเอียดการเตรียมการ (Preparation)

ขั้นตอนการเตรียมการเป็นขั้นตอนที่สำคัญที่สุดและมักถูกมองข้ามอย่างง่ายดาย หากไม่มีการเตรียมการที่เหมาะสม กิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์อาจไม่เป็นระเบียบ มีราคาสูงและอาจก่อให้เกิดอันตรายต่อหน่วยงานที่ไม่สามารถแก้ไขได้ ลักษณะงานที่รวมอยู่ในขั้นตอนการเตรียมการมีต่อไปนี้

- จัดตั้งทีมจัดการเหตุภัยคุกคามทางไซเบอร์ (Cyber Security Incident Handling Team: IHT) และทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)
- ตรวจสอบให้แน่ใจว่าฝ่ายที่เกี่ยวข้องตระหนักถึงกระบวนการรายงานเหตุภัยคุกคามทางไซเบอร์ (ดูการรายงานเหตุภัยคุกคามทางไซเบอร์ (Reporting Incidents))
- จัดทำเอกสารและแบ่งปันรายละเอียดการประกันภัยทางไซเบอร์กับฝ่ายที่เกี่ยวข้อง (ดูภาคผนวก 9)
- ตรวจสอบการปฏิบัติตามนโยบายการบันทึก การแจ้งเตือน และการเฝ้าระวัง (Monitoring)
- ตรวจสอบให้แน่ใจว่า CIRT ได้รับการฝึกอบรมที่เหมาะสมตามการวิเคราะห์ช่องว่างทักษะความพยายามในการพัฒนาอาชีพ (Career Development Efforts) และความต้องการในการรักษาทักษะ (Skill Retention Needs)
- ตรวจสอบให้แน่ใจว่า CIRT สามารถเข้าถึงเครื่องมือและอุปกรณ์ที่จำเป็นตาม ROI โดยประมาณความเสี่ยงของหน่วยงาน
- กำหนดและจัดทำเอกสารขั้นตอนการปฏิบัติงานมาตรฐานและลำดับการดำเนินการสำหรับทั้ง IHT และ CIRT
- ปรับปรุงเอกสาร รายการตรวจสอบ ข้อมูลอ้างอิง ฯลฯ
- รักษาและตรวจสอบความถูกต้องของไดอะแกรมเครือข่ายและทะเบียนทรัพย์สิน
- ตรวจสอบรายงานการทดสอบการเจาะระบบ (Penetration Test) และตรวจสอบความถูกต้องของการแก้ไขสิ่งที่ค้นพบ
- ตรวจสอบรายงานการจัดการช่องโหว่และตรวจสอบความพยายามในการแก้ไข
- สร้างข้อมูลประจำตัวของผู้ดูแลระบบที่ใช้เฉพาะกิจและปิดใช้งาน (Disposable and Disabled Administrative Credentials) เพื่อใช้สำหรับการสืบสวนสอบสวน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- สุดท้าย ควรสังเกตว่าขั้นตอนที่ 1 เป็นไปอย่างต่อเนื่องหรืออย่างน้อยเป็นวัฏจักรเมื่อภัยคุกคามทางไซเบอร์ต่าง ๆ ได้รับการสรุปผล

หมายเหตุ : หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

3.2.1.1 การรายงานเหตุภัยคุกคามทางไซเบอร์ (*Reporting Incidents*)

วิธีที่มีประสิทธิภาพสำหรับทั้งฝ่ายภายในและภายนอกในการรายงานเหตุภัยคุกคามทางไซเบอร์มีความสำคัญเท่าเทียมกัน เนื่องจากบางครั้งผู้ใช้ระบบของหน่วยงาน และข้อมูลอาจเป็นคนแรกที่สังเกตเห็นปัญหา ทบทวนประเภทของเหตุการณ์ที่เกิดขึ้นในขั้นตอนที่ 2 ภายใต้การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization) และแสดงรายการหรือกำหนดวิธีการรายงานสำหรับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ ดังตารางด้านล่าง

ประเภทเหตุภัยคุกคามทางไซเบอร์ (Incident Type)	วิธีการรายงาน (Reporting Method)	พร้อมสำหรับ (Available To)	ทำให้นิรนาม (Anonymous)
การเปลี่ยนแปลงเว็บไซต์ให้เสียหาย การแก้ไขข้อมูล หรือการนำมาข้อมูลมาเปิดเผยโดยไม่ได้รับอนุญาต (Website Defacement, Data Modification or Exposure)	ติดต่อฝ่ายสนับสนุนเว็บไซต์	ลูกค้า/ผู้รับบริการ	ใช่
การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	ติดต่อศูนย์ปฏิบัติการฯ SOC ผ่านระบบ Email และโทรศัพท์	ลูกค้า/ผู้รับบริการ และพนักงาน	ไม่
การพยายามเข้าถึงระบบที่ไม่สำเร็จ	ติดต่อศูนย์ปฏิบัติการฯ SOC ผ่านระบบ Email และโทรศัพท์	ลูกค้า/ผู้รับบริการ และพนักงาน	ไม่

ตารางที่ 3-4 แนวทางการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Guide)

หมายเหตุ : อ้างอิงจากรายงานเหตุภัยคุกคามทางไซเบอร์จากโครงการจ้างบริการเฝ้าระวังภัยคุกคามทางไซเบอร์ (Security Operations Center)

3.2.2 ขั้นตอนที่ 2 การตรวจจับและวิเคราะห์ (Detection and Analysis)

3.2.2.1 การตรวจจับ (*Detection*)

เมื่อบุคลากรของหน่วยงาน หรือบุคคลภายนอกสังเกตเห็นความผิดปกติที่น่าสงสัยในข้อมูลระบบ หรือเครือข่าย หรือการแจ้งเตือนของระบบที่สร้างเหตุการณ์ (Event) ขึ้นมา ฝ่ายปฏิบัติการด้านความมั่นคงปลอดภัย แผนกช่วยเหลือ หรือ CIRT จะต้องดำเนินการตรวจสอบเบื้องต้นและยืนยันเหตุการณ์

3.2.2.2 เหตุการณ์กับภัยคุกคามทางไซเบอร์ (*Events Versus Incidents*)

ตามที่กำหนดไว้ข้างต้น เหตุการณ์คือการสังเกตเห็นการเปลี่ยนแปลงในลักษณะการทำงานปกติของระบบ สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร

ภัยคุกคามทางไซเบอร์ คือ เหตุการณ์ที่บ่งชี้ถึงการถูกโจมตีด้านความมั่นคงปลอดภัย หรือการไม่ปฏิบัติตามนโยบายของหน่วยงาน ที่ส่งผลกระทบในทางลบ (หรืออาจส่งผลกระทบในทางลบ) ต่อหน่วยงาน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

เพื่ออำนวยความสะดวกในการระบุภัยคุกคามทางไซเบอร์ (Incident) ต่อไปนี้คือรายการอาการทั่วไปของภัยคุกคามทางไซเบอร์ ซึ่งอาจรวมถึงสิ่งต่อไปนี้บางส่วนหรือทั้งหมด:

1) อีเมลหรือการแจ้งเตือนทางโทรศัพท์จากเครื่องมือตรวจจับการบุกรุก

2) รายการที่น่าสงสัยในระบบหรือบัญชีเครือข่ายหรือล็อก

3) ความคลาดเคลื่อนระหว่างล็อก

4) การพยายามเข้าสู่ระบบที่ไม่สำเร็จซ้ำ ๆ ภายในช่วงเวลาสั้น ๆ

5) บัญชีผู้ใช้ใหม่ที่เกิดขึ้นโดยไม่ทราบที่มา

6) ไฟล์ใหม่ที่ไม่สามารถอธิบายได้หรือชื่อไฟล์ที่ไม่คุ้นเคย

7) การแก้ไขที่เกิดขึ้นโดยไม่ทราบที่มา ที่เกิดขึ้นต่อความยาวและ/หรือวันที่ของไฟล์ โดยเฉพาะในไฟล์ระบบ

8) ความพยายามที่ไม่สามารถอธิบายได้ในการเขียนไปยังไฟล์ระบบหรือการเปลี่ยนแปลงในไฟล์ระบบ

9) การแก้ไขหรือการลบข้อมูลโดยไม่สามารถอธิบายได้

10) การปฏิเสธ/การหยุดชะงักของบริการหรือการไม่สามารถเข้าสู่ระบบบัญชีของผู้ใช้ตั้งแต่หนึ่งรายขึ้นไป

11) ระบบล่ม

12) ประสิทธิภาพของระบบที่ต่ำกว่าปกติของเซิร์ฟเวอร์

13) การทำงานของโปรแกรมหรืออุปกรณ์ดักจับ (Sniffer Device) ที่ใช้ในการจับการรับส่งข้อมูลเครือข่าย

14) เวลาใช้งานที่ผิดปกติ (เช่น ผู้ใช้เข้าสู่ระบบในช่วงเวลาที่ไม่ปกติ)

15) การใช้ทรัพยากรระบบที่ผิดปกติ (การใช้งาน CPU สูง)

16) การเข้าสู่ระบบครั้งล่าสุด (หรือการใช้งาน) สำหรับบัญชีผู้ใช้ไม่ตรงกับครั้งสุดท้ายจริงที่ผู้ใช้เข้าใช้บัญชี

17) รูปแบบการใช้งานที่ผิดปกติ (เช่น บัญชีผู้ใช้ที่เชื่อมโยงกับผู้ใช้ใน Finance กำลังถูกใช้เพื่อเข้าสู่ระบบฐานข้อมูล HR)

18) การเปลี่ยนแปลงการอนุญาตหรือการเข้าถึงของผู้ใช้โดยไม่ได้รับอนุญาต

แม้ว่าจะไม่มีอาการใดที่จะพิสูจน์ได้อย่างชัดเจนว่าเกิดภัยคุกคามทางไซเบอร์ขึ้น การสังเกตอาการเหล่านี้อย่างน้อยหนึ่งอย่างควรกระตุ้นให้ผู้สังเกตการณ์ตรวจสอบอย่างใกล้ชิดยิ่งขึ้น อย่าใช้เวลามากเกินไปกับการระบุเหตุการณ์เบื้องต้น เนื่องจากสิ่งนี้จะผ่านการพิจารณาอีกครั้งในขั้นตอนการจำกัดขอบเขต (Containment Phase)

หมายเหตุ: ควรยกเลิกการเชื่อมต่อระบบ (Disconnected) ที่ถูกบุกรุกจากเครือข่ายแทนที่จะปิดสวิตช์ (Powered Off) การปิดระบบที่ถูกบุกรุกอาจนำไปสู่การสูญเสียข้อมูล ข้อมูล หรือหลักฐานที่จำเป็นสำหรับการสืบสวนสอบสวนทางนิติวิทยาศาสตร์ในภายหลัง

3.2.2.3 การวิเคราะห์ (*Analysis)*

เมื่อมีเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และถูกวิเคราะห์ (อ้างถึงกระบวนการคัดแยกระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ (Security Event and an Incident) ในแนวทางการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เรื่องมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) และระบุว่าเป็นเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น CIRT บางส่วนหรือทั้งหมดจะถูกเปิดใช้งาน (Activate) โดยผู้บัญชาการ IR

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

(IR Commander) เพื่อสืบสวนสอบสวน (Investigate) สถานการณ์ การวิเคราะห์จะกำหนดประเภท (Category) ขอบเขต (Scope) และผลกระทบ (Impact) ที่อาจเกิดขึ้นจากเหตุภัยคุกคามทางไซเบอร์ CIRT ควรทำงานอย่างรวดเร็วเพื่อวิเคราะห์และตรวจสอบแต่ละเหตุภัยคุกคามทางไซเบอร์ ตามกระบวนการที่ระบุไว้ด้านล่าง และจัดทำเอกสารแต่ละขั้นตอนที่ดำเนินการ

ควรใช้การประเมินเหตุภัยคุกคามทางไซเบอร์ 2 นาที (2 Minute Incident Assessment) ที่พบในภาคผนวก 2 เพื่อพิจารณาอย่างรวดเร็วว่าจำเป็นต้องมีการสืบสวนสอบสวนเพิ่มเติมหรือไม่ นอกจากนี้ยังสามารถแก้ไขและใช้เพื่อรายงานภัยคุกคามทางไซเบอร์ต่อผู้บริหารที่เหมาะสมตามความจำเป็น

ผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์จะมอบหมายให้สมาชิกในทีมเป็น “ผู้บันทึก” เพื่อเริ่มเอกสารอย่างเป็นทางการของภัยคุกคามทางไซเบอร์ การจำแนกหมวดหมู่ ขอบเขต และผลกระทบที่กำหนดไว้ด้านล่างจะต้องรวมอยู่ในเอกสารของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
0	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลหน่วยงานเพื่อโจมตี (Reconnaissance)
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สืบสวนสอบสวน (Investigating)
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

ตารางที่ 3-5 การจำแนกหมวดหมู่เหตุภัยคุกคามทางไซเบอร์ (Incident Categorization)

หมายเหตุ: อ้างอิงตามภาคผนวก ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

	หมวดหมู่ภัยคุกคาม						
ประเภทอุปกรณ์เครือข่าย	1	2	3	4	5	6	7
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่าย หรือ ดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่องเวิร์กสเตชัน	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

ตารางที่ 3-6 ตัวอย่างลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

นอกจากนี้ หน่วยงานอาจพิจารณาใช้งานกรอบงาน MITER ATT&CK ซึ่งเป็นฐานความรู้ที่เข้าถึงได้ทั่วโลกเกี่ยวกับกลวิธีและเทคนิคของฝ่ายตรงข้าม (Adversary Tactics and Techniques) และควรใช้เมื่อจัดหมวดหมู่ภัยคุกคามทางไซเบอร์ แม้ว่าอาจใช้เทคนิคหลายอย่างในเหตุภัยคุกคามทางไซเบอร์เดียว ให้เลือกวิธีการที่ฝ่ายตรงข้ามใช้ประโยชน์เป็นหลัก ตัวอย่างบางส่วนอาจเป็น:

- Phishing
- UnSecured Credentials
- Network Sniffing
- Man-in-the-Middle
- Data Destruction
- OS Credential Dumping
- Event Triggered Execution
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Hijacking
- Defacement
- File and Directory Permissions Modification

สังเกตว่ากรอบงาน MITER ATT&CK อาจไม่สามารถระบุสถานการณ์บางสถานการณ์ โดยเฉพาะสถานการณ์ที่ไม่มีเจตนาร้ายที่ก่อให้เกิดแผนการจัดการการรับมือเหตุภัยคุกคามทางไซเบอร์ ข้อยกเว้นต่อไปนี้อาจต้องใช้หมวดหมู่ของตนเองตามที่กำหนดโดยหน่วยงานหรือนโยบายการบริหารความเสี่ยงของหน่วยงาน:

- Data Loss
- Administrative Errors
- UnSecured Credentials
- Data Destruction
- Lax File and Directory Permissions
- Account Creation
- Disk Wipe
- Network Denial of Service
- Resource Misuse (non-malicious)
- ADD OTHERS AS APPLICABLE TO THE ORGANIZATION/INDUSTRY

ขอบเขตภัยคุกคามทางไซเบอร์ (Incident Scope)

การกำหนดขอบเขตจะช่วยให้ CIRT เข้าใจถึงผลกระทบทางธุรกิจที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ดังกล่าว ต่อไปนี้เป็นปัจจัยบางประการที่ควรพิจารณาเมื่อกำหนดขอบเขต:

- มีกี่ระบบที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์นี้?
- ข้อมูลที่เป็นความลับหรือได้รับการคุ้มครองเกี่ยวข้องหรือไม่?
- อะไรคือ/เป็นจุดเริ่มต้นของภัยคุกคามทางไซเบอร์ (เช่น อินเทอร์เน็ต เครือข่าย กายภาพ)?
- ความเสียหายที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์คืออะไร?
- เวลาโดยประมาณในการกู้คืนจากภัยคุกคามทางไซเบอร์คือเท่าไร?
- ทรัพยากรใดบ้างที่จำเป็นในการจัดการสถานการณ์?
- การวิเคราะห์สามารถทำได้อย่างมีประสิทธิภาพสูงสุดได้อย่างไร?

ผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ (Incident Impact)

เมื่อมีการกำหนดประเภทและขอบเขตของภัยคุกคามทางไซเบอร์แล้ว จะต้องตกลงกันถึงผลกระทบที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ ความรุนแรงของภัยคุกคามทางไซเบอร์จะเป็นตัวกำหนดแนวทางการดำเนินการแก้ไข อย่างไรก็ตาม ในทุกกรณี รายงานภัยคุกคามทางไซเบอร์จะต้องกรอก และตรวจสอบโดยผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์ ผลกระทบด้านการทำงานและข้อมูลถูกกำหนดด้วยกิจกรรมการรับมือ ดังตาราง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ระดับความรุนแรง	ผลกระทบการทำงาน (Functional Impact)	คำนิยาม	ลักษณะของภัยคุกคามทางไซเบอร์ มาตรา 60	การตอบสนองของ CIRT
น้อยที่สุด (1)	ไม่มี (Incidental)	ไม่มีผลกระทบต่อความสามารถของหน่วยงานในการให้บริการทั้งหมดแก่ผู้ใช้ทั้งหมด (All Users)	**(1)** ไม่มี	สร้างตั๋ว (Ticket) และมอบหมายให้แก้ไข
น้อย (2)	ไม่ร้ายแรง (Minor)	ผลน้อยที่สุด (Minimal Effect) หน่วยงานยังคงสามารถให้บริการที่สำคัญทั้งหมดแก่ผู้ใช้ทั้งหมด แต่ประสิทธิภาพด้อยลง	**(2) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง**	• สร้างตั๋วและมอบหมายให้แก้ไข • แจ้ง CIO และ IHT
ปานกลาง (3)	เริ่มร้ายแรง (Moderate)	หน่วยงานสูญเสียความสามารถในการให้บริการที่สำคัญแก่ผู้ใช้ระบบบางส่วน (Subset of System Users) กระทบต่อการให้บริการศูนย์คอมพิวเตอร์เกิน 3-6 ชั่วโมง	**(3) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง (แต่มีแนวโน้มจะร้ายแรงขึ้น)**	• เริ่ม CIRT เต็มรูปแบบ • เกี่ยวข้องกับ CIO และ IHT
สูง (4)	ร้ายแรง (Major)	หน่วยงานสูญเสียความสามารถในการให้บริการที่สำคัญแก่ผู้ใช้ระบบบางส่วน (Subset of System Users) กระทบต่อการให้บริการระบบสารสนเทศกลางเกิน 6-12ชั่วโมง	**(4) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง**	• เริ่ม CIRT เต็มรูปแบบ • เกี่ยวข้องกับ CIO และ IHT • CIO และ IHT พิจารณาเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ
สูงมาก (5)	วิกฤติ (Extreme)	หน่วยงานไม่สามารถให้บริการที่สำคัญบางอย่าง (Some Critical Services) แก่ผู้ใช้ได้อีกต่อไป	**(5) ภัยคุกคามทางไซเบอร์ในระดับวิกฤติ**	• เริ่ม CIRT เต็มรูปแบบ • CIO และ IHT พิจารณาเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) หรือแผนความต่อเนื่องจากธุรกิจ (Business Continuity Plan: BCP)

ตารางที่ 3-7 ตัวอย่างเกณฑ์ผลกระทบการทำงาน (Functional Impact)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ผลกระทบต่อสารสนเทศ (Functional Impact)	คำนิยาม	การตอบสนองของ CIRT
(1) ไม่มี (Incidental/None)	ไม่มีการเข้าถึงข้อมูล นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● ไม่ต้องดำเนินการใด ๆ
(2) ไม่ร้ายแรง ((Minor /Limited)	มีการเข้าถึงข้อมูลสาธารณะ (Public) หรือข้อมูลที่ไม่ละเอียดอ่อน (Non-sensitive) นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้งเจ้าของข้อมูลเพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(3) ปานกลาง (Moderate) หรือ เริ่มร้ายแรง	ข้อมูลภายในถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับผู้บริหาร ฝ่ายกฎหมาย และเจ้าของข้อมูล เพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(4) ร้ายแรง (Major/High)	ข้อมูลภายในถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก จำนวนมากอย่างต่อเนื่อง	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับผู้บริหาร ฝ่ายกฎหมาย และเจ้าของข้อมูล เพื่อกำหนดแนวทางปฏิบัติที่เหมาะสม
(5) วิกฤติ (Extreme/Critical)	ข้อมูลที่ได้รับการคุ้มครอง (Protected Data) ถูกเข้าถึง นำข้อมูลออก เปลี่ยนแปลง ลบ หรือถูกบุกรุก	● แจ้ง CIO และ IHT ● CIO จะทำงานร่วมกับฝ่ายกฎหมาย เพื่อพิจารณาว่าสามารถรายงานได้หรือไม่ และข้อกำหนดการแจ้งเตือนที่เหมาะสม

ตารางที่ 3-8 ตัวอย่างเกณฑ์ผลกระทบต่อสารสนเทศ (Informational Impact)

ภัยคุกคามทางไซเบอร์ทั้งหมดต้องถูกบันทึกไว้ในบันทึกกิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์และเครื่องมือการประเมิน (Incident Handling Log & Assessment Tool) บันทึกของการดำเนินการทั้งหมดเพื่อแก้ไขเหตุภัยคุกคามทางไซเบอร์ รวมถึงบันทึกห่วงโซ่การดูแล (Chain of Custody) และการเบี่ยงเบนจาก SOP จะต้องรวมอยู่ในเอกสาร

ตารางบันทึกกิจกรรมการรับมือเหตุภัยคุกคามทางไซเบอร์และเครื่องมือประเมิน และระดับการรับมือด้านล่างจะช่วยระบุความรุนแรงของภัยคุกคามทางไซเบอร์และความเร่งด่วนของกิจกรรมการรับมือ

จาก Incident Response Plan Template, FRSecure (Version 1.0.0) มีการระบุ การจำแนกระดับการตอบสนอง (Response Level Classification) และระดับความรุนแรง (Severity Level) ตามตารางด้านล่าง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

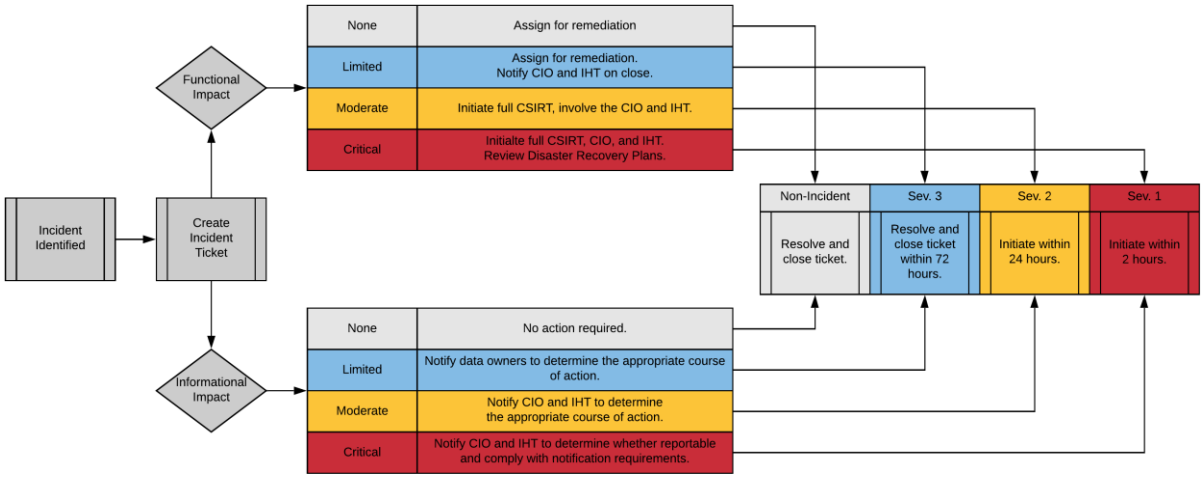
การจำแนกระดับการตอบสนอง (Response Level Classification)		ผลกระทบต่อสารสนเทศ (Informational Impact)			
		ไม่มี (None)	ไม่ร้ายแรง (Limited)	ร้ายแรง (Moderate)	วิกฤต (Critical)
ผลกระทบการทำงาน (Functional Impact)	(1) ไม่มี (Incidental/None)	N/A	Sev. 3	Sev. 2	Sev. 1
	(2) ไม่ร้ายแรง ((Minor /Limited)	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	(3) ปานกลาง (Moderate)หรือ เริ่มร้ายแรง	Sev. 3	Sev. 3	Sev. 2	Sev. 1
	(4) ร้ายแรง ร้ายแรง(Major/High)	Sev. 2	Sev. 2	Sev. 2	Sev. 1
	(5) วิกฤติ (Extreme/Critical)	Sev. 1	Sev. 1	Sev. 1	Sev. 1

ตารางที่ 3-9 การจำแนกระดับการตอบสนอง

ควรใช้ระดับความรุนแรง (Severity Level) เพื่อกำหนดว่ากิจกรรมตอบสนองเริ่มต้นควรเกิดขึ้นเร็วเพียงใด

ระดับความรุนแรง	SLA
Sev. 3	ภายใน 1-12 ชั่วโมง
Sev. 2	ภายใน 1-6 ชั่วโมง
Sev. 1	ภายใน 1 ชั่วโมง

ตารางที่ 3-10 ระดับความรุนแรงและการตอบสนองตาม SLA



รูปที่ 3-5: ระดับการรับมือช่วยระบุความรุนแรงของภัยคุกคามทางไซเบอร์และความเร่งด่วนของกิจกรรมการรับมือ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการตรวจจับและวิเคราะห์ (Key Decisions for Exiting Detection and Analysis Phase):

- หากกระบวนการตรวจจับและวิเคราะห์ได้กำหนดว่าเหตุการณ์นั้นเป็นภัยคุกคามทางไซเบอร์จริง กระบวนการ IR จะต้องดำเนินต่อไป
- รายละเอียดทั้งหมดในขั้นตอนการตรวจจับจะต้องบันทึกไว้ในแบบฟอร์มการรายงานภัยคุกคามทางไซเบอร์ หากเหตุการณ์นั้นถูกกำหนดให้เป็นภัยคุกคามทางไซเบอร์

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

3.2.3 ขั้นตอนที่ 3 การจำกัดขอบเขต (Containment) การกำจัด (Eradication) และการกู้คืน (Recovery)

3.2.3.1 ขั้นตอนที่ 3.1 การจำกัดขอบเขต (*Containment*)

วัตถุประสงค์ของขั้นตอนการจำกัดขอบเขตในการรับมือเหตุภัยคุกคามทางไซเบอร์คือเพื่อควบคุมสถานการณ์ได้อีกครั้งและจำกัดขอบเขตของความเสียหาย เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานได้กำหนดกลยุทธ์การจำกัดขอบเขตจำนวนหนึ่งที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ อ้างอิงขั้นตอนที่เกี่ยวข้องกับกลยุทธ์การจำกัดขอบเขตอย่างน้อยหนึ่งรายการตามรายการด้านล่าง

3.2.3.1.1 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)

ใช้รายการกลยุทธ์ด้านล่างเพื่อเลือกขั้นตอนที่เหมาะสมที่สุดสำหรับสถานการณ์ ขั้นตอนทั้งหมดสำหรับแต่ละกลยุทธ์ที่ระบุไว้ด้านล่างมีอยู่ในภาคผนวก VIII หากไม่มีกลยุทธ์ใดที่ตรงกับสถานการณ์ปัจจุบันให้อ้างอิงถึงขั้นตอนการจำกัดขอบเขตทั่วไปที่แสดงด้านล่าง

- ข้อมูลประจำตัวที่ถูกขโมย (Stolen Credentials) ปิดใช้งานข้อมูลประจำตัวของบัญชี รีเซ็ตการเชื่อมต่อที่ใช้งานอยู่ทั้งหมด ตรวจสอบกิจกรรมของผู้ใช้ ย้อนกลับการเปลี่ยนแปลง (Reverse Changes) ไปสู่สภาวะเดิม เพิ่มการแจ้งเตือน เสริมความแข็งแกร่งจากการโจมตีในอนาคต
- แรนซัมแวร์ (Ransomware) แยกระบบที่ได้รับผลกระทบ ตรวจสอบการเรียกร้องค่าไถ่ ติดต่อผู้ให้บริการประกันภัย ระบุว่าระบบเพิ่มเติมได้รับผลกระทบหรือไม่ และแยกตามความจำเป็น
- DOS/DDOS ควบคุม WAN/ISP
- การระบาดของไวรัส (Virus Outbreak) แยก LAN/ระบบ ออกจากการเชื่อมต่อเครือข่าย
- การสูญหายของข้อมูล (Data Loss) ตรวจสอบกิจกรรมของผู้ใช้ ดำเนินการตามขั้นตอนการรับมือต่อการละเมิดข้อมูล
- การทำให้เว็บไซต์เสียหาย (Website Defacement) ซ่อมแซมเว็บไซต์ เสริมความแข็งแกร่งจากการโจมตีในอนาคต
- API โดนโจมตี (Compromised API) – ตรวจสอบการเปลี่ยนแปลงที่เกิดขึ้น ซ่อมแซม API เสริมความแข็งแกร่งจากการโจมตีในอนาคต

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.2.3.1.2 ขั้นตอนการจำกัดขอบเขตทั่วไป (Common Containment Steps)

การจำกัดขอบเขตต้องมีการตัดสินใจที่สำคัญเกี่ยวกับธรรมชาติของภัยคุกคามทางไซเบอร์ ผู้จัดการการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Manager) ร่วมกับผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Commander) และสมาชิกคนอื่น ๆ ของฝ่ายบริหารควรทบทวนขั้นตอนการจำกัดขอบเขตทั้งหมดที่ระบุไว้ด้านล่าง เพื่อกำหนดกลยุทธ์ในการจำกัดขอบเขตและจำกัดความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

ความพยายามทั้งหมดในการยับยั้งภัยคุกคามจะต้องพิจารณาทุกความพยายามเพื่อลดผลกระทบต่อการดำเนินธุรกิจให้เหลือน้อยที่สุด อาจจำเป็นต้องแจ้งบุคคลที่สามหรือผู้มีส่วนได้ส่วนเสีย ในกรณีที่อาจ มีการบังคับใช้กฎหมายเข้ามาเกี่ยวข้อง จะต้องพยายามรักษาความสมบูรณ์ของข้อมูลทางนิติวิทยาศาสตร์หรือบันทึกข้อมูลที่เกี่ยวข้อง และรักษาห่วงโซ่การควบคุม (Chain-of-custody) ที่ชัดเจน ในกรณีที่ไม่สามารถรักษาหลักฐานอย่างเหมาะสมเนื่องจากความพยายามในการจำกัดขอบเขต จะต้องจัดทำเอกสารความคลาดเคลื่อน (Discrepancy) ที่เกิดขึ้น

เมื่อประเมินขั้นตอนการจำกัดขอบเขต ให้พิจารณาสิ่งต่อไปนี้:

- เปิดใช้งานบัญชีการดูแลระบบแบบใช้แล้วสิ้นสุด (ใช้เฉพาะกิจ) เพื่อใช้ในระหว่างการสืบสวนสอบสวนและรีเซ็ตรหัสผ่านที่เกี่ยวข้องหากเชื่อว่ามีความเสี่ยงที่จะถูกโจมตีขณะใช้งาน (ดูขั้นตอนที่ 1 รายละเอียดการจัดเตรียม)
- ความสามารถในการให้บริการที่สำคัญจะได้รับผลกระทบหรือไม่? ยังไง? นานแค่ไหน?
- ควรแจ้งผู้ให้บริการประกันภัยไซเบอร์เมื่อใด (ดูข้อมูลการติดต่อ)
- มีการสืบสวนสอบสวนทางกฎหมายหรือการดำเนินการอื่น ๆ หรือไม่? หลักฐานต้องเก็บไว้หรือไม่? (ดูการเก็บรักษาหลักฐาน)
- เป็นไปได้แค่ไหนที่ขั้นตอนการจำกัดขอบเขตจะสำเร็จ? ผลลัพธ์ที่ได้คืออะไร สมบูรณ์หรือบางส่วน?
- ทรัพยากรใดบ้างที่จำเป็นในการสนับสนุนกิจกรรมการจำกัดขอบเขต?
- ความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์และทรัพยากรอื่น ๆ คืออะไร?
- ระยะเวลาที่คาดหวังของการแก้ปัญหาคือเท่าไร? (ชั่วคราว ระยะสั้น ระยะยาว หรือถาวร)
- สมาชิกในทีม IR ควรดำเนินการอย่างไม่ต่อเนื่อง (Act Discretely) เพื่อพยายามซ่อนกิจกรรมของตนจากผู้โจมตีหรือไม่?
- จำเป็นต้องมีความช่วยเหลือจากบุคคลที่สามหรือไม่? เวลาตอบสนองที่คาดหวังคืออะไร?
- ต้องแจ้งผู้มีส่วนได้เสีย (ลูกค้า คู่ค้า นักลงทุน) หรือไม่? ถ้าเป็นเช่นนั้นเมื่อไหร่? (ดูภาคผนวก IV)
- ผลกระทบต่ออุปกรณ์ เครือข่าย หรือสิ่งอำนวยความสะดวก (ของหน่วยงาน) มีความจำเป็นต่อการเปิดใช้งานแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) หรือไม่?
- ข้อมูลที่ได้รับผลกระทบรวมถึงข้อมูลที่ได้รับการคุ้มครอง เช่น ข้อมูลผู้ถือบัตรหรือไม่ ถ้าใช่ โปรดดูข้อกำหนดการแจ้งเตือน

3.2.3.1.3 การใช้ทรัพยากร (Engage Resources)

CIRT ควรเลือกตัวเลือกตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์ ความเสียหายที่เกิดขึ้นโดยของหน่วยงาน และข้อพิจารณาทางกฎหมาย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	การสืบสวนสอบสวนภายใน (In-house Investigation)	การบังคับใช้กฎหมาย (Law Enforcement)	ผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์เอกชน (Private Forensic Specialist)
เวลาในการตอบสนอง	ตอบสนองอย่างรวดเร็ว	แตกต่างกันไปตามพื้นที่และหน่วยงาน	ตอบสนองอย่างรวดเร็ว
ความสามารถ	ทักษะแตกต่างกันไป	ขึ้นอยู่กับการบังคับใช้กฎหมายในท้องถิ่น	มีทักษะสูง มักมีพื้นฐานด้านการบังคับใช้กฎหมาย
การเก็บรักษาหลักฐาน	ไม่รับรองความถูกต้องของหลักฐาน	รักษาความสมบูรณ์ของหลักฐานและนำเสนอหลักฐานในศาล	รักษาความสมบูรณ์ของหลักฐานและนำเสนอหลักฐานในศาล
ผลกระทบด้านชื่อเสียง	ผลกระทบน้อยที่สุด	อาจสูญเสียชื่อเสียงหากเกิดเหตุภัยคุกคามทางไซเบอร์บางอย่างขึ้นสู่สาธารณะ	อาจสูญเสียชื่อเสียงหากเกิดเหตุภัยคุกคามทางไซเบอร์บางอย่างขึ้นสู่สาธารณะ

ตารางที่ 3-11 ตัวเลือกการใช้ทรัพยากรตามความรุนแรงของเหตุภัยคุกคามทางไซเบอร์

3.2.3.1.4 เก็บรักษาหลักฐาน (Preserve Evidence)

การเก็บหลักฐานตามลำดับของการสูญสลาย (Order of Volatility)

ตามลำดับของการสูญสลาย (Order of Volatility) หมายถึงลำดับที่หน่วยงานควรรวบรวมหลักฐานที่ไม่ถาวร (หมายถึงเมื่อไม่มีแหล่งพลังงานไฟฟ้าหรือรีสาร์ทเครื่อง ข้อมูลเหล่านั้นจะหายไป) โดยทั่วไป หน่วยงานควรรวบรวมหลักฐานโดยเริ่มจากจุดที่มีการสูญสลายเร็วมากที่สุดและเคลื่อนไปสู่จุดที่มีการสูญสลายน้อยที่สุดตัวอย่างเช่น หน่วยความจำเข้าถึงโดยสุ่ม (Random Access Memory: RAM) จะหายไปหลังจากปิดเครื่องคอมพิวเตอร์ ด้วยเหตุนี้ จึงเป็นสิ่งสำคัญที่ต้องตระหนักว่า ไม่ควรปิดเครื่องคอมพิวเตอร์หากสงสัยว่าคอมพิวเตอร์เกี่ยวข้องกับเหตุการณ์ด้านความปลอดภัยและอาจมีหลักฐานอันมีค่า

โปรเซสเซอร์สามารถทำงานได้กับข้อมูลใน RAM เท่านั้น ดังนั้นข้อมูลทั้งหมดใน RAM จะบ่งบอกว่าระบบกำลังทำอะไรอยู่ ซึ่งรวมถึงข้อมูลที่ผู้ใช้กำลังดำเนินการอยู่ กระบวนการของระบบ (System Processes)กระบวนการเครือข่าย (Network Processes) ส่วนที่เหลือของแอปพลิเคชัน (Application Remnants) และอื่น ๆ อีกมากมาย ทั้งหมดนี้อาจเป็นหลักฐานอันมีค่าในการสืบสวน แต่หากช่างเทคนิคมือใหม่ปิดคอมพิวเตอร์ หลักฐานก็จะสูญหายไป

เครื่องมือทางนิติวิทยาศาสตร์หลายอย่างมีความสามารถในการเก็บข้อมูลที่มีการสูญสลาย ตัวอย่างเช่น Kali Linux มีแอปพลิเคชัน Volatility (มีอยู่ใน Applications > Forensics > Volatility) ที่สามารถจับเนื้อหาของ RAM ได้ เมื่อบันทึกข้อมูลแล้ว ผู้เชี่ยวชาญจะสามารถวิเคราะห์และรับข้อมูลเชิงลึกว่าคอมพิวเตอร์และผู้ใช้กำลังทำอะไรอยู่

ในทางตรงกันข้าม ข้อมูลบนไดรฟ์จะยังคงอยู่ในไดรฟ์แม้ว่าจะปิดระบบไปแล้วก็ตาม ซึ่งรวมถึงไฟล์ใด ๆ และแม้แต่ข้อมูลระดับต่ำ เช่น Master Boot Record บนไดรฟ์ อย่างไรก็ตาม การปกป้องข้อมูลบนดิสก์ก่อนที่จะวิเคราะห์เป็นสิ่งสำคัญ และวิธีการทั่วไปคือการจับภาพของดิสก์ (Capturing an Image of the Disk)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ลำดับของการสูญสลายมากที่สุดไปการสูญสลายน้อยที่สุด คือ:

- ข้อมูลในหน่วยความจำแคช (Cache Memory) รวมถึงแคชของโปรเซสเซอร์และแคชของฮาร์ดไดรฟ์
- ข้อมูลใน RAM รวมถึงโปรเซสของระบบและเครือข่าย (System and Network Processes)
- ไฟล์เก็บเพจ (Paging File) (บางครั้งเรียกว่าไฟล์สว็อป (Paging File)) บนดิสก์ไดรฟ์ระบบ
- ข้อมูลที่จัดเก็บไว้ในดิสก์ไดรฟ์ภายในเครื่อง (Local Disk Drives)
- บันทึกที่จัดเก็บไว้ในระบบระยะไกล (Remote Systems)
- สื่อเก็บถาวร (Archive Media)

การดำเนินการเก็บหลักฐานต้องดำเนินการโดยผู้ที่ผ่านการฝึกอบรมและมีความเชี่ยวชาญและดำเนินการตามขั้นตอนมาตรฐานที่เป็นที่ยอมรับ เพื่อให้หลักฐานนั้นมีความเชื่อถือและสามารถนำไปใช้ได้ในชั้นศาล

การดำเนินการเก็บหลักฐานต้องดำเนินการโดยผู้ที่ผ่านการฝึกอบรมและมีความเชี่ยวชาญและดำเนินการตามขั้นตอนมาตรฐานที่เป็นที่ยอมรับ เพื่อทำให้หลักฐานนั้นมีความเชื่อถือและสามารถนำไปใช้ได้ในชั้นศาล

หมายเหตุ: หากมีเหตุผลหนักแน่นที่เชื่อได้ว่ามีแนวโน้มว่าจะมีการดำเนินคดีทางอาญาหรือทางแพ่ง แบบฟอร์มห่วงโซ่การคุ้มครอง (Chain of Custody Form) ของหน่วยงาน จะต้องถูกใช้ทุกครั้งที่มีการนำหลักฐานเข้าควบคุม หรือโอนสิทธิ์การดูแลเพื่อวัตถุประสงค์ในการสืบสวนสอบสวน

กฎหมายเกี่ยวกับกฎหมายและระเบียบข้อบังคับที่เกี่ยวข้องกับการรวบรวมและการรักษามีรายละเอียดดังนี้

- หลักฐาน สร้างบันทึกโดยละเอียดสำหรับหลักฐานทั้งหมดที่รวบรวม รวมถึง:
- ข้อมูลการระบุ (เช่น หมายเลขซีเรียล รุ่น ชื่อโฮสต์ ที่อยู่ MAC ที่อยู่ IP หรือตัวระบุอื่น ๆ)
- ชื่อและข้อมูลติดต่อของบุคคลทั้งหมดที่จัดการหลักฐานในระหว่างการสืบสวนสอบสวน
- วันที่และเวลาของการโอนหรือการจัดการหลักฐานในแต่ละครั้ง
- รายชื่อสถานที่ทั้งหมดที่จัดเก็บหลักฐาน
- การเบี่ยงเบนจาก SOP และเหตุผลที่เกี่ยวข้อง

3.2.3.1.5 ลดผลกระทบ (Reduce Impact)

ขึ้นอยู่กับประเภทของภัยคุกคามทางไซเบอร์ ทีมต้องดำเนินการอย่างรวดเร็วเพื่อลดผลกระทบต่อระบบที่ได้รับผลกระทบและ/หรือลดการเข้าถึงของผู้โจมตี การดำเนินการอาจรวมถึงแต่ไม่จำกัดเพียงสิ่งต่อไปนี้:

- หยุดผู้โจมตีโดยใช้การควบคุมการเข้าถึง (Access Controls) เช่น ปิดใช้งานบัญชี รีเซ็ตการเชื่อมต่อที่ใช้งานอยู่ เปลี่ยนรหัสผ่าน ใช้ ACL ของหน่วยงานหรือกฎไฟร์วอลล์ ฯลฯ)
- แยกระบบที่ถูกบุกรุกออกจากเครือข่าย
- หลีกเลี่ยงการเปลี่ยนแปลงข้อมูลที่สูญสลายได้ง่าย (Volatile State Data) หรือข้อมูลสถานะของระบบตั้งแต่ต้น
- ระบุระบบภายนอกที่สำคัญที่ต้องทำงานอยู่ (เช่น อีเมล แอปพลิเคชันไคลเอนต์ DNS) และปฏิเสธกิจกรรมอื่น ๆ ทั้งหมด

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- รักษาโปรไฟล์ให้ต่ำ (Maintain a Low Profile) ถ้าเป็นไปได้ เพื่อหลีกเลี่ยงการแจ้งเตือนผู้โจมตีว่าหน่วยงานทราบถึงการปรากฏตัวของพวกเขาหรือให้โอกาสพวกเขาเรียนรู้กลวิธี เทคนิค หรือขั้นตอนของ CIRT
- ในขอบเขตที่เป็นไปได้ ให้พิจารณาการรักษาสถานะของระบบไว้สำหรับการตรวจสอบเพิ่มเติมหรือใช้เป็นหลักฐาน

3.2.3.1.6 รวบรวมข้อมูลและเพิ่มการบันทึกกิจกรรม (Collect Data and Increase Activity Logging)

เพิ่มการเฝ้าระวังและดักจับแพ็กเก็ตบนระบบที่ได้รับผลกระทบ ในขณะที่ CIRT ตรวจสอบขอบเขตและผลกระทบของภัยคุกคามทางไซเบอร์ ดำเนินการบันทึกและติดตามเพิ่มขึ้นต่อไปเมื่อหน่วยงานเข้าสู่ขั้นตอนการกำจัดและการกู้คืน (Eradication and Recovery Phases)

- เปิดใช้งานการดักจับแพ็กเก็ตแบบเต็ม (Enable Full Packet Capture)
- รวบรวมและตรวจสอบระบบ เครือข่าย และล็อกอื่น ๆ ที่เกี่ยวข้อง
- สร้างอิมเมจหน่วยความจำ (Memory Image) ของระบบที่ได้รับผลกระทบ
- เก็บอิมเมจทางนิติวิทยาศาสตร์ (Forensic Image) ของระบบที่ได้รับผลกระทบ
- เฝ้าระวังช่องทางการสื่อสารของผู้โจมตีที่เป็นไปได้

3.2.3.1.7 ทำการค้นหาข้อมูลเพิ่มเติม (Conduct Research)

ดำเนินการค้นหาทางอินเทอร์เน็ต ปรึกษาทรัพยากรบุคคลที่สาม และ/หรือ ปรึกษากับผู้ให้บริการประกันภัยเทคโนโลยีสารสนเทศ (IT Insurance) โดยใช้ข้อมูลจากอาการที่ชัดเจนและข้อมูลอื่น ๆ ที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์ที่หน่วยงานกำลังประสบอยู่ อาจนำไปสู่ข้อมูลเพิ่มเติมเกี่ยวกับการโจมตี ตัวอย่างเช่น หากผู้ให้บริการประกันภัยได้รับรายงานภัยคุกคามทางไซเบอร์ที่คล้ายคลึงกันหลายฉบับ หรือหากข้อความรายชื่อผู้รับจดหมาย (Mailing List Message) มี IP หรือข้อความเดียวกันของข้อความที่หน่วยงานได้รับ

3.2.3.1.8 แจ้งผู้ที่เกี่ยวข้อง (Notify Interested Parties)

เมื่อระบุเหตุภัยคุกคามทางไซเบอร์ได้แล้ว ให้พิจารณาว่ามีผู้อื่นที่จำเป็นต้องได้รับแจ้งหรือไม่ ทั้งภายใน เช่น ทรัพยากรบุคคล กฎหมาย การเงิน สื่อสารหน่วยงาน เจ้าของธุรกิจ เป็นต้น และภายนอก เช่น ผู้ให้บริการ หน่วยงานควบคุมหรือกำกับดูแล งานสาธารณะ สื่อ สัมพันธ์ ลูกค้า ประชาชนทั่วไป เป็นต้น ปฏิบัติตามหลักการ “จำเป็นต้องรู้ (Need to Know)” เสมอในการสื่อสารทั้งหมด ที่สำคัญที่สุดยังคงเป็นการสื่อสารข้อเท็จจริงและหลีกเลี่ยงการคาดเดา

ทั้งนี้ขึ้นอยู่กับระดับความอ่อนไหวของเหตุภัยคุกคามทางไซเบอร์ ฝ่ายกฎหมาย/ฝ่ายจัดการอาจจำเป็นต้องกำหนดให้พนักงานลงนามข้อตกลงรักษาความลับ (NDA) หรือออกคำสั่งให้รักษาความลับกับพนักงานที่จำเป็นต้องมีส่วนร่วม ทั้งนี้ขึ้นอยู่กับระดับความอ่อนไหวของเหตุภัยคุกคามทางไซเบอร์

3.2.3.1.9 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการจำกัดขอบเขต (Key Decisions for Exiting Containment Phase)

- ความสามารถของผู้โจมตีในการส่งผลกระทบต่อเครือข่ายได้รับการควบคุม/หยุดอย่างมีประสิทธิภาพ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ระบุระบบที่ได้รับผลกระทบ
- ระบบที่ถูกบุกรุก ข้อมูลที่สูญสลายได้ (volatile Data) ที่สามารถรวบรวมได้ อิมเมจหน่วยความจำที่รวบรวม และดิสก์ที่ถูกอิมเมจสำหรับการวิเคราะห์

3.2.3.1.10 การสืบสวนสอบสวน (Investigation)

ในขณะที่ CIRT ทำงานเพื่อจำกัดขอบเขต (Contain) กำจัด (Eradicate) และฟื้นฟู (Recover) จากเหตุภัยคุกคามทางไซเบอร์ดังกล่าว การสืบสวนสอบสวนจะดำเนินต่อไป ในขณะที่การสืบสวนสอบสวนดำเนินไป หน่วยงานอาจพบว่าเหตุภัยคุกคามทางไซเบอร์นั้นไม่ได้ถูกจำกัดขอบเขต กำจัดหรือกู้คืน อย่างสมบูรณ์หากเป็นสถานการณ์ดังกล่าว อาจจำเป็นต้องทบทวนขั้นตอนก่อนหน้านี้เพิ่มเติม ขั้นตอนการจำกัดขอบเขต การกำจัด และการกู้คืนมักเป็นวัฏจักร

การสืบสวนสอบสวนพยายามระบุระบบ บริการ และข้อมูลทั้งหมดที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์อย่างครบถ้วน รวมถึงการวิเคราะห์สาเหตุที่แท้จริง (Root Cause) ซึ่งช่วยในการระบุจุดเริ่มต้นของผู้โจมตีหรือจุดอ่อนในระบบที่ทำให้เหตุการณ์ขยายไปสู่ภัยคุกคามทางไซเบอร์ได้

อาจต้องทำสัญญากับบุคคลที่สาม หากการสืบสวนสอบสวนอยู่นอกเหนือทักษะของ CIRT เช่น ระบบที่ได้รับผลกระทบนั้นเป็นของผู้ให้บริการคลาวด์ หรือจำเป็นต้องมีการวิเคราะห์ทางนิติวิทยาศาสตร์

3.2.3.1.11 การสืบสวนสอบสวนสาเหตุเบื้องต้นและสาเหตุที่แท้จริง (Root Cause)

ควรดำเนินการสืบสวนสอบสวนโดยคำนึงถึงผลกระทบอย่างต่อเนื่องต่อการดำเนินธุรกิจที่สำคัญ ตามหลักการแล้วควรสรุปการสืบสวนสอบสวนสาเหตุเบื้องต้นก่อนออกจากขั้นตอนการกำจัด อย่างไรก็ตาม ในบางครั้ง อาจจำเป็นหรือเหมาะสมที่จะดำเนินการสืบสวนสอบสวนต่อไปในระหว่างหรือหลังการกำจัดและการกู้คืน การล่าช้าในการสืบสวนสอบสวนควรพิจารณาเมื่อ CIRT มั่นใจว่าเหตุการณ์ได้รับการควบคุมอย่างสมบูรณ์และทราบขอบเขตทั้งหมดของผลกระทบแล้ว ความล่าช้าหรือการปรับเปลี่ยนขอบเขตของกิจกรรมการสืบสวนสอบสวนต้องได้รับอนุมัติจากผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์

เทคนิคการสืบสวนสอบสวนที่ใช้จะแตกต่างกันไปตามประเภทของเหตุการณ์ การสืบสวนสอบสวนอาจอาศัยบางส่วน (หรือทั้งหมด) ต่อไปนี้:

- สัมภาษณ์พยานและ/หรือบุคคลที่ได้รับผลกระทบ
- การทำอิมเมจ สแน็ปช็อต หรือดัมป์หน่วยความจำ (Memory Dumps) ของระบบที่ได้รับผลกระทบ
- การได้เอกสารที่เกี่ยวข้อง
- ดำเนินการสังเกตการณ์
- การถ่ายภาพสถานที่ทางกายภาพ
- ตรวจสอบภาพจากกล้องวงจรปิด
- วิเคราะห์ล็อกของอุปกรณ์ เทคโนโลยี และโฮสต์ต่างๆ ที่เกี่ยวข้อง (เช่น ไฟร์วอลล์ หน่วยงานเตอร์ แอนตี้ไวรัส การตรวจจับการบุกรุก (Intrusion Detection) โฮสต์)
- การตรวจสอบกฎอีเมล์ (บัญชีอีเมลที่ถูกบุกรุก)
- เปรียบเทียบระบบที่ถูกบุกรุกกับสำเนาที่ดีที่รู้จัก (Known Good Copy)
- การตรวจจับความผิดปกติ/การเฝ้าระวังพฤติกรรม (เปรียบเทียบกับค่าขั้นต่ำที่กำหนดไว้ล่วงหน้า (Pre-established Baseline)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.2.3.2 ขั้นตอนที่ 3.2 รายละเอียดการกำจัด (*Eradication*)

การกำจัดประกอบด้วยการกำจัดองค์ประกอบทั้งหมดของภัยคุกคามทางไซเบอร์ทั้งหมด

3.2.3.2.1 การกำจัด (Eradication)

หมายเหตุ: เครื่องมือการดูแลระบบที่อยู่บนโฮสต์ที่ถูกบุกรุกสามารถแก้ไขเวอร์ชันดั้งเดิมได้ ให้ใช้ชุดเครื่องมือการดูแลระบบแยกต่างหาก (เช่น ดิสก์สำหรับบูต) มากกว่าชุดเครื่องมือบนโฮสต์ที่ถูกบุกรุกเพื่อสืบสวนสอบสวนทุกครั้งที่ทำได้

ขั้นตอนในการกำจัดองค์ประกอบของภัยคุกคามทางไซเบอร์อาจรวมถึง:

- ปิดการใช้งานบัญชีผู้ใช้ที่ถูกละเมิด
- รีเซ็ตเซสชันที่ใช้งานอยู่สำหรับบัญชีที่ละเมิด
- ระบุและบรรเทาช่องโหว่ที่ผู้โจมตีใช้
- ปิดพอร์ตที่เปิดโดยไม่จำเป็น
- เพิ่มมาตรการรักษาความมั่นคงปลอดภัยในการตรวจพิสูจน์ตัวตน (Authentication Security Measures) เช่น ใช้ MFA, เพิ่มการจำกัดตำแหน่งทางภูมิศาสตร์
- เพิ่มการล็อกการรักษาความมั่นคงปลอดภัย (Security Logging) การแจ้งเตือน และการเฝ้าระวัง (Monitoring)
- ล้างการติดตั้งระบบปฏิบัติการและแอปพลิเคชันที่ได้รับผลกระทบ

ระบบปฏิบัติการและแอปพลิเคชันที่ติดตั้งใหม่ทั้งหมดจะต้องติดตั้งตามมาตรฐานการสร้างระบบ (System Build Standards) ซึ่งรวมถึงแต่ไม่จำกัดเพียง:

1) การใช้แพตช์ความมั่นคงปลอดภัยล่าสุด (Latest Security Patches) ทั้งหมด

2) ปิดการใช้งานบริการที่ไม่จำเป็นทั้งหมด

3) การติดตั้งซอฟต์แวร์ป้องกันไวรัส

4) ใช้ค่าขั้นต่ำการกำหนดค่าระบบที่แข็งขึ้น (Hardened System Configuration Baselines)

5) การเปลี่ยนรหัสผ่านของบัญชีทั้งหมด (รวมถึงโดเมน ผู้ใช้ และบัญชีบริการ)

หมายเหตุ: อาจเป็นไปได้ที่จะกู้คืนระบบโดยไม่ต้องทำการติดตั้งใหม่ทั้งหมด บุคลากรด้านเทคโนโลยีสารสนเทศจะดำเนินการตามทิศทางของ CIRT ที่จะทำการตัดสินใจนี้

3.2.3.2.2 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการกำจัด (Key Decisions for Exiting Eradication Phase)

- มีการระบุสาเหตุที่แท้จริงและช่องโหว่ที่ระบุได้รับการแก้ไขแล้วหรือไม่?
- บัญชีที่ได้รับผลกระทบทั้งหมด รวมถึงข้อมูลประจำตัวของเครื่องเขียน CIRT (CIRT Burner Credentials) ถูกรีเซ็ตหรือไม่
- CIRT มั่นใจว่าเครือข่ายและระบบได้รับการกำหนดค่าให้กำจัดการเกิดขึ้นซ้ำ
- ไม่มีหลักฐานของเหตุการณ์หรือภัยคุกคามทางไซเบอร์ที่เกิดซ้ำ
- การลงชื่อจาก IR Manager สำหรับภัยคุกคามทางไซเบอร์ที่มีความรุนแรงจำกัด (Limited-severity Incidents) หรือ CIO สำหรับภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤต

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.2.3.3 ขั้นตอนที่ 3.3 รายละเอียดการกู้คืน (*Recovery Details*)

ก่อนที่จะกู้คืนระบบสู่การทำงานปกติ เป็นสิ่งสำคัญที่ CIRT ตรวจสอบระบบเพื่อพิจารณาว่า การกำจัด (Eradication) สำเร็จ และเครือข่ายมีความมั่นคงปลอดภัย เมื่อหน่วยงานถูกโจมตีสำเร็จ ผู้โจมตีมักจะโจมตีอีกครั้งโดยใช้เครื่องมือและเทคนิคเดิมที่ใช้ในการโจมตีครั้งแรก เมื่อเข้าถึงระบบหรือเครือข่ายที่ถูกบุกรุกได้เพียงครั้งเดียว ผู้โจมตีจะมีข้อมูลเพิ่มเติมพร้อมใช้ในการโจมตีในอนาคต

หากเป็นไปได้ ควรติดตั้งระบบในสภาพแวดล้อมการทดสอบ (Test Environment) เพื่อกำหนดฟังก์ชันการทำงานก่อนที่จะนำกลับมาใช้ใหม่ในสภาพแวดล้อมการใช้งานจริง (Production Environment)

นอกจากนี้ ควรมีการเฝ้าระวังเครือข่ายนานเท่าที่จำเป็นเพื่อตรวจหาความพยายามในการเข้าถึงโดยไม่ได้รับอนุญาต

ขั้นตอนการกู้คืนอาจรวมถึง:

- การกู้คืนระบบจากการสำรองข้อมูลที่ปลอดภัย (Lean Backup)
- แทนที่ข้อมูลที่เสียหายจากการสำรองข้อมูลที่ปลอดภัย (Clean Backup)
- การกู้คืนการเชื่อมต่อเครือข่ายและกฎการเข้าถึง
- การสื่อสารกับผู้มีส่วนได้ส่วนเสียเกี่ยวกับการเปลี่ยนแปลงที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่เพิ่มขึ้น
- เพิ่มกิจกรรมการเฝ้าระวังเครือข่ายและระบบ (ระยะสั้นหรือระยะยาว)
- เพิ่มการสื่อสารภายใน/การรายงานที่เกี่ยวข้องกับการเฝ้าระวัง
- ว่าจ้างบุคคลที่สามเพื่อสนับสนุนการตรวจจับหรือป้องกันการโจมตีในอนาคต

3.2.3.3.1 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนการกู้คืน (Key Decisions for Exiting Recovery Phase)

- มีการกู้คืนการดำเนินธุรกิจแล้วหรือไม่? (Have Business Operations Been Restored)

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทาง ไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

3.2.4 ขั้นตอนที่ 4 การทบทวนหลังการดำเนินการ (After-Action Review Process)

การทบทวนหลังการดำเนินการเป็นการติดตามผล (Follow-up) ซึ่งประกอบด้วยการรายงานและการวิเคราะห์หลังภัยคุกคามทางไซเบอร์เกี่ยวกับระบบที่เป็นเป้าหมายของภัยคุกคามทางไซเบอร์และระบบอื่น ๆ ที่อาจมีความเสี่ยง วัตถุประสงค์ของขั้นตอนนี้คือการปรับปรุงอย่างต่อเนื่องในการดำเนินการด้านความมั่นคงปลอดภัย ความสามารถในการรับมือ และขั้นตอนต่าง ๆ

3.2.4.1 เอกสาร (*Documentation*)

รายละเอียดทั้งหมดที่เกี่ยวข้องกับกระบวนการรับมือเหตุภัยคุกคามทางไซเบอร์จะต้องได้รับการจัดทำเป็นเอกสารอย่างเป็นทางการและเป็นไฟล์เพื่อให้ง่ายต่อการอ้างอิง ต้องบำรุงรักษารายการต่อไปนี้เมื่อทำได้:

1) เหตุการณ์ของระบบทั้งหมด (All System Events) ดูจากบันทึกการตรวจสอบ (Audit Records) หรือล็อก (Log)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2) การดำเนินการทั้งหมด รวมถึงวันที่และเวลาที่ดำเนินการ

3) การสื่อสารภายนอกทั้งหมด

4) บันทึกของผู้สืบสวนสอบสวนที่รวบรวม

5) การเบี่ยงเบนใด ๆ จาก SOP และการให้เหตุผล

รายงานภัยคุกคามทางไซเบอร์ที่จัดทำเป็นเอกสารต่อไปนี้จะถูกเขียนโดย CIRT เมื่อสิ้นสุดการตอบสนอง (Response):

1) คำอธิบายลำดับเหตุการณ์ที่แน่นอน

2) วิธีการค้นพบ

3) มาตรการป้องกันที่มีใช้งานอยู่

4) การประเมินเพื่อพิจารณาว่าการกู้คืนเพียงพอหรือไม่และควรพิจารณาข้อเสนอแนะอื่นใด

วัตถุประสงค์ของการรายงาน คือ เพื่อระบุจุดที่อาจต้องปรับปรุงในการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรายงาน ดังนั้น การทบทวนรายงานโดยฝ่ายบริหารควรจัดทำเป็นเอกสารพร้อมกับบทเรียนที่ได้รับ เพื่อปรับปรุงพื้นที่ที่ระบุและใช้เป็นข้อมูลอ้างอิงสำหรับภัยคุกคามทางไซเบอร์ในอนาคต

3.2.4.2 บทเรียนที่ได้รับและการแก้ไข (*Lessons Learned and Remediation*)

CIRT จะหารือกับฝ่ายที่เกี่ยวข้อง เช่น เจ้าหน้าที่ด้านเทคนิค ผู้บริหาร ผู้ขาย ทีมรักษาความมั่นคงปลอดภัย เป็นต้น เพื่อรวบรวมบทเรียนที่ได้รับจากภัยคุกคามทางไซเบอร์ดังกล่าวเพื่อลดความเสี่ยงของเหตุการณ์ในอนาคต ตามความเข้าใจในสาเหตุที่แท้จริง หน่วยงานจะดำเนินการตามขั้นตอนต่าง ๆ เพื่อเสริมสร้างและปรับปรุง ระบบสารสนเทศ นโยบาย ขั้นตอน การป้องกัน และ/หรือการฝึกอบรมตามความจำเป็น ในกรณีที่การบรรเทาผลกระทบหรือการเปลี่ยนแปลงที่เสนอถูกปฏิเสธ จะต้องปฏิบัติตามกระบวนการยอมรับความเสี่ยง ควรมีการวิเคราะห์ภัยคุกคามทางไซเบอร์เพื่อค้นหาแนวโน้ม ควรพิจารณาการดำเนินการแก้ไขสาเหตุ (Corrective Action) ตามความเหมาะสม

การอภิปรายบทเรียนที่ได้รับ ควรครอบคลุม:

- ทบทวนการค้นพบและการรับมือเหตุภัยคุกคามทางไซเบอร์
- พนักงานและผู้บริหารทำงานได้ดีเพียงใดและปฏิบัติตามขั้นตอนที่เป็นเอกสารหรือไม่
- ทบทวนการกระทำที่ชะลอหรือขัดขวางความพยายามในการกู้คืน
- เสนอการปรับปรุงเพื่อการรับมือในอนาคตและความพยายามในการสื่อสาร
- คำแนะนำเพื่อเพิ่มความเร็วในการตรวจจับและตอบสนองในอนาคต
- คำแนะนำสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้น

เมื่อสิ้นสุดการประชุมบทเรียนที่เรียนรู้ ต้องมีการแก้ไขบางอย่าง ไม่ว่าจะเป็นการแก้ไขปัญหา ติดตั้งการควบคุมการชดเชย (Compensating Controls) หรืออย่างน้อยก็ประเมินและยอมรับความเสี่ยงอย่างเป็นทางการ ต้องมีการเพิ่มข้อเสนอแนะสำหรับความพยายามในการแก้ไขในระยะยาวและระยะสั้นลงในแผนการจัดการความเสี่ยง (Treatment Plan) โดยรวม

ควรพิจารณาและรวมการปรับปรุงขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์เมื่อพบส่วนต่าง ๆ ที่สามารถปรับปรุงได้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การแบ่งปันข้อมูลโดยสมัครใจควรเกิดขึ้นเมื่อใดก็ตามที่เป็นไปได้กับผู้มีส่วนได้ส่วนเสียภายนอก เพื่อให้เกิดการรับรู้ถึงสถานการณ์ความมั่นคงปลอดภัยทางไซเบอร์ในวงกว้าง ต้องปรึกษาฝ่ายกฎหมายและการจัดการก่อนที่จะทำเช่นนั้น หากไม่มีนโยบายและกระบวนการแบ่งปันข้อมูลอย่างเป็นทางการ

3.2.4.3 การวิเคราะห์ทางนิติวิทยาศาสตร์และการเก็บรักษาข้อมูล

ในกรณีที่อาจมีการดำเนินการทางกฎหมาย การวิเคราะห์ทางนิติวิทยาศาสตร์ (Forensic Analysis) จะเกิดขึ้นในลักษณะที่จะรักษาหลักฐานดิจิทัล (Preserve Digital Evidence) ที่สอดคล้องกับข้อกำหนดทางกฎหมายและกฎระเบียบที่เกี่ยวข้อง อาจจำเป็นต้องมีที่ปรึกษากฎหมายภายนอกและผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์

พิจารณาสิ่งต่อไปนี้เมื่อตัดสินใจว่าจะเก็บหลักฐานที่เกี่ยวข้องกับเหตุการณ์หรือไม่และนานแค่ไหน:

- **การดำเนินคดี (Prosecution)** เป็นไปได้ไหมที่ผู้โจมตีจะถูกดำเนินคดี? หากเป็นเช่นนั้น อาจต้องเก็บหลักฐานไว้หลายปี
- **การเกิดซ้ำ (Reoccurrence)** พิจารณาว่าหลักฐานที่รวบรวมอาจเป็นประโยชน์ในกรณีที่ผู้โจมตีหรือการโจมตีที่คล้ายกันจะเกิดขึ้นในอนาคต
- **นโยบายการเก็บรักษาข้อมูล (Data Retention Policies)** พิจารณาเนื้อหาของหลักฐานที่เก็บไว้ เช่น การจับภาพระบบ (System Image Capture) เป็นต้น และนโยบายการเก็บรักษาเกี่ยวข้องกับข้อมูลนี้ เช่น นโยบายการเก็บรักษาอีเมล์ เป็นต้น
- **ต้นทุน (Cost)** ขึ้นอยู่กับชนิดและปริมาณของข้อมูลหรืออุปกรณ์ที่เก็บรักษาไว้เป็นหลักฐาน ต้นทุนอาจเป็นปัจจัยจำกัด

3.2.4.4 การตัดสินใจที่สำคัญสำหรับการออกจากขั้นตอนบทเรียนที่เรียนรู้

- ผู้บริหารพอใจที่เหตุภัยคุกคามทางไซเบอร์สิ้นสุด
- ผู้จัดการ IR ทำการตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ที่มีความรุนแรงจำกัด (Limited-severity Incidents)
- CIO เป็นผู้ตัดสินใจสำหรับเหตุภัยคุกคามทางไซเบอร์ระดับร้ายแรงและระดับวิกฤต (Moderate and Critical-severity Incidents)
- มีแผนปฏิบัติการเพื่อตอบสนองต่อปัญหาการดำเนินงาน (Operational Issues) ที่เกิดขึ้นจากเหตุภัยคุกคามทางไซเบอร์นี้ ณ จุดนี้ ได้เวลากลับสู่ขั้นตอนที่ 1 การเตรียมการ

หมายเหตุ: หน่วยงานต้องพิจารณาดำเนินมาตรการตามรายละเอียดที่ระบุใน ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

3.3 การแจ้งเตือนและการสื่อสาร (Notification and Communication)

การแจ้งเตือนและการสื่อสารที่จำเป็นทั้งภายในและกับบุคคลที่สาม เช่น ลูกค้า ผู้ขาย สมกช. หน่วยงานบังคับใช้กฎหมาย เป็นต้น ตามข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และสัญญาต้องดำเนินการในเวลาที่เหมาะสม

- ผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์ต้องรายงานเหตุการณ์ต่อผู้บริหารระดับสูง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ผู้บริหารระดับสูงต้องรายงานการละเมิดที่อาจเกิดขึ้นและ/หรือเหตุการณ์ที่เกี่ยวข้องกับข้อมูลลูกค้าไปยัง Incident Handling Team (IHT) ทันที
- IHT มีหน้าที่รับผิดชอบในการแจ้งที่เหมาะสมไปยัง:
  - บุคลากร
  - ลูกค้าและ/หรือคู่ค้าที่ได้รับผลกระทบ ภายในระยะเวลาที่กำหนดไว้ เช่น 24 หรือ 48 ชั่วโมง เป็นต้น ตาม SLA ตามการปฏิบัติตามกฎหมาย หรือกฎระเบียบที่เกี่ยวข้อง แล้วแต่ว่าระยะเวลาใดจะสั้นกว่า
  - เจ้าหน้าที่กฎหมายท้องถิ่น หรือรัฐบาลตามที่กำหนดโดยกฎเกณฑ์และ/หรือระเบียบข้อบังคับที่บังคับใช้

ขึ้นอยู่กับประเภทและขอบเขตของการละเมิด อาจพิจารณาใช้รายงานการละเมิดข้อมูลลูกค้า (Customer Data Breach Report) เพื่อแจ้งหน่วยงานธุรกิจที่ได้รับผลกระทบ

3.3.1 การปฏิสัมพันธ์กับการบังคับใช้กฎหมาย (InterAction with Law Enforcement)

การปฏิสัมพันธ์ระหว่างเจ้าหน้าที่บังคับใช้กฎหมายกับเจ้าหน้าที่บริการฉุกเฉิน (Emergency Services Personnel) ควรได้รับการประสานงานโดยผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์

ผู้บัญชาการรับมือเหตุภัยคุกคามทางไซเบอร์จะจัดการการสื่อสารอย่างต่อเนื่อง (Ongoing Communication) กับเจ้าหน้าที่ อย่างไรก็ตาม ต้องสังเกตว่าลำดับความสำคัญของการบังคับใช้กฎหมายคือการดำเนินคดีกับผู้กระทำความผิดในท้ายที่สุด และไม่จำเป็นต้องทำให้บริษัทกลับสู่สถานะการทำงานปกติ ตรวจสอบให้แน่ใจว่ามีการปรึกษาหารือและให้คำแนะนำด้านกฎหมายก่อนและขณะสื่อสารกับหน่วยงานบังคับใช้กฎหมาย

3.3.2 หน่วยงานควบคุมหรือกำกับดูแล (Regulatory Authorities)

หน่วยงานอยู่ภายใต้การกำกับดูแลด้านกฎระเบียบต่าง ๆ ขึ้นอยู่กับข้อมูลที่ได้รับผลกระทบ หากมีความเป็นไปได้ที่ข้อมูลที่ถูกควบคุมอาจถูกละเมิด อาจจำเป็นต้องแจ้งสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล ตามที่กำหนดไว้ในพระราชบัญญัติคุ้มครองข้อมูล ส่วนบุคคล พ.ศ. 2562 หากหน่วยงานต้องปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 58 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงานนั้น รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น ต้องแจ้งต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแล

ทั้งนี้ขึ้นอยู่กับลักษณะของการละเมิด อาจจำเป็นต้องติดต่อหน่วยงานกำกับดูแลของรัฐบาลอื่น ๆ ของหน่วยงาน

- เฉพาะสมาชิกของ IHT เท่านั้นที่ได้รับอนุญาตให้หารือเกี่ยวกับลักษณะและ/หรือรายละเอียดของเหตุการณ์กับหน่วยงานควบคุมหรือกำกับดูแลใด ๆ
- IHT ควรติดต่อหน่วยงานควบคุมหรือกำกับดูแลโดยเร็วที่สุดเท่าที่เป็นไปได้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.3.3 ผู้รับบริการ (Customers)

- ผู้รับบริการทุกคนที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์จะต้องได้รับแจ้งตามที่ระบุไว้ในสัญญาที่เกี่ยวข้อง ข้อตกลงระดับการบริการ (Service Level Agreements: SLA) กฎเกณฑ์และ/หรือระเบียบข้อบังคับที่เกี่ยวข้อง
- การสื่อสารกับผู้รับบริการต้องสอดคล้องกัน โดยมีข้อความที่เหมือนกันหรือคล้ายกันที่ส่งถึงแต่ละบุคคล ข้อความที่ส่งถึงลูกค้าจะถูกสร้างขึ้นโดยสมาชิกของทีมสื่อสาร (Communications Team)
- ฝ่ายสื่อสารองค์กรจะสื่อสารกับลูกค้าตามข้อความที่ทีมสื่อสารจัดทำขึ้น

3.3.4 การจัดการสื่อสาธารณะ (Public Media Handling)

ข้อมูลทั้งหมดที่เกี่ยวข้องกับเหตุภัยคุกคามทางไซเบอร์จะถูกพิจารณาเป็นความลับ และไม่ควรมีการหารือข้อมูลใด ๆ กับบุคคลภายนอกของหน่วยงาน โดยไม่ได้รับการอนุมัติจากผู้บริหารระดับสูงและที่ปรึกษากฎหมายของหน่วยงาน

แถลงการณ์สาธารณะหรือสื่อต้องได้รับการจัดการอย่างระมัดระวังเพื่อให้แน่ใจว่าการสืบสวนสอบสวน/การดำเนินการทางกฎหมายใด ๆ จะไม่ตกอยู่ในอันตราย และลดความเสียหายต่อชื่อเสียงให้เหลือน้อยที่สุด การตัดสินใจเกี่ยวกับการเปิดเผยและวิธีการเปิดเผยข้อมูลเหตุภัยคุกคามทางไซเบอร์ของหน่วยงานจะกระทำโดยโฆษกที่ได้รับมอบหมายซึ่งได้รับมอบหมายจาก IHT เท่านั้น ซึ่งมีแนวโน้มว่ามาจากทีมสื่อสารหรือตัวแทนที่ได้รับการฝึกอบรมหรือสอนโดยทีมสื่อสาร

การสอบถามจากเอเจนซี่สื่อต้องส่งตรงไปยังตัวแทน IHT ที่ได้รับมอบหมาย พนักงานที่พบว่ากำลังพูดคุยถึงเหตุภัยคุกคามทางไซเบอร์โดยไม่ได้รับอนุมัติจากผู้บริหารระดับสูง/ที่ปรึกษากฎหมาย จะถูกลงโทษทางวินัย สูงสุดและรวมถึงการเลิกจ้าง

3.4 แผนการทดสอบและทบทวน (Plan Testing and Review)

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน และขั้นตอนต้องได้รับการทดสอบอย่างน้อยทุกปี ผู้บัญชาการ IR จะดำเนินการฝึกอบรมโดยใช้เหตุการณ์จำลองตามกำหนดเวลาเพื่อเป็นแนวทางและทดสอบขั้นตอน แผนและขั้นตอนจะต้องได้รับการอัปเดตเพื่อสะท้อนถึงบทเรียนที่ได้เรียนรู้และเพื่อรวมการพัฒนาอุตสาหกรรมใหม่ ๆ

สมาชิก CIRT, CIO และสมาชิกของ IHT ต้องเข้าร่วมในแบบฝึกหัดทดสอบอย่างน้อยปีละครั้ง

แผนรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนต่าง ๆ จะต้องได้รับการทบทวนทุกปีและมีการติดตามการอัปเดตในประวัติเวอร์ชัน (Version History) ของเอกสาร

การทบทวนแผนควรรวมถึง:

- ทบทวนเอกสารประกอบและแบบฟอร์มที่อยู่ในรายการเอกสารประกอบ (Supporting Document List) เพื่อให้แน่ใจว่าถูกต้องและมีประสิทธิภาพ
- ทบทวนภาคผนวกเพื่อให้แน่ใจว่าถูกต้องและมีประสิทธิภาพ
- ทบทวนแบบฟอร์มการรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Forms) ที่กรอกแล้วและแผนปฏิบัติการแก้ไข (Corrective Action Plans) สำหรับการปรับปรุงแผนและขั้นตอนที่แนะนำ
- เปรียบเทียบการเปลี่ยนแปลงล่าสุดกับโครงสร้างพื้นฐานของหน่วยงานและโครงสร้างการจัดการ (Organization’s Infrastructure and Management Structure) กับแผนและขั้นตอนที่จัดทำเป็นเอกสาร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.5 รายละเอียดการซ้อมแผนบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์

1. การเตรียมการ (Preparation)

- จัดตั้ง **ทีมรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์** (Cyber Incident Response Team - CIRT) ประกอบด้วยบุคลากรที่มีบทบาทสำคัญ ได้แก่ Information Security Manager, SOC Manager, และผู้เกี่ยวข้อง
- กำหนด **แนวทางการสื่อสารและกระบวนการแจ้งเตือน** ภายในองค์กร รวมถึงการประสานงานกับหน่วยงานภายนอกที่เกี่ยวข้อง
- ตรวจสอบและเตรียมความพร้อมของ **เครื่องมือ** และ **ระบบรักษาความมั่นคงปลอดภัย** อาทิ Firewall, IDS/IPS, และ SIEM
- จัด **การฝึกอบรมบุคลากร** เพื่อสร้างความเข้าใจในแผนการบริหารจัดการเหตุการณ์และขั้นตอนการตอบสนองอย่างเหมาะสม

2. การตรวจจับและวิเคราะห์ (Detection and Analysis)

- ใช้ **ระบบตรวจจับภัยคุกคาม** (Intrusion Detection System - IDS) และการวิเคราะห์ Log Files เพื่อระบุเหตุการณ์ที่ผิดปกติ
- กำหนด **เกณฑ์การแจ้งเตือนเหตุการณ์** เมื่อพบพฤติกรรมที่อาจเป็นภัยคุกคาม เช่น การเข้าถึงระบบโดยไม่ได้รับอนุญาต
- ดำเนินการ **วิเคราะห์เหตุการณ์** เพื่อยืนยันลักษณะของภัยคุกคามและจัดหมวดหมู่ระดับความรุนแรงของเหตุการณ์

3. การตอบสนองและควบคุมสถานการณ์ (Response and Containment)

- ดำเนินการ **ควบคุมสถานการณ์** (Containment) โดยแยกระบบหรือเครือข่ายที่ได้รับผลกระทบเพื่อลดความเสียหาย
- ดำเนินการแก้ไขเหตุการณ์ **ตามขั้นตอนที่กำหนดในแผน** และจัดทำรายงานเหตุการณ์อย่างละเอียด
- ประสานงานกับ **ทีมที่เกี่ยวข้อง** เช่น ทีมกฎหมาย หรือหน่วยงานภายนอกที่มีบทบาทสำคัญในการจัดการปัญหา

4. การกู้คืนและปรับปรุง (Recovery and Lessons Learned)

- ดำเนินการ **กู้คืนระบบและข้อมูล** ให้กลับเข้าสู่สถานการณ์ปกติอย่างปลอดภัย
- ตรวจสอบและแก้ไข **ช่องโหว่ในระบบ** ที่อาจเป็นต้นเหตุของเหตุการณ์
- ทบทวนและปรับปรุง **แผนบริหารจัดการเหตุการณ์** โดยอิงจากบทเรียนที่ได้จากการซ้อมแผน

ตัวอย่างรูปแบบการซ้อมแผน

1. **การจำลองสถานการณ์ (Scenario Simulation)**
   - ใช้เหตุการณ์จำลอง เช่น การโจมตีด้วย Ransomware หรือการโจมตีแบบ DDoS
   - ให้ทีม CIRT ดำเนินการตาม **ขั้นตอนที่ระบุในแผน** เพื่อประเมินประสิทธิภาพ
2. **การวัดผลและการปรับปรุง**
   - ประเมินผลการดำเนินงานจาก **เวลาในการตอบสนอง** ความถูกต้องของการวิเคราะห์เหตุการณ์ และความรวดเร็วในการกู้คืนระบบ
   - ใช้ **บทเรียนที่ได้จากการซ้อมแผน** ในการปรับปรุงกระบวนการทำงานและเพิ่มความพร้อมในการรับมือเหตุการณ์ในอนาคต

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ประโยชน์ที่ได้รับจากการซ้อมแผน

- เพิ่มความพร้อมและความมั่นใจให้แก่บุคลากรในการรับมือเหตุการณ์ภัยคุกคาม
- ลดผลกระทบทางธุรกิจและเสริมสร้างความน่าเชื่อถือขององค์กร
- พัฒนา **กระบวนการและกลยุทธ์** ในการบริหารจัดการเหตุการณ์ที่เหมาะสมกับภัยคุกคามที่เปลี่ยนแปลง

การดำเนินการตามแนวทางนี้จะช่วยให้สำนักงานสามารถตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพและรักษาความมั่นคงปลอดภัยของข้อมูลที่สำคัญต่อองค์กรและหน่วยงานที่เกี่ยวข้อง

3.6 ภาคผนวกแผนการรับมือภัยคุกคามทางเทคโนโลยีสารสนเทศและการสื่อสาร

3.6.1 ภาคผนวก 1 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring)

กิจกรรมการบันทึก การแจ้งเตือน และการเฝ้าระวังอาจกำหนดเป้าหมายของระบบแต่ละระบบหรือกิจกรรมต่าง ๆ ในหลายระบบและแอปพลิเคชัน เก็บรายการการบันทึก การแจ้งเตือน และการเฝ้าระวังกิจกรรม และทบทวน (Review) รายการอย่างสม่ำเสมอเพื่อให้แน่ใจว่าฝ่ายเทคนิคสามารถรับมือเหตุการณ์ที่ผิดปกติได้อย่างรวดเร็ว หากหน่วยงานมีการจัดการทะเบียนทรัพย์สิน กิจกรรมเหล่านี้อาจถูกเพิ่มลงในรายการที่มีอยู่ดังตาราง

ชื่อระบบ/ แอปพลิเคชัน (System/ Application Name)	ระบบจัดเก็บล็อก (Logging System)	เหตุการณ์ที่ได้จัดเก็บไว้ (Events Logged)	เจ้าของระบบ (System Owner)	ความถี่ในการเฝ้าระวัง (Monitoring frequency)	การแจ้งเตือน (Alerting)
ระบบเครื่องเสมือน (Virtual Machines:VM)	เก็บไว้ที่เว็บเซิร์ฟเวอร์เอง (Local) HCI (Hyper-Converged Infrastructure)	รายละเอียดและวิธีเก็บ log ตาม พรบ.และประกาศที่เกี่ยวข้อง	เจ้าของโครงการแต่ละ VM	รายวัน	Line Notification
ระบบร้องทุกข์	เก็บไว้ที่เว็บเซิร์ฟเวอร์เอง (Local) HCI (Hyper-Converged Infrastructure)	รายละเอียดและวิธีเก็บ log ตาม พรบ.และประกาศที่เกี่ยวข้อง	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	รายวัน	Line Notification

ตารางที่ 3-12 รายการกิจกรรมการบันทึก (Logging) การแจ้งเตือน (Alerting) และการเฝ้าระวัง (Monitoring) จัดเตรียมโดย (Prepared by) วันที่ปรับปรุง (Date updated)

รวมถึง สคทช. ได้ว่าจ้างให้บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.) ให้บริการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Logs) สำหรับการเข้า-ออกอินเทอร์เน็ต

ข้อมูลจราจรทางคอมพิวเตอร์ (Logs) ของเครื่องคอมพิวเตอร์และอุปกรณ์ภายใต้ HCI (Hyper-Converged Infrastructure) แต่ละผู้รับผิดชอบโครงการจะทำการเก็บ Logs เองภายใต้ระบบนั้น ๆ ทั้งนี้มีระยะเวลาจัดเก็บ Log แบบ On-line จะเก็บอย่างน้อย 90 วัน แต่ยังไม่ได้ระบุอายุการจัดเก็บและทำลาย

บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด จะทำการจัดเก็บสำรองข้อมูลระบบทั้งหมดที่อยู่ภายใต้ HCI (ในนี้มี Logs ของแต่ละระบบรวมอยู่ด้วยแล้ว) ด้วยการ Snapshot ไปที่ NAS เก็บที่ สคทช.

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.2 ภาคผนวก 2 การอ้างอิงการประเมินเหตุการณ์สองนาที (Two Minute Incident Assessment Reference)

ขั้นตอนที่ 1: ทำความเข้าใจผลกระทบ (Impact)/ผลกระทบที่อาจเกิดขึ้น (Potential Impact) และความเป็นไปได้ (Likelihood) หากไม่ใช่เหตุการณ์ที่เกิดขึ้น

- มูลค่าของทรัพย์สิน (Value of the Asset) คืออะไร? ถ้าไม่สำคัญ ทำไมต้องตอบสนอง?
- ประมาณจำนวนผลกระทบที่อาจเกิดขึ้นในกรณีที่เลวร้ายที่สุด (Potential Worst-case Impact)
- คาดการณ์ความเป็นเป็นไปได้ (Estimate of Likelihood) ที่จะได้รับผลกระทบนี้

ขั้นตอนที่ 2: ระบุสาเหตุที่น่าสงสัย/ที่เป็นไปได้ของปัญหา

- ควรพิจารณาสถานการณ์ที่เป็นไปได้ทั้งหมด
- กำจัดสิ่งที่สามารถพิสูจน์ได้ว่าไม่ถูกต้องอย่างรวดเร็ว
- แบ่งปันสถานการณ์ที่เป็นไปได้มากที่สุดเมื่อสื่อสาร

ขั้นตอนที่ 3: อธิบายกิจกรรมการแก้ไขที่แนะนำ (Remediation Activities)

- ปิดช่องโหว่ และลดผลกระทบเฉพาะหน้าอย่างไร?
- ดำเนินการขั้นตอนต่าง ๆ ที่อาจลดผลกระทบที่เกิดขึ้น
- พิจารณาเกี่ยวกับความเสียหายของชื่อเสียงและความคาดหวังทางกฎหมายด้วย

ขั้นตอนที่ 4: สื่อสารกับผู้บริหาร

- อธิบายปัญหาในระดับสูง (High Level) เกิดอะไรขึ้นและอย่างไร
- อธิบายความหมายในทางธุรกิจ เช่น การเงิน ชื่อเสียง ฯลฯ
- แบ่งปันการดำเนินการในขั้นตอนในระยะสั้น ๆ (Short-term Actions) ที่จำเป็นในการย้ายความเสี่ยงจากวิกฤต/สูงไปสู่ความเสี่ยงที่ยอมรับได้มากขึ้น

มูลค่าทรัพย์สิน (Value of the Asset) สูง (H)/กลาง (M)/ต่ำ (L)	ตัวอย่างมูลค่าทรัพย์สินระดับสูง เช่น อาจเข้าถึงฐานข้อมูลไคลเอ็นต์ได้อย่างเต็มที่ เมื่อเทียบกับมูลค่าทรัพย์สินระดับต่ำ เช่น อาจเป็นเอกสารกระบวนการภายใน
ผลกระทบที่อาจเกิดขึ้น	การสูญเสียหรือจะเกิดผลกระทบอย่างไรหากเหตุการณ์เกิดขึ้นจริงและรุนแรงอย่างเต็มที่ พยายามหาปริมาณทั้งจำนวนเงิน และผลกระทบเช่นชื่อเสียงหรือความรับผิดทางกฎหมาย
ความน่าจะเป็นของผลกระทบ	ความเสี่ยงในทันที (Immediate Risk) ที่ไม่น่าจะเป็นที่รู้จักในวงกว้างและมีความซับซ้อน เช่น การเข้าถึงทางอินเทอร์เน็ตโดยการหาประโยชน์จากช่องโหว่เล็ก ๆ น้อย ๆ ที่มีในหน่วยงานนั้น โดยต้องใช้ความเชี่ยวชาญที่ซับซ้อนและสถานการณ์เฉพาะเจาะจงเพื่อใช้ประโยชน์จากช่องโหว่นั้น
สาเหตุที่น่าสงสัย (ระบุสาเหตุที่เป็นไปได้ทั้งหมดที่ควรสืบสวนสอบสวน)	ข้อผิดพลาดในการกำหนดค่า (Configuration Error) การใช้ประโยชน์จากช่องโหว่จากระยะไกล อุปกรณ์ที่สูญหาย การปฏิเสธบริการโดยมีเป้าหมาย (Targeted Denial of Service) จากพรรคการเมืองหรือฝ่ายที่มีแรงจูงใจทางการเงิน เช่น การทำ DDOS เพื่อปกปิดการฉ้อโกง เป็นต้น
สาเหตุที่เป็นไปได้มากที่สุด	ทรัพยากรสารสนเทศเหล่านี้ควรได้รับการติดตามอย่างรวดเร็วเพื่อพิสูจน์ว่าถูกต้องหรือไม่ถูกต้อง
แนวทางแก้ไขระยะสั้น (Short-term) ที่แนะนำ	ตัดการเชื่อมต่อหรือปิดอินเทอร์เน็ต (Turn Off Internet) นำเซิร์ฟเวอร์ออก (Remove) จากการเข้าถึงภายนอก ใช้แพตช์หรือการเปลี่ยนแปลง การกำหนดค่า (Configuration Change) สื่อสารปัญหากับพนักงานหรือลูกค้า ฯลฯ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การดำเนินการระยะยาว (Long-term Actions)	การเปลี่ยนแปลงในกระบวนการหรือสถาปัตยกรรม การได้มาซึ่งเครื่องมือหรือระบบ เพื่อลดความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ในระยะยาว

ตารางที่ 3-13 การประเมินผลกระทบ/ผลกระทบที่อาจเกิดขึ้น และแนวทางการตอบสนอง

การสื่อสาร	
อธิบายปัญหาแบบเข้าใจง่าย	อธิบายปัญหาในบริบททางธุรกิจหากเป็นไปได้ การใช้ตัวอย่าง (Examples) มีประโยชน์ในการอธิบายปัญหาในแง่การปฏิบัติงาน
อธิบายปัจจัย “แล้วยังไงต่อ (So What)”	ทำไมสิ่งนี้จึงสำคัญต่อธุรกิจของหน่วยงาน จะต้องเสียอะไรหากหน่วยงานไม่ลงมือทำ
แนะนำให้ดำเนินการทันที	เสนอคำตอบที่เฉพาะเจาะจงและเหตุผลที่หน่วยงานควรรับไว้ การดำเนินการดังกล่าวจะทำให้ธุรกิจได้รับผลกระทบหรือความรับผิด (Liability) ที่ลดลงอย่างไร อาจมีมากกว่าหนึ่งแนวทางที่เป็นไปได้ หากมีตัวเลือกที่เหมาะสมก็ควรนำเสนอเพื่อการตัดสินใจ
การแก้ไขอื่น ๆ ที่เสนอ	มีความเสี่ยงที่ตามมา (Follow-on Risks) ที่ต้องดำเนินการเพิ่มเติมหรือไม่? ตัวอย่าง เช่น กลยุทธ์การสื่อสาร กิจกรรมการตระหนักรู้ของผู้ใช้ (User Awareness) การเปลี่ยนแปลงกระบวนการ การปรับปรุงระบบ/เครื่องมือหรือการใช้งานซึ่งเป็นการดำเนินการระยะยาว

ตารางที่ 3-14 แนวทางการสื่อสาร

3.6.3 ภาคผนวก 3 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist)

ลำดับที่	คำอธิบาย	หมายเหตุ
ขั้นตอนการเตรียมการ (Preparation) โดยผู้บัญชาการ IR		
1.	จัดทำรายชื่อผู้ติดต่อและเผยแพร่ให้ผู้ที่เกี่ยวข้องทราบ	
การตรวจจับ (Detection) โดยฝ่ายสนับสนุนด้านไอที (IT Support)		
2.	กรอกรายละเอียดแบบฟอร์มการตอบสนองเหตุการณ์ (Incident Response Form)	
การวิเคราะห์ (Analysis) โดย CIRT		
3.	วิเคราะห์และประเมินเหตุภัยคุกคามทางไซเบอร์	
4.	แจ้งผู้ที่เกี่ยวข้อง	
การจำกัดขอบเขต (Containment) โดย CIRT/Support		
5.	ทำการสำรองข้อมูลระบบเพื่อรักษาสถานะปัจจุบันของระบบ	
6.	เปลี่ยนรหัสผ่านในเครื่องสำหรับระบบที่ได้รับผลกระทบ	
การกำจัด (Eradication) (CIRT/Support)		
7.	อย่าใช้เครื่องมือการดูแลระบบ (System Administrative Tools) ให้ใช้ชุดเครื่องมือการดูแลระบบแยกต่างหาก (Separate Administrative Tool Sets) สำหรับการสืบสวนสอบสวน	
8.	ติดตั้งระบบปฏิบัติการใหม่ทั้งหมด	
9.	ทำให้ระบบปฏิบัติการแข็งแกร่งขึ้น (Harden the Operating System) เช่น ใช้แพตช์ ปิดบริการที่ไม่จำเป็น ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น	
การกู้คืน (Recovery) (CIRT/Support)		
10.	ตรวจสอบความถูกต้องว่าระบบได้รับการทำให้แข็งแกร่งแล้ว	
11.	กู้คืนข้อมูลระบบด้วยการสำรองข้อมูลที่มั่นใจได้ว่าปลอดภัย (Clean Backup)	
12.	พิจารณาระบบที่ได้รับผลกระทบภายใต้การเฝ้าระวังเครือข่ายสำหรับความพยายามที่ไม่ได้รับอนุญาตในอนาคต (Network Surveillance for Future Unauthorized Attempts)	
ติดตามผล (Follow-up) โดยผู้บัญชาการ IR		

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ลำดับที่	คำอธิบาย	หมายเหตุ
13.	ทำการวิเคราะห์หลังเหตุการณ์บนระบบที่ได้รับผลกระทบเพื่อระบุพื้นที่เสี่ยงที่มีจุดอ่อนที่เป็นไปได้ (Potential Vulnerable Areas)	
14.	ส่งรายงานการตอบสนองเหตุภัยคุกคามทางไซเบอร์สำหรับการทบทวนของฝ่ายบริหาร (Management Review)	
15.	จัดเก็บเอกสารทั้งหมดเกี่ยวกับกระบวนการตอบสนองเหตุภัยคุกคามทางไซเบอร์เพื่อใช้อ้างอิงในอนาคต	

ตารางที่ 3-15 รายการตรวจสอบการตอบสนองเหตุการณ์ (Incident Response Checklist)

3.6.4 ภาคผนวก 4 ข้อกำหนดการแจ้งเตือน (Notification Requirements)

ข้อกำหนดหรือกฎหมายที่เกี่ยวข้อง	กลุ่มเป้าหมาย	กำหนดเวลาการแจ้งเตือน	หมายเหตุ
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)	➢ สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	โดยไม่ชักช้า ภายใน 72 ชั่วโมงนับแต่ทราบเหตุเท่าที่จะสามารถกระทำได้	กรณีมีแนวโน้มว่ามีความเสี่ยงต่อเจ้าของข้อมูล
พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 มาตรา 37(4)	➢ เจ้าของข้อมูลที่ได้รับผลกระทบ	โดยไม่ชักช้า (แต่ไม่ได้ระบุเวลาไว้ หน่วยงานควรกำหนดระยะเวลาเองด้วย)	กรณีมีแนวโน้มว่ามีความเสี่ยงสูงต่อเจ้าของข้อมูล
พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 58 ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศซึ่งอยู่ในความดูแลรับผิดชอบของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ใดให้หน่วยงานนั้นดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องข้อมูลคอมพิวเตอร์และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติการณ์แวดล้อมของตน เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ หากผลการตรวจสอบปรากฏว่าเกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ขึ้น ให้ดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานนั้น	➢ สกมช. ➢ หน่วยงานควบคุมหรือกำกับดูแล (กระทรวงพลังงาน)	โดยเร็ว (แต่ไม่ได้ระบุเวลาไว้ หน่วยงานควรกำหนดระยะเวลาเองด้วย)	
อื่น ๆ โปรดระบุ			

ตารางที่ 3-16 ตัวอย่างการระบุข้อกำหนดทั้งหมดที่ใช้กับหน่วยงาน

อ้างอิงตามภาคผนวก ท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุมหรือกำกับดูแล(ภายในเวลา)	การส่งรายงานให้สำนักงาน(ภายในเวลา)
1	ทุกเหตุการณ์	10 นาที	2 ชั่วโมง	4 ชั่วโมง
2	ทุกเหตุการณ์	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
3	ทุกเหตุการณ์	30 นาที	2 ชั่วโมง	8 ชั่วโมง
4	วิกฤต	10 นาที	30 ชั่วโมง	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
5	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง
6	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	20 นาที	1 ชั่วโมง	2 ชั่วโมง
	ไม่ร้ายแรง	30 นาที	2 ชั่วโมง	4 ชั่วโมง
7	วิกฤต	10 นาที	30 นาที	1 ชั่วโมง
	ร้ายแรง	10 นาที	1 ชั่วโมง	1 ชั่วโมง
	ไม่ร้ายแรง	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด	ตามหน่วยงานกำหนด
8	-	20 นาที	ตามเวลาที่ต้องการใช้ในการสืบสวน	4 ชั่วโมง
9	-	-	4 ชั่วโมง	12 ชั่วโมง

ตารางที่ 3-17 ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

เหตุการณ์	กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	วิธีการเผยแพร่ข้อมูล	โฆษกหลักและผู้เชี่ยวชาญด้านเทคนิค
ระบบคอมพิวเตอร์หลักของหน่วยงานโดนโจมตีจให้บริการไม่ได้	บุคลากรของหน่วยงาน ลูกค้า	ระบบสื่อสารภายในสื่อสังคมออนไลน์ อีเมล SMS	สื่อสารกับบุคลากรภายในหน่วยงาน เพื่อให้มีความเข้าใจ และช่วยกันบรรเทาปัญหาสื่อสารกับลูกค้าเพื่อสร้างความเข้าใจที่ถูกต้อง ป้องกันการตื่นตระหนก และรักษาภาพลักษณ์ของหน่วยงาน	**โฆษกหลัก:** **ภายใน** ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน **ภายนอก** - กองกฎหมาย - ผู้อำนวยการสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ **ผู้เชี่ยวชาญด้านเทคนิค:** - ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน **อ้างอิง** ผู้ให้บริการภายนอกในรายการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

เหตุการณ์	กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	วิธีการเผยแพร่ข้อมูล	โฆษกหลักและผู้เชี่ยวชาญด้านเทคนิค
ข้อมูลส่วนบุคคลในระบบถูกเจาะและนำไปเผยแพร่หรือขายหรือเรียกค่าไถ่ และเป็นที่รับรู้ของสาธารณะ	บุคลากรของหน่วยงาน ลูกค้า สาธารณชน	ระบบสื่อสารภายใน สื่อสังคมออนไลน์ อีเมล SMS สื่อมวลชน	**แถลงข่าวโดย** - กองกฎหมาย (Issue Management) - ผู้อำนวยการสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ	**โฆษกหลัก:** **ภายใน** -ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน **ภายนอก** - กองกฎหมาย - ผู้อำนวยการสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ **ผู้เชี่ยวชาญด้านเทคนิค:** -ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน **อ้างอิง** ผู้ให้บริการภายนอกในรายการ

ตารางที่ 3-18 ตัวอย่างการกำหนดช่องทางสื่อสารและวิธีการเผยแพร่ข้อมูล

3.6.5 ภาคผนวก 5 แถลงการณ์ของสื่อ

ด้านล่างนี้คือตัวอย่างข้อความที่จะใช้หากสื่อมวลชนมีการสอบถามก่อนการแถลงข่าว (Press Release) การสื่อสารทั้งหมดกับสื่อมวลชนควรส่งตรงไปยังผู้บัญชาการการรับมือเหตุภัยคุกคามทางไซเบอร์หรือตัวแทนอื่น ๆ ที่ได้รับมอบหมายจากผู้บริหารระดับสูง การรับทราบข้อเท็จจริงที่ถูกต้องเป็นสิ่งสำคัญ ห้ามให้ข้อมูลกับสื่อมวลชนก่อนยืนยันข้อเท็จจริงกับบุคลากรภายในและผู้บริหาร การเปลี่ยนแปลงข้อมูลหลังจากเผยแพร่อาจนำไปสู่ความสับสนของสื่อมวลชนและสูญเสียการโฟกัสข้อความสำคัญ

3.6.5.1 สคริปต์ที่เตรียมไว้ (Pre-scripted) การรับมือทันทีต่อการสอบถามของสื่อ

ใช้เทมเพลตนี้หากสื่อมวลชน “อยู่ที่หน้าประตูของหน่วยงาน” และหน่วยงานยังต้องการเวลาในการรวบรวมข้อเท็จจริงสำหรับคำแถลงการแถลงข่าวเบื้องต้น

การยอมรับข้อเท็จจริงเป็นสิ่งสำคัญ ดังนั้นเป็นสิ่งสำคัญที่ของหน่วยงานที่จะไม่กดดันให้ยืนยันหรือเปิดเผยข้อมูลก่อนที่จะได้รับการยืนยันข้อมูลที่ถูกต้อง

คำตอบต่อไปนี้ทำให้หน่วยงานมีเวลาที่จำเป็นในการรวบรวมข้อเท็จจริง

3.6.5.2 การตอบกลับแบบมีสคริปต์ล่วงหน้า (Pre-scripted Responses)

หากโทรศัพท์ออกสื่อ: หากผู้สื่อข่าวโทรศัพท์มาสอบถามเรื่องเหตุการณ์หรือข้อมูลที่เกี่ยวข้อง และหน่วยงานยังอยู่ระหว่างการรวบรวมข้อเท็จจริง คำตอบต้องมุ่งเน้นการควบคุมสถานการณ์และให้ข้อมูลพื้นฐานในขณะที่ปฏิเสธที่จะเปิดเผยข้อมูลที่ยังไม่ได้รับการยืนยัน

สคริปต์ตัวอย่างสำหรับการตอบกลับ:

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

1. การยืนยันการรับรู้เหตุการณ์: “ขอบคุณสำหรับการติดต่อเข้ามา ทางเราทราบถึงสถานการณ์ที่เกิดขึ้นแล้ว และขณะนี้อยู่ระหว่างการตรวจสอบข้อมูลเพิ่มเติมเพื่อให้ได้ข้อเท็จจริงที่ถูกต้องที่สุดค่ะ/ครับ”

2. การให้ข้อมูลพื้นฐาน: “ในขณะนี้หน่วยงานของเราให้ความสำคัญสูงสุดกับการตรวจสอบข้อเท็จจริงและการแก้ไขสถานการณ์ เรามีทีมที่ทำงานอย่างใกล้ชิดเพื่อให้แน่ใจว่าทุกอย่างได้รับการดูแลอย่างรอบคอบ”

3. การขอเวลาในการรวบรวมข้อมูล: “ขอให้ท่านรอการแถลงข่าวอย่างเป็นทางการซึ่งเราจะแจ้งให้ทราบทันทีเมื่อเรารวบรวมข้อเท็จจริงทั้งหมดได้ครบถ้วนค่ะ/ครับ”

4. การปฏิเสธคำถามเฉพาะเจาะจง: “ขออภัยที่ไม่สามารถตอบคำถามเพิ่มเติมในขณะนี้ได้ เนื่องจากยังอยู่ระหว่างการตรวจสอบข้อมูล เราจะติดต่อกลับไปพร้อมข้อมูลที่ชัดเจนอีกครั้งค่ะ/ครับ”

5. การเสนอช่องทางติดตามข่าวสาร: “ท่านสามารถติดตามข่าวสารและแถลงการณ์เพิ่มเติมได้ผ่านทางเว็บไซต์หรือช่องทางโซเชียลมีเดียของหน่วยงานเราค่ะ/ครับ”

3.6.5.3 “หน่วยงานได้ทราบเกี่ยวกับ [สถานการณ์ (*Situation*) เหตุภัยคุกคามทางไซเบอร์ (*Incident*) เหตุการณ์ (*Event*)] และกำลังพยายามหาข้อมูลให้ครบถ้วนมากขึ้นในขณะนี้ เราจะติดต่อคุณได้อย่างไรเมื่อมีข้อมูลเพิ่มเติม”

- “ความพยายามทั้งหมดของหน่วยงานมุ่งไปที่ [ทำให้สถานการณ์อยู่ภายใต้การควบคุม] เราจะไม่คาดเดาเกี่ยวกับ [สถานการณ์นี้] เราจะติดต่อคุณได้อย่างไรเมื่อมีข้อมูลเพิ่มเติม”
- “ฉันไม่ใช่ผู้มีอำนาจในเรื่องนี้ ให้ฉันได้ทราบ [ชื่อและข้อมูลการติดต่อกลับ] เราจะโทรหาคุณทันทีเมื่อมีข้อมูลเพิ่มเติม”
- “ตอนนี้หน่วยงานกำลังเตรียมแถลงการณ์ เราจะติดต่อกลับคุณภายใน [จำนวนนาทีหรือชั่วโมง] ได้ไหม”
- “คุณสามารถตรวจสอบเว็บไซต์ของหน่วยงานสำหรับข้อมูลพื้นฐาน และเราจะแฟ็กซ์/อีเมล์ถึงคุณพร้อมกับการอัปเดตครั้งต่อไปของหน่วยงาน”

หากมาด้วยตนเองที่จุดเกิดเหตุภัยคุกคามทางไซเบอร์หรือหน้างานแถลงข่าว:

- นี่คือ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] ที่กำลังดำเนินการอยู่ และเรารู้ว่าคุณต้องการข้อมูลให้ได้มากที่สุดในขณะนี้ ในขณะที่เราพยายามหาคำตอบสำหรับคำถามของคุณ เราต้องการบอกคุณสิ่งที่หน่วยงานสามารถยืนยันได้ในตอนนี้:
- ในเวลาประมาณ [เวลา] [คำอธิบายสั้น ๆ ว่าเกิดอะไรขึ้น]
- ณ จุดนี้ เราไม่ทราบว่า [การสรุปผลจะดำเนินการนานแค่ไหน ลูกค้าได้รับผลกระทบกี่ราย ฯลฯ
- หน่วยงานมี [ระบบ, แผน, ขั้นตอน, การดำเนินงาน] ในสถานที่ หน่วยงานกำลังได้รับความช่วยเหลือจาก [เจ้าหน้าที่ท้องถิ่น ผู้เชี่ยวชาญ ทีมกฎหมายของหน่วยงาน] ซึ่งเป็นส่วนหนึ่งของแผนดังกล่าว
- สถานการณ์ [อยู่ภายใต้ ยังไม่อยู่ภายใต้] การควบคุม หน่วยงานกำลังทำงานร่วมกับหน่วยงาน [ท้องถิ่น รัฐบาล] เพื่อ [แก้ไขสถานการณ์นี้ พิจารณาว่าสิ่งนี้เกิดขึ้นได้อย่างไร]

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- หน่วยงานจะดำเนินการรวบรวมข้อมูลและเผยแพร่ให้คุณทราบโดยเร็วที่สุด เราจะติดต่อกลับภายใน [ระยะเวลาเป็นนาทีหรือชั่วโมง] เพื่อให้ข้อมูลอัปเดตแก่คุณ ทันทีที่หน่วยงานได้ยืนยันข้อมูลที่ได้รับ
- เราขอให้คุณอดทนรอในขณะที่หน่วยงานตอบสนองต่อ [สถานการณ์ (Situation) เหตุภัยคุกคามทางไซเบอร์ (Incident) เหตุการณ์ (Event)] นี้

3.6.5.4 เคล็ดลับการเขียนคำชี้แจง (Statement Writing Tips)

ข้อมูล/เคล็ดลับต่อไปนี้สามารถใช้เพื่อสร้างคำแถลงสื่อที่ดีได้ ไม่จำเป็นต้องรวมทุกรายการ แต่โดยทั่วไปแล้วสองหรือสามรายการนี้จะรับรองได้ว่าเป็นคำชี้แจงที่มีประสิทธิภาพ

3.6.5.4.1 ความซื่อสัตย์ (Honesty)

ถ้าหน่วยงานเป็นฝ่ายผิด ยอมรับ หากพยายามที่จะเบี่ยงเบนความรับผิดชอบ นักข่าวและสาธารณชนจะให้อภัยน้อยลงเมื่อรายละเอียดเกี่ยวกับเหตุภัยคุกคามทางไซเบอร์ถูกเปิดเผยและถูกพบว่าหน่วยงานมีการปฏิบัติได้ไม่เพียงพอ แม้ในภาวะวิกฤติจริง ๆ ก็สามารถได้รับความเคารพในการยอมรับข้อเท็จจริง

หากไม่ใช่ความผิดของหน่วยงาน ต้องทำให้ชัดเจนโดยไม่กล่าวโทษบุคคลหรือหน่วยงานอื่นอย่างเปิดเผย

- คำที่ใช้: รับหรือแบ่งปันความรับผิดชอบ (Take or Share Responsibility) มุ่งมั่นในการเปิดกว้าง โปร่งใส
- คำที่ไม่ควรใช้: ตำหนิ (Blame) ความผิดพลาด (Fault)

3.6.5.4.2 บริบท (Context)

การนำเสนอเชิงลบในบริบทกว้าง ๆ สามารถช่วยลดผลกระทบของข่าวร้ายได้อย่างมาก

หากเรื่องราวเป็นเรื่องเกี่ยวกับผู้ใช้บริการที่มีประสบการณ์ไม่ดี หน่วยงานสามารถอ้างอิงถึงผู้ใช้บริการคนอื่น ๆ ที่มีประสบการณ์ที่ดีได้ นี่คือจุดที่ผู้สนับสนุนภายนอกมีประโยชน์โดยเฉพาะผู้ใช้บริการรายอื่น

บริบทที่กว้างขึ้นยังหมายถึงการแยกเหตุภัยคุกคามทางไซเบอร์ออก เพียงแต่กรณีที่ระบุว่าเหตุการณ์เชิงลบนั้น “หายากมาก” / “ถูกแยกออก” และวางไว้ในกรอบที่กว้างขึ้นและเป็นบวกมากขึ้น

- คำที่ใช้: หายากมาก (Very Rare) แยกออกมา (Isolated)
- คำที่ไม่ควรใช้: ผิดพลาดบ่อย (Frequent Mistakes) ข้อผิดพลาดอื่น (Another Error)

3.6.5.4.3 การระบุขอบเขตของผลกระทบ (Framing Effect)

การระบุขอบเขตของผลกระทบเป็นรูปแบบหนึ่งของความลำเอียงทางปัญญา (Form of Cognitive Bias) ซึ่งทำให้ผู้คนชอบข้อความที่ฟังดูเป็นบวกมากกว่าคำพูดเชิงลบ แม้ว่าจะเป็นเรื่องเดียวกันก็ตาม ตัวอย่างเช่น เมื่อพูดถึงการผ่าตัดที่มีความเสี่ยง ผู้ป่วยจะมีแนวโน้มที่จะเข้ารับการผ่าตัดมากขึ้น เมื่อมีการอธิบายว่า “โอกาสรอดชีวิตหนึ่งเดือนหลังการผ่าตัดคือ 90%” เมื่อเทียบกับ “การเสียชีวิตภายในหนึ่งเดือนของการผ่าตัดคือ 10%” แม้ว่าข้อความทั้งสองจะมีความเสี่ยงเท่ากัน พึงระวังอคติทางปัญญารูปแบบนี้เมื่อพัฒนาและส่งข้อความสู่สาธารณะ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.5.4.4 พันธมิตร (Partnership)

มีบางครั้งที่การเตือนผู้ฟังที่มีวิจารณญาณอย่างละเอียดจะเป็นประโยชน์ว่าหน่วยงานไม่ได้รับผิดชอบแต่ผู้เดียวสำหรับพฤติกรรมของบุคคลใดบุคคลหนึ่งโดยเฉพาะ สิ่งนี้สามารถบรรลุได้โดยไม่ปรากฏว่าหน่วยงานกำลัง “ยอมเสียเปรียบ” หรือละทิ้งความรับผิดชอบและไม่ทำให้ความสัมพันธ์กับพันธมิตรหลักอื่น ๆ ไม่พอใจ ตัวอย่างเช่น อาจกล่าวง่าย ๆ ว่า “ในฐานะหนึ่งในหลายหน่วยงานที่เกี่ยวข้องกับการสนับสนุนบุคคลที่เกี่ยวข้อง เรามุ่งมั่นที่จะให้บริการที่ดีที่สุดสำหรับผู้ใช้บริการในพื้นที่”

- คำที่ใช้: การทำงานร่วมกัน (Working Together) ความรับผิดชอบร่วมกัน (Joint Responsibility) เป็นหนึ่งในหลายหน่วยงาน
- คำที่ไม่ควรใช้: X คือการตำหนิ (Blame) หน่วยงานไม่รู้ว่าคนอื่นคิดอย่างไรกับเรื่องนี้ แต่...

3.6.5.4.5 การดำเนินการ (Action)

แถลงการณ์ของสื่อไม่ควรพูดถึงปัญหาเพียงอย่างเดียว ควรเน้นการดำเนินการในส่วนของหน่วยงาน หน่วยงานจะไม่สามารถปรับปรุงสถานการณ์กับของสื่อใด ๆ หากหน่วยงานถูกมองว่าไม่โต้ตอบในกรณีของสถานการณ์เชิงลบหรือวิกฤตของสื่อ

คำเตือน: หลีกเลี่ยงการพูดว่าเราจะถือว่า “การสืบสวน/การสอบสวน” ในกรณีนี้ คำเหล่านี้เป็นพาดหัวข่าวสำหรับสื่อและอาจบ่งบอกถึงความรู้สึกมีความผิด

- คำที่ใช้: ดำเนินการทันที (Taking Immediate Action) ใช้มาตรการที่เหมาะสม ทำงานอย่างใกล้ชิดกับ
- คำที่ไม่ควรใช้: หน่วยงานกำลังทำการสืบสวนสอบสวน หน่วยงานจะพิจารณามัน

3.6.5.4.6 แง่บวก (Positives)

อย่ากลัวที่จะชี้ให้เห็นว่าหน่วยงานประสบความสำเร็จเพียงใดในแถลงการณ์ของสื่อ ข้อผิดพลาดเกิดขึ้นและเน้นย้ำสิ่งที่หน่วยงานได้ทำไปแล้วสามารถช่วยให้คนอื่นมองเห็นจุดบกพร่องเล็ก ๆ น้อย ๆ ในอดีตได้

- คำที่ใช้: เราได้เห็นผลลัพธ์ที่ดี เราประสบความสำเร็จ เราจะให้บริการที่ดีที่สุดต่อไป
- คำที่ไม่ควรใช้: มีหลายส่วนที่หน่วยงานต้องแก้ไข (เว้นแต่จะมาพร้อมกับข้อความเชิงบวก เช่น จะใช้มาตรการเพื่อเปลี่ยนแปลงสิ่งนี้)

3.6.5.4.7 ความเข้าอกเข้าใจ (Empathy)

เห็นได้ชัดว่าสถานการณ์สื่อเชิงลบสร้างช่องว่างระหว่างหน่วยงานกับสาธารณะที่เกี่ยวข้อง การแสดงความเห็นอกเห็นใจสามารถช่วยลดช่องว่างได้

- คำที่ใช้: เราเข้าใจ เราซาบซึ้ง เรารู้ เรารับรู้
- คำพูดที่ไม่ควรใช้: สิ่งเหล่านี้เกิดขึ้น ทุกคนต้องเผชิญกับปัญหาเหล่านี้

3.6.5.4.8 กระชับ (Be Concise)

นักข่าวมักไม่สนใจข้อความที่ยาวเหยียด พวกเขาอยากจะใช้ความพยายามในรายละเอียดของเหตุการณ์/เหตุภัยคุกคามทางไซเบอร์ นอกจากนี้ หากผู้พูดกับสื่อไม่คุ้นเคยกับการทำเช่นนั้น คำพูดที่ยาวอาจส่งผลให้ผู้พูดทำผิด

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตามกฎแล้ว ข้อความสำหรับสื่อสิ่งพิมพ์ไม่ควรยาวเกินสองย่อหน้า – หนึ่งประโยคแน่นต่อย่อหน้า

สื่อออกอากาศอาจทำให้หน่วยงานมีพื้นที่มากขึ้น แต่ควรคำนึงถึงความยาวเนื่องจากผู้ผลิต/บรรณาธิการอาจต้องการจัดทำคำแถลงของหน่วยงานในแบบที่สั้นลงเพื่อส่งไปยังกระดานข่าวในภายหลัง

3.6.5.4.9 ข้อความควรหลีกเลี่ยง (Statements Should Avoid)

- **การเผชิญหน้า (Confrontation)** วัตถุประสงค์ของคำแถลงของสื่อในภาวะวิกฤตคือเพื่อคลี่คลายสถานการณ์ ไม่ทำให้สถานการณ์แย่ลง หลีกเลี่ยงการกล่าวโทษ/โยนความผิดเพราะจะส่งผลให้เกิดการโต้เถียงกันตามสื่อระหว่างฝ่ายตรงข้าม จำไว้ว่านักข่าวชอบเรื่องราวการเผชิญหน้า เช่น พวกเขาผิดมันไม่ใช่ความผิดของหน่วยงาน
- **ความคลุมเครือ (Ambiguity)** ข้อความที่ไม่ชัดเจนและคลุมเครือไม่ช่วยในการจัดการกับสถานการณ์ของสื่อเชิงลบ และอาจเปิดโอกาสให้นักข่าวตีความคำตอบใหม่ จงเข้มแข็งและชัดเจนตลอดเวลาใช้คำพูดเชิงบวกที่แข็งแกร่งเช่น “หน่วยงานมุ่งมั่นที่จะ X และจะไม่ยอมให้ Y” ตรวจสอบให้แน่ใจว่าข้อความของหน่วยงานมีความชัดเจนอย่างสมบูรณ์
- **คำสรรพนามส่วนบุคคล (Personal Pronouns)** พยายามหลีกเลี่ยงการอ้างถึงหน่วยงาน โดยใช้ชื่อในคำแถลงของสื่อ เนื่องจากการทำเช่นนี้อาจช่วยเสริมความเชื่อมโยงระหว่างหน่วยงานกับประเด็นเชิงลบที่เกี่ยวข้อง สามารถใช้พหูพจน์แรก เช่น เรา พวกเรา เป็นต้น สิ่งนี้ยังมีข้อได้เปรียบในการเพิ่มความรู้สึกส่วนตัวเล็กน้อยและให้ความรู้สึกเป็นข้าราชการน้อยลงในแถลงการณ์

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.6 ภาคผนวก 6 เทมเพลตจดหมายผู้รับบริการ (Customer Letter Template)

3.6.6.1 เทมเพลตอีเมลและ/หรือจดหมายอย่างเป็นทางการ (*Formal Email and/or Letter Template*)

เรียน ผู้รับบริการ

อย่างที่ท่านอาจทราบ เครือข่ายคอมพิวเตอร์ในสำนักงานบางแห่งของเราถูกบุกรุกที่อาจส่งผลให้มีการขโมยชื่อ - นามสกุล ข้อมูลการติดต่อ ข้อมูลการถือครองกรรมสิทธิ และข้อมูลอื่น ๆ เราอยู่ระหว่างตรวจสอบข้อมูลสมาชิกที่ผู้บุกรุกอาจเข้าถึง แต่ขณะนี้ยังไม่มีหลักฐานของการใช้ข้อมูลดังกล่าวในทางที่ผิด

เราจัดทำประกาศนี้ด้วยความระมัดระวังอย่างยิ่งต่อผู้ใช้บริการทุกคนที่ให้ข้อมูลติดต่อของท่านกับหน่วยงานของเราไม่ให้ได้รับผลกระทบที่ร้ายแรง โดยเราประเมินว่าระบบที่อาจได้รับผลกระทบถูกบุกรุกในช่วงระยะเวลา <ระบุวันที่เริ่ม> ถึง <ระบุวันที่สิ้นสุด>

เมื่อทราบการบุกรุกแล้ว เราได้ดำเนินการทันทีเพื่อรักษาความมั่นคงปลอดภัยเครือข่ายส่วนที่ได้รับผลกระทบ โดยได้รับการสนับสนุนจากผู้เชี่ยวชาญด้านนิติวิทยาศาสตร์ดำเนินการสืบสวนข้อเท็จจริงและขอบเขตของภัยคุกคามทางไซเบอร์นี้ ขอให้ท่านเชื่อมั่นว่าการบุกรุกดังกล่าวอยู่ภายใต้การควบคุม และปัจจุบันยังไม่ปรากฏหลักฐานมีว่าข้อมูลอื่นใดถูกขโมยนอกเหนือจากที่กล่าวข้างต้น อย่างไรก็ตาม เราจะแจ้งให้ทราบโดยเร็วหากมีความคืบหน้าเพิ่มเติมจากการสืบสวนที่ดำเนินอยู่

เราได้แจ้งเหตุต่อหน่วยงานรัฐบาลและให้ความร่วมมือตามกฎหมายเพื่อนำไปสู่การพิสูจน์ทราบบุคคลที่อยู่เบื้องหลัง แถลงข่าวและจดหมายฉบับนี้เป็นการปฏิบัติตามที่กฎหมายกำหนดให้แจ้งผู้มีส่วนเกี่ยวข้องทราบข้อเท็จจริงโดยเร็วที่สุด

ทั้งนี้ หน่วยงานได้จัดตั้งศูนย์บริการทางโทรศัพท์ขึ้นเพื่อตอบข้อซักถามจากผู้ใช้บริการเกี่ยวกับเหตุการณ์บุกรุก และการให้บริการปกป้องความปลอดภัยข้อมูลส่วนบุคคล โดยจะมีเจ้าหน้าที่ประจำการวันจันทร์ถึงวันศุกร์ ระหว่างเวลา 08.00 น. - 16.00 น.

ต้องขออภัยในความไม่สะดวกที่อาจเกิดขึ้น หน่วยงานของเราจะปรับปรุงแก้ไขจุดอ่อนด้านความปลอดภัยของระบบ เพื่อไม่ให้เกิดเหตุการณ์ลักษณะนี้ขึ้นอีกในอนาคต

ขอแสดงความนับถือ,

<ข้อควรพิจารณาอื่น ๆ ขึ้นอยู่กับลักษณะของเหตุการณ์>

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.7 ภาคผนวก 7 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response Organizations)

รายชื่อหน่วยงานที่เกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์ที่อาจเป็นประโยชน์ในการวางแผนหรือตอบสนองต่อเหตุการณ์:

หน่วยงาน	URL
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	https://www.ncsa.or.th/ncsc.html
Anti-Phishing Working Group (APWG)	https://www.antiphishing.org/
Computer Crime and Intellectual Property Section (CCIPS), US Department of Justice	https://www.justice.gov/criminal-ccips
CERT Coordination Center	https://www.sei.cmu.edu/about/divisions/cert/index.cfm
European Network and Information Security Agency (ENISA)	https://www.enisa.europa.eu/
Government Forum of Incident Response and Security Teams (GFIRST)	https://www.us-cert.gov/government-Users/collaboration/gfirst
High Technology Crime Investigation Association (HTCIA)	https://htcia.org/
InfraGard	https://www.infragard.org/
Internet Store Center (ISC)	https://isc.sans.edu/
National Council of ISACs	https://www.nationalisacs.org/
United States Computer Emergency Response Team (US-CERT)	https://www.us-cert.gov/

ตารางที่ 3-19 หน่วยงานเกี่ยวข้องกับการตอบสนองเหตุภัยคุกคามทางไซเบอร์

3.6.8 ภาคผนวก 8 กลยุทธ์การจำกัดขอบเขต (Containment Strategies)

กลยุทธ์การจำกัดขอบเขตต่อไปนี้ได้รับการกำหนดเพื่อช่วยในการรับมือเหตุภัยคุกคามทางไซเบอร์ หากไม่มีกลยุทธ์การจำกัดขอบเขตที่สรุปไว้ด้านล่างที่เหมาะกับสถานการณ์ปัจจุบัน ให้อ้างอิงกับขั้นตอนที่ 3.1 การจำกัดขอบเขตทั่วไป (Containment)

3.6.8.1 ข้อมูลประจำตัวที่ถูกขโมย (Stolen Credentials)

3.6.8.1.1 การจำกัดขอบเขต (Containment)

การลดผลกระทบ:

- เปลี่ยนรหัสผ่านหรือปิดการใช้งานบัญชีที่ได้รับผลกระทบ
- หากบัญชีที่ถูกบุกรุกมีสิทธิ์การเข้าถึงของผู้ดูแลระบบ (Administrator Access) ทบทวนบันทึกกิจกรรม (Review Activity Logs)สำหรับบัญชีเพิ่มเติมที่อาจสร้างขึ้น ปิดการใช้งานบัญชีใด ๆ ที่สร้างโดยผู้โจมตี

แจ้งผู้ที่เกี่ยวข้อง:

- แจ้งผู้ใช้ที่รับผิดชอบบัญชีที่ได้รับผลกระทบ
- การสืบสวนสอบสวน:
- พยายามระบุวันที่และเวลาที่บัญชีถูกบุกรุก

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ทบทวนกิจกรรมทั้งหมดที่เกิดขึ้นแล้วโดยบัญชีที่ถูกบุกรุกในช่วงระยะเวลาของการโจมตี หากไม่มีบันทึกกิจกรรม (Logs) ให้ตรวจสอบการกำหนดค่าทั้งหมด (All Configurations) ที่บัญชีนั้นมีสิทธิ์เข้าถึงเพื่อแก้ไข เช่น สำหรับบัญชีอีเมลที่ถูกบุกรุก ให้ตรวจสอบกฎการส่งต่อ (Forwarding Rules) ที่เพิ่มหรือเปลี่ยนแปลง เป็นต้น

3.6.8.1.2 การกำจัดและการกู้คืน (Eradication and Recovery)

- ย้อนกลับการเปลี่ยนแปลง (Reverse Changes) ที่ทำโดยบัญชีที่ถูกบุกรุกในช่วงเวลาของการโจมตี

3.6.8.2 แรนซัมแวร์ (Ransomware)

3.6.8.2.1 การจำกัดขอบเขต (Containment)

1) บล็อกการเข้าถึงเซิร์ฟเวอร์คำสั่งและการควบคุม (Command and Control: C2)

2) ตั้งค่าการแชร์ไฟล์เป็นโหมดอ่านอย่างเดียว (Read-only Mode)

3) ตรวจสอบความเป็นเจ้าของไฟล์ที่ถูกเข้ารหัส (Encrypted Files) เพื่อระบุผู้ใช้ที่ติดไวรัส

4) เรียกคืน (Recall) อีเมลฟิชชิ่งที่รู้จักจากกล่องจดหมายของผู้ใช้

5) ออฟไลน์ระบบที่ติดมัลแวร์

3.6.8.2.2 การกำจัดและการกู้คืน (Eradication and Recovery)

1) แพตช์แอปพลิเคชันบุคคลที่สามโดยเร็วที่สุด

2) ทดสอบและตรวจสอบความถูกต้องของกระบวนการสำรองข้อมูล

3) ปรับใช้ GPO เพื่อบล็อกไฟล์เรียกทำงานและปิดใช้งานมาโคร

4) บล็อกไฟล์แนบอีเมลตามลายเซ็นไฟล์ (File Signature) และ/หรือนามสกุล

5) ลบสิทธิ์ของผู้ดูแลระบบบนเครื่องหรือบนระบบนั้น (Local Administrative Rights)

3.6.8.3 การระบาดของไวรัส (*Virus Outbreak*)

3.6.8.3.1 การจำกัดขอบเขต (Containment)

1) อัปเดตซอฟต์แวร์ป้องกันไวรัส

1.1) รับลายเซ็นการตรวจจับ (Detection Signature) และคำอธิบายทางเทคนิคสำหรับไวรัสจากผู้จำหน่าย Antivirus (AV)

1.2) ทดสอบการอัปเดตลายเซ็นการตรวจจับในสภาพแวดล้อมการทดสอบ

1.3) กระจายการแก้ไขสู่สิ่งแวดล้อมจริง (Distribute Fix to Environment)

2) ส่งไฟล์ตัวอย่างไปยังผู้จำหน่าย AV หากลายเซ็นไวรัสล่าสุดตรวจไม่พบการติดไวรัส

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.8.3.2 การกำจัดและการกู้คืน (Eradication and Recovery)

1) กำจัดไวรัส ถ้าจำเป็น

1.1) จำกัดขอบเขตของไวรัส/การโจมตี โดยขึ้นอยู่กับไวรัสซึ่งอาจรวมถึงการแบ่งพาร์ติชันเครือข่าย การปิดใช้งานอีเมล SMPT (Disabling SMPT Email) การเปลี่ยนการกรองเนื้อหา (Content Filtering) เพื่อบล็อกไฟล์แนบหรือสตริงข้อความเฉพาะ การลบเวิร์กสเตชันออกจากเครือข่าย ฯลฯ

1.2) ระบุระบบที่ติดไวรัส (Infected Systems)

2) การชำระล้างสภาพแวดล้อม (Environment Cleanup):

1.1) รับลายเซ็นการตรวจจับและเครื่องมือแก้ไขที่จำเป็นสำหรับไวรัสจากผู้จำหน่ายโปรแกรมป้องกันไวรัสของหน่วยงาน

1.2) ทดสอบการแก้ไขที่ผู้ขายของหน่วยงานจัดหาให้สำหรับไวรัสในสภาพแวดล้อมทดสอบของหน่วยงาน (Virus Signatures Staging Lab) ซึ่งอาจรวมถึงเครื่องมือซ่อมแซม (Repair Tools) แยกต่างหากที่หน่วยงานต้องเรียกใช้ก่อนที่จะใช้ลายเซ็นไวรัสที่อัปเดต

1.3) พัฒนาวิธีการปรับใช้สำหรับกระบวนการแก้ไข (Fix Process)

1.4) สร้างแผนการชำระล้าง (Cleanup Plan) และตรวจสอบความถูกต้องกับทีมที่ได้รับผลกระทบทั้งหมดและผู้จำหน่ายโปรแกรมป้องกันไวรัสของหน่วยงาน

1.5) ทำการชำระล้างขอบเขตและเซิร์ฟเวอร์อีเมลที่ติดไวรัสทั้งหมด (Clean all Infected Perimeter and Email Servers) และอัปเดตลายเซ็นไวรัสของซอฟต์แวร์ป้องกันไวรัสซึ่งให้การป้องกันช่องทางการติดไวรัสเหล่านี้

1.6) แจกจ่ายโปรแกรมแก้ไขไปยังเวิร์กสเตชันและเซิร์ฟเวอร์ทั้งหมดในสภาพแวดล้อมของหน่วยงาน โดยใช้วิธีการใดก็ตามที่มีเพื่อการปรับใช้อย่างรวดเร็ว

1.7) แยก (Isolate) ระบบที่ติดไวรัสและต้องการการซ่อมแซมออก

1.8) เรียกใช้เครื่องมือแก้ไขที่จำเป็นทั้งหมดบนระบบที่ติดไวรัสทั้งหมดเพื่อลบไวรัสออกจากหน่วยความจำหรือปิดใช้งาน

1.9) สแกนระบบทั้งหมดด้วยลายเซ็นไวรัสที่อัปเดตเพื่อลบไฟล์ที่ติดไวรัสทั้งหมด

1.10) กำจัดไฟล์ชั่วคราวและไฟล์ที่น่าสงสัยทั้งหมด รวมถึงไดเรกทอรีและไฟล์ที่ซ่อนอยู่

1.11) ลบหรือแก้ไขข้อมูลการกำหนดค่าที่ใช้สำหรับการทำงานของไวรัสหรือที่อาจอนุญาตให้ไวรัสปรากฏขึ้นอีกครั้ง

1.12) ลบข้อมูลการกำหนดค่าที่อาจทำให้ระบบล้มเหลว

1.13) ค้นหาพาร์ติชันที่ติดตั้งใหม่ที่สร้างโดยไวรัสและกำจัดออก

1.14) ค้นหาพาร์ติชันการบันทึก (Log Partitions) ที่หายไปและกู้คืน

1.15) ค้นหาบัญชีผู้ใช้ที่เพิ่มหรือเปลี่ยนแปลง แล้วลบหรือกู้คืน

1.16) กู้คืนไฟล์ที่เปลี่ยนแปลงหรือถูกลบ

1.17) แจกจ่ายการอัพเดตแพตช์ไปยังทุกระบบและอัปเดตระดับการแพตช์ (Update Patch Levels)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

3.6.9 ภาคผนวก 9 ข้อตกลงการประกันภัยทางไซเบอร์และการบริการบุคคลที่สาม (Cyber Insurance and Third-Party Service Agreements)

ในกรณีที่เกี่ยวข้องกับการประกันภัยทางไซเบอร์หรือบริการจากบุคคลภายนอก การมีความเข้าใจที่ชัดเจนเกี่ยวกับบริการรับมือและตรวจจับเหตุภัยคุกคามทางไซเบอร์ (Incident Response and Detection Services) เป็นสิ่งสำคัญ ตัวอย่างเช่น ผู้ให้บริการประกันภัยทางไซเบอร์จำนวนมากต้องการให้หน่วยงานที่ดูแลดำเนินการตามกระบวนการที่กำหนดไว้ล่วงหน้า เป็นต้น ตัวอย่างของผู้ให้บริการบุคคลที่สามที่อาจเกี่ยวข้องกับกิจกรรม IR ได้แก่ ผู้ให้บริการประกันภัย ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider: ISP) ผู้ให้บริการระบบคลาวด์ (Cloud Service Provider: CSP) ผู้จำหน่ายซอฟต์แวร์ หรือผู้ให้บริการหลายบริการ (Multiservice Provider: MSP) เป็นต้น

CIO มีหน้าที่ตรวจสอบ SLA ทั้งหมดกับผู้ให้บริการเพื่อให้แน่ใจว่ามีการกำหนดความรับผิดชอบและความคาดหวังที่เกี่ยวข้องกับการรับมือเหตุภัยคุกคามทางไซเบอร์

ผู้บัญชาการ IR มีหน้าที่รับผิดชอบในการทำความเข้าใจ SLA กับผู้ให้บริการและรู้ว่าเมื่อใดที่ทีมควรมีส่วนร่วมกับผู้ให้บริการ

การสนับสนุนและการตอบสนองของบุคคลที่สาม สคทช. ได้ว่าจ้างให้บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) ให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์ ภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) และเหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ สคทช. โดยต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Use case) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม ที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง ต่อวัน 7 วัน ต่อสัปดาห์ (24/7) และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสาร ตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่ สคทช. ตลอดระยะเวลาสัญญา

ตามสัญญากับบริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) จะต้องให้บริการเฝ้าระวังภัยคุกคาม วิเคราะห์ความเกี่ยวโยงของเหตุการณ์ ภัยคุกคามด้านความปลอดภัยสารสนเทศ (IT Security Monitoring Services) และเหตุการณ์ผิดปกติทางด้านบริหารจัดการระบบคอมพิวเตอร์และระบบเครือข่ายสื่อสารและอินเทอร์เน็ต จากข้อมูลจราจรทางคอมพิวเตอร์ (Log) ของอุปกรณ์ต่าง ๆ ของ สคทช. โดยต้องมีการวิเคราะห์แบบรวมศูนย์และเงื่อนไขการโจมตี (Correlation and Usecase) เพื่อช่วยในการเฝ้าระวังและแจ้งเตือนภัยคุกคาม ที่เกี่ยวข้องทุกวันตลอด 24 ชั่วโมง ต่อวัน 7 วัน ต่อสัปดาห์ (24/7) และดำเนินการแจ้งเตือนเมื่อเกิดเหตุการณ์ภัยคุกคามด้านเทคโนโลยีสารสนเทศและการสื่อสารตาม Service Level Agreement (SLA) ที่กำหนด รวมทั้ง ให้คำแนะนำด้านเทคนิคในการแก้ไขเหตุการณ์ภัยคุกคามดังกล่าวแก่ สคทช. ตลอดระยะเวลาสัญญา โดย สคทช. กำหนดเกณฑ์ Service Level Agreement เบื้องต้น โดยต้องมีการแจ้งเตือนภายหลังการตรวจพบและวิเคราะห์เหตุ ภายในระยะเวลาอย่างน้อย ดังนี้

ระดับความรุนแรง (Severity)	Incident Notification
Critical	15 นาที
Non-Critical	30 นาที

ตารางที่ 3-20 เกณฑ์ Service Level Agreement

นอกจากนี้ การสนับสนุนและการตอบสนองของบุคคลที่สาม สคทช. ยังได้ว่าจ้างให้บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด หากเกิดสถานการณ์ฉุกเฉินขึ้นกับระบบเทคโนโลยีสารสนเทศ ดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ผู้ให้บริการ (Service Provider)	แอปพลิเคชัน/บริการ (Applications/Services)	เมื่อไหร่จะติดต่อ (When to contact)	ระดับการบริการ/ เวลาตอบสนอง (Service Level/ Response Time)
บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด (iNEXT Broadband Co., Ltd.)	➢ อินเทอร์เน็ต ➢ ดูแลอุปกรณ์	หากเกิดสถานการณ์ฉุกเฉินขึ้นกับระบบเทคโนโลยนสารสนเทศ	ภายใน 12 ชั่วโมง

ตารางที่ 3-21 การสนับสนุนและการตอบสนองของบุคคลที่สาม

ผู้ให้บริการประกันภัย (Insurance Provider)	ข้อจำกัด (Limits)	วันที่กรมธรรม์มีผลและสิ้นสุด (Term Dates)	เมื่อไหร่จะติดต่อ (When to contact)	ข้อมูลติดต่อ (Contact Information)
XXXX	เฉพาะทรัพย์สินคอมพิวเตอร์ เช่น ไฟไหม้ เป็นต้น แต่ไม่รวมประกันภัยไซเบอร์	ตามรอบปีงบประมาณ	ในทันที เมื่อมีการสูญเสียทางการเงินหรือข้อมูลใด ๆ	XXXX

ตารางที่ 3-22 ความคุ้มครองประกันภัยและข้อมูลการติดต่อ

*อาจมีการจำกัดความคุ้มครองเพิ่มเติมต่อการเรียกร้อง (Additional Coverage Sub-limit May Apply per Claim)

ค้นหาสำเนาหน้าใบประกาศประกันภัย (Insurance Declaration Page) ได้ที่ฝ่ายบริหารงานองค์กรส่งคำถามโดยตรงเกี่ยวกับวงเงินประกัน (Insurance Coverage) ต่อผู้จัดการความเสี่ยง (Risk Manager) แจ้งผู้จัดการความเสี่ยงเพื่อเปิดใช้งานแผนประกัน (Activate the Insurance Plan)

3.6.10 ภาคผนวก 10 การสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ไปยังบุคลากรที่เกี่ยวข้องทั้งหมด

กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	เป้าหมาย
บุคลากรที่รับแจ้งเหตุการณ์	➢ แจ้งผ่านเบอร์โทรศัพท์มือถือ ➢ แจ้งผ่าน Email ➢ แจ้งเหตุเบอร์โทรของสำนักงาน ➢ สื่อสารและเผยแพร่ผ่าน Line Group ➢ สื่อสารและเผยแพร่ผ่าน Website ➢ สื่อสารและเผยแพร่ผ่าน Facebook ➢ หนังสือแจ้ง ➢ การประชุม	➢ เพื่อสื่อสารกับบุคลากรภายในหน่วยงานเพื่อให้มีความเข้าใจ และช่วยกันบรรเทาปัญหา ➢ เพื่อให้บุคลากรที่รับแจ้งเหตุการณ์สามารถรายงานข้อมูลเหตุการณ์ทางไซเบอร์ได้อย่างทันกาล
ทีมตอบสนองเหตุการณ์	➢ แจ้งผ่านเบอร์โทรศัพท์มือถือ ➢ แจ้งผ่าน Email ➢ แจ้งเหตุเบอร์โทรของสำนักงาน ➢ สื่อสารและเผยแพร่ผ่าน Line Group ➢ สื่อสารและเผยแพร่ผ่าน Website ➢ สื่อสารและเผยแพร่ผ่าน Facebook ➢ หนังสือแจ้ง ➢ การประชุม	➢ เพื่อสื่อสารกับทีมตอบสนองเหตุการณ์เพื่อให้เข้าใจแนวทางการดำเนินการ ➢ สื่อสารและการส่งต่อข้อมูลเหตุการณ์ทางไซเบอร์ไปยังผู้ที่เกี่ยวข้อง เพื่อให้ทีมตอบสนองเหตุการณ์ สามารถตอบสนองต่อเหตุการณ์ทางไซเบอร์ได้อย่างทันกาล

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

กลุ่มเป้าหมาย	แพลตฟอร์ม/ช่องทางการเผยแพร่	เป้าหมาย
ผู้บริหาร CIRT	➢ แจ้งผ่านเบอร์โทรศัพท์มือถือ ➢ แจ้งผ่าน Email ➢ แจ้งเหตุเบอร์โทรของสำนักงาน ➢ สื่อสารและเผยแพร่ผ่าน Line Group ➢ สื่อสารและเผยแพร่ผ่าน Website ➢ สื่อสารและเผยแพร่ผ่าน Facebook ➢ หนังสือแจ้ง ➢ การประชุม	➢ เพื่อให้เข้าใจบทบาทและกำกับดูแลการดำเนินการ ได้อย่างเหมาะสม
ผู้ให้บริการสนับสนุนบริการสำคัญ	➢ แจ้งผ่านเบอร์โทรศัพท์มือถือ ➢ แจ้งผ่าน Email ➢ แจ้งเหตุเบอร์โทรของสำนักงาน ➢ สื่อสารและเผยแพร่ผ่าน Line Group ➢ สื่อสารและเผยแพร่ผ่าน Website ➢ สื่อสารและเผยแพร่ผ่าน Facebook ➢ หนังสือแจ้ง ➢ การประชุม	➢ เพื่อสื่อสารเหตุการณ์ผิดปกติทางไซเบอร์ไปยังองค์กรหรือหน่วยงานภายนอกที่เกี่ยวข้องหรือที่ได้รับผลกระทบ ➢ เพื่อให้สามารถดำเนินการได้อย่างเหมาะสมและทันการณ์ ➢ เพื่อร่วมกันพัฒนาปรับปรุงการรักษาความมั่นคงปลอดภัยของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากบุคคลภายนอกอย่างต่อเนื่อง

ตารางที่ 3-23 ตัวอย่างการกำหนดการสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์

4. แผนการตรวจสอบและประเมินผลการปฏิบัติงาน

ในรายละเอียดของการพัฒนาแผนการตรวจสอบและประเมินผลการปฏิบัติงาน ถูกพัฒนาจากผลการศึกษาในระยะก่อนหน้าที่ให้ความสำคัญกับการปกป้องข้อมูลที่ดินและทรัพยากรดิน แผนการตรวจสอบและประเมินผลการปฏิบัติงานจึงมีวัตถุประสงค์เพื่อให้มั่นใจว่าข้อมูลสำคัญได้รับการคุ้มครองและสอดคล้องกับข้อกำหนดทางกฎหมายและมาตรฐานสากล มีการระบุขอบเขตที่ต้องตรวจสอบ เช่น เครือข่าย ระบบคลาวด์, และการจัดการข้อมูลในองค์กร โดยมีการนำมาตรฐาน ISO/IEC 27001 และ PDPA มาใช้กำหนดเกณฑ์การตรวจสอบที่ใช้เป็นมาตรฐานเปรียบเทียบความมั่นคงปลอดภัยและความสอดคล้องกับกฎหมาย อีกทั้งข้อเสนอแนะจากผลการศึกษาระยะก่อนหน้าให้มีการตรวจสอบประจำปีตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 จึงมีการวางแผนตรวจสอบเป็นประจำเพื่อให้ทันต่อการเปลี่ยนแปลงของภัยคุกคามและปรับปรุงมาตรการความปลอดภัย ทั้งนี้ในแผนการตรวจสอบและประเมินผลการปฏิบัติงานมีการระบุผู้รับผิดชอบในการดำเนินงานตรวจสอบและการติดตามผล รวมถึงความรับผิดชอบต่อการปรับปรุงและแก้ไขข้อบกพร่อง รวมถึงใช้เครื่องมือที่ทันสมัยเพื่อช่วยให้การตรวจสอบมีประสิทธิภาพและได้ผลลัพธ์ที่สามารถนำไปปรับปรุงระบบได้จริง และส่งเสริมการปรับปรุงมาตรการด้านความปลอดภัยโดยใช้บทเรียนจากเหตุการณ์ภัยคุกคามในอดีตและการติดตามภัยคุกคามใหม่ ๆ

4.1 แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

ความมั่นคงปลอดภัยไซเบอร์เป็นหัวใจสำคัญในการรับประกันความต่อเนื่องของการดำเนินงานและการปกป้องข้อมูลที่สำคัญขององค์กร ในบริบทของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ซึ่งเป็นหน่วยงานที่มีหน้าที่ดูแลข้อมูลที่ดินและทรัพยากรดินของประเทศ การตรวจสอบความมั่นคงปลอดภัยไซเบอร์จึงมีบทบาทสำคัญในการเสริมสร้างความน่าเชื่อถือและป้องกันภัยคุกคามที่อาจเกิดขึ้น

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพช่วยให้องค์กรสามารถระบุช่องโหว่ที่อาจเกิดขึ้นในระบบ รวมถึงตรวจสอบการปฏิบัติตามนโยบายและมาตรฐานที่กำหนด เช่น ISO/IEC 27001 และข้อกำหนดในพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 บทนี้จะกล่าวถึงกระบวนการที่ครอบคลุมตั้งแต่การวางแผนตรวจสอบ การดำเนินการตรวจสอบ การรายงานผล ตลอดจนการติดตามผลการแก้ไขปัญหาที่พบ

4.1.1 บทนำแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

การตรวจสอบและประเมินผลการปฏิบัติงาน (หรือเรียกว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564) จะต้องดำเนินการอย่างน้อยปีละหนึ่ง หรือความถี่ที่สูงกว่านั้นตามที่สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) กำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดยหน่วยงาน

4.1.1.1 ตัวชี้วัดของแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์มีรายละเอียดเกี่ยวกับค่าเป้าหมายและวิธีการวัดผลในด้านต่าง ๆ ดังนี้

1. ตัวชี้วัดด้านประสิทธิภาพ (Efficiency Metrics)

1.1 อัตราการดำเนินการตรวจสอบตามแผน

- เป้าหมาย : ดำเนินการตรวจสอบครบถ้วน 100% ตามแผนที่กำหนดไว้ในแต่ละปี
- วิธีวัด : เปรียบเทียบจำนวนงานตรวจสอบที่เสร็จสมบูรณ์กับจำนวนงานที่กำหนดในแผน

1.2 ระยะเวลาที่ใช้ในการตรวจสอบแต่ละรายการ

- เป้าหมาย : ระยะเวลาที่ใช้ไม่เกินระยะเวลาที่กำหนดในแผน
- วิธีวัด : บันทึกและเปรียบเทียบระยะเวลาที่ใช้จริงกับระยะเวลาที่วางแผน

2. ตัวชี้วัดด้านประสิทธิผล (Effectiveness Metrics)

2.1 จำนวนข้อบกพร่องที่ตรวจพบ

- เป้าหมาย : ตรวจพบและรายงานข้อบกพร่องด้านความมั่นคงปลอดภัยทุกประเด็นที่มีความเสี่ยง
- วิธีวัด : นับจำนวนข้อบกพร่องที่ตรวจพบระหว่างการตรวจสอบ

2.2 อัตราการแก้ไขข้อบกพร่องภายในระยะเวลาที่กำหนด

- เป้าหมาย : แก้ไขข้อบกพร่องได้ไม่น้อยกว่า 90% ภายในระยะเวลาที่กำหนด
- วิธีวัด : เปรียบเทียบจำนวนข้อบกพร่องที่ได้รับการแก้ไขกับจำนวนข้อบกพร่องทั้งหมด

2.3 การนำข้อเสนอแนะจากการตรวจสอบมาปรับปรุง

- เป้าหมาย : นำข้อเสนอแนะทั้งหมดมาดำเนินการปรับปรุงภายในระยะเวลาที่กำหนด
- วิธีวัด : นับจำนวนข้อเสนอแนะที่ได้รับการดำเนินการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4.1.1.2 วัตถุประสงค์

แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ฉบับนี้มีวัตถุประสงค์เพื่อกำหนดความคาดหวังในการตรวจสอบและประเมินผลการปฏิบัติงาน และใช้เป็นระเบียบวิธีปฏิบัติสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์นี้ไม่ได้หมายถึงแหล่งข้อมูลที่ละเอียดถี่ถ้วนสำหรับการดำเนินการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในเอกสารนี้ ผู้ตรวจสอบควรใช้ดุลยพินิจเยี่ยงผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบ

4.1.1.3 กลุ่มเป้าหมาย

กลุ่มเป้าหมายของแผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์นี้:

1. ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ และ
2. ผู้มีส่วนได้ส่วนเสีย (เช่น หัวหน้าหน่วยงาน เจ้าของระบบและผู้ขาย หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล ฯลฯ) ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

4.1.1.4 ขอบเขต

แผนการตรวจสอบความมั่นคงปลอดภัยไซเบอร์นี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 54 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

4.1.2 การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติเพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

เกณฑ์การพิจารณามี 2 ประการ ได้แก่ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (Audit Firm/team) และผู้ตรวจสอบ (Auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง:

- ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์
- ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติอาจพิจารณาแตกต่างกันไปตามที่สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติเห็นสมควร ในประเด็นต่อไปนี้

(1) จำนวนผู้ตรวจสอบที่มี

(2) ระยะเวลาในการขออนุญาต เช่น รายปี หรือตามรอบการตรวจสอบ เป็นต้น

4.1.3 ความคาดหวังในการตรวจสอบ

ส่วนนี้กำหนดความคาดหวังในการตรวจสอบ มีวัตถุประสงค์เพื่อช่วยให้เข้าใจว่าควรดำเนินการและรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติได้ระบุความคาดหวังในการตรวจสอบไว้ 7 ด้าน ในหัวข้อ 4.1.3.1 ถึง 4.1.3.7

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน



รูปที่ 4-1: หลักการตรวจสอบ (Principles of Auditing)

4.1.3.1 หลักการตรวจสอบ (*Principles of Auditing)*

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้ เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

1) ความซื่อสัตย์ (Integrity) : รากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

2) การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจนและครบถ้วน

3) การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

4) การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

5) ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบ และความเที่ยงธรรมของข้อสรุปการตรวจสอบ

- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
- ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
- รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (Audit Evidence) เท่านั้น

4.1.3.2 วัตถุประสงค์ในการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบ คือ:

1) ตรวจสอบการปฏิบัติตามของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

2) ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติตามหลักการบริหารความเสี่ยง

4.1.3.3 ขอบเขตการตรวจสอบ (*Audit Scope*)

การตรวจสอบจะครอบคลุมสิ่งต่อไปนี้:

รายการ	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระบบหรือบริการที่ตรวจสอบ (System or Service Audit)	(1) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ในกรณีที่หน่วยงานเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ตรวจสอบตรวจสอบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ ซึ่งหน่วยงานได้ดำเนินการเพื่อให้ได้มาซึ่งบริการที่สำคัญตามมาตรา 49 แห่ง พ.ร.บ. ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ด้วย (2) บริการที่สำคัญของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติตามผลการวิเคราะห์ในข้อ (1) ในกรณีที่หน่วยงานเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ตรวจสอบตรวจสอบบริการที่สำคัญตามมาตรา 49 แห่ง พ.รบ.ความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ด้วย (3) บริการอื่น ๆ ที่หน่วยงานต้องการตรวจสอบ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ 1 ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่ง ที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด เช่น นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 - 2570) ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะ หน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. 2564 ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. 2566 ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564

ตารางที่ 4-1 ขอบเขตการตรวจสอบ (Audit Scope)

การพิจารณาเกณฑ์การประเมินผลในแต่ละระดับ

การจัดทำเกณฑ์ประเมินผลการตรวจสอบ อ้างอิงจากกรอบการประเมินที่เป็นมาตรฐานสากล ได้แก่ International Organization for Standardization (ISO) โดยแบ่งหมวดหมู่เกณฑ์ (Category) ออกเป็น 4 ระดับ ดังนี้

1. ระดับผลการตรวจ Major Non-Conformity (Major NC) พบข้อกำหนดข้อใดข้อหนึ่งหรือทั้งหมดไม่มีการนำไปฏิบัติ หรือมีเหตุนำมาซึ่งความเสียหายอย่างร้ายแรงต่อระบบหรือกรณีที่มีความไม่สอดคล้องย่อย (Minor Non-Conformity) หลาย ๆ จุดรวมกัน ซึ่งเมื่อพิจารณาแล้วมีผลกระทบต่อระบบการจัดการโดยรวม

2. ระดับผลการตรวจ Minor Non-Conformity (Minor NC) พบบางส่วนของข้อกำหนดหรือข้อใดข้อหนึ่งมีการละเลย หรือปฏิบัติไม่ครอบคลุม

3. ระดับผลการตรวจ Observation (OBS) พบประเด็นที่อาจมีผลกระทบโดยไม่ถือเป็นความไม่สอดคล้องย่อย (Minor Non-Conformity) แต่หากปล่อยทิ้งไว้ หรือละเลย อาจนำไปสู่ความไม่สอดคล้องได้ (Potential Non-Conformity) เป็นข้อควรปรับปรุงเพื่อป้องกันความไม่สอดคล้องหรือการติดตาม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4. ระดับผลการตรวจ Conformity (C) ผ่านเกณฑ์สอดคล้องตามที่ประกาศกำหนดทั้งหมด

ทั้งนี้ อาจพบโอกาสในการปรับปรุง (Opportunity For Improvement: OFI) ซึ่งหมายความว่า มีข้อเสนอแนะหรือโอกาสเพื่อการปรับปรุงในการปฏิบัติให้ดียิ่งขึ้น หรือเพื่อป้องกันความไม่สอดคล้อง

4.1.3.4 แนวทางการตรวจสอบ (*Audit Approach*)

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (Compliance Approach) และตามความเสี่ยง (Risk-based Approach)

1) การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ตัวอย่างเช่น

- ข้อกำหนดหรือกฎหมายระบุให้หน่วยงานมีการจัดทำระเบียบปฏิบัติและกระบวนการบริหารความเสี่ยง หน่วยงานได้มีการดำเนินการดังกล่าว และนำเอกสารไปใช้งานหรือไม่
- ข้อกำหนดหรือกฎหมายระบุให้หน่วยงานมีการจัดทำกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

ในการตรวจสอบ ผู้ตรวจสอบต้องตรวจสอบ

1) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) โดยผู้ตรวจสอบควรตรวจสอบผลวิเคราะห์ที่ได้จากกระบวนการจัดทำ BIA ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติที่สอดคล้องกับข้อกำหนดการจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เรื่องมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) ซึ่งมักจะระบุไว้ในแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) หรือเป็นส่วนที่แยกมาต่างหากก็ได้

โดยการตรวจสอบผลการวิเคราะห์ดังกล่าวให้ตรวจสอบรายการต่อไปนี้

- ผลการวิเคราะห์ผลกระทบทางธุรกิจที่ได้จากผู้มีส่วนได้ส่วนเสียพิจารณาร่วมกัน และได้รับอนุมัติจากผู้บริหารสูงสุดของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติหรือผู้ที่ได้รับมอบหมาย หรือคณะกรรมการที่ได้รับมอบหมาย
- รายการกระบวนการทางธุรกิจ พร้อมระบุระดับผลกระทบ ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก ระยะเวลาในการกู้คืนระบบ และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
- ทรัพยากรที่ต้องใช้ดำเนินการแก้ปัญหาการหยุดชะงัก
- บริการที่สำคัญที่ได้จากผลการวิเคราะห์ผลกระทบทางธุรกิจ โดยบริการที่สำคัญดังกล่าวต้องมีความเชื่อมโยงกับวัตถุประสงค์ และพันธกิจของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

โดยผู้ตรวจสอบควรตรวจสอบด้วยว่า

- บริการที่สำคัญตามมาตรา 49 ดังกล่าวได้มาจากการดำเนินการตามกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจจริงหรือไม่
- หน่วยงานควบคุมหรือกำกับดูแลได้ร่วมกับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศในการดำเนินการตามกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจจริงหรือไม่

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- หน่วยงานควบคุมหรือกำกับดูแลได้ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการทบทวนความถูกต้องของการระบุบริการที่สำคัญตามมาตรา 49 แห่งพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์พ.ศ.2562

2) บริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ผลกระทบทางธุรกิจ โดยผู้ตรวจสอบควรตรวจสอบนโยบาย การกำหนดหน้าที่รับผิดชอบ ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้องกับผลลัพธ์ และแผนการปรับปรุงของการดำเนินการตามประมวลแนวปฏิบัติและกรอบมาตรฐาน ดังตัวอย่างต่อไปนี้

- การจัดทำทะเบียนทรัพย์สิน และการจัดทำขอบเขตเครือข่ายของบริการที่สำคัญ
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมบริการที่สำคัญ
- การประเมินช่องโหว่ และแผนการการจัดการช่องโหว่ที่ครอบคลุมบริการที่สำคัญ
- การจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการที่สำคัญ
- การควบคุมการเข้าถึงบริการที่สำคัญ
- การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ที่ครอบคลุมถึงบริการที่สำคัญ
- การควบคุมเชื่อมต่อระยะไกล (Remote Connection) ที่เชื่อมต่อมายังบริการที่สำคัญ
- การควบคุมสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ที่เชื่อมต่อกับบริการที่สำคัญ
- การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลที่เกี่ยวข้องกับบริการที่สำคัญ
- การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้กับบริการที่สำคัญ
- การจัดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

นอกจากที่ผู้ตรวจสอบต้องตรวจสอบบริการที่สำคัญของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติจากผลการวิเคราะห์ทางธุรกิจดังกล่าวข้างต้นแล้ว ผู้ตรวจสอบต้องตรวจสอบบริการที่สำคัญตามมาตรา 49 แห่งพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ด้วย

3) การปฏิบัติตามพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงานและที่คณะกรรมการประกาศกำหนด

หมายเหตุ

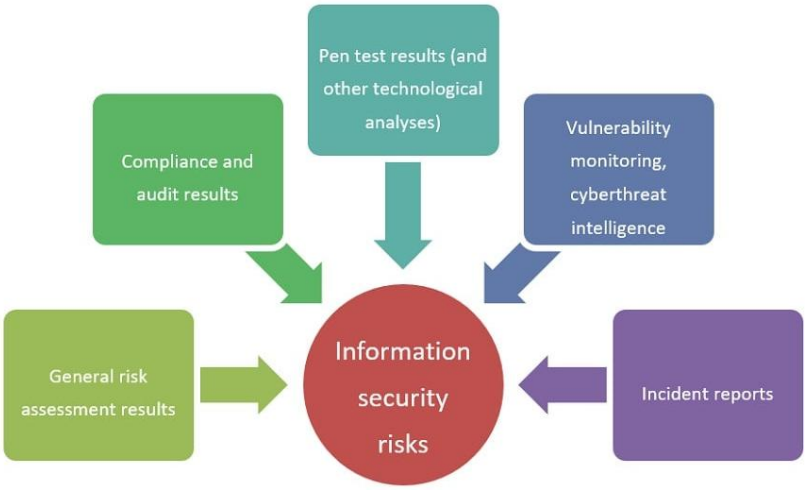
- ผู้ตรวจสอบไม่จำเป็นต้องตรวจสอบระบบสารสนเทศที่มีระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับต่ำ ยกเว้นผู้ตรวจสอบได้พิจารณาแล้วเห็นว่าจำเป็นต้องตรวจสอบด้วย
- ทั้งนี้ ผู้ตรวจสอบอาจตรวจสอบบริการอื่นที่ไม่ใช่บริการที่สำคัญที่ได้จากผลการวิเคราะห์ผลกระทบทางธุรกิจของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติหรือบริการอื่นที่ไม่ใช่บริการที่สำคัญตามมาตรา 49 แห่งพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 หากผู้บริหารพิจารณาพบว่าบริการดังกล่าวมีระดับความเสี่ยงที่จำเป็นต้องได้รับการตรวจสอบ

2. ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การตรวจตามความเสี่ยงอาจพิจารณาจากผลการตรวจสอบครั้งที่ผ่านมา การเกิดเหตุภัยคุกคามทางไซเบอร์ครั้งล่าสุด ที่ส่งผลต่อหน่วยงานและผู้ใช้บริการ ข้อร้องเรียนของผู้ใช้บริการ ผลการประเมินช่องโหว่หรือผลการทดสอบเจาะระบบ (Pentest Results) เหตุละเมิดข้อมูลส่วนบุคคลที่ผ่านมา การไม่ปฏิบัติตามกฎหมายกฎระเบียบ (Noncompliance) ผลการประเมินความเสี่ยงของหน่วยรับตรวจ หรือที่รุนแรงที่ส่งผลต่อหน่วยงาน เป็นต้น ซึ่งผู้ตรวจต้องให้ความสำคัญและเวลามากขึ้นในการตรวจสอบประเด็นความเสี่ยงที่เกี่ยวข้องกับเรื่องนั้น ๆ



รูปที่ 4-2: ตัวอย่างองค์ประกอบในการพิจารณาเพื่อการตรวจสอบตามความเสี่ยง[3]

4.1.3.5 ข้อค้นพบการตรวจสอบ (*Audit Finding*)

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้:

1) ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ
2) เน้นการค้นหาอย่างเป็นระบบ (Systemic Finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม
3) เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (Corrective Action) แล้วก็ตาม
4) เน้นแนวปฏิบัติที่ดี (Good Practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน โดยใช้แบบฟอร์มข้อค้นพบการตรวจสอบ ดังนี้

ข้อค้นพบการตรวจสอบ

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
หมวดหมู่เกณฑ์ความไม่สอดคล้อง (Non-Conformity Category)	Major NC/ Minor NC/ OBS

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุ (Cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ (ทันที ในอนาคต หรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

ตารางที่ 4-2 แบบฟอร์มข้อค้นพบการตรวจสอบ

4.1.3.6 สรุปผลการตรวจสอบ (*Audit Conclusion*)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

1) ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ
2) ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติและโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

4.1.3.7 รูปแบบรายงานการตรวจสอบ (*Audit Report Format*)

รายงานการตรวจสอบควรมีอย่างน้อยดังต่อไปนี้:

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
เกณฑ์ที่ใช้ในการตรวจสอบ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ 6.2 ของเอกสารนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

เนื้อหา	คำอธิบาย
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน 6.3 ของเอกสารนี้ อ้างถึงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ข้อ 17.1 (ก)-(ค)
วันเวลาที่ตรวจสอบ	
ผู้ตรวจสอบ	
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน 6.5 ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน 6.6 ของเอกสารนี้

ตารางที่ 4-3 รายงานการตรวจสอบ

4.1.4 ขั้นตอนการปฏิบัติในการตรวจสอบ

1. ผู้ตรวจสอบทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

2. ผู้ตรวจสอบและคณะทำงานของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

3. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

4. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้นโดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ
- ข้อเสนอแนะในการปรับปรุง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

5. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

6. คณะทำงานรับทราบผลการตรวจสอบ

7. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้องที่พบจากการตรวจสอบลงแบบฟอร์มในข้อ 6.5 ข้อค้นพบการตรวจสอบ (Audit Finding) (ตารางที่ 4-2: แบบฟอร์มข้อค้นพบการตรวจสอบ) และการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR) (ตารางที่ 4-4: แบบฟอร์มการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR) ในส่วนของสำหรับคณะผู้ตรวจประเมิน (Auditor)) ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติและจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนดเพื่อรักษาความลับในการตรวจสอบ

8. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติหรือคณะกรรมการตรวจสอบของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติหรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

9. คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ

10. ผู้ตรวจสอบดำเนินการติดตามการแก้ไขความไม่สอดคล้องของคณะทำงาน

4.1.5 การจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติจะต้องจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายในวันที่ 30 มกราคม ของปีถัดไป พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลเพื่อทราบสถานะการดำเนินการของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติภายใต้การกำกับหรือดูแล ตามวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดด้วย

ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สกมช. ได้ประกาศกำหนดให้ใช้รูปแบบรายงานการตรวจสอบ (Audit Report Format) (รูปที่ 12 37: รายงานการตรวจสอบ)

การแก้ไขความไม่สอดคล้อง

ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา 54 ให้สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติส่งแผนการดำเนินการแก้ไขในกรณีที่พบความไม่สอดคล้องในระดับ Major Non-Conformity ไปยัง สกมช. ภายในกำหนด 30 (สามสิบ) วันนับแต่วันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย (โดยใช้แบบฟอร์มการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR) ดังตารางที่ 4-4: แบบฟอร์มการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)) ดังนี้

(1) ให้รายละเอียดการดำเนินการแก้ไขที่สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(2) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ (1)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)	**CAR No.** .....
หน่วยงาน / ผู้รับตรวจ : ..... ครั้งที่ตรวจ (Audit No.)..... วันที่ตรวจ (Date:) ..... ผู้ตรวจ (Auditor) :	ประเภท NCR ☐ Major ☐ Minor ☐ Observation ☐ OFI กฎหมาย/มาตรฐาน:..... ข้อกำหนด/รายการที่: .....

๑. รายละเอียดความไม่สอดคล้องหรือการไม่ปฏิบัติตาม *(สำหรับคณะผู้ตรวจประเมิน (Auditor))*

.....

.....

ผู้ตรวจ (Auditor) : ..... Date : ...../...../.....

2. วิเคราะห์สาเหตุและแนวทางการ แก้ไข/ป้องกัน *(สำหรับคณะทำงานหน่วยงานรัฐ หรือ CII)*

วิเคราะห์สาเหตุ (Root Cause) (กรณีที่เป็น Major NC หรือ Minor NC) : .....

.....

.....

รายละเอียดการแก้ไข (Action details)	**วันที่เริ่มต้น (Start Date)**	**วันที่คาดว่าจะแล้วเสร็จ (Expected Due Date)**	**วันที่เสร็จจริง (Finish Date)**	**สอบทานโดย (Verified by)**
<u>การแก้ไขเบื้องต้น (Correction)</u>				
<u>การแก้ไขโดยไม่ให้เกิดซ้ำ (Corrective Action)</u> กิจกรรมย่อย 1..... กิจกรรมย่อย 2.....				

ผู้ดำเนินการแก้ไข :..... Date : ...../...../.....

3. พิจารณาความเหมาะสมของแนวทางการแก้ไข (สำหรับคณะผู้ตรวจประเมิน (Auditors) หรือกรรมการบริหารสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ)

ความเห็น ☐ เห็นชอบ ☐ ไม่เห็นชอบ

รายละเอียด .....

.....

ผู้ให้ความเห็นชอบ :..... Date : ...../...../.....

Remark: โปรดส่งกลับให้ผู้ตรวจสอบหรือผู้รับผิดชอบ ภายใน ...../...../.....

ต้องส่งต่อให้ ☐ สกมช. (ส่งต่อ กกม.) ...../...../..... ☐ หน่วยงานควบคุมหรือกำกับดูแล ...../...../.....

☐ อื่น ๆ โปรดระบุ.....

ส่งให้ *กกม.* พิจารณา ภายใน...../...../..... (สำหรับ สกมช.)

4. พิจารณาความเหมาะสมของแนวทางการแก้ไข *(สำหรับ กกม.)*

ความเห็น ☐ อนุมัติ ☐ ไม่อนุมัติ

รายละเอียด .....

.....

ให้ดำเนินการแก้ไขให้แล้วเสร็จภายใน ...../...../.....

ผู้ให้ความเห็นชอบ :..... Date : ...../...../.....

5. พิจารณาผลการแก้ไข *(สำหรับคณะผู้ตรวจประเมิน (Auditors) หรือกรรมการบริหารสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ)*

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

สถานะการดำเนินการ ☐ ดำเนินการเรียบร้อย ☐ ดำเนินการยังไม่แล้วเสร็จ .... ผู้ให้ความเห็นชอบ : ..... Date : ...../...../.....
6. ส่งผลการแก้ไขให้ กกม. **ส่งให้** *สกมช.* ภายใน...../...../..... **สำเนา**ให้หน่วยงานควบคุมหรือกำกับดูแล...../...../

ตารางที่ 4-4 แบบฟอร์มการแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)

4.2 การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงไม่เพียงแต่ช่วยลดผลกระทบจากภัยคุกคามที่อาจเกิดขึ้น แต่ยังสนับสนุนให้เกิดการตัดสินใจเชิงกลยุทธ์ในการป้องกันและจัดการความเสี่ยงอย่างมีประสิทธิภาพ กระบวนการนี้ต้องอาศัยกรอบการทำงานที่เป็นมาตรฐาน เช่น ISO/IEC 27005 และ NIST Risk Management Framework เพื่อให้มั่นใจว่าผลการประเมินสามารถนำไปสู่การจัดลำดับความสำคัญและการดำเนินงานที่เหมาะสม

ในบทนี้จะกล่าวถึงกระบวนการประเมินความเสี่ยง ตั้งแต่การระบุสินทรัพย์สำคัญ (Critical Assets Identification) การวิเคราะห์ภัยคุกคาม (Threat Analysis) การประเมินความเปราะบาง (Vulnerability Assessment) และการจัดลำดับความเสี่ยง (Risk Prioritization) โดยเชื่อมโยงกับผลการศึกษาจากระยะก่อนหน้า เพื่อให้แน่ใจว่าการบริหารความเสี่ยงด้านไซเบอร์ของ สคทช. มีความครอบคลุม สอดคล้องกับบริบทขององค์กร และตอบสนองต่อภัยคุกคามได้อย่างมีประสิทธิภาพ

4.2.1 บทนำการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ในยุคที่เทคโนโลยีสารสนเทศและการสื่อสารเป็นรากฐานสำคัญของการดำเนินงานขององค์กร ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ได้กลายเป็นหนึ่งในปัจจัยที่ส่งผลกระทบโดยตรงต่อประสิทธิภาพและความน่าเชื่อถือขององค์กร โดยเฉพาะอย่างยิ่งสำหรับสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ที่ดูแลข้อมูลสำคัญเกี่ยวกับที่ดินและทรัพยากรของประเทศ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จึงเป็นกระบวนการที่สำคัญในการระบุจุดอ่อน วิเคราะห์ภัยคุกคาม และจัดทำแผนการป้องกันที่เหมาะสม

4.2.1.1 ตัวชี้วัดของการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตัวชี้วัดของการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์มีรายละเอียดเกี่ยวกับค่าเป้าหมายและวิธีการวัดผลในด้านต่าง ๆ ดังนี้

1. ตัวชี้วัดด้านประสิทธิภาพ (Efficiency Metrics)

1.1 อัตราการดำเนินการประเมินความเสี่ยงตามแผน

- เป้าหมาย: ดำเนินการประเมินความเสี่ยง 100% ตามแผนที่กำหนดไว้ในแต่ละปี
- วิธีวัด: เปรียบเทียบจำนวนงานประเมินที่เสร็จสมบูรณ์กับจำนวนงานที่กำหนดในแผน

1.2 ระยะเวลาที่ใช้ในการประเมินความเสี่ยงแต่ละรายการ

- เป้าหมาย: ระยะเวลาที่ใช้ไม่เกินระยะเวลาที่กำหนดในแผน
- วิธีวัด: บันทึกและเปรียบเทียบระยะเวลาที่ใช้จริงกับระยะเวลาที่วางแผน

1.3 ความครอบคลุมของการประเมินความเสี่ยง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- เป้าหมาย: ครอบคลุมทุกสินทรัพย์สำคัญที่ระบุไว้ในแผน
- วิธีวัด: เปรียบเทียบจำนวนสินทรัพย์ที่ได้รับการประเมินกับจำนวนสินทรัพย์สำคัญที่ระบุ

2. ตัวชี้วัดด้านประสิทธิผล (Effectiveness Metrics)

2.1 จำนวนความเสี่ยงที่ตรวจพบ

- เป้าหมาย: ตรวจพบความเสี่ยงที่มีผลกระทบสูงทั้งหมดในระบบที่ประเมิน
- วิธีวัด: นับจำนวนความเสี่ยงที่ตรวจพบในกระบวนการประเมิน

2.2 การจัดลำดับความสำคัญของความเสี่ยง

- เป้าหมาย: จัดลำดับความเสี่ยงทั้งหมดตามระดับผลกระทบและโอกาสที่เกิดขึ้น
- วิธีวัด: ตรวจสอบว่าทุกความเสี่ยงได้รับการจัดอันดับตามเกณฑ์ที่กำหนด

2.3 อัตราการจัดทำแผนจัดการความเสี่ยง

- เป้าหมาย: ความเสี่ยงที่สำคัญได้รับการจัดทำแผนจัดการไม่น้อยกว่า 90% ภายในระยะเวลาที่กำหนด
- วิธีวัด: เปรียบเทียบจำนวนความเสี่ยงที่มีแผนจัดการกับจำนวนความเสี่ยงที่ตรวจพบ

2.4 การปรับปรุงกระบวนการประเมินความเสี่ยง

- เป้าหมาย: ปรับปรุงกระบวนการประเมินความเสี่ยงตามข้อเสนอแนะทั้งหมด
- วิธีวัด: นับจำนวนข้อเสนอแนะที่ได้รับการดำเนินการ

3. ตัวชี้วัดด้านความครอบคลุมและความยั่งยืน (Sustainability Metrics)

3.1 การฝึกอบรมบุคลากรที่เกี่ยวข้อง

- เป้าหมาย: บุคลากรที่เกี่ยวข้องได้รับการฝึกอบรมไม่น้อยกว่า 90% ต่อปี
- วิธีวัด: เปรียบเทียบจำนวนบุคลากรที่ผ่านการฝึกอบรมกับจำนวนบุคลากรทั้งหมด

3.2 การปรับปรุงระบบตรวจสอบและจัดการความเสี่ยง

- เป้าหมาย: ระบบที่เกี่ยวข้องได้รับการปรับปรุงตามความเสี่ยงที่ตรวจพบไม่น้อยกว่า 95%
- วิธีวัด: ตรวจสอบการอัปเดตระบบและการดำเนินงานตามแผนที่กำหนด

3.3 การลดระดับความเสี่ยงรวมในองค์กร

- เป้าหมาย: ลดระดับความเสี่ยงโดยรวมลงอย่างน้อย 30% ภายในหนึ่งปี
- วิธีวัด: เปรียบเทียบผลการประเมินความเสี่ยงครั้งล่าสุดกับการประเมินครั้งก่อนหน้า

4.2.1.2 ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น หน่วยงานต่าง ๆ อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงาน ดังนั้นจึงมีความจำเป็นสำหรับหน่วยงานในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ:

1) ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจาก การกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์

2) กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอเพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด

3) สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

4.2.1.3 ปัญหาทั่วไปที่สังเกตได้

ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติ ในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่ง ก็ประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วน ที่สังเกตเห็น ได้แก่

1) การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

2) การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุมความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่างเทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยงทำให้เกิดพฤติกรรม “รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัย ว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

3) การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงาน จึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยง ที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

4) การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้อาจไม่ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

5) จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุ ที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

4.2.1.4 วัตถุประสงค์

วัตถุประสงค์ของเอกสารนี้คือเพื่อให้คำแนะนำแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ กรมประชาสัมพันธ์ เกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

4.2.1.5 กลุ่มเป้าหมายและขอบเขต

เอกสารนี้มีขึ้นเพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

1) ผู้มีส่วนได้ส่วนเสีย (Stakeholders) (เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบ หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ ฯลฯ) ภายในหน่วยงาน

2) ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน

3) ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

4.2.2 สร้างบริบทความเสี่ยง

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณาและความรับผิดชอบของเจ้าของความเสี่ยง

4.2.2.1 กำหนดความเสี่ยง (*Define Risk*)

มีคำจำกัดความมากมายเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนั้นก่อนที่จะกำหนดรายละเอียดเพิ่มเติมเกี่ยวกับการประเมินความเสี่ยง สิ่งสำคัญคือต้องกำหนดคำนิยามทั่วไปของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ 2 ปัจจัย คือ:

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (**Likelihood**, **Impact**)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor)[4] ใช้เวกเตอร์ภัยคุกคาม การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย เรียกว่า

[4] ผู้คุกคามหมายถึงบุคคลหรือองค์กรที่รับผิดชอบต่อเหตุการณ์ที่อาจก่อให้เกิดอันตราย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

เวกเตอร์การโจมตี (Threat Vector)[5] กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตรายในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP)) ที่ใช้โดยผู้คุกคาม

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ

ความน่าจะเป็น (Likelihood)

ความน่าจะเป็น หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์ จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

ระดับที่โอกาสความเสี่ยงที่จะเกิดขึ้น (Likelihood)		
สูงมาก	5	ปัจจุบันกำลังเกิดขึ้น/อาจเกิดขึ้นภายในปีนี้/เกิดขึ้นเป็นประจำทุกปี
สูง	4	อาจเกิดขึ้น 1 ครั้งทุกๆ 2-3 ปี /เคยเกิดขึ้นเมื่อปีที่แล้ว
ปานกลาง	3	เคยเกิดขึ้นแล้วในช่วงเวลา 2-3 ปีที่ผ่านมา
ต่ำ	2	อาจเกิดขึ้น 1 ครั้งทุกๆ 4-5 ปี /เคยเกิดขึ้นแล้วในช่วงเวลา 4-5 ปีที่ผ่านมา
ต่ำมาก	1	เป็นไปได้ทางทฤษฎีแต่ไม่น่าจะเกิดขึ้น

ตารางที่ 4-5 ระดับที่โอกาสความเสี่ยงที่จะเกิดขึ้น (Likelihood)

ผลกระทบ (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

ระดับผลกระทบ	ด้าน Operation	ด้าน Reputation	ด้าน Compliance
สูงมาก (5)	หยุดการดำเนินงานขององค์กร/ หน่วยงานฯ ทรัพย์สินเสียหายมากและหรือต้องหยุดกระบวนการทั้งหมดเป็นระยะเวลามากกว่า 1 วันขึ้นไป	หน่วยงานที่เกี่ยวข้องให้ข้อสังเกตด้วยเอกสาร/ผู้มีส่วนได้ส่วนเสียร้องเรียนเป็นเอกสาร มีการแสดงความคิดเห็นเชิงลบ/ไม่พอใจผ่านสื่อกว้างขวาง มีการหยุดการดำเนินงาน/เกิดการต่อต้านรุนแรงจากสาธารณะทุกช่องทางและมีการฟ้องร้องดำเนินคดี ถูกตัดสินว่ามีความผิดจริง	ความรับผิดทางอาญาต้องระวางโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินหนึ่งล้านบาท หรือทั้งจำทั้งปรับ
สูง (4)	มีผลกระทบต่อกระบวนการอย่างรุนแรง/กระทบต่อแผนงานทรัพย์สินเสียหายและต้องหยุดการดำเนินงาบางส่วนทรัพย์สินเสียหายมาก และ	หน่วยงานที่เกี่ยวข้องให้ข้อสังเกตด้วยเอกสาร/ผู้มีส่วนได้ส่วนเสียร้องเรียนเป็นเอกสาร มีการแสดงความคิดเห็นเชิงลบ/ไม่พอใจผ่านสื่อกว้างขวาง มี	ความรับผิดทางปกครองต้องระวางโทษปรับทางปกครองไม่เกินห้าล้านบาท

[5] เวกเตอร์ภัยคุกคามหมายถึงเส้นทางหรือเส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ระดับผลกระทบ	ด้าน Operation	ด้าน Reputation	ด้าน Compliance
	หรือต้องหยุดกระบวนการทั้งหมดเป็นระยะเวลา 1 วัน	ผลกระทบรุนแรงต่อแผนงานและมีการตั้งคณะกรรมการสอบสวนความผิด	
ปานกลาง (3)	มีผลกระทบต่อกระบวนการปานกลางทรัพย์สินเสียหายมากและต้องหยุดกระบวนการในบางส่วน	หน่วยงานที่เกี่ยวข้องให้ข้อสังเกตด้วยเอกสาร/ผู้มีส่วนได้ส่วนเสียร้องเรียนเป็นเอกสาร มีผลกระทบต่กระบวนการปานกลาง ต้องเสียทรัพยากรในการชี้แจงและแก้ไข (ยังไม่มีหน่วยงานจัดทำข้อสังเกตเป็นทางการ)	ความรับผิดทางแพ่ง ต้องชดใช้ค่าสินไหมทดแทนเพื่อการนั้นแก่เจ้าของข้อมูลส่วนบุคคล
น้อย (2)	มีผลกระทบต่อกระบวนการเล็กน้อยทรัพย์สินเสียหายปานกลางและหรือสามารถดำเนินการของกระบวนการต่อไปได้	หน่วยงานที่เกี่ยวข้อง/ผู้มีส่วนได้ส่วนเสียให้ข้อสังเกตด้วยวาจา ต้องเสียทรัพยากรในการชี้แจง	เกิดการร้องเรียนของเจ้าของข้อมูลส่วนบุคคล ซึ่งอาจกระทบต่อภาพลักษณ์ชื่อเสียงขององค์กร
น้อยที่สุด (1)	ไม่มีการชะงักงันของกระบวนการและการดำเนินงานขององค์กร/ หน่วยงานฯ ทรัพย์สินเสียหายน้อยมากหรือไม่เสียหายเลย	ผู้มีส่วนได้ส่วนเสียพึงพอใจน้อย กระบวนการสามารถดำเนินการไปได้ตามปกติ	ไม่เกิดการร้องเรียน หรือการละเมิดข้อมูลส่วนบุคคลอันใด จากกระบวนการปฏิบัติงานขององค์กร

ตารางที่ 4-6 ระดับผลกระทบ (Impact)

4.2.2.2 กำหนดความเสี่ยงที่ยอมรับได้ (*Determine Risk Tolerance*)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ขององค์กรที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

		ระดับความรุนแรง (Impact Level)				
		น้อยมาก (1)	น้อย (2)	ปานกลาง (3)	สูง (4)	สูงมาก (5)
ระดับที่โอกาสความเสี่ยงที่จะเกิดขึ้น (Likelihood)	สูงมาก (5)	5	10	15	20	25
	สูง (4)	4	8	12	16	20
	ปานกลาง (3)	3	6	9	12	15
	น้อย (2)	2	4	6	8	10
	น้อยมาก (1)	1	2	3	4	5

ตารางที่ 4-7 ตารางระดับความเสี่ยง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ระดับความเสี่ยงโดยรวม (Risk Exposure)	คะแนน	ความหมาย	ระดับความเร่งด่วน/แนวทางปฏิบัติ
สูงมาก (E: Extremely high)	15-25	ไม่สามารถยอมรับได้ จะต้องบริหารความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้โดยเร่งด่วน	ระดับที่ 1 หมายถึง แผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) ซึ่งต้องเริ่มดำเนินการแก้ไขภายใน 1 เดือน นับจากวันที่ได้รับอนุมัติผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง และเร่งดำเนินการให้แล้วเสร็จโดยเร็ว
สูง (High: H)	8-12	ไม่สามารถยอมรับได้ จะต้องบริหารความเสี่ยง เพื่อให้อยู่ในระดับที่ยอมรับได้	ระดับที่ 1 หมายถึง แผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) ซึ่งต้องเริ่มดำเนินการแก้ไขภายใน 3 เดือน นับจากวันที่ได้รับอนุมัติผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง และเร่งดำเนินการให้แล้วเสร็จโดยเร็ว
ปานกลาง (Medium: M)	4-6	ความเสี่ยงอยู่ในระดับปานกลาง ต้องเฝ้าระวัง/ควบคุม/ติดตามผลอย่างต่อเนื่องเพื่อไม่ให้ความเสี่ยงเพิ่มมากขึ้นไปอยู่ในระดับที่ยอมรับได้	ระดับที่ 2 หมายถึง แผนจัดการความเสี่ยงประเภทแผนโอกาสในการปรับปรุง (Opportunity for Improvement: OFI) ซึ่งควรเริ่มดำเนินการภายใน 6 เดือน นับจากวันที่ได้รับอนุมัติผลการประเมินความเสี่ยงและแผนจัดการความเสี่ยง
ต่ำ (Low: L)	1-3	ยอมรับความเสี่ยงได้ โดยไม่ต้องมีการจัดการความเสี่ยงเพิ่มเติม	ควรดำเนินการแก้ไขเมื่อมีความพร้อมทางทรัพยากรในด้านต่าง ๆ หรือเฝ้าระวังการเปลี่ยนแปลง

ตารางที่ 4-8 ตารางการยอมรับความเสี่ยง

4.2.2.3 กำหนดบทบาทและความรับผิดชอบ (*Define Roles and Responsibilities*)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

หัวหน้าหน่วยงาน (Head of Organization)

เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยง ได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

ผู้นำองค์กร (Organization Leader)

เจ้าหน้าที่อาวุโสระดับสูงสุดของหน่วยงาน ที่รับผิดชอบในการตรวจสอบให้แน่ใจว่าการดำเนินงานขององค์กรบรรลุเป้าหมาย หรือแบ่งปันข้อกังวลเกี่ยวกับผลกระทบที่มีต่อหน่วยงานในกรณีที่ระบบมีการหยุดชะงัก

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและภารกิจของหน่วยงานในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนการทำงานขององค์กร ควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุม ความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนการทำงานขององค์กร โดยบุคคลดังกล่าวควรระบุภัยคุกคาม ที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามทางไซเบอร์

4.2.3 ดำเนินการประเมินความเสี่ยง

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)



รูปที่ 4-3: กระบวนการดำเนินการประเมินความเสี่ยง

4.2.3.1 ขั้นตอนที่ 1: การระบุความเสี่ยง *(Risk Identification)*

ระบุทรัพย์สิน (Identify Assets)

การระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง เมื่อระบุทรัพย์สิน สิ่งสำคัญคือต้องจดบันทึกทรัพย์สินเหล่านั้น

- **ทรัพย์สินสำคัญ (Crown Jewels)** – ทรัพย์สินเหล่านี้มีความสำคัญต่อการดำเนินงานขององค์กรโดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์

ตัวอย่าง: ในระบบควบคุมแบบกระจาย (Distributed Control System (DCS)) ของโรงไฟฟ้า โปรแกรมควบคุมลอจิกแบบตั้งโปรแกรมได้ (Programmable Logic Controller (PLC)) ที่ควบคุมระบบไฟฟ้ามักจะได้รับการพิจารณาว่าเป็นทรัพย์สินสำคัญ เนื่องจากมีผลโดยตรงต่อการผลิตไฟฟ้า ซึ่งเป็นงานหลักสำคัญของโรงไฟฟ้า ผู้โจมตีที่ต้องการขัดขวางการผลิตไฟฟ้ามีแนวโน้มที่จะโจมตีและควบคุมตรรกะภายใน PLC

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- **ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones)** - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

ตัวอย่าง: ในสภาพแวดล้อม Windows ทั่วไป เซิร์ฟเวอร์ Active Directory (AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ไปยังเซิร์ฟเวอร์หลายเครื่องมักจะได้รับการพิจารณาว่าเป็นทรัพย์สินที่เกี่ยวข้อง เนื่องจากเป็นสะพานเชื่อมให้ผู้โจมตีเปลี่ยนเข้าสู่เซิร์ฟเวอร์เหล่านี้

ใช้รายการทรัพย์สินที่รวมเข้าด้วยกันเพื่อสร้างแผนผังสถาปัตยกรรมเครือข่ายที่ให้การแสดงภาพของเส้นทางการเชื่อมต่อระหว่างกันและการสื่อสารระหว่างทรัพย์สิน ระบุจุดเข้าทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่ายในระบบ รวมถึงทรัพย์สินที่เกี่ยวข้องและทรัพย์สินสำคัญ สิ่งนี้ จะช่วยอำนวยความสะดวกในงานต่อไปในการระบุภัยคุกคาม

การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

ด้วยรายการทะเบียนทรัพย์สินและไดอะแกรมสถาปัตยกรรมเครือข่าย ควรระบุเหตุการณ์ภัยคุกคามที่อาจใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการเพื่อการวิเคราะห์เชิงลึก เทคนิคประการหนึ่งที่หน่วยงานควรใช้คือการสร้างแบบจำลองภัยคุกคาม โดยการสร้างแบบจำลองภัยคุกคามเป็นกระบวนการที่มีโครงสร้างสำหรับการระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับระบบ เพื่อให้หน่วยงานสามารถสร้างการป้องกันที่มุ่งเน้นมากขึ้นเพื่อปกป้องระบบ ซึ่งการสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

1. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) – สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคาม

2. การระบุภัยคุกคาม (Threat Identification) – หน่วยงานควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

3. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบทขององค์กร สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยัง ผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก 4 ประการ ต่อไปนี้:

1) **ทรัพย์สิน (Asset)** - สิ่งที่มีค่า

2) **เหตุการณ์ภัยคุกคาม (Threat event)** - เหตุการณ์การโจมตี

3) **ช่องโหว่ (Vulnerability)** – จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สิน ที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการทดสอบการเจาะระบบ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4) **ผลที่ตามมา (Consequence)**[6] – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

4.2.3.2 ขั้นตอนที่ 2: การวิเคราะห์ความเสี่ยง (*Risk Analysis*)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(1) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น

(2) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

กำหนดโอกาส (Determine Likelihood)

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าว เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคต

ตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับการประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้[7]

1) ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

2) ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

3) **ความสามารถในการทำซ้ำ (Reproducibility)** – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

กำหนดผลกระทบ (Determine Impact)

โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบใน 3 ประเภท (ตารางที่ 4-6: ระดับผลกระทบ (Impact)) คือด้าน Operation, ด้าน Reputation, ด้าน Compliance

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบ

---

[6] คำว่า "ผลที่ตามมา (consequence)" และ "ผลกระทบ (consequence)" มักใช้แทนกันได้ อย่างไรก็ตามมีความหมายต่างกันและไม่ควรสับสน ในขณะที่ “ผลที่ตามมา” เป็นผลโดยตรงจากเหตุการณ์ภัยคุกคาม (เช่น ไฟดับ การหยุดชะงักของบริการ การสูญเสียข้อมูลที่เป็นความลับ) “ผลกระทบ” คือระดับที่ผลที่ตามมาจะส่งผลกระทบต่อธุรกิจ การดำเนินงาน ฯลฯ (เช่น ขนาดของอันตราย)

[7] ปัจจัย (Discoverability, Exploitability and Reproducibility) ถูกดัดแปลงมาจากโมเดล DREAD ของ Microsoft สำหรับการประเมินภัยคุกคาม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

สูงสุดควรถือเป็นคะแนนสุดท้าย

4.2.3.3 ขั้นตอนที่ 3: การประเมินความเสี่ยง *(Risk Evaluation)*

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับ ความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

1) กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritize Risk)
2) ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritize Risk)

ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นดังตารางที่ 4-7: ตารางระดับความเสี่ยง และตารางที่ 4-8: ตารางการยอมรับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงควรเป็นเอกสารที่เป็นปัจจุบัน ซึ่งได้รับการตรวจสอบและปรับปรุง ให้ทันสมัย รายงานการประเมินความเสี่ยงหน่วยงาน ทะเบียนความเสี่ยงต้องมีองค์ประกอบอย่างน้อย 8 ประการดังต่อไปนี้

1) **สถานการณ์ความเสี่ยง (Risk Scenario)** – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคาม ช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินมีผลกระทบในทางลบ
2) **วันที่ระบุความเสี่ยง (Identification Date)** – วันที่ที่ระบุสถานการณ์ความเสี่ยง
3) **มาตรการที่มีอยู่ (Existing Measures)** – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง
4) **ความเสี่ยงในปัจจุบัน (Current Risk)** – ระดับความเสี่ยงที่กำหนดของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk)[8]
5) **แผนจัดการความเสี่ยง (Treatment Plan)** – กิจกรรมที่วางแผนไว้ เช่น การใช้มาตรการเพิ่มเติมและระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ เช่น ระดับการยอมรับความเสี่ยงของหน่วยงาน
6) **สถานะความคืบหน้า (Progress Status)** – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

[8] ความเสี่ยงโดยธรรมชาติ (Inherent risk) หมายถึง ระดับความเสี่ยงที่มีอยู่โดยพิจารณาถึงมาตรการควบคุมในปัจจุบัน แต่ไม่คำนึงถึงมาตรการใด ๆ ที่จะดำเนินการเพิ่มเติม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

7) **ความเสี่ยงที่คงเหลืออยู่ (Residual Risk)** – ระดับความเสี่ยงที่กำหนดของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม
8) **เจ้าของความเสี่ยง (Risk Owner)** – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลือ อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

4.2.4 ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

4.2.4.1 ประเภทของตัวเลือกการตอบสนองความเสี่ยง *(Types of Risk Response Options)*

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน 4 ตัวเลือก ที่ต้องพิจารณา

(1) ยอมรับ (Accept)

การยอมรับความเสี่ยง หมายถึง การรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(2) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยง หมายถึง การยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์ผ่านอินเทอร์เน็ตหรือคอมพิวเตอร์สาธารณะ เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยงที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(3) โอนย้าย *(*Transfer)

การโอนความเสี่ยง หมายถึง การแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของ การแบ่งปันความเสี่ยงกับบุคคลที่สาม

(4) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยง หมายถึง การวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดการเข้าถึงเครือข่าย เป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

4.2.4.2 การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (*Choosing the Appropriate Risk Response Actions*)

การจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคมีค่าใช้จ่ายสูง หน่วยงานอาจสำรวจการรักษาความเสี่ยง ด้วยการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

หลีกเลี่ยงหรือถ่ายโอน ซึ่งอาจมีความคุ้มค่ามากกว่า เช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบ เมื่อเจ้าหน้าที่เข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานอาจต้องพิจารณาหลีกเลี่ยงความเสี่ยง โดยการกำหนดหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการ ใช้ระบบตรวจจับหรือป้องกันการบุกรุกที่มีราคาแพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยงหรือการลดผลกระทบจากความเสี่ยง

5. แผนที่นำทาง (Road Map) ในการนำแผนฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรม

การจัดทำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารให้มีประสิทธิภาพและบรรลุผลตามเป้าหมาย จำเป็นต้องมีแผนที่นำทาง (Road Map) ที่ชัดเจนและครอบคลุม เพื่อกำหนดทิศทางและลำดับขั้นตอนในการดำเนินงานอย่างเป็นรูปธรรม แผนที่นำทางนี้เป็นเครื่องมือสำคัญในการเชื่อมโยงระหว่างยุทธศาสตร์ ความเสี่ยง และทรัพยากรที่จำเป็นสำหรับการปฏิบัติแผนฯ

5.1 บทนำของแผนที่นำทาง (Road Map)

ในบริบทของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ซึ่งดูแลข้อมูลสำคัญระดับประเทศ การนำแผนฯ ไปสู่การปฏิบัติต้องอาศัยความร่วมมือระหว่างหน่วยงานภายในและภายนอก พร้อมทั้งการวางแผนการดำเนินงานที่ตอบสนองต่อความท้าทายทางไซเบอร์อย่างเป็นระบบ บทนี้จะกล่าวถึงลำดับขั้นตอนของแผนที่นำทาง ตั้งแต่การจัดสรรทรัพยากร การกำหนดเป้าหมายในระยะสั้น ระยะกลางและระยะยาว ไปจนถึงการกำหนดตัวชี้วัดที่ชัดเจนสำหรับการติดตามและประเมินผล เพื่อให้มั่นใจว่าแผนบริหารจัดการความปลอดภัยสามารถดำเนินไปได้อย่างมีประสิทธิภาพ ครอบคลุม และสอดคล้องกับความต้องการและบริบทเฉพาะของ สคทช.

5.1.1 ตัวชี้วัดของแผนที่นำทาง (Road Map)

ตัวชี้วัดของแผนที่นำทาง (Road Map) ประกอบด้วย 4 ด้าน ได้แก่ ตัวชี้วัดระดับยุทธศาสตร์ ตัวชี้วัดระดับการปฏิบัติการ ตัวชี้วัดด้านการพัฒนาบุคลากร และตัวชี้วัดด้านความร่วมมือ มีรายละเอียดดังนี้

1. ตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators)

ตัวชี้วัดยุทธศาสตร์ จากบทนำแผนฯ	ตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators) ของแผนที่นำทาง (Road Map)
ยุทธศาสตร์ที่ 1	
ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์	ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์
การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง	การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง (Incident Reduction Rate)
การพัฒนาทักษะบุคลากรด้านไซเบอร์	อัตราการพัฒนาทักษะบุคลากรด้านไซเบอร์ (Cybersecurity Skill Development Rate)
ยุทธศาสตร์ที่ 2	

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ตัวชี้วัดยุทธศาสตร์ จากบทนำแผนฯ	ตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators) ของแผนที่นำทาง (Road Map)
การพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน	อัตราความสำเร็จในการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Data Exchange Standard Implementation Rate)
การดำเนินแผน BCP สำหรับระบบสำคัญ	อัตราการดำเนินแผน BCP สำหรับระบบสำคัญ (BCP Implementation Rate)
ระดับความพึงพอใจของหน่วยงานพันธมิตร	ระดับความพึงพอใจของหน่วยงานพันธมิตร (Partner Satisfaction Level)
ยุทธศาสตร์ที่ 3	
การได้รับการรับรองมาตรฐาน ISO/IEC 27001	จำนวนมาตรฐานที่ได้รับการรับรอง (Standard Certification Achievement)
	ระดับความพร้อมในการตรวจสอบและประเมินผล (Audit Readiness Level)
	อัตราความโปร่งใสและความรับผิดชอบต่อการดำเนินงาน (Transparency and Accountability Rate)

ตารางที่ 5-1 ความสอดคล้องของตัวชี้วัดยุทธศาสตร์ของแผนฯ กับตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators) ของแผนที่นำทาง (Road Map)

จากตารางด้านบน ตัวชี้วัดระดับยุทธศาสตร์ (Strategic-Level Indicators) ของแผนที่นำทาง (Road Map) มีรายละเอียดดังนี้

1.1. ยุทธศาสตร์ที่ 1: พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (Integrating cybersecurity capabilities)

1.1.1. ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์

- **เป้าหมาย**: ระบบเฝ้าระวังและตอบสนองภัยคุกคามครอบคลุม 100% ของระบบสำคัญ
- **การวัดผล**: สัดส่วนของระบบที่มี SOC และใช้ MSSP

1.1.2. การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง (Incident Reduction Rate)

- **เป้าหมาย**: ลดจำนวนเหตุการณ์ภัยคุกคามที่ส่งผลกระทบต่อระบบสำคัญ ≥ 50% ในปีแรก
- **การวัดผล**: ข้อมูลจากรายงานเหตุการณ์ของ SOC

1.1.3. อัตราการพัฒนาทักษะบุคลากรด้านไซเบอร์ (Cybersecurity Skill Development Rate)

- **เป้าหมาย**: บุคลากรที่ผ่านการฝึกอบรมด้านไซเบอร์ ≥ 95%
- **การวัดผล**: รายงานการอบรมและแบบทดสอบหลังอบรม

1.2. ยุทธศาสตร์ที่ 2: บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติ (Partnership)

1.2.1. อัตราความสำเร็จในการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน (Data Exchange Standard Implementation Rate)

- **เป้าหมาย**: 100% ของมาตรฐานการแลกเปลี่ยนข้อมูลได้รับการพัฒนาภายในปีที่ 2
- **การวัดผล**: รายงานความคืบหน้าจากโครงการที่เกี่ยวข้อง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

1.2.2. อัตราการดำเนินแผน BCP สำหรับระบบสำคัญ (BCP Implementation Rate)

- **เป้าหมาย**: ระบบสำคัญทั้งหมดมีแผน BCP ครอบคลุม 100%
- **การวัดผล**: รายงานการจัดทำและทดสอบแผน BCP

1.2.3. ระดับความพึงพอใจของหน่วยงานพันธมิตร (Partner Satisfaction Level)

- **เป้าหมาย**: ความพึงพอใจเฉลี่ย ≥ 90%
- **การวัดผล**: แบบสำรวจความพึงพอใจ

1.3. ยุทธศาสตร์ที่ 3: เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)

1.3.1. จำนวนมาตรฐานที่ได้รับการรับรอง (Standard Certification Achievement)

- **เป้าหมาย**: ได้รับการรับรอง ISO/IEC 27001 ภายในปี พ.ศ. 2570
- **การวัดผล**: รายงานผลการรับรองจากหน่วยงานตรวจประเมิน

1.3.2. ระดับความพร้อมในการตรวจสอบและประเมินผล (Audit Readiness Level)

- **เป้าหมาย**: การตรวจสอบภายในและภายนอกผ่านเกณฑ์ ≥ 90%
- **การวัดผล**: รายงานผลการตรวจสอบ

1.3.3. อัตราความโปร่งใสและความรับผิดชอบต่อการดำเนินงาน (Transparency and Accountability Rate)

- **เป้าหมาย**: ≥ 95% ของโครงการดำเนินการสอดคล้องกับนโยบายและแผนที่วางไว้
- **การวัดผล**: รายงานผลการตรวจติดตามและประเมินผล

ตัวชี้วัดเหล่านี้จะช่วยให้องค์กรสามารถติดตามผลลัพธ์ในระดับยุทธศาสตร์ และเชื่อมโยงไปยังตัวชี้วัดระดับกลยุทธ์และโครงการได้อย่างสอดคล้องและเป็นระบบ โดยมีรายละเอียดของค่าเป้าหมายรายปีต่าง ๆ ตามที่ได้ระบุไว้ในส่วนของบทนำของแผนฯ ดังนี้

ยุทธศาสตร์ที่ 1: พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์

1) ระดับความพร้อมของระบบเฝ้าระวังและตอบสนองภัยคุกคามไซเบอร์

- พ.ศ. 2568: มีระบบเฝ้าระวังครอบคลุมระบบสำคัญ 1 ระบบ
- พ.ศ. 2569: ครอบคลุมระบบสำคัญ 2 ระบบ พร้อมบูรณาการ AI ในการตรวจจับภัยคุกคาม
- พ.ศ. 2570: ครอบคลุมระบบสำคัญ 3 ระบบ พร้อมปรับใช้ระบบแจ้งเตือนแบบเรียลไทม์

2) การลดจำนวนเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริง

- พ.ศ. 2568: จัดทำแผนการลดความเสี่ยงที่เป็นระบบ
- พ.ศ. 2569: ขยายแผนการลดความเสี่ยงให้ครอบคลุมภัยคุกคามในระดับเครือข่าย พร้อมทดสอบระบบ Incident Response Plan
- พ.ศ. 2570: สามารถลดความเสี่ยงในทุกประเภทภัยคุกคามที่สำคัญ พร้อมสร้างกลไกแจ้งเตือนล่วงหน้า

3) การพัฒนาทักษะบุคลากรด้านไซเบอร์

- พ.ศ. 2568: จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ
- พ.ศ. 2569: จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ และจัดอบรมเชิงปฏิบัติการสำหรับผู้เชี่ยวชาญ
- พ.ศ. 2570: จัดอบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรทุกระดับ และจัดอบรมเชิงปฏิบัติการสำหรับผู้เชี่ยวชาญร่วมกับหน่วยงานพันธมิตร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์ที่ 2: บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์

1) การพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลระหว่างหน่วยงาน

- พ.ศ. 2569: จัดทำร่างมาตรฐานและเริ่มทดลองใช้กับ 3 หน่วยงาน
- พ.ศ. 2570: ขยายการทดลองใช้งานให้ครอบคลุม 70% ของหน่วยงานที่เกี่ยวข้อง

2) การดำเนินแผน BCP สำหรับระบบสำคัญ

- พ.ศ. 2568: มีแผน BCP ครอบคลุมระบบสำคัญ 1 ระบบ และจัดการทดสอบแผน 1 ครั้ง
- พ.ศ. 2569: ขยายการจัดทำแผน BCP ให้ครอบคลุมระบบสำคัญ 2 ระบบ พร้อมทดสอบแผน 1 ครั้ง
- พ.ศ. 2570: ครอบคลุมระบบสำคัญ 100% พร้อมบูรณาการแผน BCP ข้ามหน่วยงาน

3) ระดับความพึงพอใจของหน่วยงานพันธมิตร

- พ.ศ. 2569: จัดตั้งกลไกการประชุมเชิงปฏิบัติการร่วมกับพันธมิตร และจัดเวิร์กชอป 2 ครั้งต่อปี
- พ.ศ. 2570: ความพึงพอใจเฉลี่ย 85% จากการจัดประชุมและเวิร์กชอป 2 ครั้งต่อปี พร้อมจัดทำแผนความร่วมมือระยะยาว

ยุทธศาสตร์ที่ 3: เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน

1) การได้รับการรับรองมาตรฐาน ISO/IEC 27001

- พ.ศ. 2569: พัฒนากระบวนการและระบบตามข้อกำหนดของมาตรฐาน พร้อมดำเนินการตรวจสอบภายใน
- พ.ศ. 2570: ดำเนินการตรวจรับรองจากหน่วยงานภายนอกและได้รับการรับรองมาตรฐาน

2. ตัวชี้วัดระดับการปฏิบัติการ

2.1. ระยะเวลาตอบสนองต่อเหตุการณ์ (Incident Response Time)

- **เป้าหมาย**: ลดระยะเวลาตอบสนองภัยคุกคามให้เหลือไม่เกิน 1 ชั่วโมง
- **การวัดผล**: ตรวจสอบข้อมูลจากรายงาน SOC (Security Operations Center)

2.2. ประสิทธิภาพของศูนย์เฝ้าระวังภัยคุกคาม (SOC Efficiency)

- **เป้าหมาย**: อัตราการตรวจจับเหตุการณ์ไซเบอร์ที่มีความสำคัญ > 95%
- **การวัดผล**: สถิติการตรวจจับและแจ้งเตือนของ SOC

2.3. อัตราการสำรองข้อมูลและกู้คืน (Backup and Recovery Success Rate)

- **เป้าหมาย**: ระบบสำรองข้อมูลและกู้คืนต้องทำงานสำเร็จไม่น้อยกว่า 98% ในเหตุการณ์จำลอง
- **การวัดผล**: ตรวจสอบผลการทดสอบ Disaster Recovery Plan (DRP)

3. ตัวชี้วัดด้านการพัฒนาบุคลากร

3.1. จำนวนผู้เข้ารับการอบรม (Training Participation Rate)

- **เป้าหมาย**: บุคลากรที่เกี่ยวข้องต้องผ่านการอบรมไม่น้อยกว่า 95% ในแต่ละปี
- **การวัดผล**: ใช้รายงานจากหน่วยงาน HR และผลการทดสอบหลังอบรม

3.2. ระดับความพึงพอใจในโปรแกรมการเรียนรู้ (Learning Satisfaction Level)

- **เป้าหมาย**: ความพึงพอใจเฉลี่ย > 85% จากแบบสอบถาม
- **การวัดผล**: วิเคราะห์ผลสำรวจความพึงพอใจ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

4. ตัวชี้วัดด้านความร่วมมือ

4.1. การพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล (Data Exchange Standard Implementation Rate)

- **เป้าหมาย**: พัฒนามาตรฐานสำเร็จ 100% ภายในปีที่ 2
- **การวัดผล**: ตรวจสอบความคืบหน้าในเอกสารและแพลตฟอร์มที่ใช้งานร่วมกัน

4.2. ความพึงพอใจของหน่วยงานพันธมิตร (Partner Satisfaction Rate)

- **เป้าหมาย**: ระดับความพึงพอใจจากการทำงานร่วมกันไม่น้อยกว่า 90%
- **การวัดผล**: ผลการสำรวจความพึงพอใจจากหน่วยงานพันธมิตร

5.1.2 การจัดลำดับความสำคัญของการดำเนินงาน

ในการวางแผนปฏิบัติงานและการลงทุนในแต่ละปีตามหลักเกณฑ์ เพื่อให้การบริหารจัดการแผนปฏิบัติการด้านความมั่นคงปลอดภัยเป็นไปอย่างมีประสิทธิภาพและสอดคล้องกับเป้าหมายเชิงกลยุทธ์ขององค์กร จึงได้กำหนดแนวทางการจัดลำดับความสำคัญของโครงการหรือแผนงาน โดยอิงจากปัจจัย "ความสำคัญ" ซึ่งแบ่งออกเป็น 5 ระดับ ได้แก่ สูงมาก (Critical), สูง (High), ปานกลาง (Moderate), ต่ำ (Low), ต่ำมาก (Very Low) และ "ความเร่งด่วน" ซึ่งแบ่งออกเป็น 3 ระดับ ได้แก่ สูง (High) กลาง (Medium) และต่ำ (Low) โดยมีการพิจารณาร่วมกับผลการศึกษาสถานการณ์ภัยคุกคามในประเทศและต่างประเทศช่วยให้เข้าใจถึงระดับความรุนแรงของภัยคุกคาม เช่น การโจมตีด้วยมัลแวร์และแรนซัมแวร์ การละเมิดข้อมูล (Data Breach) และการโจมตีแบบฟิชชิง (Phishing Attack) ดังนั้น การจัดลำดับความสำคัญเริ่มต้นจาก การป้องกันและตรวจจับภัยคุกคามในระบบสำคัญ เช่น ฐานข้อมูลที่ดินของ สคทช. โดยกำหนดให้การติดตั้งระบบ Intrusion Detection System (IDS) และการปรับปรุง Firewall เป็นขั้นตอนแรก อีกทั้งการวิเคราะห์นโยบายและกฎหมาย เช่น พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ช่วยกำหนดกรอบการดำเนินงานให้สอดคล้องกับข้อบังคับทางกฎหมาย การจัดลำดับความสำคัญในส่วนนี้เน้น การกำหนดนโยบายความมั่นคงปลอดภัยระดับองค์กร และ การฝึกอบรมบุคลากร เพื่อให้มั่นใจว่าการดำเนินงานเป็นไปตามมาตรฐานและข้อกำหนด ยิ่งไปกว่านั้นผลการศึกษาบริบทเฉพาะของ สคทช. ชี้ให้เห็นถึงการจัดการข้อมูลที่ดินซึ่งมีความสำคัญระดับประเทศและมีความอ่อนไหวสูง การจัดลำดับความสำคัญในส่วนนี้เน้นการบูรณาการระบบเทคโนโลยีใหม่ เช่น Blockchain สำหรับการป้องกันข้อมูลปลอมแปลง และการปรับปรุงกระบวนการเชื่อมโยงข้อมูลข้ามหน่วยงานด้วยระบบความปลอดภัยสูง ทั้งนี้ รายละเอียดของแต่ละปัจจัยในการจัดลำดับความสำคัญของการดำเนินงานมีดังนี้

5.1.2.1 ความสำคัญ (*Importance)*

หลักเกณฑ์การพิจารณา "ความสำคัญ" จะถูกกำหนดโดยการพิจารณาความเกี่ยวข้องกับแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ ซึ่งครอบคลุมแนวทางปฏิบัติและมาตรฐานที่จำเป็นต่อการลดความเสี่ยงไซเบอร์และการปฏิบัติตามกฎระเบียบ:

- ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
  - การระบุความเสี่ยง (Identify)
  - การป้องกันความเสี่ยง (Protect)
  - การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
- การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

➢ มาตรการรักษาความมั่นคงปลอดภัย ของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. 2565

➢ ยุทธศาสตร์ในนโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565-2570)

- ยุทธศาสตร์ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Capacity)
- ยุทธศาสตร์ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)
- ยุทธศาสตร์ 3 สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Resilience)
- ยุทธศาสตร์ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน (Standard)

ระดับความสำคัญและเกณฑ์การพิจารณามี 5 ระดับตั้งแต่ระดับสูงมากไปจนถึงต่ำมาก ซึ่งมีรายละเอียดดังนี้

1) สูงมาก (Critical)

- ความเกี่ยวข้องโดยตรง: โครงการหรือแผนงานที่จำเป็นต้องดำเนินการทันทีเพื่อปฏิบัติตามข้อกำหนดของกฎหมายหรือมาตรฐานที่สำคัญ
- ผลกระทบหากไม่ดำเนินการ: อาจเกิดความเสียหายต่อองค์กร เช่น การถูกปรับโดนลงโทษทางกฎหมาย หรือเกิดเหตุการณ์ความไม่ปลอดภัยไซเบอร์ร้ายแรง

2) สูง (High)

- ความเกี่ยวข้องใกล้ชิด: โครงการหรือแผนงานที่ช่วยเสริมสร้างความมั่นคงปลอดภัย และสอดคล้องกับข้อกำหนดทางกฎหมายหรือมาตรฐาน แม้ไม่จำเป็นต้องดำเนินการทันที
- ผลกระทบหากไม่ดำเนินการ: อาจส่งผลต่อความน่าเชื่อถือและความปลอดภัยในระยะยาว

3) ปานกลาง (Moderate)

- ความเกี่ยวข้องบางส่วน: โครงการหรือแผนงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยในระดับที่มีความสำคัญรองลงมา หรือเป็นการปรับปรุงระบบที่มีอยู่
- ผลกระทบหากไม่ดำเนินการ: ความเสี่ยงอยู่ในระดับที่จัดการได้ แต่ควรพิจารณาดำเนินการในอนาคต

4) ต่ำ (Low)

- ความเกี่ยวข้องต่ำ: โครงการหรือแผนงานที่เสริมสร้างความมั่นคงปลอดภัยในลักษณะการเพิ่มประสิทธิภาพ หรือเป็นทางเลือกเสริม
- ผลกระทบหากไม่ดำเนินการ: ไม่มีผลกระทบสำคัญต่อกฎหมายหรือความปลอดภัย

5) ต่ำมาก (Very Low)

- ความเกี่ยวข้องน้อยมาก: โครงการหรือแผนงานที่ไม่เกี่ยวข้องกับกฎหมายหรือมาตรฐานโดยตรง และไม่ได้มีผลกระทบต่อความมั่นคงปลอดภัย

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ผลกระทบหากไม่ดำเนินการ: ไม่ส่งผลกระทบต่อการดำเนินงานขององค์กร

5.1.2.2 ความเร่งด่วน (*Urgency)*

ความเร่งด่วน หมายถึง ระดับความจำเป็นในการดำเนินงานภายในระยะเวลาที่กำหนด เพื่อป้องกันความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นในอนาคต แบ่งเป็น 3 ระดับ ได้แก่:

1) **สูง (High Urgency):** แผนงานหรือโครงการที่ต้องดำเนินการในทันที เนื่องจากมีความจำเป็นเร่งด่วน เช่น การแก้ไขช่องโหว่ด้านความปลอดภัย หรือการตอบสนองเหตุการณ์ฉุกเฉิน
2) **กลาง (Medium Urgency):** แผนงานหรือโครงการที่สามารถวางแผนดำเนินการในระยะเวลาอันเหมาะสมได้ แต่ต้องดำเนินการเพื่อป้องกันปัญหาในอนาคต
3) **ต่ำ (Low Urgency):** แผนงานหรือโครงการที่สามารถรอการดำเนินการได้ในระยะยาว โดยไม่มีผลกระทบสำคัญในทันที

5.2 แผนที่นำทาง (Road Map) ในระยะ 3 ปี (พ.ศ. 2568-2570)

แผนที่นำทาง (Road Map) ในการนำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติไปสู่การปฏิบัติอย่างเป็นรูปธรรม มีรายละเอียด ดังนี้

แผนที่นำทาง (Road Map) ในการนำแผนฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรมปี พ.ศ. 2568-2570

	2568	2569	2570
ยุทธศาสตร์ที่ 1 บูรณาการความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	• จัดจ้าง MSSP ในการเฝ้าระวังระบบที่สำคัญ (P1) • สร้างความรู้และความตระหนักให้กับบุคลากรที่เกี่ยวข้อง (P6) • พัฒนาทักษะความมั่นคงปลอดภัย ระดับพื้นฐาน (P7)	• จัดจ้าง MSSP ในการเฝ้าระวังระบบที่สำคัญ (P1) • เพิ่มความแข็งแกร่งของระบบ Blockchain (P3) • ตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน เพื่อระบุช่องโหว่ที่อาจเป็นความเสี่ยงต่อระบบสำคัญ (P3) • จัดหาระบบจัดการ Client และ Mobile Device (P4) • จัดทำ Enterprise Architecture ทั้งด้านเทคโนโลยีและการรักษาความมั่นคงปลอดภัย (P5) • สร้างความรู้และความตระหนักให้กับบุคลากรที่เกี่ยวข้อง (P6) • พัฒนาทักษะความมั่นคงปลอดภัย ระดับกลาง (P7) • จัดหาแพลตฟอร์มการเรียนรู้ออนไลน์ (P8)	• จัดจ้าง MSSP ในการเฝ้าระวังระบบที่สำคัญ (P1) • จัดหาระบบจัดการ Client และ Mobile Device (P4) • สนับสนุนการใช้งานแพลตฟอร์มการเรียนรู้ (P9)
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	• จัดทำแผน BCP ระบบที่สำคัญ และจัดหาเทคโนโลยีที่เกี่ยวข้อง (P12)	• จัดทำแผน BCP ระบบที่สำคัญ และจัดหาเทคโนโลยีที่เกี่ยวข้อง (P12) • พัฒนามาตรฐานการแลกเปลี่ยนข้อมูล (P10)	• ทดสอบ BCP ระบบที่สำคัญร่วมกับพันธมิตร (P12) • ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย • ประเมินและจัดหาเทคโนโลยี Cloud (P13) • ประชุมและเวิร์คช็อปการแบ่งปันข้อมูล (P11)
ยุทธศาสตร์ที่ 3 สร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)		• เตรียมความพร้อม ISO/IEC 27001 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (P14)	• ขอรับรองมาตรฐานISO/IEC 27001 ระบบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (P14)

รูปที่ 5-1: แผนที่นำทาง (Road Map)

แผนที่นำทาง (Road Map) ในการนำแผนบริหารจัดการความปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติไปสู่การปฏิบัติอย่างเป็นรูปธรรม แบ่งการดำเนินงานออกเป็นระยะเวลา 3 ปี ซึ่งแต่ละปีจะมีเป้าหมายและกิจกรรมที่สอดคล้องกัน ดังนี้

ปีที่ 1 (2568) : การวางรากฐานและจัดการความมั่นคงปลอดภัยเร่งด่วน

ในปีแรก มุ่งเน้นการดำเนินโครงการที่มีความสำคัญสูงและเร่งด่วน เพื่อเสริมสร้างความพร้อมและความมั่นคงปลอดภัยขององค์กร โดยมีแผนการดำเนินการดังนี้:

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- เริ่มต้น โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อให้สามารถตรวจจับและแจ้งเตือนภัยคุกคามไซเบอร์แบบเรียลไทม์ (P1) ด้วยเทคโนโลยีขั้นสูง เช่น ปัญญาประดิษฐ์ (Artificial Intelligence: AI)
- ตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน เพื่อระบุช่องโหว่ที่อาจเป็นความเสี่ยงต่อระบบสำคัญ (P2)
- จัดทำและทดสอบแผนความต่อเนื่องทางธุรกิจ (BCP) สำหรับระบบที่สำคัญ (P12) เพื่อรองรับสถานการณ์ฉุกเฉิน เช่น ภัยไซเบอร์หรือความล้มเหลวของระบบ
- สื่อสารความก้าวหน้าและประโยชน์ของโครงการให้ผู้เกี่ยวข้องทราบ
- วางรากฐานระบบติดตามและวิเคราะห์ผลการดำเนินงานเพื่อใช้ในปีถัดไป

ปีที่ 2 (2569) : การขยายขอบเขตและการพัฒนาศักยภาพเชิงลึก

ปีที่ 2 จะเน้นการดำเนินงานต่อเนื่องจากปีแรก และเพิ่มศักยภาพด้านการจัดการและการพัฒนาเชิงกลยุทธ์ โดยมีแผนดังนี้:

- ต่อยอดการดำเนินงานของโครงการ SOC และแผน BCP โดยจัดการประเมินผลการดำเนินงานและปรับปรุงตามความเหมาะสม
- เริ่มดำเนินการ โครงการอัพเกรดอุปกรณ์และระบบป้องกัน เพื่อเพิ่มประสิทธิภาพในการจัดการภัยคุกคามและลดความเสี่ยงในระยะยาว (P3)
- จัดซื้อและติดตั้ง ระบบ Enterprise Device Management (EDM) เพื่อสนับสนุนการจัดการอุปกรณ์ในองค์กร (P4)
- เริ่มต้นพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 เพื่อยกระดับการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศ (P14)
- จัดการฝึกอบรมเบื้องต้นให้บุคลากรเกี่ยวกับความรู้ด้านความมั่นคงปลอดภัยพื้นฐาน เพื่อสร้างความตระหนัก (P6)
- เริ่ม วิเคราะห์และออกแบบระบบ Enterprise Architecture (EA) เพื่อวางโครงสร้างเทคโนโลยีและกระบวนการทำงานที่เหมาะสม (P5)
- จัด ฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก เพื่อเพิ่มความเชี่ยวชาญในการรับมือภัยคุกคามที่ซับซ้อน (P7)
- เริ่มดำเนิน โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล เพื่อเสริมสร้างความชัดเจนและประสิทธิภาพในการแบ่งปันข้อมูลระหว่างหน่วยงาน (P10)
- ประเมินความเหมาะสมและวางแผนการจัดหา เทคโนโลยี Cloud สำหรับระบบที่สำคัญ (P13)
- เริ่มสำรวจและติดตั้ง แพลตฟอร์มการเรียนรู้ รวมถึงสนับสนุนการใช้งานเพื่อเพิ่มการเข้าถึงและความหลากหลายของเนื้อหา (P8, P9)
- รายงานผลการดำเนินงานในระยะกลาง พร้อมวางแผนการปรับปรุงให้สอดคล้องกับเป้าหมายระยะยาว
- ส่งเสริมการพัฒนาทักษะของบุคลากรในระดับเชิงลึก เพื่อสร้างความยั่งยืนในด้านความมั่นคงปลอดภัย

ปีที่ 3 (2570): การยกระดับความยั่งยืนและการปฏิบัติการเต็มรูปแบบ

ในปีที่ 3 จะเน้นการขยายผลและการประเมินประสิทธิภาพของโครงการที่ดำเนินการในปีที่ผ่านมา พร้อมทั้งปรับปรุงและยกระดับระบบเพื่อความยั่งยืน โดยมีแผนดังนี้:

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ขยายขอบเขตการดำเนินงานของ SOC ให้ครอบคลุมภัยคุกคามในทุกมิติ พร้อมปรับปรุงการตอบสนองภัยคุกคามให้มีประสิทธิภาพมากขึ้น (P1)
- ตรวจสอบและทบทวนความพร้อมของ BCP และความเหมาะสมของเทคโนโลยี Cloud ที่นำมาใช้ (P12, P13)
- บริหารจัดการกระบวนการตามมาตรฐาน ISO/IEC 27001 อย่างเต็มรูปแบบ และตรวจสอบการปฏิบัติตามนโยบายในทุกหน่วยงาน (P14)
- ทดสอบและใช้งาน มาตรฐานการแลกเปลี่ยนข้อมูล ในระดับพันธมิตร พร้อมรายงานผลการดำเนินงาน (P10)
- จัดประชุมและเวิร์คช็อปการแบ่งปันข้อมูล เพื่อสนับสนุนความร่วมมือกับพันธมิตร (P11)
- ติดตามและประเมินผลการใช้งาน แพลตฟอร์มการเรียนรู้ เพื่อเพิ่มความพึงพอใจและการเข้าถึงของบุคลากร (P8, P9)
- สรุปผลการออกแบบและดำเนินงาน EA เพื่อใช้เป็นแนวทางการพัฒนาองค์กรในระยะยาว (P5)
- เพิ่มขีดความสามารถของบุคลากรในระดับผู้เชี่ยวชาญผ่านการประเมินและพัฒนาทักษะต่อเนื่อง (P7)
- ปรับปรุงระบบประชุมและเวิร์คช็อปการแบ่งปันข้อมูล ให้สอดคล้องกับสถานการณ์ปัจจุบัน (P11)
- เผยแพร่ความสำเร็จของโครงการต่อผู้เกี่ยวข้องและพันธมิตร เพื่อสร้างความมั่นใจและความต่อเนื่อง
- วางแผนการขยายโครงการและพัฒนาศักยภาพเพิ่มเติมในระยะ 3 ปีถัดไป

5.3 แนวทางการดำเนินงานและแผนพัฒนาสำหรับสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ในระยะถัดไป (ปี พ.ศ. 2571-2575 และ 2576-2580)

แผนที่นำทาง (Road Map) ในการนำแผนฯ ไปสู่การปฏิบัติอย่างเป็นรูปธรรมนอกเหนือจากการดำเนินการระยะ 3 ปีตามที่กล่าวมาข้างต้นแล้ว มีการกำหนดแนวทางของการดำเนินงานในระยะถัดไป เป็นการระบุให้หน่วยงานเห็นเป้าหมายในอนาคตพอสังเขป การนำเสนอทิศทางเกี่ยวกับเทคโนโลยีที่จะนำมาใช้ในอนาคตนั้น ได้มีการศึกษาจากผลการศึกษาจากแหล่งที่น่าเชื่อถือต่าง ๆ เช่น จากการศึกษาของ MIT Sloan[9] พบว่าการประมวลผลควอนตัม (Quantum Computing) ซึ่งเป็นนวัตกรรมที่คนส่วนใหญ่ยังไม่สามารถนิยามได้และยังไม่เข้าใจอย่างถ่องแท้ อาจกลายเป็นเทคโนโลยีที่ไม่คุ้นเคยซึ่งจะส่งผลกระทบครั้งใหญ่ต่อธุรกิจในอนาคต การประมวลผลควอนตัมใช้กฎของกลศาสตร์ควอนตัม (Quantum Mechanics) เพื่อจำลองและแก้ไขปัญหาที่ซับซ้อนซึ่งยากเกินกว่าคอมพิวเตอร์แบบดั้งเดิมจะสามารถจัดการได้

ในบางกรณี คอมพิวเตอร์ที่มีความสามารถควอนตัมสามารถแก้ปัญหาขนาดใหญ่ได้รวดเร็วกว่าคอมพิวเตอร์แบบดั้งเดิม ตัวอย่างเช่น การจำลองพฤติกรรมของสสาร การวิเคราะห์สารประกอบเพื่อพัฒนายาใหม่ การปรับปรุงประสิทธิภาพของการจัดการโรงงานหรือห่วงโซ่อุปทานทั่วโลก และการระบุรูปแบบการฉ้อโกงและความเสี่ยงในธุรกรรมทางการเงิน เป็นต้น

อย่างไรก็ตาม ปัจจุบันวงการคอมพิวเตอร์ควอนตัมยังไม่พร้อมใช้งานในระดับกว้าง McKinsey ประมาณการว่าจะมีคอมพิวเตอร์ควอนตัมจำนวน 5,000 เครื่องที่สามารถใช้งานได้ภายในปี ค.ศ.2 030 (พ.ศ.2575) แต่ฮาร์ดแวร์และซอฟต์แวร์ที่จำเป็นสำหรับการแก้ไขปัญหาที่ซับซ้อนที่สุดอาจยังไม่พร้อมใช้งานจนถึงปี 2035 (พ.ศ.2580) หรือหลังจากนั้น อย่างไรก็ตาม องค์กรต่าง ๆ จำเป็นต้องเริ่มคิดตั้งแต่ตอนนี้เกี่ยวกับ

[9] Quantum computing: What leaders need to know now, need to know now, Beth Stackpole Jan 11, 2024
https://mitsloan.mit.edu/ideas-made-to-matter/quantum-computing-what-leaders-need-to-know-now

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

จุดที่สามารถนำเทคโนโลยีนี้มาใช้ เพื่อแก้ไขปัญหาทางธุรกิจในโลกแห่งความเป็นจริง บริษัทบางแห่งคาดว่าจะลงทุนในเทคโนโลยีนี้มากกว่า 15 ล้านดอลลาร์ต่อปี ตามรายงานเมื่อเดือนพฤศจิกายน 2022

ดังนั้น แนวทางการดำเนินงานและแผนพัฒนาสำหรับสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) ในระยะถัดไป (ปี พ.ศ. 2571 - 2575 และ พ.ศ. 2576 - 2580) สามารถแสดงรายละเอียดได้ดังนี้

5.3.1 แผนปี พ.ศ. 2571 - 2575: "บูรณาการความมั่นคงปลอดภัยไซเบอร์และการบริหารจัดการที่ดิน" (Integrating Cybersecurity and Land Management)

1. วัตถุประสงค์

1.1 เสริมสร้างศักยภาพของระบบ **Blockchain** ในการจัดการข้อมูลสิทธิ์ที่ดิน และสนับสนุนความร่วมมือระหว่างหน่วยงานพันธมิตร

1.2 พัฒนาศูนย์เฝ้าระวังภัยคุกคามทางไซเบอร์ (SOC) ด้วยเทคโนโลยีปัญญาประดิษฐ์ (Artificial Intelligence: AI) และเทคโนโลยีขั้นสูง ให้สามารถตรวจจับภัยคุกคามที่เกี่ยวข้องกับ Blockchain ได้แบบเรียลไทม์

1.3 จัดทำมาตรฐานข้อมูลสำหรับการแลกเปลี่ยนระหว่างหน่วยงานบนระบบ **Blockchain**

2. โครงการสำคัญ

2.1 การขยายระบบ Private Blockchain เป็น Consortium Blockchain

- เพิ่มจำนวนโหนด (Nodes) และเชื่อมโยงหน่วยงานพันธมิตรเพื่อให้เกิดการบริหารจัดการข้อมูลที่โปร่งใสและตรวจสอบได้

2.2 การพัฒนา Smart Contracts สำหรับการจัดการข้อมูลสิทธิ์ที่ดิน

- รองรับกระบวนการตรวจสอบสิทธิ์ การโอนสิทธิ์ และการบันทึกประวัติการเปลี่ยนแปลง

2.3 การพัฒนา SOC ด้วย AI เพื่อปกป้องระบบ Blockchain

- เพิ่มศักยภาพการตรวจจับและตอบสนองต่อภัยคุกคามทางไซเบอร์

3. ตัวชี้วัดความสำเร็จ

- เวลาตอบสนองต่อเหตุการณ์ในระบบ **Blockchain**: ไม่เกิน 15 นาที
- ความถูกต้องและความโปร่งใสของข้อมูลใน **Blockchain**: ไม่น้อยกว่า 99%
- ระดับความพึงพอใจของหน่วยงานพันธมิตร: ไม่น้อยกว่า 95%

5.3.2 แผนปี พ.ศ. 2576 - 2580: "การบริหารจัดการที่ดินอย่างยั่งยืนด้วย Blockchain และนวัตกรรม" (Blockchain-Driven Land Management for Sustainability)

1. วัตถุประสงค์

1.1 ยกระดับการใช้งาน **Blockchain** ควบคู่กับ **AI** และ **Quantum Computing** เพื่อเพิ่มความปลอดภัยและประสิทธิภาพของระบบ

1.2 ส่งเสริมการใช้ **Digital Twin** ในการจัดการทรัพยากรที่ดิน

1.3 ขยายการเชื่อมโยงข้อมูลระดับสากลผ่านระบบ **Blockchain**

2. โครงการสำคัญ

2.1 การใช้งาน Blockchain ในการบริหารจัดการข้อมูลที่ดิน

- สร้างระบบตรวจสอบข้อมูลที่ดินที่มีความโปร่งใสและปลอดภัย

2.2 การพัฒนา Digital Twin เพื่อประเมินความเสี่ยงและการใช้ประโยชน์ทรัพยากรที่ดิน

- ใช้เทคโนโลยีจำลองเพื่อการคาดการณ์และวางแผนการใช้ที่ดินอย่างเหมาะสม

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

2.3 การพัฒนา Quantum Security สำหรับระบบ Blockchain

- รองรับการป้องกันภัยคุกคามทางไซเบอร์ขั้นสูงและเพิ่มความเชื่อมั่นในระดับสากล

3. ตัวชี้วัดความสำเร็จ

3.1 การเพิ่มประสิทธิภาพการจัดการข้อมูลที่ดิน: ไม่น้อยกว่า 90%

3.2 ลดระยะเวลาที่ใช้ในการตรวจสอบสิทธิ์การใช้ที่ดิน: ลดลง 50%

3.3 การเชื่อมโยงข้อมูลกับหน่วยงานนานาชาติ: ไม่น้อยกว่า 80%

5.3.3 แนวทางการพัฒนาทั้งสองช่วง (พ.ศ. 2571 - 2580)

1. เสริมสร้างการบูรณาการเทคโนโลยี **Blockchain** และระบบบริหารจัดการที่ดิน เพื่อรองรับการทำงานร่วมกันระหว่างหน่วยงาน
2. พัฒนานวัตกรรมทางเทคโนโลยีที่รองรับการจัดการข้อมูลที่ยั่งยืนและโปร่งใส
3. มุ่งเน้นการขับเคลื่อนองค์กรสู่การเป็นผู้นำด้านการบริหารจัดการที่ดินในระดับสากล

การดำเนินงานตามแผนดังกล่าวจะช่วยเพิ่มขีดความสามารถของ สคทช. ในการตอบสนองต่อความต้องการและความเปลี่ยนแปลงในอนาคตอย่างมีประสิทธิภาพ พร้อมทั้งสร้างความเชื่อมั่นให้แก่พันธมิตรและประชาชนผู้เกี่ยวข้องทุกภาคส่วน

อย่างไรก็ตาม Blockchain มีข้อกังวลเรื่องการเพิ่ม node เพราะเป็นการเพิ่มงบประมาณไปเรื่อย ๆ ในอนาคตอาจมีเทคโนโลยีเพิ่มเติมโดย node เท่าเดิมได้

แผนที่นำทาง (Road Map) พ.ศ. 2571-2575 และ 2576-2580 ที่ได้นำเสนอแนวทางนั้นจะต้องได้รับการทบทวนให้สอดคล้องกับทิศทางของเทคโนโลยีใหม่ ๆ ที่จะมีเข้ามาในอนาคต และเหมาะสมกับการลงทุน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

6. กลไกการดำเนินงาน

ในการดำเนินงานของแผนบริหารจัดการความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีโครงการสำคัญเพื่อเป็นกลไกในการดำเนินงานให้ สคทช. มีความมั่นคงปลอดภัยทางไซเบอร์และดำเนินการได้บรรลุตัวชี้วัดของแผนฯ

	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ						นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์				
โครงการสำคัญ	การระบุความเสี่ยง (Identify)	การป้องกันความเสี่ยง (Protect)	การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล	ยุทธศาสตร์ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	ยุทธศาสตร์ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	จำนวนความเกี่ยวข้อง
P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์	✓	✓	✓	✓		✓	✓	✓	✓	✓	9
P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน	✓	✓	✓			✓	✓	✓	✓	✓	8

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ						นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์				
โครงการสำคัญ	การระบุความเสี่ยง (Identify)	การป้องกันความเสี่ยง (Protect)	การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล	ยุทธศาสตร์ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	ยุทธศาสตร์ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	จำนวนความเกี่ยวข้อง
P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน	✔	✔	✔	✔		✔	✔	✔	✔	✔	9
P4: โครงการจัดซื้อระบบ EDM	✔	✔	✔	✔		✔	✔		✔	✔	8
P5: โครงการวิเคราะห์และออกแบบ EA	✔						✔		✔	✔	4
P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน		✔				✔	✔	✔			4
P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก		✔				✔	✔	✔			4
P8: โครงการจัดหาแพลตฟอร์มการเรียนรู้ออนไลน์		✔					✔				2

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ						นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์				
โครงการสำคัญ	การระบุความเสี่ยง (Identify)	การป้องกันความเสี่ยง (Protect)	การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล	ยุทธศาสตร์ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	ยุทธศาสตร์ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	จำนวนความเกี่ยวข้อง
P9: โครงกาสนับสนุนการใช้งาแพลตฟอร์มการเรียนรู้		✓					✓				2
P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล		✓						✓			2
P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล		✓						✓			2
P12: โครงการจัดทำและทดสอบ BCP	✓	✓		✓	✓	✓	✓	✓	✓	✓	9
P13: โครงการประเมินและจัดหาเทคโนโลยี Cloud							✓	✓	✓		3
P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการ	✓	✓	✓	✓	✓	✓	✓		✓	✓	9

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ						นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์				
โครงการสำคัญ	การระบุความเสี่ยง (Identify)	การป้องกันความเสี่ยง (Protect)	การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	การเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล	ยุทธศาสตร์ 1 สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ	ยุทธศาสตร์ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 3 สร้างบริการภาครัฐและโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ 4 สร้างศักยภาพของหน่วยงานระดับชาติให้มีคุณภาพและมาตรฐาน	จำนวนความเกี่ยวข้อง
การรักษาความมั่นคงปลอดภัยสารสนเทศ											

ตารางที่ 6-1 การจัดลำดับความสำคัญโดยพิจารณาจากความเกี่ยวข้องกับกฎหมายและแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	จำนวนความเกี่ยวข้อง	ลำดับโครงการที่ควรดำเนินการก่อนตามความเกี่ยวข้อง (ความสำคัญ)
P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์	9	1 (สูงมาก)
P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน	9	1 (สูงมาก)
P12: โครงการจัดทำและทดสอบ BCP	9	1 (สูงมาก)
P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ	9	1 (สูงมาก)
P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน	8	2 (สูง)
P4: โครงการจัดซื้อระบบ EDM	8	2 (สูง)
P5: โครงการวิเคราะห์และออกแบบ EA	4	3 (ปานกลาง)
P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน	4	3 (ปานกลาง)
P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก	4	3 (ปานกลาง)
P13: โครงการประเมินและจัดหาเทคโนโลยี Cloud	3	4 (ต่ำ)
P8: โครงการจัดหาแพลตฟอร์มการเรียนรู้ออนไลน์	2	5 (ต่ำมาก)
P9: โครงการสนับสนุนการใช้งานแพลตฟอร์มการเรียนรู้	2	5 (ต่ำมาก)
P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล	2	5 (ต่ำมาก)
P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล	2	5 (ต่ำมาก)

ตารางที่ 6-2 สรุปผลการจัดลำดับความสำคัญโดยพิจารณาจากความเกี่ยวข้องกับกฎหมายและแผนด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยิ่งไปกว่านั้น ในการพิจารณาดำเนินการสำหรับโครงการสำคัญต่าง ๆ มีเหตุผลประกอบการพิจารณาให้เห็นถึงลำดับความสำคัญและความเร่งด่วนตามตารางด้านล่าง

ยุทธศาสตร์	โครงการสำคัญ	ความสำคัญ	ความเร่งด่วน	ลำดับการดำเนินการตามความสำคัญและความเร่งด่วน	เหตุผลประกอบการพิจารณา
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **กลยุทธ์ที่ 1.1** : เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ	P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์	สูงมาก	สูง	1	เนื่องจากภัยคุกคามทางไซเบอร์มีจำนวนและความซับซ้อนเพิ่มขึ้นอย่างรวดเร็ว หากไม่มีระบบเฝ้าระวังและแจ้งเตือนแบบเรียลไทม์ องค์กรอาจเผชิญความเสียหายต่อข้อมูล ระบบ และชื่อเสียง รวมถึงความเสี่ยงด้านกฎหมายและข้อบังคับ เช่น PDPA และพรบ. ไซเบอร์ การใช้ MSSP ช่วยให้องค์กรได้รับการสนับสนุนจากผู้เชี่ยวชาญ ลดต้นทุน และเพิ่มประสิทธิภาพในการป้องกันภัยคุกคามแบบครบวงจร พร้อมทั้งเสริมสร้างความมั่นคงปลอดภัยเพื่อสนับสนุนเป้าหมายทางธุรกิจในระยะยาวอย่างมีประสิทธิภาพ
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **กลยุทธ์ที่ 1.2**: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน	สูง	สูง	2	โครงสร้างพื้นฐานเป็นหัวใจของการดำเนินงานในองค์กร การตรวจสอบช่วยระบุช่องโหว่ที่อาจถูกโจมตีและประเมินความเสี่ยงที่มีต่อระบบสำคัญ ลดโอกาสการหยุดชะงักของธุรกิจและความเสียหายที่อาจเกิดขึ้น นอกจากนี้ยังช่วยให้องค์กรปฏิบัติตามกฎหมายและมาตรฐานด้านความมั่นคงปลอดภัย เช่น พ.ร.บ. ไซเบอร์ และ ISO 27001 ได้อย่างมีประสิทธิภาพ
	P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน	สูง	ปานกลาง	3	ช่วยเพิ่มประสิทธิภาพและความสามารถในการป้องกันภัยคุกคามไซเบอร์ที่มีความซับซ้อนมากขึ้น รวมถึงลดความเสี่ยงต่อการโจมตีและการละเมิดข้อมูลซึ่งอาจส่งผลกระทบต่อการดำเนินงานและชื่อเสียงขององค์กร อย่างไรก็ตาม ความเร่งด่วนอยู่ในระดับปานกลางเนื่องจากอุปกรณ์และระบบเดิมยังสามารถใช้งานได้ในระยะสั้น แต่การอัพเกรดจำเป็นต่อการรองรับความต้องการในระยะยาวและสร้างความมั่นคงปลอดภัยที่ยั่งยืน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์	โครงการสำคัญ	ความสำคัญ	ความเร่งด่วน	ลำดับการดำเนินการตามความสำคัญและความเร่งด่วน	เหตุผลประกอบการพิจารณา
	P4: โครงการจัดซื้อระบบ EDM (Enterprise Device Management)	สูง	ปานกลาง	3	ช่วยเพิ่มประสิทธิภาพในการบริหารจัดการอุปกรณ์ภายในองค์กร ลดความเสี่ยงจากการใช้งานที่ไม่ได้มาตรฐาน เช่น การเข้าถึงข้อมูลสำคัญจากอุปกรณ์ที่ไม่ได้รับอนุญาต นอกจากนี้ยังช่วยให้สามารถติดตามและควบคุมอุปกรณ์ได้อย่างมีประสิทธิภาพ อย่างไรก็ตาม ความเร่งด่วนอยู่ในระดับปานกลาง เนื่องจากปัจจุบันสามารถใช้กระบวนการหรือเครื่องมือที่มีอยู่ชั่วคราวได้ แต่ควรวางแผนจัดซื้อเพื่อลดภาระในระยะยาว
	P5: โครงการวิเคราะห์และออกแบบ EA (Enterprise Architecture)	ปานกลาง	ปานกลาง	4	ช่วยให้องค์กรสามารถจัดโครงสร้างระบบเทคโนโลยีและกระบวนการทำงานได้อย่างมีประสิทธิภาพ สอดคล้องกับเป้าหมายทางธุรกิจ และลดความซ้ำซ้อนของทรัพยากร นอกจากนี้ยังช่วยในการวางแผนพัฒนาระบบในระยะยาว อย่างไรก็ตาม ความเร่งด่วนอยู่ในระดับปานกลาง เนื่องจากการออกแบบ EA เป็นกระบวนการเชิงกลยุทธ์ที่ต้องอาศัยเวลาและข้อมูลเชิงลึกในการวิเคราะห์เพื่อสร้างผลลัพธ์ที่ยั่งยืน และทาง สคทช. เองก็ได้มีการจัดทำ EA เดิมอยู่แล้ว
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **กลยุทธ์ที่ 1.3**: พัฒนาทักษะความมั่นคงปลอดภัย	P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน	ปานกลาง	ปานกลาง	4	การเสริมสร้างความรู้และความตระหนักให้กับพนักงานในการป้องกันความเสี่ยงไซเบอร์ที่เกิดจากพฤติกรรมมนุษย์ เช่น การหลอกลวงทางอีเมลหรือการใช้งานรหัสผ่านที่ไม่ปลอดภัย การฝึกอบรมช่วยลดโอกาสการเกิดเหตุที่อาจกระทบต่อองค์กร แต่ความเร่งด่วนอยู่ในระดับปานกลาง เนื่องจากสามารถจัดทำได้ควบคู่กับมาตรการป้องกันอื่น ๆ โดยไม่กระทบต่อการดำเนินงานในระยะสั้นมากนัก
	P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก	ปานกลาง	ปานกลาง	4	ช่วยเสริมสร้างความเชี่ยวชาญให้กับบุคลากรในองค์กรในการรับมือกับภัยคุกคามที่ซับซ้อนและเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว การได้รับคำแนะนำจากผู้เชี่ยวชาญช่วยเพิ่มขีดความสามารถและความมั่นใจของทีม อย่างไรก็ตาม ความเร่งด่วนอยู่ในระดับปานกลาง

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์	โครงการสำคัญ	ความสำคัญ	ความเร่งด่วน	ลำดับการดำเนินการตามความสำคัญและความเร่งด่วน	เหตุผลประกอบการพิจารณา
					เพราะสามารถวางแผนฝึกอบรมเป็นระยะได้โดยไม่กระทบต่อการดำเนินงานในระยะสั้น แต่ควรเริ่มต้นเพื่อเตรียมความพร้อมในอนาคต
	P8: โครงการจัดหาแพลตฟอร์มการเรียนรู้ออนไลน์	ต่ำมาก	ต่ำ	6	เนื่องจากปัจจุบันมีช่องทางการเรียนรู้หลากหลายที่สามารถใช้งานได้อยู่แล้ว โดยไม่ส่งผลกระทบสำคัญต่อการพัฒนาบุคลากรในระยะสั้น ความเร่งด่วนอยู่ในระดับต่ำ เพราะการดำเนินการดังกล่าวสามารถเลื่อนออกไปได้โดยไม่กระทบต่อเป้าหมายหลักขององค์กร และสามารถวางแผนให้สอดคล้องกับทรัพยากรที่มีในอนาคต
	P9: โครงการสนับสนุนการใช้งานแพลตฟอร์มการเรียนรู้	ต่ำมาก	ต่ำ	6	เนื่องจากการพัฒนาทักษะและความรู้ของบุคลากรสามารถดำเนินการผ่านช่องทางอื่นที่มีอยู่แล้ว โดยไม่ส่งผลกระทบต่อการดำเนินงานหลักขององค์กรในระยะสั้น ความเร่งด่วนอยู่ในระดับต่ำ เพราะการสนับสนุนเพิ่มเติมสามารถดำเนินการได้ในช่วงเวลาที่เหมาะสม และไม่มีความจำเป็นเร่งด่วนที่จะต้องเร่งรัดการใช้งานในทันที
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) **กลยุทธ์ที่ 2.1**: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร	P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล	ต่ำมาก	ต่ำ	6	เนื่องจากช่วยเพิ่มความชัดเจนและประสิทธิภาพในการแบ่งปันข้อมูลเฉพาะกลุ่ม เพื่อตอบสนองต่อภัยคุกคามได้อย่างเหมาะสมและรวดเร็ว แม้จะมี สกมช. กำกับดูแลในภาพรวมอยู่แล้ว แต่การมีมาตรฐานเฉพาะกลุ่มจะช่วยให้การสื่อสารและการดำเนินงานภายในกลุ่มเกิดประโยชน์สูงสุด ความเร่งด่วนอยู่ในระดับต่ำ เพราะยังสามารถใช้แนวทางที่มีอยู่เดิมได้ในระยะสั้น และต้องใช้เวลาสำหรับการพัฒนารายละเอียดให้ครอบคลุม
	P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล	ต่ำมาก	ต่ำ	6	เนื่องจากปัจจุบันมีหน่วยงานหลัก เช่น NCSA ที่ดำเนินการในด้านนี้อยู่แล้ว และสามารถใช้ข้อมูลหรือแนวทางที่จัดทำไว้รองรับความต้องการได้ ความเร่งด่วนอยู่ในระดับต่ำ เพราะต้องรอให้โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูลเสร็จสมบูรณ์ก่อน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์	โครงการสำคัญ	ความสำคัญ	ความเร่งด่วน	ลำดับการดำเนินการตามความสำคัญและความเร่งด่วน	เหตุผลประกอบการพิจารณา
					เพื่อให้การประชุมและเวิร์คช็อปมีประสิทธิภาพและสอดคล้องกับมาตรฐานที่กำหนด
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership) **กลยุทธ์ที่ 2.2**: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน	P12: โครงการจัดทำและทดสอบ BCP	สูงมาก	สูง	1	ช่วยให้องค์กรสามารถดำเนินงานต่อเนื่องในกรณีเกิดเหตุไม่คาดฝัน เช่น ภัยพิบัติ การโจมตีทางไซเบอร์ หรือระบบล่ม ลดผลกระทบทางธุรกิจและความเสียหายที่อาจเกิดขึ้น นอกจากนี้ยังเป็นการปฏิบัติตามข้อกำหนดด้านกฎหมายและสร้างความเชื่อมั่นให้กับผู้ใช้บริการและพันธมิตร
	P13: โครงการประเมินและจัดหาเทคโนโลยี Cloud	ต่ำ	ต่ำ	5	ความสำคัญระดับปานกลาง เนื่องจากช่วยให้องค์กรสามารถเตรียมพร้อมสำหรับการใช้งานเทคโนโลยีที่ยืดหยุ่น รองรับการขยายตัวของธุรกิจ และเพิ่มประสิทธิภาพในการจัดเก็บและประมวลผลข้อมูล อย่างไรก็ตาม ความเร่งด่วนอยู่ในระดับต่ำ เนื่องจากองค์กรยังสามารถใช้งานโครงสร้างพื้นฐานเดิมในระยะสั้นได้ และการเลือกเทคโนโลยี Cloud ต้องใช้เวลาในการประเมินความเหมาะสมและวางแผนเพื่อการเปลี่ยนผ่านที่มีประสิทธิภาพ
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard) **กลยุทธ์ที่ 3.1**: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ	สูงมาก	ปานกลาง	3	ช่วยให้องค์กรมีระบบจัดการความมั่นคงปลอดภัยสารสนเทศที่เป็นมาตรฐานสากล ป้องกันการละเมิดข้อมูล ลดความเสี่ยงทางไซเบอร์ และสร้างความเชื่อมั่นให้กับผู้ใช้บริการและพันธมิตร ความเร่งด่วนอยู่ในระดับปานกลาง เนื่องจากการดำเนินการต้องใช้เวลาในการออกแบบและพัฒนาระบบ แต่เป็นสิ่งจำเป็นเพื่อรองรับข้อกำหนดด้านกฎหมายและความท้าทายทางธุรกิจในระยะยาว

ตารางที่ 6-3 เหตุผลประกอบการพิจารณาระดับความสำคัญของโครงการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	ความสำคัญ	ความเร่งด่วน	ลำดับการดำเนินการตามความสำคัญและความเร่งด่วน
P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์	สูงมาก	สูง	1
P12: โครงการจัดทำและทดสอบ BCP	สูงมาก	สูง	1
P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน	สูง	สูง	2
P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน	สูง	ปานกลาง	3
P4: โครงการจัดซื้อระบบ EDM (Enterprise Device Management)	สูง	ปานกลาง	3
P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ	สูงมาก	ปานกลาง	3
P5: โครงการวิเคราะห์และออกแบบ EA (Enterprise Architecture)	ปานกลาง	ปานกลาง	4
P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน	ปานกลาง	ปานกลาง	4
P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก	ปานกลาง	ปานกลาง	4
P13: โครงการประเมินและจัดหาเทคโนโลยี Cloud	ต่ำ	ต่ำ	5
P8: โครงการจัดหาแพลตฟอร์มการเรียนรู้ออนไลน์	ต่ำมาก	ต่ำ	6
P9: โครงการสนับสนุนการใช้งานแพลตฟอร์มการเรียนรู้	ต่ำมาก	ต่ำ	6
P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล	ต่ำมาก	ต่ำ	6
P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล	ต่ำมาก	ต่ำ	6

ตารางที่ 6-4 สรุปผลการเรียงลำดับความสำคัญและความเร่งด่วนของโครงการ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แม้ว่า **P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน** และ **P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก** จะถูกจัดลำดับการดำเนินการตามความสำคัญและความเร่งด่วนในระดับที่ค่อนข้างต่ำ แต่ยังคงเป็นโครงการที่ควรได้รับการพิจารณาให้ดำเนินการอย่างต่อเนื่อง โดยมีเหตุผลสำคัญดังนี้:

1. **งบประมาณที่ใช้ต่ำ:** โครงการเหล่านี้ไม่ต้องการการลงทุนที่สูง แต่สามารถสร้างผลกระทบที่ดีต่อองค์กรในระยะยาว
2. **การพัฒนาบุคลากร:** การฝึกอบรมเหล่านี้ช่วยส่งเสริมให้บุคลากรมีความตระหนักรู้ในด้านความมั่นคงปลอดภัยที่ดี และเพิ่มพูนความสามารถในการปฏิบัติตามกฎหมายและแนวปฏิบัติที่ดี
3. **การปฏิบัติตามกฎหมาย:** โครงการนี้มีส่วนช่วยให้องค์กรสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยตามกฎหมายและระเบียบต่าง ๆ เช่น พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคลหรือพระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์
4. **ส่งเสริมวัฒนธรรมองค์กร:** การจัดอบรมอย่างสม่ำเสมอช่วยสร้างวัฒนธรรมความมั่นคงปลอดภัยในองค์กร ซึ่งส่งผลให้ทุกคนมีส่วนร่วมในการป้องกันความเสี่ยง
5. **เตรียมความพร้อมระยะยาว:** โครงการฝึกอบรมเหล่านี้เป็นการวางรากฐานที่มั่นคงให้กับองค์กรในการพัฒนาทักษะและความรู้ของบุคลากร เพื่อรับมือกับความท้าทายในอนาคต

ดังนั้น การดำเนินโครงการ P6 และ P7 อย่างต่อเนื่องแม้ในระดับที่ไม่เร่งด่วน จะช่วยเสริมสร้างความแข็งแกร่งให้กับองค์กรทั้งในด้านบุคลากรและการปฏิบัติงานโดยรวมในระยะยาว

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

จากโครงการสำคัญที่กล่าวมาข้างต้น โครงการต่าง ๆ มีรายละเอียดความสอดคล้องของโครงการตามยุทธศาสตร์ กลยุทธ์ และความสอดคล้องกับตัวชี้วัดต่าง ๆ ตามตารางด้านล่าง ดังนี้

ยุทธศาสตร์	กลยุทธ์	โครงการสำคัญ	ตัวชี้วัดที่สอดคล้อง
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	**กลยุทธ์ที่ 1.1** : เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ	P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์	➢ เวลาตอบสนองต่อภัยคุกคามที่ตรวจพบ: < 1 ชั่วโมง ➢ อัตราการตรวจจับเหตุการณ์ที่เป็นอันตราย: > 95% ➢ ความพึงพอใจของผู้ใช้ MSSP: > 90%
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	**กลยุทธ์ที่ 1.2**: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน P4: โครงการจัดซื้อระบบ EDM (Enterprise Device Management) P5: โครงการวิเคราะห์และออกแบบ EA (Enterprise Architecture)	➢ อุปกรณ์สำคัญในการรักษาความมั่นคงปลอดภัยต้องได้รับการบำรุงรักษาอย่างต่อเนื่อง: 100% ➢ การปฏิบัติตามนโยบายอุปกรณ์: > 98% ➢ การลดปัญหาด้านการใช้งานอุปกรณ์: > 30% ลดลงในปีแรก ➢ การอัปเดต EA ตามเป้าหมายองค์กร: ทุก 6 เดือน ➢ ความพึงพอใจจากการใช้ EA: > 90%
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	**กลยุทธ์ที่ 1.3**: พัฒนาทักษะความมั่นคงปลอดภัย	P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก	➢ อัตราการเข้าร่วมฝึกอบรมความมั่นคงปลอดภัยเบื้องต้น: > 95% ➢ การเพิ่มระดับความตระหนักรู้ด้านความมั่นคงปลอดภัย: ประเมินจากแบบสอบถาม > 80% ➢ จำนวนพนักงานที่ได้รับการพัฒนาเป็นผู้เชี่ยวชาญด้านความมั่นคงปลอดภัย: เพิ่มขึ้น 30% ภายในสองปี
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้	**กลยุทธ์ที่ 1.4**: บูรณาการหลักสูตรการเรียนรู้ผ่าน Platform ออนไลน์	P8: โครงการจัดหา Platform การเรียนรู้ออนไลน์ P9: โครงการสนับสนุนการใช้งาน Platform การเรียนรู้	➢ อัตราการเข้าใช้งาน Platform การเรียนรู้ออนไลน์: > 75% ของบุคลากร ➢ ความหลากหลายของเนื้อหาบน Platform: เพิ่มขึ้นทุกปี > 20% ➢ ความพึงพอใจจากการใช้ Platform: > 90%

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

ยุทธศาสตร์	กลยุทธ์	โครงการสำคัญ	ตัวชี้วัดที่สอดคล้อง
และเทคโนโลยี) (Integrating cybersecurity capabilities)			
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	**กลยุทธ์ที่ 2.1**: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร	P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล	➢ มาตรฐานการแลกเปลี่ยนข้อมูลที่หน่วยงานพันธมิตรใช้งานร่วมกัน: 1 รูปแบบมาตรฐาน
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	**กลยุทธ์ที่ 2.2**: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน	P12: โครงการจัดทำและทดสอบ BCP P13: โครงการประเมินและจัดหาเทคโนโลยี Cloud	➢ การจัดทำ BCP สำหรับทุกระบบสำคัญ 50% ภายในปีแรก ➢ ความพร้อมของระบบระหว่างเหตุการณ์ฉุกเฉิน: > 95% ➢ อัตราการใช้ Cloud สำหรับระบบที่ต้องการปรับตัวสูง: > 50% ในปีแรก
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	**กลยุทธ์ที่ 3.1**: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 ระบบจัดการการรักษาความมั่นคงปลอดภัยสารสนเทศ	➢ เหตุการณ์ด้านความมั่นคงปลอดภัยที่ตรวจพบจะต้องได้รับการตอบสนองภายในระยะเวลาเป้าหมาย (เช่น ภายใน 24 ชั่วโมง) 100% ➢ ระดับความรู้เกี่ยวกับมาตรฐานสากลภายในองค์กร: > 90% ของบุคลากรที่เกี่ยวข้อง ➢ ระยะเวลาเฉลี่ยในการกู้คืนระบบหลังเกิดเหตุการณ์ฉุกเฉิน (Mean Time to Recovery - MTTR) ลดระยะเวลาในการกู้คืนระบบให้อยู่ภายในระยะเวลาเป้าหมายที่กำหนด เช่น ไม่เกิน 2 ชั่วโมงสำหรับระบบที่สำคัญ

ตารางที่ 6-5 รายละเอียดความสอดคล้องของโครงการตามยุทธศาสตร์ กลยุทธ์ และความสอดคล้องกับตัวชี้วัดต่าง ๆ

นอกจากรายละเอียดความสอดคล้องของโครงการตามยุทธศาสตร์ที่กล่าวมาตามตารางข้างต้น ที่ปรึกษามีการจัดทำรายละเอียดของโครงการรายยุทธศา สตร์ ซึ่งประกอบด้วยชื่อโครงการสำคัญ กลไกและวิธีการปฏิบัติ กรอบระยะเวลา และผู้รับผิดชอบ ดังนี้

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

6.1 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
P1: โครงการจัดตั้งศูนย์เฝ้าระวังภัยคุกคาม (SOC) ผ่าน MSSP เพื่อการตรวจจับและแจ้งเตือนภัยคุกคามแบบเรียลไทม์ **กลยุทธ์ที่ 1.1** : เพิ่มประสิทธิภาพในการเฝ้าระวังระบบที่สำคัญ	**วางแผนและจัดทำข้อกำหนด (Requirement Analysis)** ➢ จัดซื้อและติดตั้งอุปกรณ์ที่จำเป็น เช่น ระบบ SIEM, ระบบการตรวจจับและตอบสนองภัยคุกคาม (EDR) ➢ พัฒนาและทดสอบระบบ (System Development and Testing) ดำเนินการตั้งค่าระบบเฝ้าระวังภัยคุกคามและทดสอบระบบเพื่อให้แน่ใจว่าการตรวจจับและแจ้งเตือนสามารถทำงานได้อย่างแม่นยำ ➢ ฝึกอบรมบุคลากรในการใช้ SOC อบรมให้บุคลากรเข้าใจวิธีการทำงานของ SOC และเครื่องมือต่าง ๆ ที่จะใช้ในการเฝ้าระวัง **เริ่มใช้งาน SOC และเก็บข้อมูล** ➢ เริ่มต้นการเฝ้าระวังแบบเรียลไทม์ในระบบที่สำคัญ รวมถึงการเก็บรวบรวมข้อมูลภัยคุกคามเพื่อใช้วิเคราะห์และวางแผนในอนาคต **ปรับปรุงการตั้งค่าและเพิ่มประสิทธิภาพของ SOC** ➢ ตรวจสอบและปรับแต่งระบบเพื่อลดความผิดพลาดและเพิ่มประสิทธิภาพในการตรวจจับภัยคุกคาม **สร้างรายงานประจำและวิเคราะห์ผลการเฝ้าระวัง** ➢ สร้างรายงานสรุปผลการเฝ้าระวังและวิเคราะห์ข้อมูลที่ได้จาก SOC เพื่อใช้ในการวางแผนเชิงรุก **การฝึกซ้อมจำลองเหตุการณ์ภัยคุกคาม** ➢ จัดการฝึกซ้อมเพื่อจำลองเหตุการณ์ภัยคุกคามจริง เพื่อเตรียมความพร้อมและประเมินความสามารถของทีมในการตอบสนอง	พ.ศ. 2568 – 2570 (ระยะเวลา 2 ปี 6 เดือน)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
P2: โครงการตรวจสอบและประเมินความมั่นคงปลอดภัยโครงสร้างพื้นฐาน **กลยุทธ์ที่ 1.2**: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	**1. การวิเคราะห์และวางแผนการประเมิน (Assessment Planning)** ➢ กำหนดขอบเขตและเป้าหมายการตรวจสอบ วิเคราะห์ความเสี่ยง และกำหนดเกณฑ์การประเมินสำหรับความมั่นคงปลอดภัยของโครงสร้างพื้นฐาน **2. การตรวจสอบและประเมินความมั่นคงปลอดภัย (Security Assessment & Evaluation)** ➢ ตรวจสอบโครงสร้างพื้นฐานโดยใช้เครื่องมือและเทคนิค เช่น การทดสอบเจาะระบบ (Penetration Testing) การตรวจสอบช่องโหว่ (Vulnerability Assessment) และการทบทวนการตั้งค่าระบบ **3. การปรับปรุงและแก้ไขข้อบกพร่อง (Remediation & Improvement)** ➢ ดำเนินการแก้ไขช่องโหว่และข้อบกพร่องที่ตรวจพบ ปรับปรุงการตั้งค่าความปลอดภัย และติดตามการดำเนินการแก้ไข **4. การทดสอบและประเมินผลการปรับปรุง (Post-Remediation Testing & Evaluation)** ➢ ทดสอบระบบอีกครั้งหลังการแก้ไขเพื่อยืนยันว่าช่องโหว่ได้รับการปิด และประเมินผลการปรับปรุงว่าตรงตามมาตรฐานความมั่นคงปลอดภัยที่กำหนด	พ.ศ. 2569 – 2570 (ระยะเวลา 2 ปี)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน
P3: โครงการอัพเกรดอุปกรณ์และระบบป้องกัน **กลยุทธ์ที่ 1.2**: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	**1. การวิเคราะห์ความต้องการและการประเมินความเสี่ยง** ➢ สำรวจและวิเคราะห์อุปกรณ์และระบบป้องกันที่มีอยู่ เพื่อประเมินความเสี่ยง ช่องโหว่ และความต้องการที่ต้องการอัพเกรด ➢ จัดทำรายงานความเหมาะสม (Feasibility Study) เพื่อเลือกเทคโนโลยีและอุปกรณ์ที่ตอบสนองต่อความเสี่ยงและความต้องการทางธุรกิจ **2. การจัดซื้อและติดตั้งอุปกรณ์ตามมาตรฐาน** ➢ จัดซื้ออุปกรณ์และระบบที่ผ่านการรับรองมาตรฐาน เช่น ISO/IEC 27001 หรือมาตรฐานความปลอดภัยที่เกี่ยวข้อง ➢ ติดตั้งและตั้งค่าระบบให้เหมาะสม โดยอิงตาม Best Practices เพื่อให้สามารถป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ **3. การทดสอบและติดตามผลการดำเนินงาน**	พ.ศ. 2570 (ระยะเวลา 1 ปี)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ ทดสอบระบบหลังการติดตั้ง เช่น การจำลองการโจมตี (Penetration Testing) หรือการประเมินช่องโหว่ (Vulnerability Assessment) ➢ ตั้งระบบ Monitoring เพื่อตรวจสอบประสิทธิภาพการทำงานของอุปกรณ์และระบบอย่างต่อเนื่อง พร้อมปรับปรุงตามความเหมาะสม		
P4: โครงการจัดซื้อระบบ EDM (Enterprise Device Management) **กลยุทธ์ที่ 1.2**: ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	**1. การวิเคราะห์ความต้องการและการวางแผน (Needs Analysis & Planning)** ➢ วิเคราะห์ความต้องการด้านการจัดการอุปกรณ์ Endpoint ทั้ง Client และ Mobile Device ขององค์กร เช่น ความต้องการด้านความมั่นคงปลอดภัย การควบคุมการเข้าถึง การอัปเดตซอฟต์แวร์ และการป้องกันข้อมูล ➢ กำหนดคุณสมบัติและความสามารถที่ระบบ EDM ต้องมี เช่น การจัดการการเข้าถึงระยะไกล การลบข้อมูลจากระยะไกล การติดตั้งและอัปเดตซอฟต์แวร์อัตโนมัติ การควบคุมการเข้าถึงไฟล์หรือแอปพลิเคชัน เป็นต้น ▪ จัดทำเอกสารข้อกำหนดทางเทคนิค (Technical Specifications) และเกณฑ์การประเมินผู้ให้บริการ (Vendor Selection Criteria) เพื่อใช้ในการคัดเลือกและประเมินผู้ขาย **2. การคัดเลือกผู้ให้บริการระบบ EDM (Vendor Selection)** ➢ ประกาศเชิญชวนผู้ให้บริการส่งข้อเสนอ (RFP) โดยแนบข้อกำหนดทางเทคนิคและเงื่อนไขที่จำเป็นสำหรับระบบ EDM ➢ ประเมินข้อเสนอจากผู้ให้บริการตามเกณฑ์การประเมินที่กำหนด ซึ่งอาจรวมถึงการประเมินด้านเทคนิค ความน่าเชื่อถือ ประสบการณ์ และต้นทุน ➢ เลือกผู้ให้บริการที่สามารถตอบสนองความต้องการได้ดีที่สุดและทำสัญญาจัดซื้อระบบ EDM **3. การติดตั้งและการตั้งค่าระบบ (System Implementation & Configuration)** ➢ ติดตั้งและตั้งค่าระบบ EDM บนอุปกรณ์ที่ต้องการจัดการ เช่น คอมพิวเตอร์ตั้งโต๊ะ แล็ปท็อป และอุปกรณ์มือถือของบุคลากร	พ.ศ. 2569 – 2570 (ระยะเวลา 2 ปี)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ กำหนดการตั้งค่าการเข้าถึง การจัดการซอฟต์แวร์ และมาตรการความมั่นคงปลอดภัยที่สอดคล้องกับนโยบายขององค์กร เช่น การควบคุมการใช้งานอุปกรณ์ USB การตั้งค่าการเข้ารหัสข้อมูล และการตั้งค่าโปรไฟล์สำหรับอุปกรณ์มือถือ ➢ ทดสอบระบบ EDM เพื่อให้แน่ใจว่าทำงานได้อย่างมีประสิทธิภาพและสอดคล้องกับข้อกำหนด **4. การฝึกอบรมและการสร้างความตระหนัก (Training & Awareness)** ➢ จัดการฝึกอบรมให้แก่บุคลากรและผู้ดูแลระบบเกี่ยวกับการใช้งานระบบ EDM และการปฏิบัติตามนโยบายการใช้อุปกรณ์ขององค์กร ➢ สร้างความตระหนักเกี่ยวกับการรักษาความมั่นคงปลอดภัยของข้อมูลในอุปกรณ์ปลายทาง และวิธีการปฏิบัติตนให้ปลอดภัยขณะใช้งาน Client และ Mobile Device **5. การติดตามผลและการบำรุงรักษา (Monitoring & Maintenance)** ➢ ติดตามการทำงานของระบบ EDM เพื่อตรวจสอบการใช้งานและรักษาความปลอดภัยของอุปกรณ์ รวมถึงการตรวจสอบเหตุการณ์ที่อาจเป็นภัยคุกคาม ➢ บำรุงรักษาระบบและปรับปรุงการตั้งค่าตามความจำเป็น เช่น การอัปเดตระบบให้ทันสมัย การปรับตั้งค่าความปลอดภัยใหม่เมื่อมีภัยคุกคามใหม่ หรือการขยายขีดความสามารถของระบบ		
P5: โครงการวิเคราะห์และออกแบบ EA (Enterprise Architecture) **กลยุทธ์ที่ 1.2** : ปรับปรุงโครงสร้างพื้นฐานให้มีความมั่นคงปลอดภัย	**การวิเคราะห์และวางแผนโครงสร้าง EA** 1. **วิเคราะห์สถานะปัจจุบัน (As-Is Analysis):** ศึกษาและวิเคราะห์โครงสร้างเทคโนโลยีและความมั่นคงปลอดภัยที่มีอยู่ในปัจจุบัน รวมถึงกำหนดขอบเขตและความต้องการของระบบในอนาคต 2. **การกำหนดแนวทางการพัฒนา (To-Be Vision):** สร้างวิสัยทัศน์และแนวทางการพัฒนา EA ที่สอดคล้องกับเป้าหมายทางธุรกิจและความต้องการด้านความมั่นคงปลอดภัย 3. **การกำหนดมาตรฐานและหลักเกณฑ์:** จัดทำมาตรฐานการออกแบบ EA และกำหนดหลักเกณฑ์การรักษาความมั่นคงปลอดภัยของข้อมูลและระบบ รวมถึงเกณฑ์การพัฒนาที่ต้องการในแต่ละขั้นตอน **การออกแบบ EA และการทดสอบโครงสร้างเบื้องต้น**	พ.ศ. 2569 (ระยะเวลา 1 ปี)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	1. **การออกแบบโครงสร้าง EA แบบองค์รวม:** สร้างแผนผัง EA ที่ครอบคลุมทุกมิติของเทคโนโลยี เช่น โครงสร้างระบบสารสนเทศ การจัดการข้อมูล โครงสร้างระบบเครือข่าย และการรักษาความมั่นคงปลอดภัยในทุกระดับ 2. **ทดสอบโครงสร้างในกลุ่มระบบย่อย:** เลือกกลุ่มระบบย่อยเพื่อทำการทดสอบโครงสร้าง EA ที่ออกแบบมาเพื่อตรวจสอบประสิทธิภาพและความสามารถในการรองรับความมั่นคงปลอดภัย 3. **ปรับปรุงและพัฒนาตามผลการทดสอบ:** ปรับปรุงโครงสร้าง EA ตามผลการทดสอบ พร้อมทำการประเมินความเสี่ยงและความมั่นคงปลอดภัย **การใช้งานและปรับปรุง EA อย่างเต็มรูปแบบ** 1. **การนำ EA ไปใช้จริง (Implementation):** เปิดใช้งาน EA ที่ออกแบบมาในทุกหน่วยงานที่เกี่ยวข้อง และให้การสนับสนุนในการใช้งานระบบตามแนวทางที่วางไว้ 2. **การติดตามผลและประเมินผลการใช้งาน:** ติดตามการใช้งาน EA ในทุกหน่วยงาน รวมถึงการรวบรวมความคิดเห็นจากผู้ใช้เพื่อประเมินประสิทธิภาพและความสามารถในการรองรับความมั่นคงปลอดภัย **การปรับปรุง EA อย่างต่อเนื่อง:** ปรับปรุงโครงสร้าง EA ตามผลการประเมินและความคิดเห็นของผู้ใช้ รวมถึงพัฒนาแผนการบำรุงรักษาระบบและความมั่นคงปลอดภัยในระยะยาว		
P6: โครงการจัดทำและดำเนินการฝึกอบรมความมั่นคงปลอดภัยพื้นฐาน **กลยุทธ์ที่ 1.3**: พัฒนาทักษะความมั่นคงปลอดภัย	**การวางแผนและพัฒนาหลักสูตร** 1. **การวิเคราะห์ความต้องการการฝึกอบรม:** วิเคราะห์ทักษะที่จำเป็นและข้อกำหนดทางด้านความมั่นคงปลอดภัยที่ต้องการในองค์กร รวมถึงการทำความเข้าใจแนวโน้มภัยคุกคามไซเบอร์ล่าสุด 2. **พัฒนาหลักสูตรฝึกอบรม:** สร้างหลักสูตรความมั่นคงปลอดภัยพื้นฐานที่ครอบคลุมทักษะและความรู้ที่เกี่ยวข้อง เช่น ความรู้พื้นฐานด้านความปลอดภัยไซเบอร์ การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต และการรักษาความลับข้อมูล 3. **การทดสอบหลักสูตร:** ดำเนินการทดลองฝึกอบรมกับกลุ่มบุคลากรเป้าหมายกลุ่มเล็กเพื่อทดสอบประสิทธิภาพและปรับปรุงตามผลการทดสอบ **การดำเนินการฝึกอบรมเต็มรูปแบบและการติดตามผล**	พ.ศ. 2568 – 2570 (ระยะเวลา 2 ปี 6 เดือน)	➢ กลุ่มงานบริหารทรัพยากรบุคคล ➢ สำนักงานผู้อำนวยการ ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	1. **การอบรมบุคลากร:** ขยายการฝึกอบรมให้ครอบคลุมบุคลากรทุกระดับที่เกี่ยวข้อง โดยจัดอบรมทั้งแบบออนไลน์และออนไซต์ 2. **การวัดผลหลังการอบรม:** จัดทำข้อสอบหรือแบบประเมินเพื่อวัดผลการเรียนรู้และความเข้าใจของผู้เข้าร่วมอบรม 3. **ติดตามผลและการให้คำปรึกษา:** ติดตามผลการเรียนรู้ของบุคลากรหลังการอบรมและจัดให้มีคำแนะนำเพิ่มเติมในกรณีที่พบว่ามีความต้องการในการพัฒนาทักษะเพิ่มเติม **การประเมินผลและการพัฒนาอย่างต่อเนื่อง** 1. **การประเมินผลและสรุปบทเรียน:** ประเมินผลการฝึกอบรมในปีที่ผ่านมา รวบรวมข้อมูลและข้อเสนอแนะจากผู้เข้าร่วมอบรมเพื่อสรุปบทเรียน 2. **การพัฒนาหลักสูตรเพิ่มเติม:** ปรับปรุงและพัฒนาหลักสูตรเพิ่มเติมตามผลการประเมิน รวมถึงการเพิ่มเนื้อหาที่เกี่ยวข้องกับภัยคุกคามและเทคโนโลยีใหม่ ๆ 3. **การวางแผนการฝึกอบรมระยะยาว:** สร้างแผนฝึกอบรมระยะยาวเพื่อรองรับการพัฒนาทักษะอย่างยั่งยืนและตอบสนองต่อการเปลี่ยนแปลงของภัยคุกคามไซเบอร์ในอนาคต		
P7: โครงการฝึกอบรมร่วมกับผู้เชี่ยวชาญภายนอก **กลยุทธ์ที่ 1.3**: พัฒนาทักษะความมั่นคงปลอดภัย	**1. การวิเคราะห์ความต้องการและวางแผนหลักสูตร (Needs Analysis & Curriculum Planning)** ➢ วิเคราะห์ความต้องการด้านทักษะความมั่นคงปลอดภัยขององค์กร เช่น การวิเคราะห์ภัยคุกคาม การจัดการความเสี่ยง การตรวจจับการละเมิดข้อมูล การตอบสนองต่อเหตุการณ์ด้านความปลอดภัย ฯลฯ ➢ จัดทำ Training Roadmap สำหรับบุคลากรต่าง ๆ **2. การจัดฝึกอบรมและการประเมินผล (Training Sessions & Evaluation)** ➢ ดำเนินการฝึกอบรมในรูปแบบเชิงลึก โดยอาจใช้การฝึกอบรมแบบในห้องเรียน การฝึกอบรมออนไลน์ หรือการฝึกปฏิบัติในสถานการณ์จำลองเพื่อให้ผู้เรียนได้ทดลองใช้ทักษะที่เรียนรู้ในสถานการณ์ที่เสมือนจริง	พ.ศ. 2569 – 2570 (ระยะเวลา 2 ปี)	➢ กลุ่มงานบริหารทรัพยากรบุคคล ➢ สำนักงานผู้อำนวยการ ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ จัดให้มีการอภิปรายกลุ่ม การถามตอบ และกิจกรรมที่สนับสนุนการมีส่วนร่วมของผู้เรียน เพื่อให้เกิดการแลกเปลี่ยนความคิดเห็นและเสริมสร้างความเข้าใจในเนื้อหา ➢ ประเมินผลการเรียนรู้ของผู้เข้าอบรมด้วยการสอบวัดผล การประเมินความสามารถในการปฏิบัติงานจริง และการให้คะแนนการทำงานในสถานการณ์จำลอง **3. การติดตามผลและการพัฒนาต่อเนื่อง (Follow-up & Continuous Development)** ➢ ติดตามผลการนำทักษะไปใช้จริงในงานของผู้เรียนหลังจากการอบรม เช่น การประเมินความสามารถในการใช้งานเครื่องมือด้านความมั่นคงปลอดภัย การปฏิบัติตามแนวทางความปลอดภัย และการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ➢ จัดทำระบบการสนับสนุนการพัฒนาทักษะอย่างต่อเนื่อง เช่น การจัดทำคลังความรู้หรือแพลตฟอร์มการเรียนรู้ออนไลน์ที่ให้ผู้เรียนสามารถเข้ามาทบทวนความรู้ หรือศึกษาเนื้อหาเพิ่มเติมได้ทุกเวลา ➢ ประเมินและปรับปรุงหลักสูตรตามข้อเสนอแนะและผลการติดตาม เพื่อให้มั่นใจว่าหลักสูตรเชิงลึกยังคงมีประสิทธิภาพและสอดคล้องกับสถานการณ์ปัจจุบัน		
P8: โครงการจัดหาแพลตฟอร์มการเรียนรู้ออนไลน์ **กลยุทธ์ที่ 1.4**: บูรณาการหลักสูตรการเรียนรู้ผ่าน Platform ออนไลน์	**1. การวิเคราะห์ความต้องการและการสำรวจแพลตฟอร์ม (Needs Analysis & Platform Research)** ➢ สำรวจความต้องการขององค์กรและผู้ใช้งาน เช่น ประเภทของหลักสูตรที่ต้องการนำเสนอ รูปแบบการเรียนรู้ (เช่น การเรียนรู้ด้วยตนเอง การเรียนรู้ผ่านวิดีโอ การเรียนรู้แบบโต้ตอบ) และฟีเจอร์ที่ต้องการ เช่น ระบบการติดตามความก้าวหน้า การประเมินผล และการสื่อสารระหว่างผู้เรียน ➢ การกำหนดคอร์สความรู้พื้นฐานทั่วไปที่บุคลากรทุกคนต้องทราบ เช่น PDPA, Cybersecurity Awareness, การบริหารความเสี่ยง เป็นต้น และมีคอร์สเฉพาะเจาะจง/หลักสูตรที่เกี่ยวข้องโดยตรงกับหน่วยงาน เช่น secure coding, network configuration เป็นต้น ➢ กำหนดข้อกำหนดและคุณสมบัติที่แพลตฟอร์มการเรียนรู้ควรมี เช่น ความยืดหยุ่นในการปรับแต่ง ความง่ายในการใช้งาน ความปลอดภัยในการจัดการข้อมูล และความสามารถในการรองรับผู้ใช้จำนวนมาก	พ.ศ. 2569 (ระยะเวลา 1 ปี)	➢ กลุ่มงานบริหารทรัพยากรบุคคล ➢ สำนักงานผู้อำนวยการ ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ สำรวจและคัดเลือกผู้ให้บริการแพลตฟอร์มการเรียนรู้ที่สอดคล้องกับความต้องการขององค์กร โดยพิจารณาแพลตฟอร์มที่มีความน่าเชื่อถือ ความเสถียร และสามารถขยายขีดความสามารถในอนาคตได้ เช่น FutureSkill, WISIMO เป็นต้น **2. การประเมินและคัดเลือกผู้ให้บริการแพลตฟอร์ม (Evaluation & Vendor Selection)** ➢ ประเมินแพลตฟอร์มการเรียนรู้จากผู้ให้บริการต่าง ๆ โดยใช้เกณฑ์การประเมินที่กำหนดไว้ เช่น ฟีเจอร์การใช้งาน การสนับสนุนด้านเทคนิค ต้นทุน และการรองรับความต้องการเฉพาะขององค์กร ➢ ทำการทดลองใช้งาน (Demo) ของแพลตฟอร์มที่ผ่านการคัดกรองเบื้องต้นเพื่อให้แน่ใจว่าแพลตฟอร์มมีความเหมาะสมและเป็นมิตรกับผู้ใช้ ➢ เลือกผู้ให้บริการที่ตรงตามข้อกำหนดมากที่สุด และทำสัญญาจัดซื้อแพลตฟอร์มการเรียนรู้เพื่อให้สามารถเริ่มการติดตั้งและใช้งานได้ **3. การติดตั้งและการตั้งค่าระบบ (Platform Implementation & Configuration)** ➢ ติดตั้งและตั้งค่าแพลตฟอร์มการเรียนรู้ให้พร้อมใช้งาน เช่น การกำหนดโครงสร้างหลักสูตร การตั้งค่าระบบการติดตามผลการเรียนรู้ การตั้งค่าความปลอดภัยของข้อมูลและการกำหนดสิทธิ์การเข้าถึงของผู้ใช้งาน ➢ ทดสอบการทำงานของแพลตฟอร์มการเรียนรู้เพื่อให้แน่ใจว่าแพลตฟอร์มสามารถทำงานได้ตามข้อกำหนดที่กำหนดและรองรับการใช้งานจริงในองค์กร ➢ ปรับแต่งและจัดทำเนื้อหาการเรียนรู้ เช่น การอัปโหลดหลักสูตร วิดีโอ แบบฝึกหัด และเอกสารประกอบการเรียนรู้ตามโครงสร้างที่กำหนดไว้ **4. การฝึกอบรมและสร้างความตระหนักให้กับผู้ใช้งาน (User Training & Awareness)** ➢ จัดการฝึกอบรมการใช้งานแพลตฟอร์มการเรียนรู้ให้กับบุคลากรในองค์กรที่เกี่ยวข้อง เช่น ผู้ดูแลระบบ ผู้สอน และผู้เรียน เพื่อให้ทุกฝ่ายเข้าใจการใช้งานฟีเจอร์ต่าง ๆ อย่างครบถ้วน		

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ สร้างความตระหนักถึงความสำคัญของการเรียนรู้ผ่านแพลตฟอร์มออนไลน์ และให้คำแนะนำในการเข้าถึง การเรียนรู้ และการประเมินผลผ่านระบบ ➢ จัดทำคู่มือการใช้งานแพลตฟอร์มการเรียนรู้และเผยแพร่ให้แก่บุคลากรในองค์กรเพื่อให้บุคลากรสามารถศึกษาด้วยตนเองได้ **5. การติดตามผลและการบำรุงรักษา (Monitoring & Maintenance)** ➢ ติดตามผลการใช้งานแพลตฟอร์มการเรียนรู้ เช่น อัตราการเข้าใช้งาน การสำเร็จการเรียนรู้ และปัญหาที่พบในการใช้งาน เพื่อปรับปรุงการใช้งานและประสบการณ์ผู้ใช้ ➢ ประเมินความพึงพอใจและความคุ้มค่าในการใช้งานแพลตฟอร์ม โดยเก็บรวบรวมข้อมูลจากผู้ใช้งาน เช่น ข้อเสนอแนะและคำติชม เพื่อใช้ในการปรับปรุงต่อไป ➢ บำรุงรักษาแพลตฟอร์มและอัปเดตระบบตามความจำเป็น เช่น การอัปเดตซอฟต์แวร์ การเพิ่มความปลอดภัย และการขยายขีดความสามารถของแพลตฟอร์ม		
P9: โครงการสนับสนุนการใช้งาน Platform การเรียนรู้ **กลยุทธ์ที่ 1.4**: บูรณาการหลักสูตรการเรียนรู้ผ่าน Platform ออนไลน์	**1. การให้ความรู้และการสร้างความตระหนัก** ➢ จัดอบรมหรือสัมมนาให้พนักงานเข้าใจการใช้งาน Platform เช่น วิธีเข้าถึง การใช้ฟีเจอร์ต่าง ๆ และประโยชน์จากการเรียนรู้ผ่าน Platform ➢ จัดทำคู่มือการใช้งานในรูปแบบที่เข้าใจง่าย เช่น วิดีโอแนะนำหรือเอกสาร PDF **2. การสนับสนุนและให้คำปรึกษาอย่างต่อเนื่อง** ➢ ตั้งทีมสนับสนุนการใช้งาน (Support Team) เพื่อช่วยเหลือเมื่อเกิดปัญหาหรือคำถามเกี่ยวกับแพลตฟอร์ม ➢ เปิดช่องทางการสื่อสาร เช่น อีเมล แชท หรือโทรศัพท์ สำหรับคำปรึกษาและการแจ้งปัญหา **3. การส่งเสริมการใช้งานผ่านแรงจูงใจ** ➢ จัดกิจกรรมที่กระตุ้นให้พนักงานใช้แพลตฟอร์ม เช่น การให้คะแนนสะสม การมอบรางวัลหรือการยกย่องความสำเร็จในการเรียนรู้ ➢ ติดตามการใช้งานผ่านระบบและให้ Feedback เชิงบวกเพื่อสนับสนุนการใช้งานต่อเนื่อง	พ.ศ. 2570 (ระยะเวลา 1 ปี)	➢ กลุ่มงานบริหารทรัพยากรบุคคล ➢ สำนักงานผู้อำนวยการ ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน ➢ หน่วยงานพันธมิตร

ตารางที่ 6-6 ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

6.2 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
P10: โครงการพัฒนามาตรฐานการแลกเปลี่ยนข้อมูล **กลยุทธ์ที่ 2.1**: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร	**1. การวางแผนและการกำหนดมาตรฐาน** ➢ จัดตั้งคณะทำงานร่วมระหว่าง สคทช. และหน่วยงานพันธมิตร ➢ ศึกษาความต้องการและปัญหาของข้อมูลที่ต้องแลกเปลี่ยน ➢ กำหนดโครงสร้างข้อมูลมาตรฐาน (Data Schema) และข้อกำหนดเบื้องต้น เช่น รูปแบบข้อมูล (XML, JSON, CSV) และโปรโตคอลการเชื่อมต่อ (API) ➢ วางแผนด้านความปลอดภัย เช่น การเข้ารหัสข้อมูลและการควบคุมการเข้าถึง ➢ จัดทำเอกสารนโยบายและแนวทางปฏิบัติ **2. การพัฒนาระบบและการทดสอบ** ➢ ออกแบบและพัฒนาระบบการแลกเปลี่ยนข้อมูล เช่น API หรือ Web Services ➢ ตั้งค่าระบบการตรวจสอบสิทธิ์ (Authentication) และการอนุญาต (Authorization) ➢ ทดสอบการเชื่อมต่อระหว่างหน่วยงานเพื่อประเมินความถูกต้องของข้อมูลและประสิทธิภาพ ➢ จัดทำ Test Cases และจำลองสถานการณ์เพื่อประเมินการใช้งานในสถานการณ์จริง	พ.ศ. 2569 (ระยะเวลา 1 ปี)	➢ กองส่งเสริมความร่วมมือและขับเคลื่อนการบริหารจัดการที่ดิน ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน ➢ หน่วยงานพันธมิตร
P11: โครงการประชุมและเวิร์คช็อปการแบ่งปันข้อมูล **กลยุทธ์ที่ 2.1**: แบ่งปันข้อมูลด้านความมั่นคงปลอดภัยกับหน่วยงานพันธมิตร	**1. การเริ่มต้นและสร้างรากฐานความร่วมมือ** 1. **การระบุและคัดเลือกหน่วยงานพันธมิตร:** เลือกหน่วยงานที่เกี่ยวข้องและมีศักยภาพในการแลกเปลี่ยนข้อมูลด้านความมั่นคงปลอดภัย 2. **จัดการประชุมเริ่มต้น:** จัดการประชุมเริ่มต้นเพื่อทำความเข้าใจร่วมกันและสร้างข้อตกลงเกี่ยวกับแนวทางการแบ่งปันข้อมูล ข้อกำหนดความปลอดภัย และความเป็นส่วนตัวของข้อมูล 3. **พัฒนากลไกการแบ่งปันข้อมูล:** พัฒนากลไกการแบ่งปันข้อมูลเบื้องต้น เช่น ระบบแพลตฟอร์มออนไลน์หรือช่องทางการสื่อสารที่ปลอดภัยสำหรับการแบ่งปันข้อมูลสำคัญ **2. การขยายความร่วมมือและการดำเนินการแบ่งปันข้อมูล**	พ.ศ. 2570 (ระยะเวลา 1 ปี)	➢ กองส่งเสริมความร่วมมือและขับเคลื่อนการบริหารจัดการที่ดิน ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน ➢ หน่วยงานพันธมิตร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	1. **จัดเวิร์คช็อปและการประชุมเชิงปฏิบัติการ:** จัดเวิร์คช็อปเพื่อแบ่งปันข้อมูลด้านความมั่นคงปลอดภัย เช่น การวิเคราะห์ภัยคุกคามร่วมกัน การวิเคราะห์สถานการณ์ และการแลกเปลี่ยนวิธีปฏิบัติที่ดีที่สุด (Best Practices) 2. **การแบ่งปันข้อมูลผ่านแพลตฟอร์มออนไลน์:** ใช้แพลตฟอร์มที่พัฒนาขึ้นสำหรับการแบ่งปันข้อมูลระหว่างหน่วยงานพันธมิตร โดยให้มีระบบความปลอดภัยในการตรวจสอบการเข้าถึงข้อมูล 3. **การติดตามและประเมินผลการแบ่งปันข้อมูล:** ติดตามผลการใช้งานแพลตฟอร์มและรวบรวมความคิดเห็นเพื่อปรับปรุงการแบ่งปันข้อมูลให้มีประสิทธิภาพมากขึ้น **3. การประเมินผลและการพัฒนาความร่วมมือในระยะยาว** 1. **การประเมินผลและสรุปบทเรียน:** รวบรวมข้อมูลและข้อเสนอแนะจากทุกฝ่ายที่เข้าร่วมเพื่อประเมินประสิทธิผลของโครงการและสรุปบทเรียนในการแบ่งปันข้อมูล 2. **การปรับปรุงและขยาย Platform การแบ่งปันข้อมูล:** ปรับปรุง Platform การแบ่งปันข้อมูลให้มีฟีเจอร์ใหม่ ๆ ที่รองรับการใช้งานมากขึ้นและเสริมสร้างระบบความปลอดภัย 3. **การพัฒนาเครือข่ายความร่วมมือระยะยาว:** สร้างแผนความร่วมมือระยะยาวเพื่อให้เกิดการแบ่งปันข้อมูลอย่างต่อเนื่องและยั่งยืน รวมถึงการพัฒนากรอบการดำเนินงานที่สามารถปรับตัวตามภัยคุกคามใหม่ ๆ		
P12: โครงการจัดทำและทดสอบ BCP **กลยุทธ์ที่ 2.2**: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน	**1. การวิเคราะห์ความเสี่ยงและผลกระทบทางธุรกิจ (Risk & Business Impact Analysis)** ➢ วิเคราะห์ความเสี่ยงที่อาจส่งผลกระทบต่อระบบที่สำคัญและประเมินผลกระทบต่อการดำเนินธุรกิจ เช่น การสูญเสียข้อมูล ความเสียหายต่อทรัพย์สิน หรือความเสี่ยงด้านการดำเนินงาน **2. การจัดทำแผน BCP และกำหนดขั้นตอนการตอบสนอง (BCP Development & Response Planning)** ➢ จัดทำแผน BCP ที่ครอบคลุมขั้นตอนการตอบสนองเมื่อเกิดเหตุฉุกเฉิน การกู้คืนระบบ และการกลับมาดำเนินงานตามปกติ โดยกำหนดบทบาทและความรับผิดชอบของบุคลากรในแต่ละส่วน **3. การฝึกอบรมและสื่อสารแผน BCP (Training & Communication)** ➢ ฝึกอบรมพนักงานที่เกี่ยวข้องให้เข้าใจบทบาทและขั้นตอนในแผน BCP และสื่อสารแผนไปยังผู้ที่มีส่วนเกี่ยวข้องทั้งหมดเพื่อให้พร้อมปฏิบัติเมื่อเกิดเหตุ **4. การทดสอบและประเมินผลแผน BCP (BCP Testing & Evaluation)**	พ.ศ. 2568 – 2570 (ระยะเวลา 2 ปี 6 เดือน)	➢ สำนักงานผู้อำนวยการ ➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน ➢ หน่วยงานพันธมิตร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
	➢ จัดทำการทดสอบแผน BCP ในสถานการณ์จำลองเพื่อตรวจสอบความสามารถในการตอบสนองของระบบและบุคลากร และประเมินผลการทดสอบเพื่อปรับปรุงแผนตามข้อบกพร่องที่พบ		
P13: โครงการประเมินและจัดหาเทคโนโลยีคลาวด์ (Cloud) **กลยุทธ์ที่ 2.2**: บริหารความต่อเนื่องในการดำเนินการตามภารกิจของหน่วยงาน	**1. การวิเคราะห์ความต้องการและการวางแผนการใช้ Cloud (Needs Analysis & Cloud Planning)** ➢ วิเคราะห์ความต้องการและข้อกำหนดของระบบที่สำคัญ เพื่อกำหนดประเภท คลาวด์ (Cloud) ที่เหมาะสม (ภาครัฐหรือ Public Cloud) โดยคำนึงถึงความปลอดภัย ความยืดหยุ่น และความสามารถในการรองรับการกู้คืนในสถานการณ์ฉุกเฉิน **2. การสำรวจและคัดเลือกผู้ให้บริการ คลาวด์ (Cloud) (Vendor Research & Selection)** ➢ สำรวจและประเมินผู้ให้บริการคลาวด์ (Cloud) ที่มีความน่าเชื่อถือ โดยพิจารณาฟีเจอร์ที่ตอบโจทย์ความต้องการ เช่น ความปลอดภัย การปฏิบัติตามมาตรฐาน และการสนับสนุนการกู้คืนข้อมูล รวมถึงต้นทุน ทั้งนี้จะมีการพิจารณาการเลือกใช้ คลาวด์ (Cloud) จาก คลาวด์ (Cloud) ภาครัฐก่อนในลำดับแรก **3. การติดตั้งและตั้งค่าระบบบนคลาวด์ (Cloud) (Cloud Implementation & Configuration)** ➢ ติดตั้งและตั้งค่าระบบบนแพลตฟอร์มคลาวด์ (Cloud) ที่เลือก โดยกำหนดการตั้งค่าที่เน้นความปลอดภัย การสำรองข้อมูล และการเข้าถึงในสถานการณ์ฉุกเฉิน **4. การทดสอบและประเมินประสิทธิภาพคลาวด์ (Cloud) สำหรับ BCP (Testing & Performance Evaluation)** ➢ ทดสอบการใช้งานระบบบนคลาวด์ (Cloud) โดยจำลองสถานการณ์ฉุกเฉิน เพื่อประเมินประสิทธิภาพในการกู้คืนข้อมูล ความรวดเร็วในการเข้าถึง และความเสถียร	พ.ศ. 2570 (ระยะเวลา 1 ปี 0 เดือน)	➢ ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน ➢ คลาวด์ (Cloud) ภาครัฐ

ตารางที่ 6-7 ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

6.3 ยุทธศาสตร์ที่ 3 การขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดี (Driving Security with Good Governance)

โครงการสำคัญ	กลไกและวิธีการปฏิบัติ	กรอบระยะเวลา	ผู้รับผิดชอบ
P14: โครงการพัฒนากระบวนการและระบบตามมาตรฐาน ISO/IEC 27001 กลยุทธ์ที่ 3.1: พัฒนาสู่มาตรฐานสากลด้านบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ	**การประเมินและวางแผน (Assessment & Planning)** 1.การประเมินช่องว่าง (Gap Analysis): วิเคราะห์กระบวนการและระบบที่มีอยู่ เพื่อเปรียบเทียบกับข้อกำหนดของมาตรฐาน ISO/IEC 27001 และระบุช่องว่างที่ต้องปรับปรุง 2.การพัฒนาแผนการปรับปรุง (Improvement Planning): จัดทำแผนการปรับปรุงระบบและกระบวนการเพื่อให้เป็นไปตามมาตรฐาน รวมถึงกำหนดทรัพยากรที่จำเป็น บุคลากรที่เกี่ยวข้อง และกำหนดการดำเนินงาน 3.การจัดตั้งทีมงานและกำหนดความรับผิดชอบ (Team Formation & Responsibility Allocation): จัดตั้งทีมงานรับผิดชอบโครงการ โดยระบุบทบาทและความรับผิดชอบสำหรับบุคลากรในแต่ละส่วน **การพัฒนากระบวนการและระบบ (Process & System Development)** 1.การพัฒนากระบวนการและเอกสารตามมาตรฐาน (Process & Documentation Development): ปรับปรุงกระบวนการและจัดทำเอกสารตามมาตรฐาน ISO/IEC 27001 เช่น นโยบายความมั่นคงปลอดภัยสารสนเทศ การจัดการความเสี่ยง การควบคุมการเข้าถึง และการจัดการเหตุการณ์ 2.การฝึกอบรมและสร้างความตระหนัก (Training & Awareness): จัดฝึกอบรมให้กับพนักงานทุกระดับ เพื่อให้ความรู้เรื่องการปฏิบัติตามมาตรฐาน ISO/IEC 27001 และการรักษาความมั่นคงปลอดภัยข้อมูล 3.การทดสอบระบบและกระบวนการ (System & Process Testing): ทดสอบกระบวนการและระบบเพื่อให้แน่ใจว่าทำงานได้ตามที่วางแผนไว้ และสอดคล้องกับข้อกำหนดของมาตรฐาน **การตรวจสอบภายในและการปรับปรุง (Internal Audit & Improvement)** 1.การตรวจสอบภายใน (Internal Audit): จัดทำการตรวจสอบภายในระบบและกระบวนการทั้งหมดเพื่อตรวจสอบการปฏิบัติตามข้อกำหนดของ ISO/IEC 27001 และระบุจุดที่ต้องปรับปรุง 2.การปรับปรุงตามผลการตรวจสอบ (Improvement Based on Audit Results): ปรับปรุงระบบตามผลการตรวจสอบภายในเพื่อให้มั่นใจว่าระบบและกระบวนการเป็นไปตามมาตรฐานสากล 3.การเตรียมความพร้อมสำหรับการตรวจสอบภายนอก (Preparation for External Audit): ตรวจสอบและเตรียมความพร้อมสำหรับการตรวจสอบภายนอกโดยปรับปรุงตามคำแนะนำที่ได้รับ **การตรวจสอบภายนอกและการรับรองมาตรฐาน (External Audit & Certification)**	พ.ศ. 2569 - 2570 (ระยะเวลา 2 ปี)	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

	1.การตรวจสอบภายนอก (External Audit): ดำเนินการตรวจสอบภายนอกโดยผู้ตรวจสอบที่ได้รับการรับรอง เพื่อยืนยันว่าระบบและกระบวนการเป็นไปตามมาตรฐาน ISO/IEC 27001 2.การปรับปรุงตามคำแนะนำ (Post-Audit Improvement): ปรับปรุงและแก้ไขจุดบกพร่องที่พบระหว่างการตรวจสอบภายนอกเพื่อให้มั่นใจว่าระบบพร้อมสำหรับการรับรอง 3.การรับรองมาตรฐาน (Certification): รับรองมาตรฐาน ISO/IEC 27001 จากหน่วยงานที่รับรองอย่างเป็นทางการ เพื่อยืนยันความสอดคล้องตามมาตรฐานสากล		

ตารางที่ 6-8 ยุทธศาสตร์ที่ 3 การขับเคลื่อนด้านการรักษาความมั่นคงปลอดภัยด้วยธรรมาภิบาลที่ดี (Driving Security with Good Governance)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

7. ข้อเสนอเพื่อเพิ่มแผนเร่งด่วนในแผนแม่บทของสำนักงานคณะกรรมการ นโยบายที่ดินแห่งชาติ (สคทช.)

ในสภาวะแวดล้อมปัจจุบัน เทคโนโลยีมีการพัฒนาและเปลี่ยนแปลงอย่างรวดเร็ว รวมถึงนโยบายของรัฐบาลที่สามารถปรับเปลี่ยนได้ในระยะเวลาอันสั้น ซึ่งอาจส่งผลกระทบต่อการดำเนินงานด้านการจัดการนโยบายที่ดินและความต่อเนื่องของภารกิจที่เกี่ยวข้อง ดังนั้น เพื่อเตรียมความพร้อมสำหรับการรับมือกับสถานการณ์ที่ไม่คาดคิด และเสริมสร้างความยืดหยุ่นในการดำเนินงานของ สคทช. จึงเสนอแนะให้เพิ่มแผนเร่งด่วน (Contingency Plan) ในรูปแบบบทใหม่ในแผนแม่บท โดยมีรายละเอียดดังนี้:

แนวทางการรับมือเหตุการณ์ฉุกเฉินและการเปลี่ยนแปลงนโยบาย

1. **วัตถุประสงค์ของแผนเร่งด่วน**
   - เพื่อกำหนดแนวทางการรับมือกรณีเกิดเหตุการณ์ฉุกเฉินหรือการเปลี่ยนแปลงนโยบายอย่างกะทันหันที่มีผลกระทบต่อภารกิจและการดำเนินงานของ สคทช.
   - เพื่อสร้างกลไกการตัดสินใจและการปฏิบัติการที่รวดเร็วและมีประสิทธิภาพในสถานการณ์ที่ต้องการการตอบสนองเร่งด่วน
   - เพื่อส่งเสริมการบูรณาการระหว่างหน่วยงานที่เกี่ยวข้องเพื่อสนับสนุนความต่อเนื่องในการดำเนินงาน
2. **แนวทางการจัดทำแผนเร่งด่วน**

   2.1 การวิเคราะห์ความเสี่ยงและสถานการณ์
   - สำรวจและประเมินความเสี่ยงที่อาจเกิดขึ้นจากการเปลี่ยนแปลงของเทคโนโลยีและนโยบาย เช่น การเปลี่ยนแปลงในระบบการจัดเก็บข้อมูล การบังคับใช้กฎหมายใหม่ หรือการเปลี่ยนแปลงกระบวนการทำงานที่เกี่ยวข้องกับที่ดิน

   2.2 การจัดลำดับความสำคัญของเหตุการณ์
   - กำหนดลำดับความสำคัญของกรณีที่อาจเกิดขึ้น โดยพิจารณาผลกระทบต่อองค์กรและประชาชนผู้มีส่วนได้ส่วนเสีย

   2.3 การวางแผนและเตรียมความพร้อม
   - จัดทำขั้นตอนการปฏิบัติในกรณีฉุกเฉิน เช่น แนวทางการปรับเปลี่ยนกระบวนการทำงาน การปรับใช้งานเทคโนโลยีที่ทันสมัย หรือการประสานงานกับหน่วยงานที่เกี่ยวข้อง
3. **การดำเนินการตามแผนเร่งด่วน**
   - จัดตั้ง คณะทำงานเฉพาะกิจ (Task Force) เพื่อรับผิดชอบการจัดการเหตุการณ์ในกรณีฉุกเฉิน
   - พัฒนาระบบการแจ้งเตือนและการรายงานสถานการณ์ที่ครอบคลุมและรวดเร็ว
   - จัดอบรมบุคลากรเกี่ยวกับแนวทางการปฏิบัติตามแผนเร่งด่วนเพื่อเพิ่มความพร้อมและประสิทธิภาพในการตอบสนอง
4. **การบูรณาการแผนเร่งด่วนในแผนแม่บท**
   - แนวทางแผนเร่งด่วนจะถูกระบุไว้ในรูปแบบของบทในแผนแม่บท เพื่อให้สามารถนำไปปฏิบัติได้ทันทีในกรณีฉุกเฉิน

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

- ข้อมูลรายละเอียดของแผนเร่งด่วน เช่น ขั้นตอนการปฏิบัติการ รายชื่อผู้รับผิดชอบและทรัพยากรที่จำเป็น จะถูกบันทึกและจัดทำในภาคผนวก เพื่อเป็นคู่มือการปฏิบัติงานที่ครบถ้วนและชัดเจน

5. ประโยชน์ที่คาดว่าจะได้รับ

- เพิ่มความสามารถในการตอบสนองต่อสถานการณ์ฉุกเฉินและการเปลี่ยนแปลงนโยบายได้อย่างมีประสิทธิภาพ
- ลดผลกระทบที่อาจเกิดขึ้นต่อภารกิจหลักของ สคทช.
- เสริมสร้างความเชื่อมั่นแก่ประชาชนและผู้มีส่วนได้ส่วนเสียว่าการดำเนินงานของ สคทช. มีความต่อเนื่องและโปร่งใส

ข้อเสนอเพื่อเพิ่มแผนเร่งด่วนในแผนแม่บทของสำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ (สคทช.) จะช่วยให้องค์กรมีความพร้อมและยืดหยุ่นต่อความท้าทายในอนาคต และยังสนับสนุนเป้าหมายหลักของ สคทช. ในการจัดการนโยบายที่ดินของประเทศอย่างยั่งยืนและมีประสิทธิภาพ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

8. ภาคผนวกความเชื่อมโยงของแผนฯ และการตอบสนองของแผนฯ ต่อการประเมินต่าง ๆ

8.1 ความเชื่อมโยงระหว่างนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรฐานสากล ISO 27002 : 2022

แนวปฏิบัติ	ISO 27002 : 2022
1 มาตรการควบคุมด้านองค์กร (Organizational controls)	**A.5**
1.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)	A.5.1
1.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)	A.5.2
1.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)	A.5.3
1.4 หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities)	A.5.4
1.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)	A.5.5
1.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)	A.5.6
1.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)	A.5.7 Y
1.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)	A.5.8
1.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น (Inventory of information and other associated assets)	A.5.9
1.10 การใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)	A.5.10
1.11 การคืนทรัพย์สิน (Return of assets)	A.5.11
1.12 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification of information)	A.5.12
1.13 การทำป้ายบ่งชี้สารสนเทศ (Labelling of information)	A.5.13
1.14 การถ่ายโอนสารสนเทศ (Information transfer)	A.5.14
1.15 การควบคุมการเข้าถึง (Access control)	A.5.15
1.16 การบริหารจัดการพิสูจน์ตัวตน (Identity management)	A.5.16
1.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)	A.5.17
1.18 การควบคุมสิทธิ์และการเข้าถึงระบบสารสนเทศ (Access rights)	A.5.18
1.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)	A.5.19
1.20 การระบุถึงความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงกับผู้ให้บริการภายนอก (Addressing information security within supplier agreements)	A.5.20

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ISO 27002 : 2022
1.21 การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (Managing information security in the ICT supply chain)	A.5.21
1.22 การติดตาม ทบทวน และการจัดการ การเปลี่ยนแปลงสำหรับบริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)	A.5.22
1.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)	A.5.23 Y
1.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)	A.5.24
1.25 การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)	A.5.25
1.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)	A.5.26
1.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)	A.5.27
1.28 การรวบรวมหลักฐาน (Collection of evidence)	A.5.28
1.29 ความมั่นคงปลอดภัยสารสนเทศในช่วงภาวะหยุดชะงัก (Information security during disruption)	A.5.29
1.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)	A.5.30 Y
1.31 ความมั่นคงปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด (Legal, statutory, regulatory and contractual requirements)	A.5.31
1.32 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)	A.5.32
1.33 การป้องกันบันทึก (Protection of records)	A.5.33
1.34 การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล (Privacy and protection of PII)	A.5.34
1.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Intellectual property rights)	A.5.35
1.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานสำหรับความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)	A.5.36
1.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)	A.5.37
2. มาตรการควบคุมด้านบุคลากร (People controls)	**A.6**
2.1 การคัดกรอง (Screening)	A.6.1
2.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)	A.6.2
2.3 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศข้อกำหนด (Information security awareness, education and training)	A.6.3

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ISO 27002 : 2022
2.4 กระบวนการทางวินัย (Disciplinary process)	A.6.4
2.5 ความรับผิดชอบหลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)	A.6.5
2.6 ข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or non-disclosure agreements)	A.6.6
2.7 การปฏิบัติงานจากระยะไกล (Remote working)	A.6.7
2.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)	A.6.8
3. มาตรการควบคุมด้านกายภาพ (Physical Controls)	**A.7**
3.1 ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters)	A.7.1
3.2 การเข้า-ออกพื้นที่ทางกายภาพ (Physical entry)	A.7.2
3.3 การรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)	A.7.3
3.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)	A.7.4 Y
3.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats)	A.7.5
3.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	A.7.6
3.7 การจัดเก็บโต๊ะทำงานและการจัดการหน้าจอ (Clear desk and clear screen)	A.7.7
3.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)	A.7.8
3.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสถานที่ (Security of assets off-premises)	A.7.9
3.10 สื่อบันทึกข้อมูล (Storage media)	A.7.10
3.11 ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities)	A.7.11
3.12 การรักษาความมั่นคงปลอดภัยของการเดินสาย (Cabling security)	A.7.12
3.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	A.7.13
3.14 การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment)	A.7.14
4. มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)	**A.8**
4.1 อุปกรณ์ของผู้ใช้งาน (User endpoint devices)	A.8.1
4.2 สิทธิพิเศษในการเข้าถึงสารสนเทศ (Privileged access rights)	A.8.2
4.3 การจำกัดการเข้าถึงระบบสารสนเทศ (Information access restriction)	A.8.3
4.4 การเข้าถึงซอร์สโค้ด (Access to source code)	A.8.4
4.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)	A.8.5

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ISO 27002 : 2022
4.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity management)	A.8.6
4.7 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection against malware)	A.8.7
4.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	A.8.8
4.9 การบริหารจัดการ การกำหนดค่า (Configuration Management)	A.8.9
4.10 การลบข้อมูล (Information deletion)	A.8.10
4.11 การซ่อนข้อมูล (Data masking)	A.8.11
4.12 การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)	A.8.12
4.13 การสำรองข้อมูล (Information backup)	A.8.13
4.14 ระบบทดแทน (Redundancy of information processing facilities)	A.8.14
4.15 การลงบันทึกเหตุการณ์ (Logging)	A.8.15
4.16 กิจกรรมการเฝ้าติดตาม (Monitoring Activities)	A.8.16
4.17 การตั้งค่านาฬิกาและเวลาให้ตรงกัน (Clock synchronization)	A.8.17
4.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs)	A.8.18
4.19 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of software on operational systems)	A.8.19
4.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)	A.8.20
4.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)	A.8.21
4.22 การแบ่งแยกเครือข่าย (Segregation of networks)	A.8.22
4.23 การกรองเว็บ (Web filtering)	A.8.23
4.24 การเข้ารหัสข้อมูล (Use of cryptography)	A.8.24
4.25 วงจรการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure development life cycle)	A.8.25
4.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements)	A.8.26
4.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)	A.8.27
4.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure Coding)	A.8.28
4.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาระบบและการยอมรับ (Security testing in development and acceptance)	A.8.29
4.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)	A.8.30
4.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง (Separation of development, test and production environments)	A.8.31

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ISO 27002 : 2022
4.32 การบริหารจัดการ การเปลี่ยนแปลง (Change management)	A.8.32
4.33 ข้อมูลในการทดสอบ (Test information)	A.8.33
4.34 การป้องกันระบบสารสนเทศระหว่างการตรวจประเมิน (Protection of information systems during audit testing)	A.8.34

ตารางที่ 8-1 ความเชื่อมโยงระหว่างนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร และมาตรฐานสากล ISO 27002 : 2022

8.2 ความเชื่อมโยงระหว่างกลุ่มผู้รับผิดชอบและแนวปฏิบัติ

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
1 มาตรการควบคุมด้านองค์กร (Organizational controls)							
1.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)	✓	✓					
1.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)	✓	✓					
1.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)	✓	✓		✓			
1.4 หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities)	✓						
1.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)		✓		✓		✓	
1.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)		✓					

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
1.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)		✓					
1.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)	✓	✓				✓	✓
1.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น (Inventory of information and other associated assets)		✓				✓	
1.10 การใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)		✓	✓				
1.11 การคืนทรัพย์สิน (Return of assets)		✓	✓	✓			
1.12 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification of information)		✓				✓	
1.13 การทำป้ายบ่งชี้สารสนเทศ (Labelling of information)		✓				✓	
1.14 การถ่ายโอนสารสนเทศ (Information transfer)		✓	✓				
1.15 การควบคุมการเข้าถึง (Access control)		✓	✓				
1.16 การบริหารจัดการพิสูจน์ตัวตน (Identity management)		✓	✓	✓			

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
1.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)		✓	✓				
1.18 การควบคุมสิทธิ์และการเข้าถึงระบบสารสนเทศ (Access rights)		✓	✓				
1.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)		✓			✓	✓	
1.20 การระบุถึงความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงกับผู้ให้บริการภายนอก (Addressing information security within supplier agreements)		✓			✓	✓	
1.21 การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (Managing information security in the ICT supply chain)		✓			✓	✓	
1.22 การติดตาม ทบทวน และการจัดการการเปลี่ยนแปลงสำหรับบริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)		✓			✓	✓	

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
1.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)		✓			✓	✓	
1.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)	✓	✓	✓				
1.25 การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)		✓					
1.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)	✓	✓	✓				
1.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)		✓	✓				
1.28 การรวบรวมหลักฐาน (Collection of evidence)		✓					
1.29 ความมั่นคงปลอดภัยสารสนเทศในช่วงภาวะหยุดชะงัก (Information security during disruption)	✓	✓	✓				

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
1.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)	✓	✓	✓				
1.31 ความมั่นคงปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด (Legal, statutory, regulatory and contractual requirements)		✓			✓		✓
1.32 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)		✓			✓		✓
1.33 การป้องกันบันทึก (Protection of records)		✓					
1.34 การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล (Privacy and protection of PII)		✓			✓		✓
1.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Intellectual property rights)	✓	✓					✓
1.36 การปฏิบัติตามนโยบาย กฎระเบียบและมาตรฐานสำหรับความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)		✓	✓				
1.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)	✓	✓	✓				✓

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
2. มาตรการควบคุมด้านบุคลากร (People controls)							
2.1 การคัดกรอง (Screening)				✓			
2.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)				✓	✓		
2.3 การสร้างความตระหนัก การให้ความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศข้อกำหนด (Information security awareness, education and training)	✓	✓	✓	✓			
2.4 กระบวนการทางวินัย (Disciplinary process)	✓			✓	✓		
2.5 ความรับผิดชอบหลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)		✓		✓			
2.6 ข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or non-disclosure agreements)			✓	✓			
2.7 การปฏิบัติงานจากระยะไกล (Remote working)		✓	✓				

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
2.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)		✓	✓				
3. มาตรการควบคุมด้านกายภาพ (Physical Controls)							
3.1 ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters)		✓	✓				
3.2 การเข้า-ออกพื้นที่ทางกายภาพ (Physical entry)		✓	✓				
3.3 การรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)		✓	✓				
3.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)		✓					
3.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats)		✓	✓				
3.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)		✓	✓				
3.7 การจัดเก็บโต๊ะทำงานและการจัดการหน้าจอ (Clear desk and clear screen)		✓	✓				
3.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)		✓	✓				

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
3.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสถานที่ (Security of assets off - premises)		✓	✓				
3.10 สื่อบันทึกข้อมูล (Storage media)		✓	✓				
3.11 ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities)		✓					
3.12 การรักษาความมั่นคงปลอดภัยของการเดินสาย (Cabling security)		✓					
3.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)		✓	✓				
3.14 การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment)		✓				✓	
4. มาตรการควบคุมด้านเทคโนโลยี (Technological Controls)							
4.1 อุปกรณ์ของผู้ใช้งาน (User endpoint devices)		✓	✓				
4.2 สิทธิพิเศษในการเข้าถึงสารสนเทศ (Privileged access rights)		✓	✓	✓			
4.3 การจำกัดการเข้าถึงระบบสารสนเทศ (Information access restriction)		✓					
4.4 การเข้าถึงซอร์สโค้ด (Access to source code)		✓					

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
4.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)		✓					
4.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity management)		✓					
4.7 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection against malware)		✓	✓				
4.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)		✓					
4.9 การบริหารจัดการ การกำหนดค่า (Configuration Management)		✓					
4.10 การลบข้อมูล (Information deletion)		✓	✓				
4.11 การซ่อนข้อมูล (Data masking)		✓	✓				
4.12 การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)		✓	✓				
4.13 การสำรองข้อมูล (Information backup)		✓					
4.14 ระบบทดแทน (Redundancy of information processing facilities)		✓					
4.15 การลงบันทึกเหตุการณ์ (Logging)		✓					
4.16 กิจกรรมการเฝ้าติดตาม (Monitoring Activities)		✓					

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
4.17 การตั้งค่านาฬิกาและเวลาให้ตรงกัน (Clock synchronization)		✓					
4.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs)		✓	✓				
4.19 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of software on operational systems)		✓					
4.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)		✓					
4.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)		✓					
4.22 การแบ่งแยกเครือข่าย (Segregation of networks)		✓					
4.23 การกรองเว็บ (Web filtering)		✓					
4.24 การเข้ารหัสข้อมูล (Use of cryptography)		✓	✓				
4.25 วงจรการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure development life cycle)		✓					
4.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements)		✓	✓				

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ผู้อำนวยการ สคทช.	ศูนย์เทคโนโลยีสารสนเทศที่ดินและทรัพยากรดิน	บุคลากรทุกคนของหน่วยงาน	สำนักงานผู้อำนวยการ (กลุ่มงานบริหารทรัพยากรบุคคล)	กองกฎหมาย	สำนักงานผู้อำนวยการ (กลุ่มงานคลังและพัสดุ)	กลุ่มตรวจสอบภายใน
4.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)		✓					
4.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure Coding)		✓					
4.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาระบบและการยอมรับ (Security testing in development and acceptance)		✓					
4.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)		✓			✓	✓	
4.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง (Separation of development, test and production environments)		✓	✓				
4.32 การบริหารจัดการ การเปลี่ยนแปลง (Change management)		✓	✓				
4.33 ข้อมูลในการทดสอบ (Test information)		✓	✓				
4.34 การป้องกันระบบสารสนเทศระหว่างการตรวจประเมิน (Protection of information systems during audit testing)		✓	✓				

ตารางที่ 8-2 ความเชื่อมโยงระหว่างกลุ่มผู้รับผิดชอบและแนวปฏิบัติ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

8.3 ความเชื่อมโยงระหว่างแนวปฏิบัติ และยุทธศาสตร์ในแผนที่นำทาง (Road Map)

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
1.1 นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ (Policies for information security)	✓	✓	✓
1.2 บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information security roles and responsibilities)	✓	✓	✓
1.3 การแบ่งงานและหน้าที่ความรับผิดชอบ (Segregation of duties)	✓	✓	✓
1.4 หน้าที่ความรับผิดชอบของฝ่ายบริหาร (Management responsibilities)	✓	✓	✓
1.5 การติดต่อหน่วยงานผู้มีอำนาจ (Contact with authorities)		✓	✓
1.6 การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ (Contact with special interest groups)		✓	✓
1.7 ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม (Threat intelligence)	✓	✓	✓
1.8 ความมั่นคงปลอดภัยสารสนเทศในการบริหารโครงการ (Information security in project management)			✓
1.9 บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น (Inventory of information and other associated assets)	✓	✓	✓
1.10 การใช้งานสารสนเทศและทรัพย์สินที่เกี่ยวข้องอย่างเหมาะสม (Acceptable use of information and other associated assets)	✓	✓	✓
1.11 การคืนทรัพย์สิน (Return of assets)	✓	✓	✓
1.12 การจัดหมวดหมู่ทรัพย์สินสารสนเทศ (Classification of information)	✓	✓	✓

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
1.13 การทำป้ายบ่งชี้สารสนเทศ (Labelling of information)	✓	✓	✓
1.14 การถ่ายโอนสารสนเทศ (Information transfer)	✓	✓	✓
1.15 การควบคุมการเข้าถึง (Access control)	✓	✓	✓
1.16 การบริหารจัดการพิสูจน์ตัวตน (Identity management)	✓	✓	✓
1.17 ข้อมูลในการพิสูจน์ตัวตน (Authentication information)	✓	✓	✓
1.18 การควบคุมสิทธิ์และการเข้าถึงระบบสารสนเทศ (Access rights)	✓	✓	✓
1.19 ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)	✓		✓
1.20 การระบุถึงความมั่นคงปลอดภัยสารสนเทศภายในข้อตกลงกับผู้ให้บริการภายนอก (Addressing information security within supplier agreements)	✓		✓
1.21 การจัดการความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร (Managing information security in the ICT supply chain)	✓		✓
1.22 การติดตาม ทบทวน และการจัดการ การเปลี่ยนแปลงสำหรับบริการของผู้ให้บริการภายนอก (Monitoring, review and change management of supplier services)	✓		✓
1.23 ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์ (Information security for use of cloud services)	✓	✓	✓
1.24 การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security incident management planning and preparation)	✓	✓	✓

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
1.25 การประเมินและการตัดสินใจเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Assessment and decision on information security events)	✔	✔	✔
1.26 การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)	✔	✔	✔
1.27 การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Learning from information security incidents)	✔	✔	✔
1.28 การรวบรวมหลักฐาน (Collection of evidence)	✔	✔	✔
1.29 ความมั่นคงปลอดภัยสารสนเทศในช่วงภาวะหยุดชะงัก (Information security during disruption)	✔	✔	✔
1.30 ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ (ICT readiness for business continuity)	✔	✔	✔
1.31 ความมั่นคงปลอดภัยเกี่ยวกับการปฏิบัติตามข้อกำหนด (Legal, statutory, regulatory and contractual requirements)	✔	✔	✔
1.32 การป้องกันสิทธิและทรัพย์สินทางปัญญา (Intellectual property rights)	✔	✔	✔
1.33 การป้องกันบันทึก (Protection of records)	✔	✔	✔
1.34 การรักษาความมั่นคงปลอดภัยสำหรับข้อมูลส่วนบุคคล (Privacy and protection of PII)	✔	✔	✔
1.35 การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ (Intellectual property rights)	✔	✔	✔

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
1.36 การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานสำหรับความมั่นคงปลอดภัยสารสนเทศ (Compliance with policies, rules and standards for information security)	✔	✔	✔
1.37 เอกสารขั้นตอนการปฏิบัติงาน (Documented operating procedures)	✔	✔	✔
2.1 การคัดกรอง (Screening)	✔		✔
2.2 ข้อตกลงและเงื่อนไขการจ้างงาน (Terms and conditions of employment)	✔		✔
2.3 การสร้างความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศข้อกำหนด (Information security awareness, education and training)	✔		✔
2.4 กระบวนการทางวินัย (Disciplinary process)	✔	✔	✔
2.5 ความรับผิดชอบหลังจากการสิ้นสุดหรือเปลี่ยนแปลงการจ้างงาน (Responsibilities after termination or change of employment)	✔	✔	✔
2.6 ข้อตกลงการรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or non-disclosure agreements)	✔	✔	✔
2.7 การปฏิบัติงานจากระยะไกล (Remote working)	✔	✔	✔
2.8 การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information security event reporting)	✔	✔	✔
3.1 ขอบเขตความมั่นคงปลอดภัยทางกายภาพ (Physical security perimeters)	✔		✔
3.2 การเข้า-ออกพื้นที่ทางกายภาพ (Physical entry)	✔		✔

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
3.3 การรักษาความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก (Securing offices, rooms and facilities)	✓		✓
3.4 การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ (Physical security monitoring)	✓		✓
3.5 การป้องกันภัยคุกคามทางกายภาพและสิ่งแวดล้อม (Protecting against physical and environmental threats)	✓		✓
3.6 การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย (Working in secure areas)	✓	✓	✓
3.7 การจัดเก็บโต๊ะทำงานและการจัดการหน้าจอ (Clear desk and clear screen)	✓	✓	✓
3.8 การจัดวางและการป้องกันอุปกรณ์ (Equipment siting and protection)	✓		✓
3.9 ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสถานที่ (Security of assets off - premises)	✓		✓
3.10 สื่อบันทึกข้อมูล (Storage media)	✓	✓	✓
3.11 ระบบสาธารณูปโภคที่สนับสนุน (Supporting utilities)	✓	✓	✓
3.12 การรักษาความมั่นคงปลอดภัยของการเดินสาย (Cabling security)	✓		✓
3.13 การบำรุงรักษาอุปกรณ์ (Equipment maintenance)	✓		✓
3.14 การกำจัดหรือการนำอุปกรณ์กลับมาใช้ใหม่อย่างมั่นคงปลอดภัย (Secure disposal or re-use of equipment)	✓		✓
4.1 อุปกรณ์ของผู้ใช้งาน (User endpoint devices)	✓	✓	✓

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
4.2 สิทธิพิเศษในการเข้าถึงสารสนเทศ (Privileged access rights)	✔	✔	✔
4.3 การจำกัดการเข้าถึงระบบสารสนเทศ (Information access restriction)	✔	✔	✔
4.4 การเข้าถึงซอร์สโค้ด (Access to source code)	✔	✔	✔
4.5 การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย (Secure authentication)	✔	✔	✔
4.6 การบริหารจัดการขีดความสามารถของทรัพยากร (Capacity management)	✔	✔	✔
4.7 การป้องกันโปรแกรมไม่พึงประสงค์ (Protection against malware)	✔	✔	✔
4.8 การบริหารจัดการช่องโหว่ทางเทคนิค (Management of technical vulnerabilities)	✔	✔	✔
4.9 การบริหารจัดการ การกำหนดค่า (Configuration Management)	✔	✔	✔
4.10 การลบข้อมูล (Information deletion)	✔	✔	✔
4.11 การซ่อนข้อมูล (Data masking)	✔	✔	✔
4.12 การป้องกันการรั่วไหลของข้อมูล (Data Leakage Prevention)	✔	✔	✔
4.13 การสำรองข้อมูล (Information backup)	✔	✔	✔
4.14 ระบบทดแทน (Redundancy of information processing facilities)	✔	✔	✔

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
4.15 การลงบันทึกเหตุการณ์ (Logging)	✔	✔	✔
4.16 กิจกรรมการเฝ้าติดตาม (Monitoring Activities)	✔	✔	✔
4.17 การตั้งค่านาฬิกาและเวลาให้ตรงกัน (Clock synchronization)	✔	✔	✔
4.18 การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ (Use of privileged utility programs)	✔		✔
4.19 การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of software on operational systems)	✔		✔
4.20 ความมั่นคงปลอดภัยของเครือข่าย (Networks security)	✔	✔	✔
4.21 ความมั่นคงปลอดภัยของบริการเครือข่าย (Security of network services)	✔	✔	✔
4.22 การแบ่งแยกเครือข่าย (Segregation of networks)	✔	✔	✔
4.23 การกรองเว็บ (Web filtering)	✔	✔	✔
4.24 การเข้ารหัสข้อมูล (Use of cryptography)	✔	✔	✔
4.25 วงจรการพัฒนาระบบสารสนเทศอย่างมั่นคงปลอดภัย (Secure development life cycle)	✔	✔	✔
4.26 ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน (Application security requirements)	✔	✔	✔

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แนวปฏิบัติ	ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี)	ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้	ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน
4.27 สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย (Secure system architecture and engineering principles)	✔	✔	✔
4.28 การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย (Secure Coding)	✔	✔	✔
4.29 การทดสอบความมั่นคงปลอดภัยในการพัฒนาระบบและการยอมรับ (Security testing in development and acceptance)	✔	✔	✔
4.30 การพัฒนาโดยหน่วยงานภายนอก (Outsourced development)	✔	✔	✔
4.31 การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง (Separation of development, test and production environments)	✔	✔	✔
4.32 การบริหารจัดการ การเปลี่ยนแปลง (Change management)	✔	✔	✔
4.33 ข้อมูลในการทดสอบ (Test information)	✔	✔	✔
4.34 การป้องกันระบบสารสนเทศระหว่างการตรวจประเมิน (Protection of information systems during audit testing)	✔	✔	✔

ตารางที่ 8-3 ความเชื่อมโยงระหว่างแนวปฏิบัติ และยุทธศาสตร์ในแผนที่นำทาง (Road Map)

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

8.4 การตอบสนองของแผนฯ ต่อการประเมินการปรับเปลี่ยนหน่วยงานไปสู่ความเป็นดิจิทัลในระบบการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร.



รูปที่ 8-1: กรอบแนวทางการประเมินส่วนราชการฯ ประจำปีงบประมาณ 2567

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนบริหารจัดการความมั่นคงปลอดภัยฯ ของ สคทช.	ระบบการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร. (ประเด็นที่เกี่ยวข้อง)
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	1.1 ตัวชี้วัดตามภารกิจ (Functional KPIs) 2.1 การพัฒนาองค์การสู่ดิจิทัล
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	1.1 ตัวชี้วัดตามภารกิจ (Functional KPIs) 2.1 การพัฒนาองค์การสู่ดิจิทัล
ยุทธศาสตร์ที่ 2 บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	1.1 ตัวชี้วัดตามภารกิจ (Functional KPIs) 1.2 ตัวชี้วัดขับเคลื่อนการบูรณาการร่วมกัน (Joint KPIs)
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	1.1 ตัวชี้วัดตามภารกิจ (Functional KPIs) 2.1 การพัฒนาองค์การสู่ดิจิทัล
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **ยุทธศาสตร์ที่ 3** เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	1.1 ตัวชี้วัดตามภารกิจ (Functional KPIs) 2.1 การพัฒนาองค์การสู่ดิจิทัล 2.2 การประเมินสถานะของหน่วยงานในการเป็นระบบราชการ 4.0 (PMQA 4.0)

ตารางที่ 8-4 ความสอดคล้องของแผนกับการประเมินส่วนราชการตามมาตรการปรับปรุงประสิทธิภาพในการปฏิบัติราชการของส่วนราชการของ ก.พ.ร.

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

8.5 การตอบสนองของแผนฯ ต่อการสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร.

แผนบริหารจัดการความมั่นคงปลอดภัยฯ ของ สคทช.	การสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. (ประเด็นที่เกี่ยวข้อง)
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **ยุทธศาสตร์ที่ 3** เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	**2. กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)** 2.1 Data Governance สำรวจการดำเนินการและปฏิบัติการด้านธรรมาภิบาลข้อมูลภาครัฐ 2.2 Open Data & Sharable Data สำรวจการดำเนินการและปฏิบัติการด้านข้อมูลเปิดภาครัฐและด้านการแลกเปลี่ยนข้อมูล 2.3 Data Privacy สำรวจการดำเนินการและปฏิบัติการด้านการคุ้มครองข้อมูลส่วนบุคคล **5. การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)** 5.1 Integrated Enterprise สำรวจการนำระบบเทคโนโลยีดิจิทัลมาบริหารงานในหน่วยงานและการเชื่อมโยงกับระบบอื่น 5.2 Process Optimization สำรวจประสิทธิภาพของกระบวนการทำงานด้วยการนำเทคโนโลยีดิจิทัลและแพลตฟอร์มมาประยุกต์ใช้ 5.2.1 Administration สำรวจการนำเทคโนโลยีดิจิทัลมาเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร 5.2.2 Platform for Communication and Collaboration)สำรวจกระบวนการติดต่อสื่อสาร การทำงานระหว่างหน่วยงานภายในองค์กรและข้ามองค์กร
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities)	**3. ศักยภาพเจ้าหน้าที่ภาครัฐด้านดิจิทัล (Digital Capability)** 3.1 Digital Leadership สำรวจบทบาทความเป็นผู้นำในการริเริ่มปรับเปลี่ยนหน่วยงานสู่การเป็นรัฐบาลดิจิทัลของ DCIO 3.2 Training and Development สำรวจการส่งเสริมให้ความรู้ การอบรมและพัฒนาบุคลากรและการวัดผลด้านทักษะดิจิทัล

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนบริหารจัดการความมั่นคงปลอดภัยฯ ของ สคทช.	การสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. (ประเด็นที่เกี่ยวข้อง)
	3.3 Digital Competency สำรวจผลการประเมินระดับทักษะ ความสามารถและความเข้าใจเทคโนโลยีดิจิทัลของบุคลากรในหน่วยงาน **4. บริการภาครัฐ (Public Services)** 4.1 Service Provision 4.1.1 Digital Service Facilitation สำรวจการอำนวยความสะดวกของการให้บริการภาครัฐในรูปแบบดิจิทัล 4.1.2 Paperless Service สำรวจการให้บริการภาครัฐโดยไม่จำเป็นต้องเรียกสำเนาเอกสาร 4.1.3 Digital Service for the Vulnerable สำรวจการให้บริการภาครัฐในรูปแบบดิจิทัลแก่ผู้รับบริการกลุ่มเปราะบาง 4.2 Promotion for Digital Service Usage สำรวจการส่งเสริมให้ใช้บริการของหน่วยงานภาครัฐผ่านช่องทางดิจิทัล 4.3 Customer Experience (Usability) สำรวจประสบการณ์ของผู้เข้าใช้งานเว็บไซต์ของหน่วยงาน 4.4 Public Participation สำรวจการสร้างการมีส่วนร่วมของผู้รับบริการโดยนำเทคโนโลยีดิจิทัลมาใช้ ในการให้ข้อมูลข่าวสาร การปรึกษาหารือ รับฟังความคิดเห็น การเสนอทางเลือกและร่วมตัดสินใจเกี่ยวกับนโยบายและการบริการจากภาครัฐ 4.4.1 e-Information สำรวจการเปิดโอกาสให้ผู้รับบริการรับข้อมูลข่าวสารและมีช่องทางการเข้าถึงข้อมูลข่าวสารผ่านช่องทางอิเล็กทรอนิกส์ 4.4.2 e-Consultation สำรวจการเปิดโอกาสให้ผู้รับบริการเข้ามามีส่วนร่วมโดยนำเทคโนโลยีดิจิทัลมาใช้ เพื่อให้สามารถแสดงความคิดเห็นเกี่ยวกับนโยบายหรือการบริการจากภาครัฐ

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนบริหารจัดการความมั่นคงปลอดภัยฯ ของ สคทช.	การสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. (ประเด็นที่เกี่ยวข้อง)
	4.4.3 e-Decision Making สำรวจการเปิดโอกาสให้ผู้รับบริการเข้ามามีส่วนร่วม โดยนำเทคโนโลยีดิจิทัลมาใช้เพื่อให้ประชาชนสามารถเสนอทางเลือกและร่วมตัดสินใจเกี่ยวกับนโยบายหรือการบริการจากภาครัฐ **7. เทคโนโลยีดิจิทัลและการนำไปใช้ (Digital Technology Practices)** 7.1 Digital Technology Practices สำรวจการใช้ประโยชน์จากเทคโนโลยีที่เกิดขึ้นใหม่
ยุทธศาสตร์ที่ 2 พัฒนาความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	**2. กระบวนการพัฒนาด้วยข้อมูล (Data-driven Practices)** 2.1 Data Governance สำรวจการดำเนินการและปฏิบัติการด้านธรรมาภิบาลข้อมูลภาครัฐ 2.2 Open Data & Sharable Data สำรวจการดำเนินการและปฏิบัติการด้านข้อมูลเปิดภาครัฐและด้านการแลกเปลี่ยนข้อมูล **5. การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)** 5.2 Process Optimization สำรวจประสิทธิภาพของกระบวนการทำงานด้วยการนำเทคโนโลยีดิจิทัลและแพลตฟอร์มมาประยุกต์ใช้ 5.2.2 Platform for Communication and Collaboration) สำรวจกระบวนการติดต่อสื่อสาร การทำงานระหว่างหน่วยงานภายในองค์กรและข้ามองค์กร
ยุทธศาสตร์ที่ 1 พัฒนาความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ (บุคลากร องค์ความรู้ และเทคโนโลยี) (Integrating cybersecurity capabilities) **ยุทธศาสตร์ที่ 2** บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์และฟื้นคืนสู่สภาพปกติได้ (Partnership)	**5. การบริหารจัดการรูปแบบดิจิทัล (Smart Back Office)** 5.1 Integrated Enterprise สำรวจการนำระบบเทคโนโลยีดิจิทัลมาบริหารงานในหน่วยงาน และการเชื่อมโยงกับระบบอื่น 5.2 Process Optimization สำรวจประสิทธิภาพของกระบวนการทำงานด้วยการนำเทคโนโลยีดิจิทัลและแพลตฟอร์มมาประยุกต์ใช้ 5.2.1 Administration สำรวจการนำเทคโนโลยีดิจิทัลมาเพิ่มประสิทธิภาพในการบริหารจัดการภายในองค์กร

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

แผนบริหารจัดการความมั่นคงปลอดภัยฯ ของ สคทช.	การสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร. (ประเด็นที่เกี่ยวข้อง)
	5.2.2 Platform for Communication and Collaboration) สำรวจกระบวนการติดต่อสื่อสาร การทำงานระหว่างหน่วยงานภายในองค์กรและข้ามองค์กร **6. โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)** 6.1 Reliable Infrastructure สำรวจการนำโครงสร้างพื้นฐานกลางภาครัฐที่มีเสถียรภาพและมีประสิทธิภาพมาปรับใช้ในหน่วยงาน
ยุทธศาสตร์ที่ 3 เสริมสร้างศักยภาพหน่วยงานให้มีคุณภาพและมาตรฐาน (Standard)	**1. แนวนโยบายและหลักปฏิบัติ (Policies & Practices)** 1.1 Digital Policy สำรวจความสอดคล้องของการจัดทำแผนปฏิบัติการหรือแผนงานของหน่วยงาน ที่สอดคล้องกับแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย พ.ศ. 2566 - 2570 1.2 Cyber Security Policy สำรวจการดำเนินการที่สอดคล้องกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และกฎหมายลำดับรองที่เกี่ยวของ 1.3 Legal & Regulatory Mechanism สำรวจการดำเนินการตามกฎหมายที่เกี่ยวข้อง และการปฏิบัติตามพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. 2565 1.4 Data Policy สำรวจการจัดทำแผนปฏิบัติการหรือแผนงานสำหรับ ธรรมาภิบาลข้อมูลภาครัฐ (Data Governance) การเปิดเผยข้อมูล (Open Data) และ การคุ้มครองข้อมูลส่วนบุคคล (PDPA) **6. โครงสร้างพื้นฐานความมั่นคงปลอดภัยและมีประสิทธิภาพ (Secure and Efficient Infrastructure)** 6.2 Cybersecurity (Cybersecurity Standard and Procedure) สำรวจการมีมาตรฐานและแนวทางในการดำเนินการด้านความมั่นคงปลอดภัยทางไซเบอร์

ตารางที่ 8-5 การตอบสนองของแผนฯ ต่อการสำรวจระดับความพร้อมรัฐบาลดิจิทัลหน่วยงานภาครัฐของประเทศไทยของ สพร.

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน

8.6 แบบฟอร์มการวัดผลตัวชี้วัด

- **ช่วงเวลาที่มีการวัดผล**
- **ผู้วัดผล**
- **ผู้วิเคราะห์**

ชื่อ ตัวชี้วัด	ขอบเขต	ข้อมูลนำเข้า	การคำนวณ	ค่าเป้าหมาย	ค่าที่ได้	ข้อเสนอแนะในการปรับปรุง

ตารางที่ 8-6 แบบฟอร์มการวัดผลตัวชี้วัด

เอกสารฉบับนี้เป็นเอกสารที่ใช้ภายใน สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ เท่านั้น ห้ามทำการเผยแพร่ส่วนหนึ่งส่วนใดโดยไม่ได้รับการอนุญาตเป็นลายลักษณ์อักษรจากหน่วยงานเจ้าของเอกสาร ผู้ฝ่าฝืนจะถูกดำเนินการตามระเบียบคำสั่งของสำนักงาน



สำนักงานคณะกรรมการนโยบายที่ดินแห่งชาติ
Office of the National Land Policy Board

สำนักงานชั่วคราว สคทช.
อาคารอารีย์ ฮิลส์ ชั้น 19-20
เลขที่ 428 ถนนพหลโยธิน แขวงสามเสนใน เขตพญาไท
กรุงเทพฯ 10400

โทรศัพท์ 0 2265 5400
โทรสาร 0 2265 5401
อีเมล saraban@onlb.go.th