



ประกาศ สำนักงานกิจการยุติธรรม
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานกิจการยุติธรรม
พ.ศ. ๒๕๖๗

เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานกิจการยุติธรรม เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยเร็วและเพื่อให้มาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานกิจการยุติธรรมเกิดความชัดเจน เป็นไปในทิศทางเดียวกัน และสอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๒๑ (๑) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ประกอบมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำนักงานกิจการยุติธรรมจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศสำนักงานกิจการยุติธรรม เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานกิจการยุติธรรมได้กำหนดขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

๓.๑ เพื่อให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานกิจการยุติธรรม

๓.๒ เพื่อใช้เป็นกรอบมาตรฐานและแนวปฏิบัติในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้กับสำนักงานกิจการยุติธรรม

๓.๓ เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนร่วมรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานกิจการยุติธรรม

๓.๔ เพื่อให้บุคลากรของสำนักงานกิจการยุติธรรม บุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงานกิจการยุติธรรม ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

๓.๕ เพื่อติดตามการดำเนินงานและทบทวนประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับสภาพแวดล้อม และกฎหมายที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานกิจการยุติธรรมถือปฏิบัติตามที่ได้มีการแก้ไข หรือเพิ่มเติม นั้น

ข้อ ๕ ให้ใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๘ เดือน พฤศจิกายน พ.ศ. ๒๕๖๗

พันตำรวจโท



(พงษ์ธร ชาญสิริ)

ผู้อำนวยการสำนักงานกิจการยุติธรรม



บัญชีแนบท้ายประกาศสำนักงานกิจการยุติธรรม
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานกิจการยุติธรรม
พ.ศ. ๒๕๖๗

สารบัญ

หน้า

๑. บทนำ.....	๑
๒. วัตถุประสงค์.....	๑
๓. ขอบเขตการใช้.....	๑
๔. คำนิยาม.....	๑
๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานกิจการยุติธรรม มี ๒ ส่วน ดังนี้.....	๓
ส่วนที่ ๑_ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์.....	๓
๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์.....	๓
๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์.....	๓
๓. แผนการรับมือภัยคุกคามทางไซเบอร์.....	๔
๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์.....	๕
ส่วนที่ ๒_กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์.....	๖
หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify).....	๖
๑.๑ การจัดการทรัพย์สิน (Asset Management).....	๖
๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy).....	๖
๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing).....	๗
๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management).....	๘
หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect).....	๘
๒.๑ การควบคุมการเข้าถึง (Access Control).....	๘
๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening).....	๙
๒.๓ การเชื่อมต่อระยะไกล (Remote Control).....	๑๐
๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media).....	๑๐
๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness).....	๑๐
๒.๖ การแบ่งปันข้อมูล (Information Sharing).....	๑๑
หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect).....	๑๑
หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond).....	๑๑

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)	๑๑
๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	๑๑
หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)	๑๒
๕.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP).....	๑๒
๕.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม (Business Continuity Plan : BCP).....	๑๓
๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident).....	๑๓

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๗

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานกิจการยุติธรรม สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

๓. ขอบเขตการใช้

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้มีผลบังคับใช้ครอบคลุมข้อมูล และระบบสารสนเทศของสำนักงานกิจการยุติธรรม

๔. คำนิยาม

๑. หน่วยงาน	หมายถึง	สำนักงานกิจการยุติธรรม กระทรวงยุติธรรม
๒. ผู้บังคับบัญชา	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสำนักงานกิจการยุติธรรม
๓. คณะอนุกรรมการ	หมายถึง	คณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม
๔. คณะบริหารจัดการความปลอดภัยด้านสารสนเทศ (ISMS Committee) ของสำนักงานกิจการยุติธรรม	หมายถึง	คณะบุคคลที่สำนักงานกิจการยุติธรรมแต่งตั้งให้ทำหน้าที่จะยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยข้อมูลของศูนย์แลกเปลี่ยนข้อมูลกระบวนการยุติธรรม (Data Exchange Center : DXC) ให้สอดคล้องกับการรับรองมาตรฐาน ISO 27001:2022 ตามมาตรฐานสากล ซึ่งเป็นการบริหารจัดการความมั่นคงปลอดภัยของข้อมูล (Data Security) ที่เน้นความสำคัญในเรื่องระบบการบริหารจัดการ เพื่อปกป้องข้อมูล ควบคุมการ

			ทำงาน และการบริหารจัดการทรัพยากรด้านสารสนเทศที่สำคัญให้ปลอดภัยจากภัยคุกคาม และความเสี่ยงในรูปแบบต่าง ๆ
๕.	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (Department Chief Information Officer : DCIO)	หมายถึง	ผู้บริหารสำนักงานกิจการยุติธรรมที่ได้รับมอบหมาย ซึ่งมีหน้าที่รับผิดชอบการกำหนดนโยบายและมาตรฐานการควบคุมดูแลการใช้งานและพัฒนาระบบเทคโนโลยีสารสนเทศของสำนักงานกิจการยุติธรรม
๖.	ศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ (ศอช.)	หมายถึง	กลุ่มศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ (ศอช.) ซึ่งเป็นหน่วยงานให้บริการเทคโนโลยีสารสนเทศให้คำปรึกษา พัฒนาปรับปรุง และบำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายภายในสำนักงานกิจการยุติธรรม
๗.	ผู้อำนวยการกองนโยบายและประสานแผนกระบวนการยุติธรรม (Director, Division of Justice Policy and Planning Coordination)	หมายถึง	ผู้บังคับบัญชาสูงสุดของกลุ่มศูนย์พยากรณ์สถานการณ์อาชญากรรมแห่งชาติ (ศอช.) รับผิดชอบกำกับดูแลการปฏิบัติงานของบุคลากร ตลอดจนทบทวนวางแผนบริหารจัดการความเสี่ยงระบบเทคโนโลยีสารสนเทศ
๘.	ผู้ใช้งาน	หมายถึง	บุคลากรของสำนักงานกิจการยุติธรรม ที่ได้รับอนุญาต (Authorized user) ให้สามารถใช้งานระบบเทคโนโลยีสารสนเทศ โดยมีสิทธิ์ และหน้าที่ขึ้นอยู่กับบทบาทความรับผิดชอบ (Role)
๙.	ผู้ให้บริการภายนอก	หมายถึง	องค์กร หรือหน่วยงาน หรือผู้มาติดต่อจากภายนอกที่สำนักงานกิจการยุติธรรมอนุญาตให้มีสิทธิ์ในการเข้าถึง และใช้งานระบบ หรือทรัพย์สินต่าง ๆ ของสำนักงานกิจการยุติธรรม โดยจะได้รับสิทธิ์ในการใช้ เข้าถึง และใช้งานสารสนเทศตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัยของสารสนเทศ และความลับของข้อมูล
๑๐.	คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๑๑.	แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

๑๒. Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๑๓. Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๔. Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๑๕. Business Continuity Plan (BCP)	หมายถึง	แผนบริหารความต่อเนื่องทางธุรกิจ

๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานกิจการยุติธรรม มี ๒ ส่วน ดังนี้

ส่วนที่ ๑

ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑ หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน

๑.๒ หน่วยงานต้องจัดส่งรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก มายังคณะกรรมการ ภายในสามสิบ (๓๐) วันนับถัดจากวันที่ได้รับรายงานการตรวจสอบ

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยต้องจัดให้มีการประเมินความ

เสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการ ตามรอบการประชุมของคณะกรรมการ

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

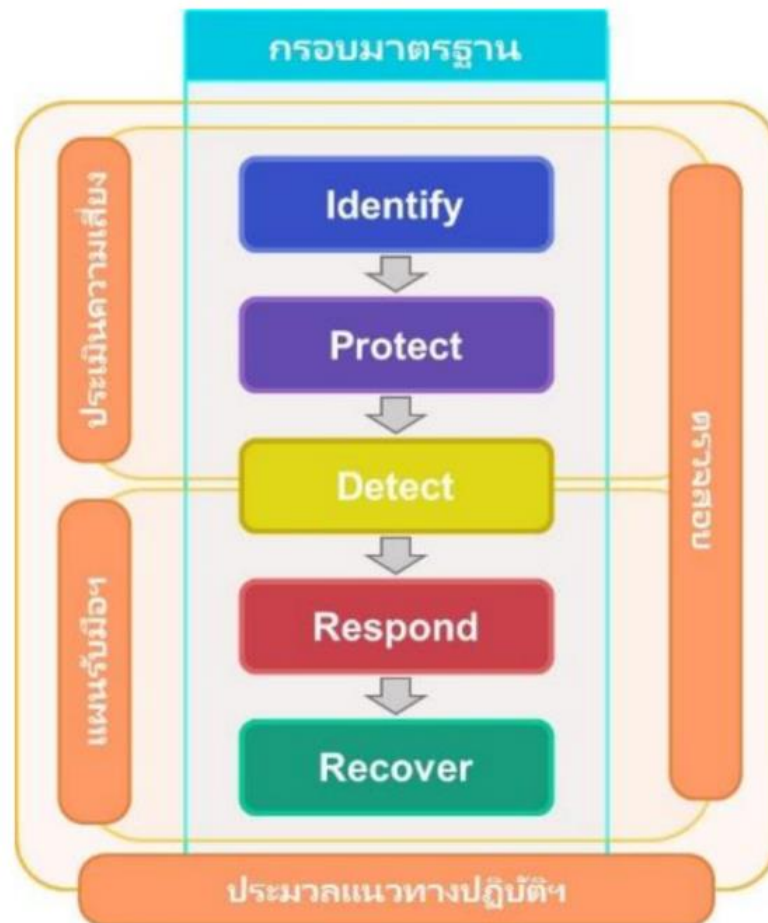
๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากร ที่เกี่ยวข้อง

๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๓.๕ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนด ในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๖ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์มายังคณะกรรมการอย่างน้อยดังนี้

- ๔.๑ แผนนโยบายหรือแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการ ในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)
- ๔.๓ การดำเนินการเพื่อให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)
- ๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)
- ๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์
- ๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๒

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมั่นคงปลอดภัยทางไซเบอร์

๑.๑.๑ หน่วยงานต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สิน ให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

- ๑) ชื่อ/คำอธิบายของทรัพย์สิน
- ๒) ประเภทของอุปกรณ์/ยี่ห้อ
- ๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
- ๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชัน
- ๕) การระบุลำดับความสำคัญของทรัพย์สิน
- ๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน
- ๗) ตำแหน่งทางกายภาพของทรัพย์สิน
- ๘) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ หน่วยงานต้องมีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ในระบบสารสนเทศโดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย

๑.๑.๓ หน่วยงานต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ หน่วยงานต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๕ หน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๑.๖ หน่วยงานต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของหน่วยงานและปรับปรุงให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

การประเมินความเสี่ยงด้านความความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน พร้อมทั้งหาแนวทางในการรับมือเพื่อลดความเสียหายที่จะเกิดกับหน่วยงาน

๑.๒.๑ หน่วยงานต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

- ๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง

- ๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)
- ๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
- ๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

๑.๒.๒ หน่วยงานต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- ๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- ๒) คำอธิบายของความเสี่ยง (Description of the Risk)
- ๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- ๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- ๕) การจัดการความเสี่ยง (Risk Treatment)
- ๖) เจ้าของความเสี่ยง (Risk Owner)
- ๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
- ๘) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

เป็นการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ครอบคลุมทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานทราบถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน

๑.๓.๑ หน่วยงานต้องดำเนินการประเมินช่องโหว่ของอุปกรณ์ของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงาน ซึ่งเป็น

- ๑) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
- ๒) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System : ICS)

๑.๓.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

- ๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- ๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
- ๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ หน่วยงานต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานโดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology : IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๕ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชัน ของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่อ อินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๖ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการ ที่สำคัญของหน่วยงาน ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูล จากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก

๑.๔.๑ หน่วยงานต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแล รักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตาม ในส่วนของบริการที่สำคัญของหน่วยงาน

๑.๔.๒ หน่วยงานต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการ ของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญา กับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

- ๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงาน ตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๒) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องบริการที่สำคัญของหน่วยงาน จากภัยคุกคามทางไซเบอร์
- ๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
- ๔) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ หน่วยงานควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอก ว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ หน่วยงานควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้นสำหรับบุคคลภายนอก ในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๑ หน่วยงานต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย อย่างน้อยดังนี้

- ๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
- ๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

- ๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย
- ๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน
- ๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ หน่วยงานต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ หน่วยงานต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิกคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น

๒.๑.๕ หน่วยงานต้องเก็บรักษานบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายาม ทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๖ ในการเข้าถึงระบบสารสนเทศของหน่วยงานต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ หน่วยงานต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงาน

๒.๒.๒ หน่วยงานต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อย ดังต่อไปนี้

- ๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- ๒) การแบ่งแยกหน้าที่ (Separation of Duties)
- ๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- ๔) การลบบัญชีที่ไม่ได้ใช้
- ๕) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
- ๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- ๗) การป้องกันมัลแวร์ (Malware)
- ๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ อย่างทันการณ์และเหมาะสม

๒.๒.๓ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๒.๒.๔ หน่วยงานต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ หน่วยงานต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาต และตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๒.๓ การเชื่อมต่อระยะไกล (Remote Control)

๒.๓.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

- ๑) เปิดใช้งานการเชื่อมต่อไคลเอนต์ระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น
- ๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)
- ๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)
- ๔) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication), กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานกิจการยุติธรรม หรืออย่างสม่ำเสมอ
- ๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น HTTPS, SSH, SCP เป็นต้น
- ๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการทำงานของบริการที่สำคัญของหน่วยงานวันแต่จะได้รับอนุญาต
- ๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของหน่วยงานโดยใช้มาตรการอย่างน้อย ดังนี้

- ๑) ในกรณีที่ฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ๒) ใช้สื่อบันทึกข้อมูลที่ได้รับการอนุญาตเท่านั้น
- ๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

๒.๔.๒ หน่วยงานต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ หน่วยงานต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ หน่วยงานต้องเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติ ให้กับผู้ใช้งานในลักษณะกระตือรือร้น หรือขอระงับในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๕.๒ หน่วยงานต้องจัดทำ ปรับปรุง คู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๒.๕.๓ หน่วยงานต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุง และเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒.๕.๔ หน่วยงานต้องสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ

๒.๕.๕ หน่วยงานควรจัดให้มีการฝึกอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุม และเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ กับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ โดยต้องรายงานต่อคณะกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ กระทรวงยุติธรรม

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้เครื่องคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้ โดยหน่วยงานต้องมีกระบวนการในการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ มีกระบวนการในการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่ตรวจพบ

๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

๓.๔ ต้องดำเนินการตรวจสอบกลไก และกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องมีการจัดทำเอกสาร สื่อสาร ฝึกอบรม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ หน่วยงานต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ หน่วยงานต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิภาพ ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

๕.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

เพื่อให้แน่ใจว่า บริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจาก เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้อย่างมีประสิทธิภาพ เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตค่านิยามและการกำหนดระยะเวลา ที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อยดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ ของการหยุดชะงักลำดับความสำคัญในการกู้คืนระบบ

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่องมีการควบคุมดูแลการแก้ไขและกู้คืนระบบ เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๕.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม (Business Continuity Plan : BCP)

อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของ (Business Continuity Plan : BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

หน่วยงานต้องจัดทำรายงาน ภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการ ให้คณะอนุกรรมการทราบทุกระยะ

ประกาศสำนักงานกิจการยุติธรรม
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๗

เอกสารอ้างอิง

- พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- (ร่าง) นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๔)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๐)
- (ร่าง) ประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เรื่อง กรอบการบริหารความเสี่ยงด้านไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ (NIST ๘๐๐-๓๗)
- ประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖
- ประกาศ สำนักงานกิจการยุติธรรม เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานกิจการยุติธรรม พ.ศ. ๒๕๖๕