กรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของศูนย์คุณธรรม

กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ
สำนักพัฒนาองค์ความรู้ นวัตกรรมและสื่อสารสนเทศ
ศูนย์คุณธรรม

สารบัญ

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของศูนย์คุณธรรม

๑. หลักการและเหตุผล

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์คุณธรรม เป็นไปในทิศทางเดียวกัน มีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล ศูนย์คุณธรรมจึงเห็นควรกำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีวัตถุประสงค์ ดังนี้

๑.๑ เพื่อให้ผู้บริหาร เจ้าหน้าที่ บุคลากร และผู้รับบริการสามารถใช้งานระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศ ได้อย่างมั่นคงปลอดภัย รวมไปถึงสามารถบรรลุผลเป้าหมายตามภารกิจของศูนย์คุณธรรมได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ กำหนดขอบเขตด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยอ้างอิงตามมาตรฐานสากล ISO/IEC ๒๗๐๐๑, พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๑.๓ เพื่อกำหนดแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ หรือบุคลากรภายในศูนย์คุณธรรม ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยไซเบอร์ และปฏิบัติตามอย่างเคร่งครัด

๑.๔ เพื่อเป็นการป้องกันไม่ให้ระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของศูนย์คุณธรรม โดนบุกรุก ขโมย ทำลาย หรือโจรกรรมในรูปแบบต่าง ๆ ที่อาจจะสร้างความเสียหายต่อภารกิจและการดำเนินงานของศูนย์คุณธรรม

๒. ขอบเขต

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ ครอบคลุมถึงการรักษาความมั่นคงปลอดภัยไซเบอร์ของศูนย์คุณธรรม โดยครอบคลุมถึง

๒.๑ ผู้บริหาร บุคลากร และผู้รับบริการของศูนย์คุณธรรม

๒.๒ บุคลากรภายนอกของศูนย์คุณธรรมที่ได้รับสิทธิเข้าถึงทรัพย์สินที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของศูนย์คุณธรรม

๓. คำนิยาม

๓.๑ ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๓.๒ ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

๓.๓ ระบบเครือข่าย หมายถึง การนำคอมพิวเตอร์หลาย ๆ เครื่องมาต่อพ่วงกัน เพื่อใช้ในการติดต่อสื่อสาร ใช้ข้อมูลร่วมกัน รวมไปถึงการใช้อุปกรณ์ร่วมกัน ทำให้ประหยัดทรัพยากรในการใช้งาน

๓.๔ ระบบสารสนเทศ หมายถึง ชุดขององค์ประกอบที่ทำหน้าที่รวบรวม ประมวลผล จัดเก็บและแจกจ่ายสารสนเทศ เพื่อช่วยการตัดสินใจ และการควบคุมในองค์กร โดยการทำงานของระบบสารสนเทศจะประกอบไปด้วยกิจกรรม ๓ อย่าง ได้แก่ การนำข้อมูลเข้าสู่ระบบ (Input) การประมวลผล (Processing) และการนำเสนอผลลัพธ์ (Output)

๓.๕ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ หมายถึง คอมพิวเตอร์หรือระบบคอมพิวเตอร์ใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยของสาธารณะ ความมั่นคงเศรษฐกิจของประเทศ และโครงสร้างพื้นฐานอันประโยชน์สาธารณะ

๓.๖ บริการที่สำคัญ หมายถึง ภารกิจหรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๗ ดัชนีชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือน เพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

๓.๘ ผู้ให้บริการภายนอก หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศหรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศได้ ทั้งนี้ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๓.๙ การรักษาความมั่นคงปลอดภัยไซเบอร์ หมายถึง มาตรการหรือการดำเนินการที่กำหนดขึ้นเพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ทั้งจากภายในและภายนอกประเทศอันกระทบต่อความมั่นคงของรัฐ ความมั่นคงทางเศรษฐกิจ ความมั่นคงทางทหาร และความสงบเรียบร้อยภายในประเทศ

๓.๑๐ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม

๓.๑๑ คอมไพเลอร์ หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่ง ไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

๓.๑๒ แพตช์ หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update เป็นต้น

๓.๑๒ Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

๓.๑๓ Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

๓.๑๔ Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

๕. หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

หลักการนี้จะช่วยให้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของศูนย์คุณธรรม มีความมั่นคงปลอดภัยจากการถูกโจมตี บุกรุก หรือโจรกรรมจากผู้บุกรุก โดยมีรายละเอียด ดังนี้

ภาพที่ ๑ หลักการปฏิบัติในการรักษาความมั่นคงปลอดภัย (Security Principles)

๔.๑ ความลับ (Confidentiality) การปกป้องความลับของข้อมูล โดยป้องกันการเข้าถึงและการเปิดเผยข้อมูลจากผู้ที่ไม่ได้รับอนุญาต

๔.๒ ความสมบูรณ์ (Integrity) การทำให้มั่นใจว่าข้อมูลต้องไม่มีการแก้ไข ดัดแปลง หรือโดนทำลายโดยผู้ที่ไม่ได้รับอนุญาต

๔.๓ ความพร้อมใช้งาน (Availability) การทำให้มั่นใจว่าผู้ใช้งานที่ได้รับอนุญาตสามารถเข้าถึงข้อมูลและบริการได้อย่างรวดเร็วและเชื่อถือได้

๔.๔ ความรับผิดชอบ (Accountability) การระบุหน้าที่ความรับผิดชอบของแต่ละบุคคล รวมถึงการรับผิดและรับชอบในผลของกระทำตามบทบาทหน้าที่นั้น ๆ

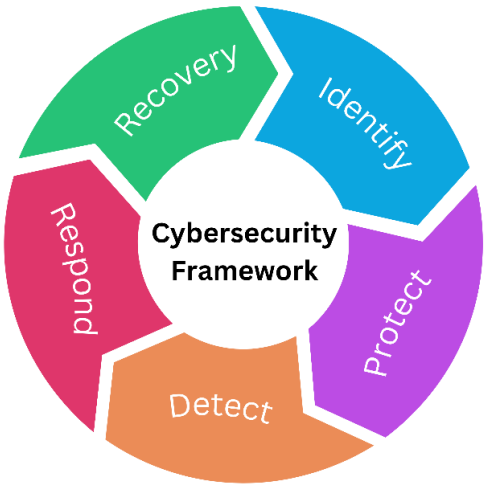
๔.๕ การพิสูจน์ตัวตน (Authentication) การทำให้มั่นใจว่าสิทธิการเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศต้องผ่านกระบวนการยืนยันตัวตนที่สมบูรณ์แล้วเท่านั้น

๔.๖ การกำหนดสิทธิ (Authorization) การทำให้มั่นใจว่าการให้สิทธิเข้าใช้งานระบบคอมพิวเตอร์และข้อมูลสารสนเทศเป็นไปตามความจำเป็น (Least Privilege) และสอดคล้องกับความต้องการพื้นฐาน (Need to Know Basis) ตามที่ได้รับอนุญาต

๔.๗ การห้ามปฏิเสธความรับผิดชอบ (Non-repudiation) เป็นการป้องกันในการสื่อสาร โดยผู้ส่งข้อมูลได้รับหลักฐานว่าได้มีการส่งข้อมูลแล้วและผู้รับก็ได้รับการยืนยันว่าผู้ส่งเป็นใคร ดังนั้นทั้งผู้ส่งและผู้รับจะไม่สามารถปฏิเสธได้ว่าไม่มีความเกี่ยวข้องกับข้อมูลดังกล่าวในภายหลัง

๖. แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ศูนย์คุณธรรม กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ที่ถูกกำหนดโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติสหรัฐ หรือ NIST Cybersecurity Framework (CSF) และจัดทำขึ้นตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ โดยใช้อ้างอิงในการสร้างความมั่นคงปลอดภัยให้กับระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศของสำนักงานปลัดกระทรวงวัฒนธรรม โดยกรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ สามารถสรุปรายละเอียดได้ ดังนี้

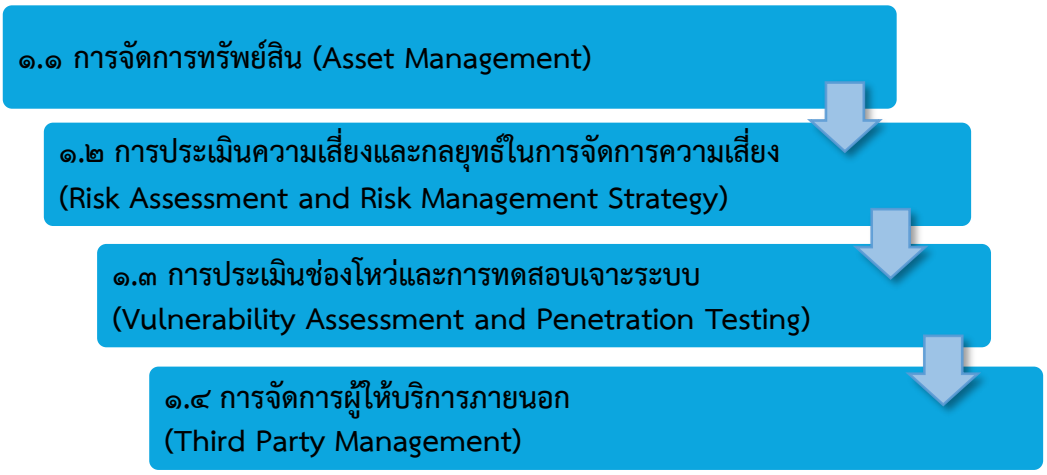


ภาพที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework)

NIST Cybersecurity Framework	ความหมาย
Identify	การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล
Protect	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น
Detect	มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
Respond	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
Respond	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

<u>หัวข้อที่ ๑</u> การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

ซึ่งประกอบไปด้วยกระบวนการดำเนินงาน ๔ ขั้นตอน ดังนี้



ภาพที่ ๓ การระบุความเสี่ยง (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

- ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้
  - (ก) ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ
  - (ข) ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ
  - (ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สิน บริการที่สำคัญ
  - (ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญ
  - (จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ
  - (ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ
- ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)
- ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ
- ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ อย่างน้อยปีละ ๑ ครั้ง

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

- ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง
- ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยทะเบียนความเสี่ยง ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้
  - (ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
  - (ข) คำอธิบายของความเสี่ยง (Description of the Risk)
  - (ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
  - (ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
  - (ฉ) การจัดการความเสี่ยง (Risk Treatment)
  - (ง) เจ้าของความเสี่ยง (Risk Owner)
  - (ฉ) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
  - (ช) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

- ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญ ได้แก่
  - (ก) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
- ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย
  - (ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
  - (ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
  - (ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)
- ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ ซึ่งการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น
- ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย
- ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

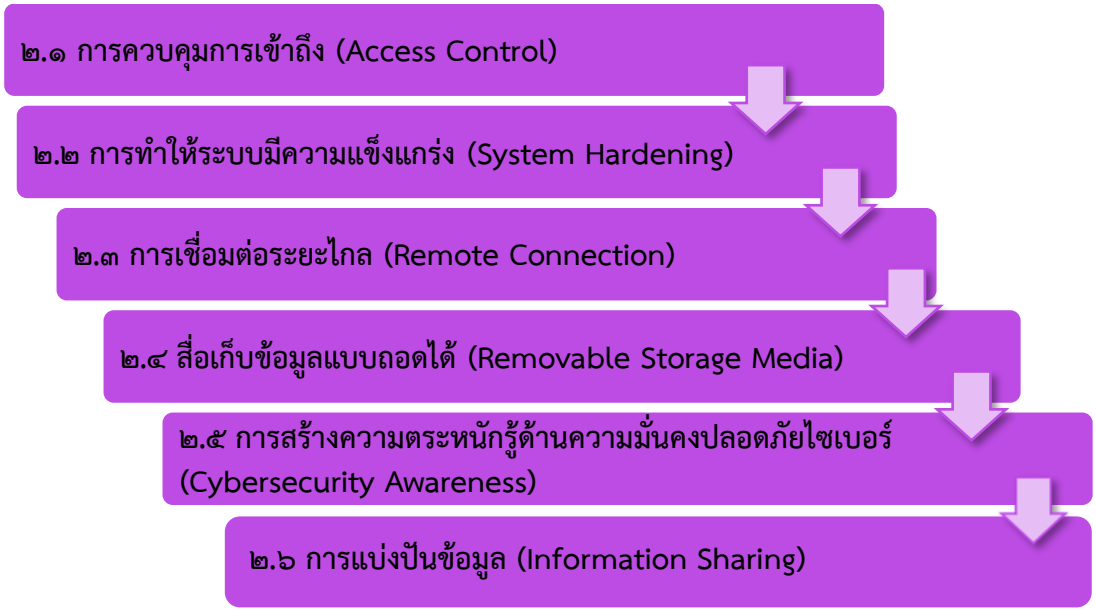
- ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ รวมไปถึงก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยีเป็นต้น
- ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด
- ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงาน
- ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ
- หากได้รับการร้องขอจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติจะต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือด้วย

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

- ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์
- ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้
    (ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญ
    (ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ
    (ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์
    (ง) สิทธิ์ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก
- ควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์
- ควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

<u>หัวข้อที่ ๒</u> มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

ซึ่งประกอบไปด้วยกระบวนการดำเนินงาน ๖ ขั้นตอน ดังนี้



ภาพที่ ๔ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

- ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญจำกัดไว้ที่
  (ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต
  (ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต
- กำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ
- ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว
- ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญและการเข้าถึงทางลอจิคอล (Logical)

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

- ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญ ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ
- มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้
  - (ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
  - (ข) การแบ่งแยกหน้าที่ (Separation of Duties)
  - (ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
  - (ง) การลบบัญชีที่ไม่ได้ใช้
  - (จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น
  - (ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
  - (ช) การป้องกันมัลแวร์ (Malware)
  - (ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch)
- ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ
- ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์
- ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

- ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต
- สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้
  - (ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล
  - (ข) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
  - (ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
  - (ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญหน่วยงานของรัฐ เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ
  - (จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

- ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยใช้มาตรการอย่างน้อย ดังนี้
  (ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
  (ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น
  (ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ
- ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญ บนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

- ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้
  (ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่
    - พนักงานใหม่ (New Employees)
    - ผู้ใช้และระดับบริหาร (Users and Management)
    - เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS
    - ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)
  (ข) การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ
  (ค) การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน
  (ง) การสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ
- ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญ และเจ้าของคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

<u>หัวข้อที่ ๓</u> มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

ซึ่งประกอบไปด้วยกระบวนการดำเนินงาน ๑ ขั้นตอน ดังนี้

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

ภาพที่ ๕ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

- ต้องสร้างกลไกและกระบวนการเพื่อ
  - (ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญ
  - (ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
  - (ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ
- ต้องดำเนินการทบทวนกลไกและกระบวนการอย่างน้อย ปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

<u>หัวข้อที่ ๔</u> มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
ซึ่งประกอบไปด้วยกระบวนการดำเนินงาน ๓ ขั้นตอน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์
(Cybersecurity Incident Response Plan)

๔.๒ แผนการสื่อสารในภาวะวิกฤต
(Crisis Communication Plan)

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์
(Cybersecurity Exercise)

ภาพที่ ๖ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

- ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

- ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีรายละเอียด ดังนี้
  (ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต
  (ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้
  (ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์
  (ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรแถลงกับสื่อมวลชน
  (จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสมสำหรับการเผยแพร่ข้อมูล
- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต
- ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง
- เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

- ศูนย์คุณธรรม ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์หากได้รับคำสั่งเป็นลายลักษณ์อักษร การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์
- ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่ และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญ

<u>หัวข้อที่ ๕</u> มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

ซึ่งประกอบไปด้วยกระบวนการดำเนินงาน ๑ ขั้นตอน ดังนี้

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

ภาพที่ ๗ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

- ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญ สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของศูนย์คุณธรรม เช่น Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น
- ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

เอกสารอ้างอิง

๑. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
Link: https://ncsa.gdcatalog.go.th/dataset/bcd๙๖๒๗๘-๒๔๘b-๔c๓๖-bc๕๖-๒๕๕๑๔๐๒๔๒๑a๗/resource/๖๗c๔๐๑๐a-๕ec๒-๔ff๐-b๒๐๗-ce๔๓d๒๒๙bcb๔/download/๑.-...-.pdf

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
Link: https://www.ncsa.or.th/documents/๒๐๒๒-๑๒-NCSAPDF๐๑.pdf