



ประกาศสำนักงานนโยบายและแผนการขนส่งและจราจร
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เพื่อให้การจัดทำมาตรฐานและแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร เป็นไปอย่างมีประสิทธิภาพ อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ดังนั้น เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ เป็นไปในทิศทางเดียวกัน และสอดคล้องตามมาตรฐานสากล สำนักงานนโยบายและแผนการขนส่งและจราจรจึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานนโยบายและแผนการขนส่งและจราจร เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้มีผลนับตั้งแต่วันที่ลงนามในประกาศ เป็นต้นไป

ข้อ ๓ การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร มีวัตถุประสงค์ ดังต่อไปนี้

๓.๑ เพื่อให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร

๓.๒ เพื่อใช้เป็นกรอบมาตรฐานและแนวปฏิบัติในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและสื่อสารให้กับสำนักงานนโยบายและแผนการขนส่งและจราจร

๓.๓ เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและการสื่อสารของสำนักงานนโยบายและแผนการขนส่งและจราจร

๓.๔ เพื่อติดตามการดำเนินงานและทบทวนประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับสภาพแวดล้อม และกฎหมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานนโยบายและแผนการขนส่งและจราจร ถือปฏิบัติตามที่แก้ไขหรือเพิ่มเติม นั้น

ข้อ ๕ ให้ใช้...

ข้อ ๕ ให้ใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร ตามแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๘ สิงหาคม พ.ศ. ๒๕๖๙



(นายจิรโรจน์ ศุภรัตน์)

ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร



บัญชีแนบท้ายประกาศสำนักงานนโยบายและแผนการขนส่งและจราจร
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
การรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
การรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็วมีประสิทธิภาพ เป็นไปในทิศทางเดียวกัน และสอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ทั้งนี้ เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. มีประสิทธิภาพมากยิ่งขึ้น จึงจำเป็นต้องมีการทบทวนประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ในปี พ.ศ. ๒๕๖๙ ต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อทบทวนประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ให้สอดคล้องกับกฎหมาย และสถานการณ์ทางไซเบอร์ในปัจจุบัน

๒.๒ เพื่อให้การดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล

๓. ขอบเขตการใช้

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้มีผลบังคับใช้ครอบคลุมข้อมูล ระบบคอมพิวเตอร์ และระบบสารสนเทศของ สนข.

๔. คำนิยาม

- ๔.๑ หน่วยงาน หมายถึง สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.)
- ๔.๒ หัวหน้าหน่วยงาน หมายถึง ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร
- ๔.๓ ผู้บริหารด้านไอซีที หมายถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)
- ๔.๔ ผู้ใช้งาน หมายถึง บุคลากรที่ได้รับอนุญาตให้ใช้งานระบบสารสนเทศของหน่วยงาน
- ๔.๕ ผู้ให้บริการภายนอก หมายถึง องค์กร หรือหน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานระบบ หรือทรัพย์สินสารสนเทศต่าง ๆ ของหน่วยงาน ตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความมั่นคงปลอดภัย และความลับของข้อมูล

๔.๖ แพตช์ หมายถึง โปรแกรมที่ใช้ปรับปรุงซอฟต์แวร์ เพื่อเพิ่มเติมความสามารถ หรือปรับปรุงแก้ไข โปรแกรมให้มีประสิทธิภาพมากยิ่งขึ้น รวมถึงปิดช่องโหว่และลดความเสี่ยงที่อาจเกิดภัยคุกคามทางไซเบอร์ให้มีความมั่นคงปลอดภัยมากขึ้น

๔.๗ Recovery Time Objective หมายถึง ระยะเวลาที่กู้คืนระบบ หรือเรียกว่า RTO

๔.๘ Recovery Point Objective หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย หรือเรียกว่า RPO

๔.๙ Maximum Tolerance Period of Disruption หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่อง หรือเรียกว่า MTPD

๔.๑๐ Business Continuity Plan หมายถึง แผนบริหารความต่อเนื่องทางธุรกิจ หรือเรียกว่า BCP

ส่วนที่ ๑

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ดำเนินการ ดังนี้

๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๑.๑.๑ ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) และดูแลรักษาปรับปรุงทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

- ๑) ชื่อหรือคำอธิบายของทรัพย์สิน
- ๒) ประเภทของอุปกรณ์/ยี่ห้อ
- ๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
- ๔) ชื่อระบบปฏิบัติการ (Operating System) และเวอร์ชัน
- ๕) การระบุลำดับความสำคัญของทรัพย์สิน
- ๖) เจ้าของ และ/หรือหน่วยงานเจ้าของทรัพย์สิน
- ๗) ตำแหน่งทางกายภาพของทรัพย์สิน
- ๘) การขึ้นต่อประกันของทรัพย์สิน

๑.๑.๒ ต้องมีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ในระบบสารสนเทศ โดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย

๑.๑.๓ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๕ ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงาน รวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๑.๑ อย่างน้อยปีละ ๑ ครั้ง

๑.๑.๖ ต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของหน่วยงานและปรับปรุงให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน พร้อมทั้งหาแนวทางในการรับมือภัยคุกคามทางไซเบอร์ เพื่อลดความเสียหายที่จะเกิดขึ้น โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๑.๒.๑ ต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

- ๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง
- ๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related Risk)
- ๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้นเพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง
- ๔) กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับการประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดการณ์ได้
- ๕) กำหนดวิธีการหรือเครื่องมือในการบริหารความเสี่ยง และการจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้

๑.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อย ดังนี้

- ๑) วันที่ระบุความเสี่ยง (Risk Identification Date)
- 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) ความเสี่ยงที่เหลืออยู่ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ครอบคลุมทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้ทราบถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศ โดยให้ สนข. ดำเนินการอย่างน้อย ดังนี้

๑.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลเจ้าของผลิตภัณฑ์ หรือแหล่งข้อมูลอื่นที่น่าเชื่อถือ เช่น ศูนย์ประสานการรักษาความปลอดภัยแห่งชาติ (ThaiCERT) หรือสำนักงานพัฒนาธุรกรรมอิเล็กทรอนิกส์ เป็นต้น

๑.๓.๒ ต้องดำเนินการประเมินช่องโหว่บริการสำคัญของหน่วยงาน โดยอ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมระบบเทคโนโลยีสารสนเทศ หรือบริการที่สำคัญของ สนข.

๑.๓.๓ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

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

Review)

๑.๓.๔ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มระบบสารสนเทศ ระบบงานบริการ ระบบแอปพลิเคชัน การปรับปรุงแก้ไขระบบอย่างมีนัยสำคัญ และการปรับเปลี่ยนด้านเทคโนโลยี

๑.๓.๕ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานโดยเฉพาะอย่างยิ่ง คือ ระบบเทคโนโลยีสารสนเทศ (Information Technology) ที่เชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๖ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๗ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงาน ก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๓.๘ การทดสอบเจาะระบบและการให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรองและได้รับประกาศนียบัตร (Accreditation and Certifications) ที่เป็นที่ยอมรับระดับสากล และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

๑.๓.๙ การทดสอบการเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การกำกับดูแลของ สนข.

๑.๓.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤตและระดับสูง

ทั้งนี้ สนข. กำหนดให้ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) จัดให้มีการตรวจประเมินช่องโหว่และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบสารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบต้องดำเนินการแก้ไขให้แล้วเสร็จโดยไม่ชักช้า หรือไม่เกินกว่า ๗ วัน นับถัดจากวันที่ได้รับแจ้งจาก ศทท. พร้อมทั้งรายงานผลการแก้ไขกลับมายัง ศทท. เพื่อทราบและดำเนินการตรวจสอบผลการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นที่อาจแก้ไขได้หรือไม่อาจปิดช่องโหว่ได้ พร้อมกำหนดมาตรการขดเซยหรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่ทางเทคนิคนั้น หรือในกรณีที่มีความจำเป็นอาจต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร หรือผู้ที่ได้รับมอบหมายเป็นผู้พิจารณาและให้ความเห็นชอบ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการเชื่อมต่อหรือเข้าถึงข้อมูลจากบุคคลภายนอก ประกอบด้วย การกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริษัทที่สำคัญของ สนข.

๑.๔.๒ ต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริษัทที่สำคัญของหน่วยงานตามความต้องการทางธุรกิจขององค์กร และลักษณะความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)

๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคามทางไซเบอร์

๓) ความเสี่ยงที่เกี่ยวข้องกับบริการ และห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิของ สนข. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ กำหนดกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขของสัญญาหรือไม่ ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) ดำเนินการ ดังนี้

๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นนั้น สำหรับบุคคลภายนอกในการเข้าถึงบริการที่สำคัญของหน่วยงาน โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๑.๑ การเข้าถึงบริการที่สำคัญของ สนข. ถูกจำกัดไว้ที่

๑) บุคลากร และกิจกรรมที่ได้รับอนุญาต

๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒.๑.๒ ต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับขั้นการเข้าถึงเวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB หรือพอร์ตต่าง ๆ) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางผู้ดูแลระบบสารสนเทศเท่านั้น

๒.๑.๕ ต้องเก็บบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน

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) โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๒.๑ ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงาน

๒.๒.๒ ต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังนี้

- 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) ความมั่นคงปลอดภัยของระบบสารสนเทศอย่างทันการณ์ และเหมาะสม

๒.๒.๓ ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๒.๒.๔ ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๒.๓ การเชื่อมต่อระยะไกล (Remote Control) โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๓.๑ ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังงานบริการสำคัญของหน่วยงาน มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

- ๑) เปิดใช้งานการเชื่อมต่อระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น
- ๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security
- ๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private

Network

๔) ในกรณีที่เป็นไปได้ ควรใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication) การกำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น HTTPS, SSH หรือ SCP เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการทำงานของบริการที่สำคัญของหน่วยงานเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๔.๑ ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของหน่วยงาน โดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่ฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

๒.๔.๒ ต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ ต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้ เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) โดยให้หน่วยงานดำเนินการอย่างน้อย ดังนี้

๒.๕.๑ ต้องเผยแพร่ ประชาสัมพันธ์เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักรู้ด้านไซเบอร์ถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ในลักษณะของการปฏิบัติตน ข้อหลีกเลี่ยงหรือข้อควรระวัง ในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้โดยง่าย

๒.๕.๒ ต้องจัดทำหรือปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๒.๕.๓ ต้องจัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศอย่างมีนัยสำคัญ

๒.๕.๔ ต้องสร้างความตระหนัก (Awareness) เรื่องการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือความเสี่ยงด้านเทคโนโลยีสารสนเทศ หรือการใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรในทุกระดับ

๒.๕.๕ ควรจัดให้มีการฝึกอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ให้แก่เจ้าหน้าที่ที่ปฏิบัติงานดูแลระบบสารสนเทศ

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

โดยให้หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) ดำเนินการ ดังนี้

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

๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยไซเบอร์

๓.๒ มีกระบวนการในการจัดประเภท และวิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ที่ตรวจพบ

๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

๓.๔ ต้องดำเนินการตรวจสอบกลไก และกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไก และกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องมีการจัดทำเอกสาร ฝึกซ้อม ทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพ และประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) ให้หน่วยงานดำเนินการ ดังนี้

๔.๒.๑ จัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ ต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต ดำเนินการ ดังนี้

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อดำเนินงานในช่วงที่เกิดเหตุการณ์วิกฤตทางไซเบอร์

๒) ระบุสถานการณ์/เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญที่จะเป็นตัวแทนขององค์กร เมื่อต้องมีการแถลงการณ์ หรือให้ข้อมูลที่เกี่ยวข้องกับเหตุการณ์

๕) ระบุแพลตฟอร์มหรือช่องทางการเผยแพร่ที่เหมาะสมสำหรับการเผยแพร่ข้อมูล

๔.๒.๓ ต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิภาพ ในช่วงที่เกิดเหตุวิกฤตอันเนื่องมาจากภัยคุกคามทางไซเบอร์

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานควรกำหนดแนวทางการดำเนินการเพื่อรองรับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication and Recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความเสี่ยง และระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น โดยดำเนินการ ดังนี้

๕.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ให้สามารถปฏิบัติงานได้จริง และพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขต คำนิยาม และการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption, Recovery Time Objective และ Recovery Point Objective เป็นต้น โดยมีรายละเอียดอย่างน้อย ดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ โดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงัก ลำดับความสำคัญในการกู้คืนระบบ

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤตสำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มีความมั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่อง มีการควบคุมดูแลการแก้ไขและกู้คืนระบบเมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๕.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินงานถึงหัวหน้าหน่วยงานผ่านผู้บริหารด้านไอซีทีที่ทราบทุกระยะ

ส่วนที่ ๒

ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ สนข.

กำหนดให้หน่วยงานมีมาตรฐานขั้นต่ำ ในการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานขึ้นเพื่อกำหนดทิศทางและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ให้กับระบบสารสนเทศและข้อมูลให้สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล สอดคล้องกับกฎหมาย มาตรฐาน ระเบียบข้อบังคับที่เกี่ยวข้อง และเพื่อให้การใช้งานระบบสารสนเทศของ สนข. มีประสิทธิภาพ มีความมั่นคงปลอดภัยทางไซเบอร์ และมีความน่าเชื่อถือ ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

๑.๑ การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

๑) มาตรการระบุความเสี่ยงที่อาจเกิดขึ้นกับคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิต ร่างกายบุคคล (Identify)

๒) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Resilience and Recovery)

๑.๒ แนวปฏิบัติสำหรับผู้ใช้งาน

๑.๓ แนวปฏิบัติการบริหารจัดการด้านความมั่นคงปลอดภัย สำหรับผู้ดูแลระบบ

๑.๔ แนวปฏิบัติสำหรับเจ้าของระบบ (System Owner)

๑.๕ แนวปฏิบัติสำหรับการจัดหา พัฒนา และดูแลรักษาระบบสารสนเทศ และการกำกับผู้ให้บริการภายนอก

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้ครอบคลุมเรื่องโครงสร้างองค์กร และบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment) ดังนี้

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่จะเกิดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการไอซีทีของหน่วยงาน

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

๓. การบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management)

หน่วยงานต้องจัดให้มีนโยบายและแนวทางในการบริหารจัดการความเสี่ยงด้านไซเบอร์อย่างถูกต้องและเหมาะสม เพื่อควบคุมความเสี่ยงให้อยู่ในระดับที่หน่วยงานยอมรับได้ และใช้เป็นกรอบแนวทางในการดูแลรักษาความปลอดภัยของข้อมูลสารสนเทศของ สนช. โดยคำนึงถึงองค์ประกอบพื้นฐานของความปลอดภัยของข้อมูลและหลักการ CIA ทั้ง ๓ ประการ ได้แก่ การรักษาความลับของข้อมูล (Confidentiality) การรักษาความคงสภาพของข้อมูลหรือความสมบูรณ์ของข้อมูล (Integrity) และความพร้อมใช้งานของข้อมูล (Availability)

๔. การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ ประกอบด้วยอย่างน้อย ดังนี้

๔.๑ หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบที่มีความเชี่ยวชาญด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน

๒) แผนการรับมือภัยคุกคามทางไซเบอร์ของหน่วยงาน

๔.๒ ต้องมีการรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระภายนอก

๕. การรับมือเหตุภัยคุกคามทางไซเบอร์

หน่วยงานต้องกำหนดแผนการรับมือภัยคุกคามทางไซเบอร์ ประกอบด้วยอย่างน้อย ดังนี้

๕.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๕.๒ มีการสื่อสารหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายในได้ สนข. อย่างมีประสิทธิภาพ

๕.๓ มีการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๕.๔ มีการฝึกซ้อมการรับมือเหตุภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๕.๕ สร้างสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการสำคัญของหน่วยงาน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๖. การสื่อสารในภาวะวิกฤตด้านไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อย ดังนี้

๖.๑ แผนการสื่อสารในภาวะวิกฤตด้านไซเบอร์

๖.๒ กำหนดโครงสร้างทีมสื่อสารในภาวะวิกฤตด้านไซเบอร์

๖.๓ กำหนดขั้นตอนการดำเนินงานเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์

๖.๔ เตรียมให้บุคลากรในองค์กรมีความพร้อมต่อการสื่อสารและประชาสัมพันธ์ เมื่อเกิดภาวะวิกฤตด้านไซเบอร์

๖.๕ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (ถ้ามี)

๗. การแก้ไขสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

หน่วยงานต้องรายงานเกี่ยวกับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ อย่างน้อย ดังนี้

๗.๑ กำหนดแผนการแก้ไขสถานการณ์ความไม่แน่นอนและสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๗.๒ กำหนดโครงสร้างทีมงาน ระเบียบวิธี แนวทางปฏิบัติ และขั้นตอนรับมือสถานการณ์ความไม่แน่นอนและสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

๘. การบริหารความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan)

หน่วยงานต้องจัดให้มีแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan) เพื่อให้แน่ใจว่าบริการระบบสารสนเทศที่สำคัญของหน่วยงานสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก โดยต้องมีการทบทวนแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan) อย่างน้อยปีละ ๑ ครั้ง

๙. การซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องจัดให้มีแผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อถ่ายทอดองค์ความรู้ ความเข้าใจ ในแนวทาง กระบวนการ และขั้นตอนการรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้เกิดการนำองค์ความรู้และแนวทางปฏิบัติในการรับมือภัยความเสี่ยงมาสู่การเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน

๑๐. การส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องจัดให้มีแผนในการส่งเสริมและขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยมีการกำหนดเป้าหมายและตัวชี้วัด รวมทั้งแผนงาน/โครงการ/กิจกรรมในการขับเคลื่อนงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ส่วนที่ ๓

เอกสารประกอบประมวลแนวทางปฏิบัติและกรอบมาตรฐาน

การรักษาความมั่นคงปลอดภัยไซเบอร์

ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

เอกสารประกอบ

๑. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๒. รายงานการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๓. แผนบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Risk Management) ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๔. แนวทางปฏิบัติในการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร
๕. แบบการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Audit : CSA) ของสำนักงานนโยบายและแผนการขนส่งและจราจร
๖. แผนการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan : CIRP) ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๗. แนวทางการแจ้งหรือรายงานเหตุการณ์คุกคามทางไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร
๘. แผนการสื่อสารในภาวะวิกฤตด้านไซเบอร์ (Crisis Communication Management Plan : CCMP) ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๙. การบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) และแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๑๐. แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙
๑๑. แผนปฏิบัติการด้านการส่งเสริมการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานนโยบายและแผนการขนส่งและจราจร ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ - ๒๕๗๐