กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงาน ป.ย.ป.
Strategic Transformation Office

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. การระบุความเสี่ยงที่อาจจะเกิดขึ้น (Identify)

หน่วยงานต้องทำการระบุว่ากระบวนการดำเนินงานและทรัพย์สินสารสนเทศใดบ้างที่มีความเสี่ยงต่อการถูกโจมตีทางไซเบอร์ และต้องได้รับการรักษาความมั่นคงปลอดภัย เพื่อบริหารจัดการความเสี่ยงด้านภัยคุกคามทางไซเบอร์ที่มีต่อระบบ ทรัพย์สิน ข้อมูล ของหน่วยงานได้อย่างเหมาะสม

สำนักงาน ป.ย.ป.
Strategic Transformation Office

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

หน่วยงานต้องมีมาตรการป้องกันที่เหมาะสมเพื่อจากัดผลกระทบของเหตุการณ์ภัยคุกคามไซเบอร์ ซึ่งครอบคลุมถึง เรื่องการควบคุมการเข้าถึง การฝึกอบรมและการสร้างความตระหนักให้แก่เจ้าหน้าที่และผู้ที่เกี่ยวข้องความปลอดภัยของข้อมูล และมาตรการด้านความมั่นคงปลอดภัยต่าง ๆ ทั้งกระบวนการและวิธีปฏิบัติ ตลอดจนเทคโนโลยี นอกจากนี้ หน่วยงานต้องทำการบารุงรักษาอุปกรณ์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบอิเล็กทรอนิกส์อย่างสม่ำเสมอ เพื่อให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง รวมทั้งการเปลี่ยนแปลงแก้ไข Patch หรือ update software

สำนักงาน ป.ย.ป.
Strategic Transformation Office

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

หน่วยงานต้องมีกระบวนการติดตามเฝ้าระวัง และตรวจจับเหตุการณ์ภัยคุกคามทางไซเบอร์อย่างต่อเนื่อง และ แจ้งเตือนถึงสิ่งที่ผิดปกติต่าง ๆ รวมถึงการติดตามเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้นจากทั้งภายในและภายนอก วิเคราะห์จุดอ่อนหรือช่องโหว่ของภัยคุกคามที่เกิดขึ้น เพื่อเป็นข้อมูลประกอบในการพิจารณาทบทวนแนวทางการป้องกัน ความเสี่ยงและผลกระทบที่จะเกิดขึ้นกับหน่วยงานในอนาคต

สำนักงาน ป.ย.ป.
Strategic Transformation Office

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Response)

๔.๑ มีการกำหนดมาตรการและกระบวนการรับมือภัยคุกคามไซเบอร์ที่ทันท่วงที

๔.๒ มีความร่วมมือกับหน่วยงานที่เกี่ยวข้องเกี่ยวกับแผนรับมือภัยคุกคามไซเบอร์

๔.๓ มีการวิเคราะห์สาเหตุภัยคุกคามหรือตรวจพิสูจน์พยานหลักฐานดิจิทัล

๔.๔ มีมาตรการป้องกันการลุกลามของภัยคุกคาม

๔.๕ มีการทดสอบ ปรับปรุงกลยุทธ์และแผนรับมือภัยคุกคามไซเบอร์อย่างสม่ำเสมอ

สำนักงาน ป.ย.ป.
Strategic Transformation Office

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recovery)

๕.๑ มีแผนการกู้คืนระบบทั้งระหว่างเกิดเหตุและหลังเกิดเหตุภัยคุกคาม

๕.๒ มีการปรับปรุงกลยุทธ์และแผนการกู้คืนอย่างสม่าเสมอ

๕.๓ มีการสื่อสารให้ผู้บริหารและ ผู้ที่เกี่ยวข้องทราบภายในองค์กรให้ทราบถึงกระบวนการกู้คืนข้อมูลหลังเกิดเหตุภัยคุกคามไซเบอร์

สำนักงาน ป.ย.ป.
Strategic Transformation Office