ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๗

.....

เพื่อให้การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.) เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว และเพื่อให้มาตรฐานความปลอดภัยไซเบอร์ของสำนักงาน ป.ป.ท. เกิดความชัดเจน เป็นไปในทิศทางเดียวกัน และสอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในใตรา ๒๑ (๑) แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ประกอบมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำนักงาน ป.ป.ท. จึงออกประกาศประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงาน ป.ป.ท. ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๗”

ข้อ ๒ ประกาศนี้ให้ใช้นับตั้งแต่วันถัดจากวันที่ประกาศเป็นต้นไป

ข้อ ๓ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน ป.ป.ท. ได้กำหนดขึ้นโดยมีวัตถุประสงค์ ดังนี้

๓.๑ เพื่อให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมันคงปลอดภัยไซเบอร์ ของสำนักงาน ป.ป.ท.

๓.๒ เพื่อใช้เป็นกรอบมาตรฐานและแนวปฏิบัติในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับบุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้กับ สำนักงาน ป.ป.ท.

๓.๓ เพื่อสร้าง....

๓.๓ เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงาน ป.ป.ท.

๓.๔ เพื่อให้บุคลากรของสำนักงาน ป.ป.ท. บุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน ป.ป.ท. ได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

๓.๕ เพื่อติดตามการดำเนินงานและทบทวนประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ให้สอดคล้องกับสภาพแวดล้อม และกฎมายที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ กรณีที่มีการแก้ไขเพิ่มเติมประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน ป.ป.ท. ถือปฏิบัติตามที่ได้มีการแก้ไขหรือเพิ่มเติม นั้น

ข้อ ๕ ให้ใช้ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามเอกสารแนบท้ายประกาศฉบับนี้

ประกาศ ณ วันที่ ๒ ธันวาคม ๒๕๖๗

(นายภูมิวิศาล เกษมศุข)

เลขาธิการคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

เอกสารแนบท้ายประกาศ
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๗

(Guideline and Cybersecurity Framework)

บัญชีแนบท้าย

ประกาศสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ พ.ศ. ๒๕๖๗

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนอง และรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จึงได้จัดทำเอกสารฉบับนี้ เพื่อให้สำนักงาน ป.ป.ท. มีรูปแบบรวมถึงขั้นตอนปฏิบัติเป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานข้อมูล ระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนด

๒. วัตถุประสงค์

เพื่อการจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสำนักงาน ป.ป.ท. และยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงาน ป.ป.ท. ให้เป็นไปในทิศทางเดียวกัน

๓. ขอบเขตการใช้

ใช้กับส่วนราชการในสังกัดสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ (สำนักงาน ป.ป.ท.)

๔. นิยาม....

๔. นิยาม

หน่วยงาน หมายถึง สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ สำนักงาน ป.ป.ท.

คณะกรรมการ CSO หมายถึง คณะกรรมการบริหารความเสี่ยงและความมั่นคงปลอดภัยทางดิจิทัลของสำนักงาน ป.ป.ท.

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หมายถึง ผู้บริหารสำนักงาน ป.ป.ท. ที่ได้รับมอบหมายจากเลขาธิการคณะกรรมการ ป.ป.ท. ให้กำกับดูแลศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ผู้ใช้งาน หมายถึง บุคลากรของสำนักงาน ป.ป.ท. ที่ได้รับอนุญาตให้ใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้ให้บริการภายนอก หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของหน่วยงาน หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยหน่วยงานของรัฐได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์หรือบริการของหน่วยงานของรัฐ

อินเตอร์เฟซ (Interface) หมายถึง การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้

คอมไพเลอร์ (Compiler) หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

แพตช์ (Patch) หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายเผยแพร่ Patch ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่ Patch ที่แก้ไขช่องโหว่ของซอฟต์แวรผ่านระบบ Windows update

Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืน

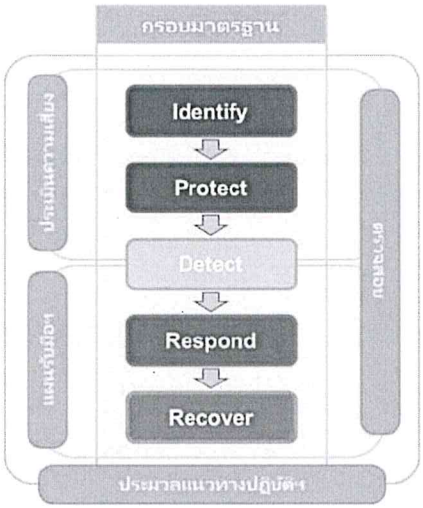
Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ระบบหยุดชะงัก เพื่อรองรับการดำเนินงานอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

๕. การจัดทำ....

๕. การจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตในภาครัฐ

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ สามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

โดยการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มี ๒ ส่วน ดังนี้

ส่วนที่ ๑
ประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๑.๑ หน่วยงานต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตการตรวจสอบ ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๑.๑.๒ หน่วยงาน....

๑.๑.๒ หน่วยงานต้องจัดส่งรายงานผลการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกมายังคณะกรรมการ CSO ภายใน ๓๐ (สามสิบ) วันนับถัดจากวันที่ได้รับรายงานการตรวจสอบ

หัวข้อที่ ๑.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานให้ครอบคลุม เรื่อง โครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้

๑.๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซคางรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่างๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจุยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะหีความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซบอร์จะเกิดขึ้น และผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรัษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๑.๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk)อยู่ในระดับที่ยอมรับได้

๑.๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้กำหนดไว้

๑.๒.๔ การรายงาน....

๑.๒.๔ การรายงานความเสี่ยง (Risk Roporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการ ตามรอบการประชุมของคณะกรรมการ CSO

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

หัวข้อที่ ๑.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามไซเบอร์ ดังต่อไปนี้

๑.๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersrcurity Incident Response Plan)

๑.๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้อง

๑.๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๑.๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

หัวข้อที่ ๑.๔ การรายงานสถานการณ์เกี่ยวกับความมันคงปลอดภัยทางไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์มายังคณะกรรมการ อย่างน้อยดังนี้

๑.๔.๑ แนวนโยบายหรือแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไวเบอร์

๑.๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ที่ตรวจพบ และผลการดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์

๑.๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง

๑.๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์

๑.๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๑.๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านการรักษาความมันคงปลอดภัย เพื่อกาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๒....

ส่วนที่ ๒
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๒.๑ การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล (Identify)

๒.๑.๑ การจัดการทรัพย์สิน (Asset Management) มีการดำเนินการ ดังนี้

๑) จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

๒) ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๓) มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๒.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) มีการดำเนินการ ดังนี้

๑) ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กาหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยงโดยมีรายละเอียดอย่างน้อย 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)

๒) กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับประเมินความเสี่ยง ที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๓) ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔) กำหนดเกณฑ์....

๔) กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ การระบุโอกาสการเกิดขึ้น ของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

๕) วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญโดยมีการบริหารจัดการความเสี่ยง ดังนี้

(ก) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(ข) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(ค) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

๒.๑.๓ การประเมินช่องโหว่และทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) มีการดำเนินการ ดังนี้

๑) ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์ หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นงคงปลอดภัยแห่งชาติ สานักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) หรือจากแหล่งอื่นที่น่าเชื่อถือ เป็นต้น

๒) ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยง ของสำนักงาน ป.ป.ท. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ

๓) การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม

๔) การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชั่น การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๕) การทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญโดยเฉพาะอย่างยิ่งระบบสารสนเทศ (Information Technology :IT) ที่เชื่อมต่อกับอินเตอร์เน็ตโดยตรง (Internet Facing) เพื่อให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๖) ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชั่นของบริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๗) ดำเนินการ....

๗) ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และ การปรับเปลี่ยนเทคโนโลยี เป็นต้น

๘) การทดสอบเจาะระบบและผู้ให้บริการทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ ต้องมีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ หรือเป็นไปตามที่กฎหมายกำหนด

๙) การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของสำนักงาน ป.ป.ท.

๑๐) ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบ และจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

ทั้งนี้ สำนักงาน ป.ป.ท. กำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดให้มีการตรวจประเมินช่องโหว่และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบสารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยเร่งด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบต้องดำเนินการแก้ไขให้แล้วเสร็จโดยไม่ชักช้า หรือไม่เกินกว่า ๗ วัน นับจากวันที่ได้รับแจ้งจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมทั้งรายงานผลการแก้ไขกลับมายังศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและดำเนินการตรวจสอบการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบที่ไม่อาจปิดช่องโหว่ได้ พร้อมกำหนดมาตรการชดเชยหรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่ทางเทคนิคนั้น หรือในกรณีที่มีความจำเป็นอาจต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้ที่ได้รับมอบหมายพิจารณาและให้ความเห็นชอบ

๒.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) มีการดำเนินการ ดังนี้

๑) แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของสำนักงาน ป.ป.ท.

๒) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระกวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของ....

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของสำนักงาน ป.ป.ท. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(ง) สิทธิของสำนักงาน ป.ป.ท. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๓) สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา

๔) ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

หัวข้อที่ ๒.๒ มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

๒.๒.๑ การควบคุมการเข้าถึง (Access Control)

๑) การเข้าถึงบริการที่สำคัญของสำนักงาน ป.ป.ท. ถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒) ให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของสำนักงาน ป.ป.ท. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๓) เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจาความสม่ำเสมอ ในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๔) ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ เช่น USB พอร์ตอนุกรม และ การเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น และอยู่ภายใต้การดูแลของสำนักงาน ป.ป.ท.

๒.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๑) สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

๒) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษ....

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชั่นที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอปพลิเคชั่นสนับสนุนผู้ให้บริการ

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware)

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

๓) มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ

๔) ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

๕) จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๒.๓ การเชื่อมต่อระยะไกล (Remote Control)

๑) ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึง โดยไม่ได้รับอนุญาต

๒) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

(ข) ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๒.๔ สื่อเก็บข้อมูล....

๒.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๑) กำหนดการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนสื่อบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรายกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒) เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลถอดได้

๒.๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๑) หน่วยงานต้องเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒) หน่วยงานต้องจัดทำ ปรับปรุง คู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๓) หน่วยงานต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุง และเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๔) หน่วยงานต้องสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัยให้แก่บุคลากรทุกระดับ

๕) หน่วยงานควรจัดให้มีการอบรม และพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุม และเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ กับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

๖) ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒.๒.๖ การแบ่งปันข้อมูล (Information Sharing)

สำนักงาน ป.ป.ท. มีการกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

หัวข้อที่ ๒.๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๒.๓.๑ มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๓.๒ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๒.๓.๓ วิเคราะห์....

๒.๓.๓ วิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของสำนักงาน ป.ป.ท. หรือไม่

๒.๓.๔ ทบทวนกลไกและกระบวนการ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๒.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๒.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity incident Response Plan)

จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน และปรับปรุงตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๒.๔.๒ แผนการสื่อสารในสภาวะวิกฤต (Crisis Communication Plan)

๑) ต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์

๒) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

(ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

(ค) ระบุกลุ่มเป้าหมาย และผู้ที่มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

(ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนของหน่วยงานเมื่อกล่าวแถลงกับสื่อมวลชน

(จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๓) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงที และมีประสิทธิภาพในช่วงวิกฤต

๒.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๑) หน่วยงานต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษร ให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน หน่วยงานต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ ดังกล่าว

๒) ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการเพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของหน่วยงาน

หัวข้อที่ ๒.๕....

หัวข้อที่ ๒.๕ มาตรการรักษาและฟื้นฟูความสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๒.๕.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของสำนักงาน ป.ป.ท. สามารถให้บริการที่จำเป็นต่อไปได้ ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของสำนักงาน ป.ป.ท. เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๒.๕.๒ ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับ ความมั่นคงปลอดภัยไซเบอร์

๒.๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการให้คณะกรรมการ CSO ทราบทุกระยะ