สภาองค์กรของผู้บริโภค
Thailand Consumers Council

ประกาศคณะกรรมการนโยบายสภาองค์กรของผู้บริโภค
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสภาองค์กรของผู้บริโภค พ.ศ. ๒๕๖๙

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามมาตรา ๔๔ กำหนดให้ หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวล แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว

สภาองค์กรของผู้บริโภค ได้มีการประกาศแนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำนักงานสภาองค์กรของผู้บริโภค เมื่อวันที่ ๒๒ สิงหาคม ๒๕๖๗ เพื่อเป็นนโยบายดำเนินงานและกำหนดแนวทางการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของสภาองค์กรของผู้บริโภค

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และข้อ ๒๗ (๑๓) แห่งข้อบังคับสภาองค์กรของผู้บริโภค พ.ศ. ๒๕๖๕ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๖๖ ประกอบมติคณะกรรมการนโยบายสภาองค์กรของผู้บริโภค ครั้งที่ ๘/๒๕๖๙ เมื่อวันที่ ๒๗ เดือน สิงหาคม พ.ศ. ๒๕๖๙ สภาองค์กรของผู้บริโภคโดยคณะกรรมการนโยบาย จึงออกประกาศนี้ไว้เพื่อให้การรักษาความมั่นคงปลอดภัยข้อมูลระบบเทคโนโลยีสารสนเทศของสภาองค์กรของผู้บริโภคเป็นไปตามกฎหมายกำหนด ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการนโยบายสภาองค์กรของผู้บริโภค เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสภาองค์กรของผู้บริโภค พ.ศ.๒๕๖๙

ข้อ ๒ ประกาศนี้ให้ใช้ตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ของสภาองค์กรของผู้บริโภคได้กำหนดขึ้นโดยมีวัตถุประสงค์ ดังต่อไปนี้

(๑) เพื่อให้มีแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสภาองค์กรของผู้บริโภค

(๒) เพื่อใช้เป็นกรอบมาตรฐานและแนวปฏิบัติในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับบุคลากรผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารให้กับสภาองค์กรของผู้บริโภค

/(๓) เพื่อสร้างความ...

(๓) เพื่อสร้างความตระหนัก ความเข้าใจ และมีส่วนรับผิดชอบในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของสภาองค์กรของผู้บริโภค

(๔) เพื่อให้คณะกรรมการนโยบายสภาองค์กรของผู้บริโภค คณะอนุกรรรมการ คณะทำงาน ผู้บริหารและเจ้าหน้าที่ของสำนักงานสภาองค์กรของผู้บริโภค หัวหน้าและผู้ปฏิบัติงานในหน่วยงานเขตพื้นที่ หน่วยงาน ประจำจังหวัด หน่วยงานอื่นที่ได้รับการจัดตั้งขึ้นโดยคณะกรรมการนโยบายสภาองค์กรของผู้บริโภค รวมถึงบุคลากรใน โครงการความร่วมมือ องค์กรสมาชิก องค์กรของผู้บริโภค พนักงานจ้างเหมาบริการและบุคคลภายนอกที่ปฏิบัติงานให้กับ สภาองค์กรของผู้บริโภคได้รับทราบและถือปฏิบัติตามอย่างเคร่งครัด

(๕) เพื่อติดตามการดำเนินงานและทบทวนแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับสภาพแวดล้อม และกฎหมาย ที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ของสภาองค์กรของผู้บริโภคปฏิบัติตามที่ได้มีการแก้ไขหรือเพิ่มเติมนั้น

ข้อ ๕ ให้ใช้แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ของสภาองค์กรของผู้บริโภค แนบท้ายประกาศนี้

ข้อ ๖ ให้เลขาธิการสำนักงานสภาองค์กรของผู้บริโภคซึ่งเป็นผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) ของสภาองค์กรของผู้บริโภคเป็นผู้กำกับดูแลและติดตามให้มีการดำเนินการและ ถือปฏิบัติแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามประกาศนี้

ข้อ ๗ ให้ประธานกรรมการนโยบายสภาองค์กรของผู้บริโภคเป็นผู้รักษาการตามประกาศนี้ กรณีที่มีปัญหาจากการปฏิบัติตามประกาศนี้หรือที่ประกาศนี้มิได้กำหนดไว้ ให้เลขาธิการสภาองค์กรของผู้บริโภคเป็นผู้วินิจฉัยและคำวินิจฉัยนั้นให้ถือเป็นที่สุด

ประกาศ ณ วันที่ ๒๗ เดือน สิงหาคม พ.ศ. ๒๕๖๙

(นางสาวบุญยืน ศิริธรรม)
ประธานกรรมการนโยบายสภาองค์กรของผู้บริโภค

สภาองค์กรของผู้บริโภค
Thailand Consumers Council

กรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สภาองค์กรของผู้บริโภค

Cybersecurity Framework

งานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ

สภาองค์กรของผู้บริโภค

ปี 2569

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(Cybersecurity Framework)

สภาองค์กรของผู้บริโภค

1. หลักการ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศรวมทั้งกำหนดมาตรการในการประเมินความเสี่ยงการตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ

สภาองค์กรของผู้บริโภค จึงจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ 2564 จากสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานรัฐปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

2. นิยาม

1) องค์กร หรือ สภา หมายถึง สภาองค์กรของผู้บริโภค
2) คณะกรรมการ หมายถึง คณะอนุกรรมการบริหาร คณะกรรมการนโยบาย หรือคณะทำงานที่ได้รับมอบหมายโดยตรง
3) บริการที่สำคัญ หมายถึง ภารกิจหรือบริการที่สำคัญขององค์กร
4) ตัวชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงเพิ่มขึ้นพร้อมทั้งสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์และความเสี่ยงในอนาคต และเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

5) ผู้ให้บริการภายนอก หมายถึง บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศหรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศขององค์กร หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญขององค์กร หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยองค์กรได้

6) Interface หมายถึง การเชื่อมต่อกันระหว่างเครื่องคอมพิวเตอร์กับเครื่องคอมพิวเตอร์สามารถถ่ายโอนข้อมูลซึ่งกันและกันได้

7) คอมไพเลอร์ (Compiler) หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทาหน้าที่แปลงชุดคาสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

8) แพตช์ (Patch) หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท ไมโครซอฟท์ (Microsoft) จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบวินโดว์อัพเดท (Windows Update)

9) Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

10) Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

11) Maximum Tolerance Period of Disruption (MTPD) หมายถึง ระยะเวลาสูงสุดที่ยอมให้การดำเนินงานตามภารกิจหยุดชะงัก เพื่อรองรับการดำเนินภารกิจหรือบริการสำคัญอย่างต่อเนื่องขององค์กร และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ระยะเวลาแก้ไขภัยคุกคามให้ทำงานได้ตามปกติให้เร็วที่สุด

12) เหตุการณ์ (Event) หมายถึง การเกิดขึ้นที่สังเกตได้ (Observable Occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการลำดับ การดำเนินการ หรือบุคลากร เหตุการณ์อาจมี หรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

13) เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident) หมายถึง เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

14) ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายถึง การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือ โปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทางานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

15) เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายถึง เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทาง สารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการการ

รักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตาม มาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

3. ขอบเขตและการบังคับใช้

เอกสารนี้อ้างอิงตามกรอบมาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 ซึ่งครอบคลุมระบบ เทคโนโลยี บุคลากร และกระบวนการที่เกี่ยวข้อง ด้านเทคโนโลยีสารสนเทศขององค์กร

การปฏิบัติงาน ควบคุม กำกับดูแล และตรวจสอบ รวมถึงการกำหนดนโยบาย (Policy) มาตรฐานกลาง (Standards) ขั้นตอนปฏิบัติ (Procedure) หรือกระบวนการ (Process) ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ข้อมูล และการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องปฏิบัติตามกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ เพื่อเป็นการปฏิบัติตามกฎหมาย ข้อกำหนด มาตรฐานสากล และแนวปฏิบัติที่ดี

4. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย 5 หัวข้อหลักและหัวข้อย่อย ได้แก่

4.1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

1) การจัดการทรัพย์สิน (Asset Management)
2) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)
3) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)
4) การจัดการผู้ให้บริการภายนอก (Third Party Management)

4.2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

1) การควบคุมการเข้าถึง (Access Control)
2) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)
3) การเชื่อมต่อระยะไกล (Remote Connection)
4) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)
5) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)
6) การแบ่งปันข้อมูล (Information Sharing)

4.3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

4.4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

1) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)
2) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)
3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

4.5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

1) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

หัวข้อหลักที่ 1 การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

<u>กรอบมาตรฐาน</u>

1.1 การจัดการทรัพย์สิน (Asset Management)

1.1.1 องค์กรต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญขององค์กร และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

ก) ชื่อ/คำอธิบายของทรัพย์สินของบริการที่สำคัญ

ข) ฟังก์ชันที่สำคัญของทรัพย์สินของบริการที่สำคัญ

ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สินบริการที่สำคัญ

ง) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญ

จ) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญแต่ละรายการ และ

ฉ) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญบนระบบ/เครือข่ายภายใน และ/หรือภายนอก

1.1.2 องค์กรต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญขององค์กร และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงกับเครือข่ายสาธารณะ (Internet Facing) และ/หรือมีนัยสำคัญ (Critical Asset)

1.1.3 องค์กรต้องมีการตรวจสอบทะเบียนทรัพย์สิน (IT Asset Inventory Review) อย่างน้อยปีละหนึ่งครั้ง หากมีการเปลี่ยนแปลงใดๆ กับทรัพย์สินของบริการที่สำคัญขององค์กรให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

1.1.4 องค์กรต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญขององค์กร ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สิน อย่างน้อยปีละหนึ่งครั้ง

1.2 การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

1.2.1 องค์กรต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้งหรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศขององค์กร ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด

1.2.2 องค์กรต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

ก) วันที่ระบุความเสี่ยง (Risk Register Date)

ข) คำอธิบายของความเสี่ยง (Description of the Risk)

ค) โอกาสที่จะเกิดขึ้น (Likelihood or Occurrence)

ง) ความรุนแรงของเหตุการณ์ (Severity or Impact)

จ) ระดับความเสี่ยง (Risk Level)

ฉ) การจัดการความเสี่ยง (Risk Treatment)

ช) เจ้าของความเสี่ยง (Risk Owner)

ซ) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ

ฌ) ระดับความเสี่ยงที่เหลือ (Residual Risk)

1.3 การประเมินช่องโหว่เชิงเทคนิค และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

1.3.1 ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญขององค์กร อ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญขององค์กร ซึ่งเป็น

ก) ระบบเทคโนโลยีสารสนเทศ (IT system)

ข) ระบบงานด้านเทคโนโลยีสารสนเทศ (IT application)

ค) ระบบโครงสร้างด้านเทคโนโลยีสารสนเทศ (IT infrastructure)

1.3.2 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่ ต้องครอบคลุมส่วนที่เกี่ยวข้องเช่น

ก) การประเมินความมั่นคงปลอดภัยของระบบงาน (Application Security Assessment)

ข) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

ค) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

ง) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

1.3.3 ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญขององค์กร เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใดๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ กับบริการที่สำคัญขององค์กรการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่การเพิ่มโมดูล แอปพลิเคชั่น การปรับปรุงระบบ การปรับปรุงมาตรการรักษาความปลอดภัย และการปรับเปลี่ยนเทคโนโลยี

1.3.4 ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญขององค์กร โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

1.3.5 ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญขององค์กร โดยเฉพาะอย่างยิ่ง ทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

1.3.6 ควรพิจารณาดำเนินการทดสอบเจาะระบบซ้ำอย่างน้อยปีละหนึ่งครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญขององค์กร ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

1.3.7 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม หรือสากล และเป็นอิสระจากระบบที่จะทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่องค์กร หรือหน่วยงานควบคุมหรือกำกับดูแลกำหนด

1.3.8 ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การอนุญาตและกำกับดูแลขององค์กร

1.3.9 ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุ หรือตรวจพบในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ ภายในระยะเวลาที่เหมาะสม

1.3.10 หากได้รับการร้องขอจากคณะกรรมการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือ กกม. หรือ สกมช. หรือหน่วยงานกำกับดูแล (Regulator) องค์กรต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ขององค์กรดังกล่าวไปยังผู้ร้องขอภายในกำหนด 30 วัน นับแต่วันที่ ได้รับหนังสือ ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่องค์กรกำหนด

1.4 การจัดการผู้ให้บริการภายนอก (Third Party Management)

1.4.1 องค์กรต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เมื่อผู้ให้บริการภายนอกดำเนินงานใดๆ ซึ่งเกี่ยวข้องกับบริการหรือระบบเทคโนโลยีสารสนเทศขององค์กร

1.4.2 องค์กรต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของ ผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อยดังต่อไปนี้

ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญขององค์กรตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญขององค์กรจากภัยคุกคามทางไซเบอร์ หรือความเสี่ยงทางไซเบอร์

ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์ (Supply Chain Risk)

ง) สิทธิ์ขององค์กรในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Rights To Audit)

1.4.3 องค์กรควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม การตรวจสอบผลิตภัณฑ์ การบริหารจัดการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

1.4.4 องค์กรควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เป็นปัจจุบัน

หัวข้อหลักที่ 2 มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

กรอบมาตรฐาน

2.1 การควบคุมการเข้าถึง (Access Control)

2.1.1 องค์กรต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญขององค์กรถูกจำกัดไว้ที่

ก) บุคลากร (Personnel) และกิจกรรมหรือกระบวนการ (Process) ที่ได้รับอนุญาต

ข) ทรัพย์สิน (Asset) และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

2.1.2 ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ 2.1.1 องค์กรต้องกำหนดให้แต่ละบุคลากรกิจกรรมและกระบวนการที่ได้รับอนุญาต มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญขององค์กร

2.1.3 องค์กรต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญขององค์กรและตรวจสอบ บันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ ควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

2.1.4 องค์กรต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญขององค์กร (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทาง ลอจิคอล (Logical) มีการกำกับดูแลโดย

ก) ทำภายใต้การดูแลขององค์กรเท่านั้น และ

ข) ดำเนินการในสถานที่ หากเป็นไปได้

ค) การเข้าถึงผ่านทางไกล (Remote Access) จะต้องมีการเข้ารหัสเครือข่ายที่เชื่อมต่อด้วยเทคโนโลยีที่ปลอดภัยที่เป็นปัจจุบัน

2.1.5 องค์กรต้องมีการควบคุมและบริหารผู้ใช้งาน (Access Rights Management) การยืนยันตัวตน (Authentication) และสิทธิ์การเข้าถึงที่ (Authorization) ที่มีความปลอดภัย

2.2 การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

2.2.1 องค์กรต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการแอปพลิเคชั่น และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญขององค์กรที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญขององค์กร

2.2.2 องค์กรต้องกำหนดมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

ข) การแบ่งแยกหน้าที่ (Separation of Duties)

ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน (Strong password)

ง) การลบบัญชีที่ไม่ได้ใช้

จ) การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

ช) การป้องกันมัลแวร์ (Anti-Malware) และ

ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

2.2.3 องค์กรต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญขององค์กร

2.2.4 องค์กรต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญขององค์กร อย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

2.2.5 องค์กรต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญขององค์กร

2.3 การเชื่อมต่อระยะไกล (Remote Connection)

2.3.1 องค์กรต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญองค์กรมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

2.3.2 องค์กรสำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญขององค์กรต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

ก) ในกรณีที่เป็นไปได้ให้เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

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

ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น และใช้เทคโนโลยีการเข้ารหัสที่ปลอดภัยเพียงพอที่เป็นปัจจุบัน

ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญองค์กร เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการทางธุรกิจ

จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

2.4 สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

2.4.1 องค์กรต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น คอมพิวเตอร์พกพา (Laptop)) กับบริการที่สำคัญขององค์กร โดยใช้มาตรการอย่างน้อย ดังนี้

ก) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นและต้องได้รับอนุญาต เท่านั้น

ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตตามข้อ 2.1.1 (ข) เท่านั้น และ

ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ (Malware) ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญขององค์กร

2.4.2 องค์กรต้องเข้ารหัสข้อมูลที่ละเอียดอ่อน (Sensitive Information) ทั้งหมดของบริการที่สำคัญขององค์กรบนสื่อบันทึกข้อมูลแบบถอดได้

2.5 การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

2.5.1 องค์กรต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับบุคลากรขององค์กร และผู้ให้บริการภายนอกหรือบุคคลที่สาม (Third Party) ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

ก) กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่

- บุคคลากรที่เข้าทำงานใหม่ (New Joinner)
- ผู้ใช้งานปัจจุบัน ทั้งระดับบริหาร และระดับปฏิบัติงาน (Users and Management)

- หน่วยงานหรือบุคลากรภายนอกที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ISP
- ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers) ที่มีความเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์กร

ข) เผยแพร่และให้ความรู้ตามระดับความสำคัญหรือระดับความรับผิดชอบของกลุ่มและบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญขององค์กร

ค) เผยแพร่การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

ง) มีการสื่อสารอย่างสม่ำเสมอและทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้าน ความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

2.5.2 ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

2.6 การแบ่งปันข้อมูล (Information Sharing)

องค์กรต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศและมาตรการบรรเทาผลกระทบใดๆ ที่ได้ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลหรือหน่วยงานที่ได้รับผลกระทบหรือเหตุการณ์ความเสี่ยงที่อาจเกิดขึ้นได้ เช่น ผู้ใช้งาน ผู้ให้บริการภายนอกที่ให้บริการแก่บริการที่สำคัญขององค์กร และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญขององค์กร เพื่อให้สามารถป้องกัน ตรวจจับ หรือใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่องค์กรประกาศกำหนด

หัวข้อหลักที่ 3 มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

กรอบมาตรฐาน

3.1 การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

3.1.1 องค์กรต้องสร้างมาตรการ กลไก และกระบวนการเพื่อ

ก) ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร

ข) การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

ค) การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญขององค์กรหรือไม่

3.1.2 องค์กรต้องดำเนินการทบทวนกลไกและกระบวนการภายในข้อ 3.1.1 อย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

หัวข้อหลักที่ 4 มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

กรอบมาตรฐาน

4.1 แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

4.1.1 องค์กรต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

4.2 แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

4.2.1 องค์กรต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.2.2 องค์กรต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จาลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ

จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

ฉ) ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อ ให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

ช) ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละหนึ่งครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

4.3 การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

4.3.1 ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 มาตรา 22 (13) องค์กรต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้กระทำโดยคณะกรรมการ หรือจากหน่วยงานกำกับดูแล

4.3.2 ต้องปฏิบัติตามคำขอใดๆ ของคณะกรรมการหรือหน่วยงานกำกับดูแล เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญขององค์กร เพื่อวัตถุประสงค์ในการวางแผนและ ดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ 4.1 และข้อ 4.2 ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญขององค์กร

หัวข้อหลักที่ 5 มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

กรอบมาตรฐาน

5.1 การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

5.1.1 ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญขององค์กรสามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอกเพื่อพิจารณาความสอดคล้องกับแผนขององค์กร เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น Maximum Tolerable Period of Disruption (MTPD) หรือ Maximum Tolerable Downtime (MTD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

5.1.2 การจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ให้คำนึงถึงหลักเกณฑ์ และวิธีการที่ สกมช. หรือหน่วยงานกำกับดูแล (Regulator) ประกาศกำหนด

5.1.3 ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BCP อย่างน้อยปีละหนึ่งครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์