



เอกสารแนบท้ายประกาศสำนักงานเศรษฐกิจการคลัง
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของสำนักงานเศรษฐกิจการคลัง
พ.ศ. ๒๕๖๘

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานเศรษฐกิจการคลัง

สารบัญ

	หน้า
บทนำ	๑
หลักการ	๑
วัตถุประสงค์	๑
ขอบเขตการใช้งาน	๑
คำนิยาม	๑
ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๒
แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๒
การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๓
แผนการรับมือภัยคุกคามทางไซเบอร์	๔
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๕
การระบุความเสี่ยง (Identify)	๕
มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)	๘
มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)	๑๐
มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)	๑๐
มาตรการรักษาและฟื้นฟูความเสี่ยงภัยที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)	๑๑

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework)

บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ (พ.ร.บ. ไซเบอร์ฯ) ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบต่อหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลเพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) สำนักงานเศรษฐกิจการคลังจึงได้จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework) เพื่อกำหนดกรอบการดำเนินงานและแผนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเศรษฐกิจการคลัง

วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเศรษฐกิจการคลังสามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากลที่ กมช. ประกาศกำหนด

ขอบเขต

ใช้ภายในหน่วยงานทั้งหมดภายใต้สังกัดสำนักงานเศรษฐกิจการคลัง

คำนิยาม

บริการที่สำคัญ	หมายถึง	ภารกิจหรือบริการของหน่วยงานตามมาตรา ๔๙ แห่ง พ.ร.บ. ไซเบอร์ฯ
ดัชนีชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

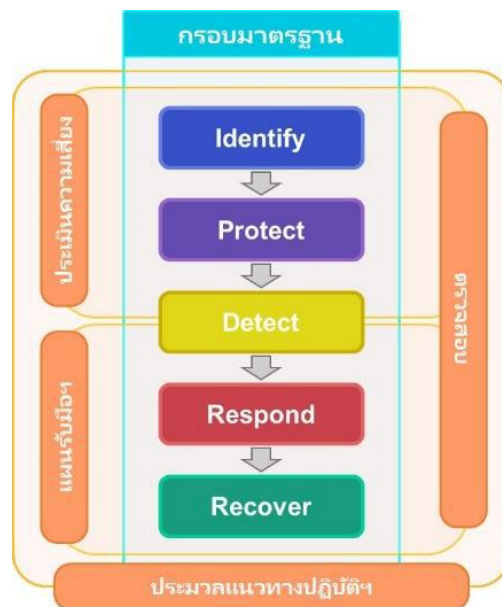
ผู้ให้บริการภายนอก	หมายถึง	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของสำนักงานเศรษฐกิจการคลัง และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของสำนักงานเศรษฐกิจการคลังและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศหรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดยสำนักงานเศรษฐกิจการคลังและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ทั้งนี้ ผู้ให้บริการภายนอกไม่ครอบคลุมถึงผู้ใช้บริการที่ใช้ผลิตภัณฑ์และบริการของสำนักงานเศรษฐกิจการคลังและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของสำนักงานเศรษฐกิจการคลังและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

/การจัดทำ ...

การจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ซึ่งการจัดทำประมวลแนวทางปฏิบัติ มีองค์ประกอบดังนี้

- ๑) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๒) การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ๓) แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

สำนักงานเศรษฐกิจการคลัง จัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายในหรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

๑.๑ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๑.๒ บริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง ตามผลการวิเคราะห์ในข้อ ๑.๑

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานเศรษฐกิจการคลัง กำหนดให้ต้องมีการประเมินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อเป็นการเตรียมความพร้อมรองรับ สถานการณ์ อุบัติการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้น รวมถึงให้มีแนวทางในการดำเนินงาน การกำกับดูแล ในช่วงสถานการณ์ที่เกิดขึ้น และให้สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีโดยต้องประกอบไปด้วย รายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๒.๑.๑ การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการ ปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒.๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหา แนวทางในการจัดการความเสี่ยงที่เหมาะสม

๒.๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้น และผลกระทบต่อการทำงาน รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมิน ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงสมดุล ระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษา ความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับสำคัญของความมั่นคง ปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ควรมีการดำเนินการอย่างสม่ำเสมอเพื่อตอบสนองต่อการเปลี่ยนแปลงอย่างทันท่วงทีและถือเป็น ส่วนหนึ่งของการปฏิบัติงาน รวมถึงการติดตามการดำเนินการภายหลังจากเกิดเหตุการณ์ขึ้น เพื่อวิเคราะห์ ถึงปัญหาที่เกิดขึ้นรวมถึงการแก้ไขปัญหาที่ถูกต้อง และมีประสิทธิภาพ

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

ให้มีการรายงานเหตุการณ์ความเสี่ยง ระดับความเสี่ยง และผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรมของสำนักงานเศรษฐกิจการคลังทุกครั้ง

ทั้งนี้ต้องทบทวนระเบียบวิธีปฏิบัติ และกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

๓.๑ ศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง ต้องจัดทำแผนรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan: CIRP) เพื่อกำหนดว่าควรรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

(๒) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) จะปฏิบัติตามภาระหน้าที่ในรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๕) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๖) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๗) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๘) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ

(๙) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๓.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของสำนักงานเศรษฐกิจการคลัง

๓.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ ในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง หรือ ข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Framework) ตามประกาศ คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญ ทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย ๕ หัวข้อหลัก ดังนี้

๑. การระบุความเสี่ยง (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

๑.๑.๑ ต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของของบริการที่สำคัญของหน่วยงาน และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

- (๑) ชื่อ/คำอธิบายของทรัพย์สินของบริการที่สำคัญ
- (๒) พังค์ชั้นที่สำคัญของทรัพย์สินของบริการที่สำคัญ
- (๓) การระบุและการจัดลำดับความสำคัญ
- (๔) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการ
- (๕) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ
- (๖) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ บนระบบ/เครือข่ายภายใน และ/หรือ

ภายนอก

๑.๑.๒ ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรง และมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๔ ต้องมีการดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์สินในข้อ ๑.๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๑.๒.๑ ต้องประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญกระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยง

๑.๒.๒ ต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลักการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยมีรายละเอียดอย่างน้อย ดังนี้

- (๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)
- (๒) คำอธิบายความเสี่ยง (Description of the Risk)
- (๓) โอกาสที่อาจจะเกิด (Likelihood of Occurrence)
- (๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- (๕) การจัดการความเสี่ยง (Risk Treatment)
- (๖) เจ้าของความเสี่ยง (Risk Owner)
- (๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment) และ
- (๘) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๑.๓.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงาน ซึ่งเป็นระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

๑.๓.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

- (ก) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
- (ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
- (ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญเพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ง และพิจารณาผลกระทบหรือความเสี่งจากการทดสอบเจาะระบบด้วย

๑.๓.๕ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ทุกระบบที่มีการเชื่อมต่อกับอินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๖ ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ตามความจำเป็น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๓.๗ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบและผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุม หรือกำกับดูแลกำหนด

๑.๓.๘ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบ ดำเนินการภายใต้การดูแลของหน่วยงาน

๑.๓.๙ ต้องสร้างกระบวนการเพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินการใด ๆ ก็ตามในส่วนของการบริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่งที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญา กับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของสำนักงานเศรษฐกิจการคลัง และโปรไฟล์ความเสี่งด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(๒) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(๔) สิทธิของสำนักงานเศรษฐกิจการคลัง ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก (Right to Audit)

๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา เช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

๒. มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

๒.๑.๑ การเข้าถึงบริการที่สำคัญของสำนักงานเศรษฐกิจการคลังถูกจำกัดไว้ที่

๒.๑.๑.๑ บุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้สำนักงานเศรษฐกิจการคลัง

๒.๑.๑.๒ อุปกรณ์ และอินเทอร์เฟซ (Interface) ของบุคลากร/เจ้าหน้าที่ที่ปฏิบัติงานให้สำนักงานเศรษฐกิจการคลัง

๒.๑.๒ ให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหนดการเข้าถึงบริการที่สำคัญ

๒.๑.๓ ต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญและตรวจสอบบันทึกเหล่านี้ เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางศูนย์เทคโนโลยีสารสนเทศเท่านั้น และทำภายใต้การดูแลของสำนักงานเศรษฐกิจการคลัง

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๒.๒.๒.๑ สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒.๒.๒.๒ การแบ่งแยกหน้าที่ (Separation of Duties)

๒.๒.๒.๓ การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๒.๒.๒.๔ การลบบัญชีที่ไม่ได้ใช้

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

๒.๒.๒.๖ การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๒.๒.๒.๗ การป้องกันมัลแวร์ (Malware)

๒.๒.๒.๘ การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันต่อเหตุการณ์และเหมาะสม

๒.๒.๓ มีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนจะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลง หรือปรับปรุงบริการที่สำคัญ

๒.๒.๔ ตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคง มีประสิทธิภาพต่อการรับมือกับภัยคุกคามทางไซเบอร์

๒.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาต และตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๒.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญ ได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้

๒.๓.๒.๑ เปิดใช้งานการเชื่อมต่อไปยังหรือจากไคลเอนต์ระยะไกล เมื่อจำเป็น

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

๒.๓.๒.๓ ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๒.๓.๒.๔ ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

๒.๓.๒.๕ จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ กำหนดมาตรฐานควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แฟลชไดรฟ์ กับบริการที่สำคัญ โดยปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนและบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรายกรณี พร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๕ การสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

การสร้างความรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่าง ๆ ที่สำนักงานเศรษฐกิจการคลังกำหนด ให้กับบุคลากรในหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องมีการกำหนดขั้นตอน รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้

๓. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

ต้องมีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ และวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง โดยต้องมีการทบทวนกลไกและกระบวนการ อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๔. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน และปรับปรุง ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อย ปีละ ๑ ครั้ง เพื่อให้การรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

ต้องมีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงการประสานงานระหว่างฝ่ายที่ได้รับผลกระทบ และมีการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤต อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันทั่วถึงและมีประสิทธิภาพในช่วงวิกฤต

๔.๓ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ทั้งในระดับชาติหรือระดับภาคส่วน โดยบุคคลที่เกี่ยวข้องที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ ต้องมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๕. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของสำนักงานเศรษฐกิจการคลัง สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อให้พิจารณาความสอดคล้องกับแผนของสำนักงานเศรษฐกิจการคลัง เช่น ความสอดคล้องกันของขอบเขตค่านิยามและการกำหนดระยะเวลา ที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

๕.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผน BCP อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
