



ประมวลแนวทางปฏิบัติและกรอบมาตรฐาน
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของสำนักงาน กสทช.

สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

ฉบับวันที่ 28 ตุลาคม 2569

จัดทำโดย
สำนักกำกับดูแลกิจการโทรคมนาคม (ดท.)
สำนักงาน กสทช.

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

ส่วนที่ ๑ บทนำ

๑.๑ เหตุผลความจำเป็น

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคมเป็นไปอย่างเหมาะสมกับลักษณะของระบบ โครงข่าย และบริการโทรคมนาคม รวมทั้งความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อการให้บริการที่สำคัญ จึงได้จัดทำประมวลแนวทางปฏิบัติฉบับนี้ขึ้น เพื่อกำหนดแนวทางและข้อกำหนดขั้นต่ำในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานดังกล่าว โดยให้ใช้ร่วมกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

การใช้และการตีความประมวลแนวทางปฏิบัติ

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ ให้ใช้สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม ซึ่งอยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. โดยให้ใช้ร่วมกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

การใช้และการตีความประมวลแนวทางปฏิบัติฉบับนี้ ให้เป็นไปตามขอบเขต คำนิยาม และหลักการประยุกต์ใช้ที่กำหนดไว้ในกรอบมาตรฐานดังกล่าว เว้นแต่ประมวลแนวทางปฏิบัติฉบับนี้จะกำหนดไว้เป็นการเฉพาะ

ข้อกำหนดในประมวลแนวทางปฏิบัติฉบับนี้เป็นข้อกำหนดขั้นต่ำที่หน่วยงานต้องดำเนินการตามขอบเขตที่เกี่ยวข้อง โดยพิจารณาตามระดับความเสี่ยง ความสำคัญของระบบและบริการ ผลกระทบที่อาจเกิดขึ้น และหลักความได้สัดส่วน (Proportionality) ทั้งนี้ ต้องไม่ขัดต่อกฎหมาย กฎ ระเบียบ ประกาศ และข้อกำหนดที่มีผลใช้บังคับ

ในกรณีที่ข้อกำหนดมิได้กำหนดวิธีการหรือเทคโนโลยีไว้เป็นการเฉพาะ หน่วยงานสามารถเลือกใช้มาตรการ วิธีการ สถาปัตยกรรม หรือเทคโนโลยีที่เหมาะสมกับบริบทของตนได้ โดยต้องสามารถแสดงหลักฐานที่เหมาะสมว่ามาตรการดังกล่าวบรรลุวัตถุประสงค์และผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ข้อกำหนดนั้นมุ่งหมาย

การใช้มาตรการชดเชย (Compensating Controls) ให้เป็นไปตามหลักการที่กำหนดไว้ในกรอบมาตรฐาน และต้องไม่เป็นการยกเว้นหรือหลีกเลี่ยงข้อกำหนดตามกฎหมายที่มีผลใช้บังคับ

๑.๒ วัตถุประสงค์

เพื่อให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม ซึ่งอยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. มีแนวทางปฏิบัติในการดำเนินการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล และเหมาะสมกับลักษณะของระบบและโครงสร้างพื้นฐานโทรคมนาคม รวมถึงความสำคัญและความต่อเนื่องของบริการที่สำคัญ

๑.๓ หลักการสำคัญที่เกี่ยวข้อง

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม ประยุกต์ใช้หลักตามมาตรฐานและแนวปฏิบัติที่เป็นที่ยอมรับในระดับสากล โดยมุ่งเน้นให้หน่วยงานสามารถใช้เป็นแนวทางในการกำหนดและดำเนินการมาตรการควบคุม

ด้านความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ เพื่อให้สามารถบริหารจัดการความเสี่ยงทางไซเบอร์ได้อย่างเหมาะสมและสอดคล้องกับภารกิจ บทบาท และลักษณะการให้บริการโทรคมนาคมของแต่ละหน่วยงานซึ่งอาจมีความแตกต่างกัน

มาตรการควบคุมแต่ละข้อจึงอาจมีความสำคัญไม่เท่ากัน หน่วยงานต้องนำไปใช้ให้เหมาะสมตามระดับความเสี่ยง ความสำคัญของระบบและบริการที่สำคัญ และทรัพยากรที่มีอยู่ของหน่วยงาน โดยอยู่บนพื้นฐานของหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) รวมทั้งการเตรียมความพร้อมในการฟื้นฟูและการให้บริการที่สำคัญได้อย่างต่อเนื่องเมื่อเกิดภัยคุกคามทางไซเบอร์ (Cyber Resilience) เพื่อให้มั่นใจได้ว่าข้อมูล ระบบและโครงสร้างพื้นฐานโทรคมนาคม รวมถึงโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมของหน่วยงานมีความมั่นคงปลอดภัยและรองรับการให้บริการที่สำคัญได้อย่างมีประสิทธิภาพ

๑.๔ โครงสร้างของเอกสาร

โครงสร้างของเอกสารประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม ประกอบด้วย ๓ ส่วน คือ บทนำ ข้อกำหนดทั่วไป และข้อกำหนดเฉพาะ ทั้งนี้ การกำหนดว่าหน่วยงานจะต้องดำเนินการในข้อกำหนดใด ให้พิจารณาตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และข้อกำหนดที่เกี่ยวข้อง

ส่วนที่ ๑ บทนำ กำหนดเหตุผลความจำเป็น วัตถุประสงค์ หลักการสำคัญ โครงสร้าง ขอบเขต และเอกสารอ้างอิงที่เกี่ยวข้อง

ส่วนที่ ๒ ข้อกำหนดทั่วไป ประกอบด้วย ๗ หัวข้อหลัก ดังนี้

- ๑) การตรวจสอบ (Audit)
- ๒) การกำกับดูแล (Govern)
- ๓) การระบุ (Identify)
- ๔) การป้องกัน (Protect)
- ๕) การตรวจพบ (Detect)
- ๖) การรับมือ (Respond)
- ๗) การฟื้นฟู (Recover)

ส่วนที่ ๓ ข้อกำหนดเฉพาะ ประกอบด้วย ๒ หัวข้อหลัก ดังนี้

- ๑) ความพร้อมรับมือทางไซเบอร์ (Cyber Resilience)
- ๒) ความมั่นคงปลอดภัยของระบบและโครงสร้างพื้นฐานโทรคมนาคม (Telecommunications Systems and Infrastructure Security)

๑.๕ ขอบเขต

ประมวลแนวทางปฏิบัติฉบับนี้ใช้กับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือให้บริการด้านโทรคมนาคม ซึ่งอยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ขอบเขตการดำเนินการให้ครอบคลุมบริการที่สำคัญ ระบบและโครงสร้างพื้นฐานโทรคมนาคม ระบบสารสนเทศ และโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่เกี่ยวข้องกับการให้บริการที่สำคัญ โดยพิจารณาตามขอบเขต คำนียาม และหลักการประยุกต์ใช้ที่กำหนดไว้ในกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

๑.๖ การอ้างอิงที่เกี่ยวข้อง

ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม อ้างอิงตามมาตรฐานและแนวปฏิบัติที่เป็นที่ยอมรับในระดับสากล ที่สำคัญ ได้แก่ The NIST Cybersecurity Framework (CSF) 2.0 และ ISO/IEC 27103:2026 รวมทั้งให้ใช้ร่วมกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

คำศัพท์ที่ใช้ในประมวลแนวทางปฏิบัติฉบับนี้ให้มีความหมายตามที่กำหนดไว้ในกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม เว้นแต่จะกำหนดไว้เป็นอย่างอื่นในประมวลแนวทางปฏิบัติฉบับนี้

๑.๗ ความเกี่ยวข้องกับเอกสารอื่น

- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. ๒๕๖๘

๑.๘ การปฏิบัติในกรณีที่ยังไม่มีหลักเกณฑ์และวิธีการเฉพาะ

ในกรณีที่ข้อกำหนดตามประมวลแนวทางปฏิบัติฉบับนี้อ้างถึงหลักเกณฑ์ วิธีการ รูปแบบ หรือแนวทางที่สำนักงาน กสทช. สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หรือหน่วยงานที่มีอำนาจตามกฎหมายกำหนด แต่ยังไม่มีการกำหนดหลักเกณฑ์หรือวิธีการเฉพาะในเรื่องนั้น ให้หน่วยงานกำหนดแนวทางและวิธีการดำเนินงานที่เหมาะสมกับลักษณะของระบบและบริการที่สำคัญ โดยพิจารณาจากผลการประเมินความเสี่ยง ความสำคัญของบริการ ข้อจำกัดทางเทคนิค ผลกระทบต่อความมั่นคงปลอดภัยและความต่อเนื่องของบริการ ตลอดจนมาตรฐานสากลหรือแนวปฏิบัติที่ได้รับการยอมรับและเกี่ยวข้อง

ทั้งนี้ หน่วยงานต้องสามารถแสดงเหตุผลและหลักฐานประกอบการกำหนดแนวทางดังกล่าวได้ตามความเหมาะสม และเมื่อหน่วยงานที่มีอำนาจได้กำหนดหลักเกณฑ์หรือวิธีการเฉพาะที่มีผลใช้บังคับแล้ว ให้หน่วยงานทบทวนและปรับปรุงการดำเนินงานให้สอดคล้องกับหลักเกณฑ์หรือวิธีการดังกล่าวภายในระยะเวลาที่กำหนด

การดำเนินการตามวรรคหนึ่งต้องไม่เป็นการยกเว้นหรือลดทอนหน้าที่ตามกฎหมาย ประกาศ หลักเกณฑ์ หรือข้อกำหนดอื่นที่มีผลใช้บังคับอยู่แล้ว

ส่วนที่ ๒ ข้อกำหนดทั่วไป

๒.๑ การตรวจสอบ (Audit)

๒.๑.๑ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

(ข) บริการที่สำคัญที่หน่วยงานเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประมวลแนวทางปฏิบัตินี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่ กมช. ประกาศกำหนด

ทั้งนี้ ผู้บริหารระดับสูงของหน่วยงานต้องรับทราบผลการตรวจสอบดังกล่าวด้วย

๒.๑.๒ หน่วยงานจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จ ตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้สำนักงาน กสทช. ด้วย

ทั้งนี้ รูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ให้เป็นไปตามที่สำนักงานประกาศกำหนด

๒.๑.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๒.๑.๑ เว้นแต่ กมช. จะกำหนดไว้เป็นอย่างอื่น ให้หน่วยงานส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๒.๑.๓ (ก)

๒.๑.๔ ในกรณีที่ กมช. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กมช. กำหนด พร้อมทั้งส่งสำเนาให้สำนักงาน กสทช. ด้วย

๒.๑.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กมช. หน่วยงานจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กมช.

๒.๒ การกำกับดูแล (Govern)

๒.๒.๑ บริบทของหน่วยงาน (Organizational Context)

ต้องดำเนินการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) เพื่อระบุทรัพย์สินและบริการที่สำคัญต่อการบรรลุภารกิจของหน่วยงาน รวมทั้งประเมินผลกระทบที่อาจเกิดขึ้นจากการสูญเสียหรือการหยุดชะงักของการดำเนินงานดังกล่าว ไม่ว่าทั้งหมดหรือบางส่วน และต้องสื่อสารผลการวิเคราะห์ให้ผู้ที่เกี่ยวข้องรับทราบอย่างเหมาะสม

๒.๒.๒ กลยุทธ์ในการจัดการความเสี่ยง (Risk Management Strategy)

๒.๒.๒.๑ ต้องจัดทำกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เป็นลายลักษณ์อักษร กรอบจะรวมถึง :

- (ก) ระบุเกณฑ์ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)
- (ข) กำหนดกลยุทธ์เกี่ยวกับทางเลือกในการตอบสนองความเสี่ยงทางไซเบอร์
- (ค) กำหนดวิธีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- (ง) กำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการกิจหรือบริการที่สำคัญของหน่วยงาน

๒.๒.๒.๒ ต้องกำหนดวิธีการและช่วงเวลาในการสื่อสารสถานะด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานไปยังบุคลากรที่เกี่ยวข้อง

๒.๒.๓ บทบาทหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ (Roles, Responsibilities, and Authorities)

๒.๒.๓.๑ ต้องจัดโครงสร้างหน่วยงาน พร้อมกำหนด อำนาจหน้าที่ บทบาทหน้าที่ และความรับผิดชอบที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ที่มีประสิทธิภาพ โดยมีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิภาพ

- (ก) หน่วยงานหรือผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในขั้นแรก (Business Unit หรือ First Line of Defense) มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่กำหนดไว้ มีการควบคุมภายใน และมีการจัดการความเสี่ยงอย่างเหมาะสม
- (ข) หน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) มีหน้าที่กำกับ ตรวจสอบ สนับสนุน ให้คำปรึกษา รวมถึงติดตามผลการปฏิบัติงานของหน่วยงานขั้นแรก ตลอดจนกำหนดกรอบนโยบายและแนวทางการบริหารความเสี่ยงให้สอดคล้องกับนโยบาย มาตรฐาน รวมถึงแนวทางปฏิบัติที่ผู้บริหารสูงสุดได้กำหนดไว้ เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance)
- (ค) หน่วยงานหรือผู้ตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) มีหน้าที่ประเมิน ตรวจสอบ และให้ความเชื่อมั่นว่าการดำเนินงาน และการควบคุมตามมาตรฐานที่หน่วยงานขั้นแรกและขั้นที่สองกำกับอยู่นั้น มีประสิทธิภาพและสอดคล้องกับกฎเกณฑ์ทั้งภายในและภายนอกหรือไม่

รวมไปถึงกำหนดให้หน่วยงานจะต้องปฏิบัติตามกฎหมายหรือหลักเกณฑ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องในปัจจุบัน รวมถึง นโยบาย หลักเกณฑ์ หรือแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จะออกโดยสำนักงาน กสทช. และจะมีผลบังคับใช้กับหน่วยงานต่อไป

ทั้งนี้ กรณีที่มีโครงสร้างการกำกับดูแลความเสี่ยงด้านเทคโนโลยีสารสนเทศร่วมกับบริษัทในกลุ่มธุรกิจเดียวกันหรือบริษัทที่มีความเกี่ยวข้อง การพิจารณาโครงสร้างการกำกับดูแลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) ให้พิจารณาโดยดูจากภาพรวมทั้งหมดของกลุ่มธุรกิจเดียวกัน

๒.๒.๓.๒ ต้องจัดให้มีผู้บริหารระดับสูงทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ดังกล่าวควรมีความเป็นอิสระจากงานด้านการปฏิบัติการ (Operation) และงานด้านการพัฒนาระบบ (Development) ทั้งในส่วนของเทคโนโลยีสารสนเทศ (Information Technology) ระบบและโครงสร้างพื้นฐานโทรคมนาคม (Telecommunications Systems and Infrastructure) และโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม (Telecommunications Supporting Infrastructure) รวมทั้งควรมีบทบาท หน้าที่ ความรับผิดชอบ และอำนาจหน้าที่อย่างเพียงพอ เพื่อให้สามารถปฏิบัติหน้าที่ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและประสิทธิผล

โดยต้องกำหนดบทบาท หน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ดังกล่าวเป็นลายลักษณ์อักษร และครอบคลุมการดำเนินการอย่างน้อย ดังนี้

- (ก) จัดทำนโยบาย มาตรฐาน และแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางปฏิบัติที่กำหนด
- (ข) จัดทำข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Specification) และสถาปัตยกรรม ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Architecture)
- (ค) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับกรอบการบริหารความเสี่ยงของหน่วยงาน และนำเสนอความเสี่ยงดังกล่าวต่อผู้บริหารสูงสุดหรือคณะกรรมการของหน่วยงานเป็นวาระประจำ
- (ง) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือเหตุภัยคุกคามทางไซเบอร์
- (จ) ดูแลและดำเนินการให้บุคลากรในหน่วยงานมีความรู้และความตระหนักรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- (ฉ) รายงานปัญหาหรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารสูงสุด และผู้บริหารที่เกี่ยวข้อง
- (ช) ให้ความเห็นเกี่ยวกับการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อผู้บริหารสูงสุดหรือคณะกรรมการของหน่วยงานที่เกี่ยวข้องกับการบริหารจัดการและกำกับดูแลด้านเทคโนโลยีสารสนเทศ ระบบและโครงสร้างพื้นฐานโทรคมนาคม โครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม หรือด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น คณะกรรมการกำกับดูแลด้านเทคโนโลยีสารสนเทศและโทรคมนาคม (IT and Telecommunications Steering Committee) คณะกรรมการบริหารความเสี่ยง (Risk Management Committee) หรือคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Committee) ตามโครงสร้างการกำกับดูแลของหน่วยงาน

ในกรณีที่หน่วยงานไม่สามารถกำหนดให้ CISO มีความเป็นอิสระจากงานด้านการปฏิบัติการหรือการพัฒนาระบบได้ หน่วยงานต้องกำหนดมาตรการทดแทนที่เหมาะสมเพื่อป้องกันหรือบรรเทาความขัดกันของหน้าที่ (Conflict of Interest) ที่อาจเกิดขึ้น รวมทั้งต้องจัดให้มีกลไกการกำกับดูแล

และการสอบทานที่เหมาะสม และกำหนดให้ CISO สามารถรายงานต่อผู้บริหารสูงสุดหรือคณะกรรมการที่เกี่ยวข้องของหน่วยงานได้อย่างเหมาะสมตามระดับความเสี่ยงของหน่วยงาน

๒.๒.๔ นโยบาย (Policy)

๒.๒.๔.๑ ต้องกำหนด และอนุมัตินโยบาย มาตรฐาน และแนวทางปฏิบัติในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และการปกป้องภารกิจหรือบริการที่สำคัญของหน่วยงานจากภัยคุกคามทางไซเบอร์ ทั้งนี้ นโยบาย มาตรฐาน และแนวทางปฏิบัติจะต้อง

- (ก) สอดคล้องกับประมวลแนวทางปฏิบัตินี้ รวมถึงข้อกำหนดการรักษาความมั่นคงปลอดภัยไซเบอร์ของภาคส่วน และอาจรวมไปถึงนโยบาย มาตรฐาน และแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับภูมิภาค หรือกฎหมายในประเทศหรือระหว่างประเทศ
- (ข) เผยแพร่และสื่อสารนโยบาย มาตรฐาน และแนวทางปฏิบัติไปยังบุคลากร และบุคคลภายนอกที่ทำหน้าที่หรือสามารถเข้าถึงภารกิจหรือบริการที่สำคัญของหน่วยงาน

๒.๒.๔.๒ ต้องทบทวนนโยบาย มาตรฐาน และแนวทางปฏิบัติกับสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของภารกิจหรือบริการที่สำคัญของหน่วยงาน และภูมิทัศน์ภัยคุกคามทางไซเบอร์ (Cyber Threat Landscape) ซึ่งครอบคลุมลักษณะและแนวโน้มของภัยคุกคามทางไซเบอร์ที่เกี่ยวข้อง เช่น รูปแบบการโจมตี ช่องโหว่ที่ถูกใช้ประโยชน์ และภัยคุกคามต่อระบบหรือโครงข่ายโทรคมนาคมในปัจจุบันอย่างน้อยปีละหนึ่งครั้ง โดยนับถัดจากวันที่ทบทวนครั้งสุดท้ายหรือวันที่มีผลบังคับใช้ของนโยบาย มาตรฐาน หรือแนวทางปฏิบัติแต่ละข้อ

๒.๒.๕ การจัดการความเสี่ยงในห่วงโซ่อุปทานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Supply Chain Risk Management)

๒.๒.๕.๑ ต้องกำหนดนโยบาย กลยุทธ์ กระบวนการ และข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อจัดการความเสี่ยงที่เกิดจากห่วงโซ่อุปทาน รวมถึงการพัฒนา การเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของบริการที่สำคัญหรือโครงสร้างพื้นฐานสำคัญของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ลูกค้า และพันธมิตรทางธุรกิจ ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

- (ก) ประเภทและโปรไฟล์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile and Type) ของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินสารสนเทศที่สนับสนุนภารกิจหรือบริการที่สำคัญของหน่วยงาน
- (ข) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องภารกิจหรือบริการที่สำคัญของหน่วยงาน
- (ค) ความเสี่ยงและการควบคุมที่เกี่ยวข้องกับภารกิจหรือบริการที่สำคัญและห่วงโซ่อุปทานผลิตภัณฑ์ โดยพิจารณาให้ครอบคลุมมิติขององค์กร เทคโนโลยี บุคลากร และสภาพแวดล้อมทางกายภาพ และ
- (ง) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๒.๒.๕.๒ กำหนดกระบวนการและเกณฑ์การประเมินด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก ผู้ผลิต ผลิตภัณฑ์ หรือบริการ ในกระบวนการจัดซื้อจัดจ้างตามระดับความเสี่ยงและ

ความสำคัญต่อบริการที่สำคัญ รวมถึงดำเนินการให้มั่นใจว่าผู้ให้บริการภายนอกปฏิบัติตามข้อตกลงกับข้อกำหนดหรือมาตรฐานด้านความมั่นคงปลอดภัยไซเบอร์และข้อกำหนดที่ระบุไว้ในสัญญา โดยอาจพิจารณาหลักฐานการรับรองตามมาตรฐานสากล การตรวจสอบโดยบุคคลที่สาม การตรวจสอบผลิตภัณฑ์ หรือมาตรฐานที่ได้รับการยอมรับในอุตสาหกรรมตามความเหมาะสม

๒.๒.๕.๓ พิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

๒.๒.๕.๔ กำหนดความรับผิดชอบและข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอกไว้ในสัญญา ข้อตกลงระดับการให้บริการ (Service Level Agreement: SLA) หรือข้อตกลงอื่นที่เกี่ยวข้องตามความเหมาะสม รวมถึงสิทธิในการตรวจสอบหรือการได้รับหลักฐานยืนยันการปฏิบัติตามข้อกำหนด โดยพิจารณาจากระดับความเสี่ยง ความสำคัญของบริการ และลักษณะของการให้บริการ

๒.๒.๕.๕ ตรวจสอบความถูกต้อง ความน่าเชื่อถือ และความมั่นคงปลอดภัยของฮาร์ดแวร์ ซอฟต์แวร์ หรือเฟิร์มแวร์ที่จัดหามา ก่อนนำไปใช้งานกับระบบสำคัญตามระดับความเสี่ยง โดยอาจใช้วิธีการตรวจสอบแหล่งที่มา การตรวจสอบความถูกต้องครบถ้วนของฮาร์ดแวร์และซอฟต์แวร์ (Hardware/Software Integrity Testing) การตรวจสอบมัลแวร์หรือช่องโหว่ หรือการตรวจสอบหลักฐานการรับรองจากผู้ผลิตหรือผู้ให้บริการตามความเหมาะสม

๒.๒.๕.๖ สำหรับซอฟต์แวร์หรือส่วนประกอบซอฟต์แวร์ที่มีนัยสำคัญต่อบริการที่สำคัญ หน่วยงานต้องมีข้อมูลที่เพียงพอสำหรับการระบุ ติดตาม และประเมินความเสี่ยงของส่วนประกอบดังกล่าว โดยอย่างน้อยให้สามารถระบุผลิตภัณฑ์หรือส่วนประกอบ รุ่น (Version) ผู้ผลิตหรือผู้พัฒนา สถานะการสนับสนุน แหล่งข้อมูลด้านช่องโหว่หรือการปรับปรุงแก้ไข และการพึ่งพาที่มีนัยสำคัญตามความเหมาะสม เพื่อสนับสนุนการบริหารช่องโหว่ การวิเคราะห์ผลกระทบ และการตอบสนองต่อเหตุการณ์

๒.๒.๕.๗ ในกรณีที่ผู้ให้บริการภายนอก ผู้ผลิต หรือผู้พัฒนามีหน้าที่สนับสนุนระบบสำคัญ ต้องกำหนดหน้าที่ในการแจ้งช่องโหว่ การจัดหาแพตช์หรือมาตรการบรรเทา การแจ้งการสิ้นสุดการสนับสนุน และการประสานงานเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ไว้ในสัญญา ข้อตกลง หรือข้อกำหนดที่เกี่ยวข้องตามความเหมาะสม

๒.๓ การระบุ (Identify)

๒.๓.๑ การบริหารทรัพย์สินและวงจรชีวิตเทคโนโลยี (Asset and Technology Lifecycle Management)

๒.๓.๑.๑ ต้องมีทะเบียนทรัพย์สินสารสนเทศ (Inventory) ที่ระบุทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงานและดูแลรักษาทะเบียนทรัพย์สินสารสนเทศให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินสารสนเทศต้องมีข้อมูลอย่างน้อย ดังนี้

- (ก) ชื่อและคำอธิบายของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงาน
- (ข) พังก์ชันที่สำคัญของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงาน
- (ค) การระบุและการจัดลำดับความสำคัญของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงาน
- (ง) เจ้าของหรือผู้ดำเนินการของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงาน

- (จ) ตำแหน่งทางกายภาพของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงานแต่ละรายการ และ
- (ฉ) การขึ้นต่อกันของทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงานบนระบบและเครือข่ายภายในหรือภายนอก
- (ช) รุ่นของซอฟต์แวร์ เฟิร์มแวร์ หรือระบบปฏิบัติการ และข้อมูลที่สำคัญต่อการระบุทรัพย์สินตามความเหมาะสม และ
- (ซ) สถานะวงจรชีวิตและการสนับสนุนของทรัพย์สิน รวมถึง End-of-Life (EOL) หรือ End-of-Support (EOS) ในกรณีที่เกี่ยวข้อง

๒.๓.๑.๒ ต้องมีแผนผังเครือข่าย (Network Diagram) รวมถึงการไหลของข้อมูลภายในเครือข่าย และต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงาน และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๒.๓.๑.๓ ต้องมีการตรวจสอบทะเบียนทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง และปรับปรุงทะเบียนทรัพย์สินสารสนเทศให้เป็นปัจจุบัน หากพบการเปลี่ยนแปลงใด ๆ กับทรัพย์สินสารสนเทศของภารกิจหรือบริการที่สำคัญของหน่วยงาน

๒.๓.๑.๔ ต้องระบุและบันทึกตำแหน่งและการเปลี่ยนแปลงตำแหน่งของข้อมูลหรือระบบสารสนเทศของหน่วยงาน และวิธีการประมวลผลข้อมูลเพื่อให้สามารถเข้าใจการไหลของข้อมูล รวมทั้งระบุและบันทึกผู้ใช้ที่มีสิทธิ์เข้าถึงระบบหรือส่วนประกอบของระบบที่ประมวลผลและจัดเก็บข้อมูลดังกล่าว

๒.๓.๑.๕ ต้องระบุและติดตามสถานะวงจรชีวิตของทรัพย์สินทางเทคโนโลยีที่มีนัยสำคัญต่อบริการที่สำคัญ รวมถึงสถานะการสนับสนุน การสิ้นสุดการสนับสนุน (End-of-Support: EOS) และการสิ้นสุดอายุผลิตภัณฑ์ (End-of-Life: EOL) และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้องตามความเหมาะสม

๒.๓.๒ การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้กับข้อมูลหรือระบบสารสนเทศโดยประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น ๓ ระดับ ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๒.๓.๓ การประเมินความเสี่ยง (Risk Assessment)

๒.๓.๓.๑ ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยง จากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยพิจารณาโอกาสที่ระดับความเสี่ยงและระดับผลกระทบจะเกิดขึ้น ซึ่งครอบคลุมทั้งผลกระทบต่อการปฏิบัติงาน และผลกระทบต่อการดำเนินภารกิจหรือการดำเนินธุรกิจของหน่วยงาน (Business Impact)

ทั้งนี้ การประเมินผลกระทบต้องอ้างอิงผลการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศตามข้อ ๒.๓.๒ นอกจากนี้ ต้องกำหนดระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เพื่อใช้เป็นเกณฑ์ในการบริหารจัดการความเสี่ยงดังกล่าว

(ง) การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

(จ) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

(ฉ) การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

๒.๓.๓.๒ สร้าง เก็บรักษา และปรับปรุงรายการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้ในทะเบียนความเสี่ยง (Risk Register) ที่เกี่ยวข้องกับการกิจหรือบริการที่สำคัญของหน่วยงานทะเบียนความเสี่ยงต้องจัดทำเอกสารโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- (ก) วันที่ระบุความเสี่ยง (Identification Date)
- (ข) คำอธิบายของความเสี่ยง (Description of the Risk)
- (ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
- (ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
- (จ) เจ้าของความเสี่ยง (Risk Owner)
- (ฉ) ความเสี่ยงในปัจจุบัน (Current Risk)
- (ช) การจัดการความเสี่ยง (Risk Treatment) และ
- (ซ) ความเสี่ยงที่เหลืออยู่ (Residual Risk)

๒.๓.๓.๓ ต้องติดตามความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุไว้อย่างสม่ำเสมอเพื่อให้แน่ใจว่าอยู่ภายใต้เกณฑ์ระดับความเสี่ยงที่ยอมรับได้ที่ระบุไว้ในข้อ ๒.๒.๒.๑ (ก)

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

๒.๓.๓.๕ ในกรณีที่มีระบบและโครงสร้างพื้นฐานโทรคมนาคม หรือโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม ซึ่งการทำงานผิดปกติ การหยุดชะงัก การถูกควบคุมโดยมิชอบ หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างมีนัยสำคัญต่อบริการที่สำคัญ หน่วยงานต้องประเมินความเสี่ยงโดยอย่างน้อยพิจารณา

- (ก) ผลกระทบต่อความพร้อมใช้ (Availability) ความเชื่อถือได้ (Reliability) และความต่อเนื่องของบริการ (Service Continuity)
- (ข) การพึ่งพาระหว่างระบบโทรคมนาคม ระบบบริหารจัดการ ระบบสนับสนุน การปฏิบัติงาน และโครงสร้างพื้นฐานสนับสนุน
- (ค) ความเสี่ยงจากการเข้าถึงหรือควบคุมระบบจากระยะไกล รวมถึงการเข้าถึงโดยผู้ให้บริการภายนอก
- (ง) ความเสี่ยงจากการเปลี่ยนแปลงการกำหนดค่า ซอฟต์แวร์ เฟิร์มแวร์ หรือองค์ประกอบของระบบ
- (จ) ความล้มเหลวขององค์ประกอบหรือการพึ่งพาจุดเดียว (Single Point of Failure) ที่อาจส่งผลกระทบต่อบริการที่สำคัญ และ
- (ฉ) มาตรการในการรักษาหรือฟื้นคืนการให้บริการในกรณีที่มาตรการด้านความมั่นคงปลอดภัยหรือระบบที่เกี่ยวข้องไม่สามารถทำงานได้ตามปกติ

๒.๓.๓.๖ ในกรณีที่มีการนำเทคโนโลยีใหม่มาใช้ หรือมีการเปลี่ยนแปลงระบบ เทคโนโลยีสถาปัตยกรรม หรือวิธีการดำเนินงานอย่างมีนัยสำคัญ และอาจส่งผลกระทบต่อระบบสำคัญหรือบริการที่สำคัญ หน่วยงานต้องประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องก่อนนำไปใช้งานหรือดำเนินการเปลี่ยนแปลงดังกล่าว

๒.๓.๓.๗ ในกรณีที่มีการนำปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้กับระบบสำคัญ หรือใช้เพื่อควบคุม บริหารจัดการ สนับสนุน หรือตัดสินใจที่อาจส่งผลกระทบต่อบริการที่สำคัญ หน่วยงานต้องประเมินและจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง โดยอย่างน้อยต้องพิจารณา

- (ก) วัตถุประสงค์ ขอบเขต และบทบาทของระบบ AI ต่อระบบสำคัญหรือบริการที่สำคัญ
- (ข) ข้อมูล แบบจำลอง (Model) ส่วนประกอบ บริการภายนอก หรือการพึ่งพาที่มีนัยสำคัญ
- (ค) ผลกระทบต่อความลับ ความถูกต้องครบถ้วน ความพร้อมใช้ ความเชื่อถือได้ และความต่อเนื่องของบริการ
- (ง) ความเสี่ยงจากการเข้าถึง การเปลี่ยนแปลง การใช้ หรือการสั่งการระบบ AI โดยไม่ได้รับอนุญาต
- (จ) กลไกในการกำกับดูแล ระบุ ย้อนกลับ หรือใช้วิธีการอื่นทดแทน ในกรณีที่ผลลัพธ์หรือการทำงานของระบบ AI อาจส่งผลกระทบต่อบริการที่สำคัญ และ
- (ฉ) การบันทึก ฝ้าระวัง และทบทวนการทำงานหรือการเปลี่ยนแปลงที่มีนัยสำคัญของระบบ AI ตามความเหมาะสม

๒.๓.๔ การบริหารช่องโหว่และการประเมินความมั่นคงปลอดภัย (Vulnerability Management and Security Assessment)

๒.๓.๔.๑ ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญตามหลักการบริหารความเสี่ยงของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยให้ครอบคลุมระบบสำคัญ ระบบและโครงสร้างพื้นฐานโทรคมนาคม และโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่อยู่ในขอบเขตตามความเหมาะสม

๒.๓.๔.๒ ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของซอฟต์แวร์ (Software Security Assessment)

(ข) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

(ค) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) และ

(ง) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๒.๓.๔.๓ ต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน อย่างน้อยทุก ๑๒ เดือน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับภารกิจหรือบริการที่สำคัญของหน่วยงาน การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี ทั้งนี้ การดำเนินการต้องคำนึงถึงผลกระทบต่อความพร้อมใช้และความต่อเนื่องของบริการ

หากได้รับการร้องขอจาก กกม. หรือสำนักงาน หน่วยงานต้องส่งสำเนารายงานการสรุปผลประเมินช่องโหว่ (Vulnerability Assessment) เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ได้รับหนังสือด้วย

๒.๓.๔.๔ ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เปิดให้บริการและเข้าถึงได้จากอินเทอร์เน็ต (Internet Facing) รวมถึงช่องทางบริหารจัดการจากภายนอกที่มีนัยสำคัญ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย รวมถึงขอบเขตการทดสอบเจาะระบบ (Scope of a Penetration Test) ได้แก่ การทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของภารกิจหรือบริการที่สำคัญของหน่วยงาน ทั้งนี้ ต้องกำหนดขอบเขต วิธีการ ระยะเวลา มาตรการป้องกันผลกระทบ และแนวทางการหยุดหรือย้อนกลับการทดสอบ เพื่อมิให้กระทบต่อความพร้อมใช้และความต่อเนื่องของบริการที่สำคัญ

๒.๓.๔.๕ ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบเป็นไปตามขอบเขตของการทดสอบเจาะระบบในการดำเนินงานตาม ๒.๓.๔.๔ และการทดสอบเจาะระบบไม่ทำให้บริการที่สำคัญดังกล่าวต้องหยุดชะงักลง

๒.๓.๔.๖ ในกรณีที่มีการนำระบบใหม่มาใช้งาน หรือมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญต่อบริการที่สำคัญ หน่วยงานต้องพิจารณาความจำเป็นในการทดสอบเจาะระบบเพิ่มเติมจากรอบการทดสอบตามข้อ ๒.๓.๔.๔ โดยคำนึงถึงลักษณะการเปลี่ยนแปลง ผลการประเมินความเสี่ยง ช่องโหว่ที่เกี่ยวข้อง และ

ผลกระทบที่อาจเกิดขึ้นต่อความพร้อมใช้และความต่อเนื่องของบริการ ทั้งนี้ อาจใช้วิธีการประเมินหรือทดสอบความมั่นคงปลอดภัยอื่นที่เหมาะสมกับลักษณะของระบบและระดับความเสี่ยงได้

๒.๓.๔.๗ ต้องตรวจสอบให้แน่ใจว่าผู้ทดสอบเจาะระบบ (Penetration Testers) ตามข้อ ๒.๓.๔.๔ และข้อ ๒.๓.๔.๖ มีความรู้ ความสามารถ และคุณสมบัติที่เหมาะสมกับลักษณะของระบบที่ทำการทดสอบ รวมถึงมีความเป็นอิสระจากระบบที่ทำการทดสอบตามความเหมาะสม

ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงาน กสทช. กำหนด โดยสำหรับการทดสอบระบบและโครงสร้างพื้นฐานโทรคมนาคม หรือโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม ผู้ทดสอบต้องมีความรู้ความเข้าใจด้านสถาปัตยกรรม การทำงาน และความมั่นคงปลอดภัยของระบบดังกล่าวอย่างเพียงพอ เพื่อป้องกันผลกระทบต่อบริการที่สำคัญ

๒.๓.๔.๘ ต้องจัดให้มีการตรวจสอบและรับทราบผลการทดสอบเจาะระบบตามข้อ ๒.๓.๔.๔ และข้อ ๒.๓.๔.๖ โดยผู้รับผิดชอบของหน่วยงาน รวมถึงพิจารณาข้อค้นพบ ผลกระทบต่อบริการที่สำคัญ และความจำเป็นในการดำเนินการแก้ไขหรือบรรเทาความเสี่ยง ทั้งนี้ ให้ติดตามและจัดการช่องโหว่ที่ตรวจพบตามข้อ ๒.๓.๔.๙

๒.๓.๔.๙ ต้องมีกระบวนการติดตามและจัดการช่องโหว่ที่ระบุจากการประเมินช่องโหว่การทดสอบเจาะระบบ การแจ้งเตือนจากผู้ผลิต ผู้ให้บริการภายนอก แหล่งข้อมูลช่องโหว่ หรือช่องทางอื่นที่เชื่อถือได้ โดยต้องประเมินและจัดลำดับความสำคัญของการแก้ไขตามระดับความรุนแรง ความสามารถในการถูกใช้ประโยชน์ ความสำคัญของระบบ และผลกระทบต่อบริการที่สำคัญ

หน่วยงานต้องกำหนดระยะเวลาเป้าหมายในการแก้ไขหรือบรรเทาช่องโหว่ตามระดับความเสี่ยง และติดตามสถานะจนแล้วเสร็จ ในกรณีที่ไม่สามารถแก้ไขภายในระยะเวลาที่กำหนด ต้องมีการประเมินความเสี่ยง บันทึกเหตุผล กำหนดมาตรการชดเชย (Compensating Controls) และได้รับการยอมรับความเสี่ยงจากผู้มีอำนาจตามที่หน่วยงานกำหนด

๒.๓.๔.๑๐ หากได้รับการร้องขอจาก กกม. หรือสำนักงาน ให้หน่วยงานส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ ไปยังสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ได้รับหนังสือร้องขอเพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว

ทั้งนี้ รูปแบบรายงานสรุปผลการทดสอบเจาะระบบ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒.๓.๕ การรับแจ้ง การจัดการ และการเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD)

๒.๓.๕.๑ หน่วยงานต้องจัดให้มีกระบวนการรับแจ้งและจัดการข้อมูลเกี่ยวกับช่องโหว่ที่เกี่ยวข้องกับระบบสำคัญหรือบริการที่สำคัญ โดยต้องกำหนดช่องทางรับแจ้งและผู้รับผิดชอบที่ชัดเจน

๒.๓.๕.๒ กระบวนการตามข้อ ๒.๓.๕.๑ ต้องครอบคลุมอย่างน้อย ดังต่อไปนี้

- (ก) การรับแจ้งและคัดกรอง (Triage)
- (ข) การตรวจสอบและยืนยันช่องโหว่ (Validation)
- (ค) การประเมินความเสี่ยงและผลกระทบ
- (ง) การประสานการแก้ไขหรือบรรเทาช่องโหว่กับผู้เกี่ยวข้อง
- (จ) การติดตามสถานะการแก้ไข และ
- (ฉ) การสื่อสารหรือเปิดเผยข้อมูลเกี่ยวกับช่องโหว่อย่างเหมาะสม โดยคำนึงถึงความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการเปิดเผยข้อมูล

๒.๓.๕.๓ หน่วยงานต้องกำหนดช่องทางติดต่อด้านช่องโหว่ที่สามารถเข้าถึงได้โดยผู้เกี่ยวข้อง และต้องมีการบันทึก ติดตามสถานะ ผู้รับผิดชอบ และผลการดำเนินการของรายงานช่องโหว่จนกว่าจะได้รับการแก้ไข บรรเทา หรือปิดประเด็นอย่างเหมาะสม ในกรณีที่ช่องโหว่เกี่ยวข้องกับผลิตภัณฑ์หรือบริการของบุคคลภายนอก ต้องมีกลไกประสานงานกับผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการที่เกี่ยวข้อง

๒.๓.๖ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๒.๓.๖.๑ ต้องมีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ในระดับชาติ ซึ่งเป็นการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น รวมถึงการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ในระดับภาคส่วนและภายในหน่วยงานของตน ทั้งนี้ หน่วยงานต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้องที่ระบุไว้ในแผนรับมือเหตุภัยคุกคามทางไซเบอร์แห่งชาติ หรือแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของหน่วยงาน มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๒.๓.๖.๒ ต้องปฏิบัติตามคำขอใด ๆ ของ กกม. โดยให้ข้อมูลที่เกี่ยวข้องกับการกิจหรือบริการที่สำคัญของหน่วยงาน เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่ กกม. อาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือเหตุภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้นตามข้อ ๒.๖.๑.๑ และข้อ ๒.๖.๓.๓ ขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินการของภารกิจหรือบริการที่สำคัญของหน่วยงาน รวมไปถึงรายงานเหตุภัยคุกคามทางไซเบอร์ด้วย

๒.๔ การป้องกัน (Protect)

๒.๔.๑ การจัดการอัตลักษณ์ การยืนยันตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication, and Access Controls)

๒.๔.๑.๑ การจัดการบัญชี (Account Management)

ต้องดำเนินการในส่วนที่เกี่ยวข้องกับบัญชีผู้ใช้ โปรแกรมประยุกต์ บริการ หรือบัญชีระบบ ดังนี้

- (ก) มีการพิสูจน์และตรวจสอบอัตลักษณ์ของบุคคล (Identity Proofing) รวมทั้งผูกข้อมูลอัตลักษณ์กับข้อมูลรับรองการเข้าถึง (Binding Identities to Credentials) ให้เหมาะสมและสอดคล้องกับระดับความเสี่ยงของการใช้งาน และทรัพยากรที่เข้าถึง ทั้งนี้ สำหรับบริการที่สำคัญที่จำเป็นต้องพิสูจน์อัตลักษณ์ของบุคคล ให้กำหนดระดับความน่าเชื่อถือในการพิสูจน์อัตลักษณ์ (Identity Assurance Level: IAL) ตามระดับความเสี่ยงและข้อกำหนดที่เกี่ยวข้อง โดยอาจใช้ระดับ IAL2 เป็นแนวทางสำหรับกรณีที่ต้องการความน่าเชื่อถือในระดับดังกล่าว และอาจใช้บริการพิสูจน์และยืนยันตัวตนดิจิทัล เช่น ThaiID, NDID หรือบริการที่เกี่ยวข้องผ่านแอปพลิเคชันทางรัฐ โดยพิจารณาระดับความน่าเชื่อถือและขอบเขตการให้บริการที่รองรับเป็นรายกรณีสำหรับระบบและโครงข่ายโทรคมนาคม เช่น ระบบโครงข่ายหลัก (Core Network) ระบบสนับสนุนการปฏิบัติงาน (OSS) ระบบบริหารจัดการเครือข่าย (NMS) อุปกรณ์โครงข่าย หรือระบบอัตโนมัติที่ไม่เหมาะสมกับการพิสูจน์อัตลักษณ์ตามระดับ IAL ดังกล่าว ให้หน่วยงานกำหนดกลไกการพิสูจน์อัตลักษณ์ การยืนยันตัวตน และการควบคุมการเข้าถึงที่เหมาะสม

กับประเภทของบัญชี ลักษณะของระบบ ระดับความเสี่ยง และข้อจำกัดทางเทคนิค โดยต้องสามารถตรวจสอบย้อนกลับได้ตามความเหมาะสม และใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับการเข้าถึงโดยบุคคลตามข้อกำหนดที่เกี่ยวข้อง

- (ข) ปกป้องและตรวจสอบความถูกต้องของข้อมูลการยืนยันตัวตน (Identity Assertions) รวมทั้งต้องส่งข้อมูลดังกล่าวผ่านช่องทางที่ปลอดภัย โดยให้สอดคล้องกับระดับความเสี่ยง
- (ค) ตรวจสอบให้แน่ใจว่าไม่มีการสร้างบัญชีผู้ใช้ร่วมกัน ยกเว้นกรณีมีความจำเป็นในด้านการดำเนินการเท่านั้น
- (ง) กำหนดกลไกและกระบวนการในการติดตามกิจกรรมของแต่ละบัญชี รวมถึงรูปแบบพฤติกรรมความผิดปกติ และเพื่อส่งสัญญาณเตือนในการสืบสวนเมื่อตรวจพบความผิดปกติ
- (จ) ลบหรือปิดการใช้งานบัญชีที่ไม่จำเป็นและบัญชีที่ไม่ได้ใช้งาน
- (ฉ) ต้องดำเนินการตรวจสอบเพื่อให้แน่ใจว่าสิทธิที่กำหนดให้กับแต่ละบัญชีถูกต้องอย่างน้อยทุก ๑๒ เดือน โดยการตรวจสอบครั้งแรกจะต้องเสร็จสิ้นภายใน ๑๒ เดือนหลังจากวันที่ปฏิบัติตามข้อกำหนด

๒.๔.๑.๒ การจัดการการเข้าถึงที่มีสิทธิพิเศษ (Privileged Access Management)

ต้องดำเนินการในส่วนของบัญชีที่มีสิทธิพิเศษ ดังนี้

- (ก) ตรวจสอบให้แน่ใจว่าการเข้าถึงที่มีสิทธิพิเศษ (เช่น การเข้าถึงระดับผู้ดูแลระบบ) จะถูกมอบให้เฉพาะบัญชีที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น
- (ข) ต้องมีรายการบัญชีที่มีสิทธิพิเศษ ระบุรายละเอียดของสิทธิและสิทธิพิเศษที่กำหนดให้แต่ละบัญชีและดูแลรักษาให้เป็นปัจจุบัน
- (ค) ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับบัญชีที่มีสิทธิพิเศษและบัญชีที่ได้รับการยกระดับไปสู่ระดับการเข้าถึงที่มีสิทธิพิเศษหลังจากเข้าสู่ระบบครั้งแรก

(ง) ตรวจสอบให้แน่ใจว่าการเข้าถึงที่มีสิทธิพิเศษเริ่มต้นจากสภาพแวดล้อมที่มีความมั่นคงปลอดภัยทางไซเบอร์ และการถ่ายโอนข้อมูลดำเนินการผ่านการเชื่อมต่อที่ได้รับอนุญาต

๒.๔.๑.๓ การควบคุมการเข้าถึง (Access Control)

- (ก) มอบสิทธิขั้นต่ำ (Least Privilege) เท่าที่จำเป็นให้กับแต่ละบัญชีตามการใช้และฟังก์ชันการทำงาน (Separation of Duties)
- (ข) ตรวจสอบให้แน่ใจว่าสิทธิในการติดตั้งซอฟต์แวร์จะได้รับการมอบให้เฉพาะบัญชีที่ได้รับอนุญาตให้ติดตั้งเท่านั้น
- (ค) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงบริการที่สำคัญของหน่วยงานถูกจำกัดไว้ที่
 - บุคลากร และกิจกรรมที่ได้รับอนุญาต และ
 - อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต
- (ง) ในส่วนที่เกี่ยวกับภาระหน้าที่ภายใต้ข้อ ๒.๔.๑.๓ (ค) หน่วยงานต้องกำหนดให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตมีการใช้เทคนิคการยืนยันตัวตนที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมด

การเข้าถึงบริการที่สำคัญของหน่วยงาน โดยโพรไฟล์ความเสี่ยงดังกล่าวสามารถจัดทำหรือกำหนดขึ้นจากข้อมูลโพรไฟล์ของหน่วยงาน (Organization Profile) และผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง โดยไม่จำเป็นต้องจัดทำเป็นเอกสารแยกต่างหาก ทั้งนี้ สำหรับการเข้าถึงระบบสำคัญหรือระบบที่เกี่ยวข้องกับบริการที่สำคัญด้วยบัญชีผู้ใช้งานที่เป็นบุคคล หน่วยงานต้องกำหนดให้ใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ตามระดับความเสี่ยงและลักษณะการเข้าถึง โดยคำนึงถึงข้อจำกัดทางเทคนิคและผลกระทบต่อความต่อเนื่องของบริการ

- (จ) ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการดำเนินการภายใต้การดูแลของหน่วยงานเท่านั้น และดำเนินการในสถานที่ หากเป็นไปได้
- (ฉ) ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ในพื้นที่สำคัญ เช่น ห้องเซิร์ฟเวอร์ ห้องควบคุม
- (ช) ต้องเก็บรักษาบันทึกของการเข้าถึง (Logs of Access) และความพยายามในการเข้าถึงบริการที่สำคัญของหน่วยงานและตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว
- (ซ) ต้องพิจารณาแยกกลไกการตรวจสอบสิทธิ์และการระบุตัวตนของบัญชีสำหรับระบบหรือเครือข่ายที่มีระดับความสำคัญหรือระดับความเสี่ยงแตกต่างกันตามความเหมาะสม เพื่อป้องกันไม่ให้ผู้ก่อภัยคุกคาม (Threat Actors) ใช้ประโยชน์จากข้อมูลบัญชีที่ได้ไปโดยไม่ได้รับอนุญาต (Compromised Credentials) โดยอาจดำเนินการ เช่น การแยกบัญชีผู้ใช้งานทั่วไปออกจากบัญชีที่มีสิทธิพิเศษ (Privileged Accounts) การกำหนดขอบเขตการยืนยันตัวตนและการเข้าถึงแยกตามระบบหรือเครือข่าย การใช้วิธียืนยันตัวตนที่เข้มงวดขึ้นสำหรับระบบสำคัญ หรือการป้องกันไม่ให้ข้อมูลบัญชีที่ถูกละเมิดในระบบหนึ่งสามารถนำไปใช้เข้าถึงระบบอื่นที่มีระดับความสำคัญสูงกว่าได้ ทั้งนี้ ไม่จำเป็นต้องใช้ระบบบริหารจัดการอัตลักษณ์หรือระบบยืนยันตัวตนแยกจากกันทางกายภาพ หากสามารถกำหนดมาตรการควบคุมที่เหมาะสมและบรรลุผลลัพธ์ด้านความมั่นคงปลอดภัยตามระดับความเสี่ยงได้

๒.๔.๑.๔ การเชื่อมต่อระยะไกล (Remote Connection)

- (ก) ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต
- (ข) สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ หน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้
 - ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังหรือจากไซต์ระยะไกลเมื่อจำเป็นเท่านั้น

- กำหนดให้การเชื่อมต่อระยะไกลต้องได้รับอนุญาตตามกระบวนการที่หน่วยงานกำหนด และการดำเนินการที่อาจส่งผลกระทบต่อบริการที่สำคัญต้องได้รับการอนุมัติพร้อมเหตุผลทางธุรกิจที่เหมาะสม
- ใช้เทคนิคการยืนยันตัวตนที่มีความมั่นคงปลอดภัย โดยกำหนดให้การเข้าถึงระบบสำคัญจากระยะไกลหรือการดำเนินงานด้วยสิทธิพิเศษของผู้ใช้งานที่เป็นบุคคลต้องใช้การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) โดยอาจดำเนินการผ่านระบบควบคุมการเข้าถึงส่วนกลางหรือระบบเชื่อมต่อที่มีความมั่นคงปลอดภัยตามความเหมาะสม
- ใช้ช่องทางการสื่อสารที่มีความมั่นคงปลอดภัยและมีการเข้ารหัสสำหรับการเชื่อมต่อเครือข่าย เช่น HTTPS, SSH หรือ SCP รวมถึงมีมาตรการรักษาความถูกต้องครบถ้วนของข้อมูลที่รับส่ง
- จำกัดสิทธิ์และระยะเวลาการเข้าถึงเท่าที่จำเป็นตามหน้าที่และวัตถุประสงค์ของการใช้งาน
- จำกัดการรับและส่งข้อมูลเฉพาะข้อมูลที่จำเป็น เพื่อป้องกันการรั่วไหลของข้อมูลหรือการใช้ทรัพยากรเกินความจำเป็น
- บันทึกกิจกรรมที่มีนัยสำคัญจากการเชื่อมต่อระยะไกล เพื่อให้สามารถตรวจสอบย้อนหลังได้ และ
- ปิดการเชื่อมต่อหรือเพิกถอนสิทธิ์การเข้าถึงเมื่อสิ้นสุดความจำเป็น

๒.๔.๑.๕ การเชื่อมต่อ API

- (ก) ต้องจัดให้มีกระบวนการยืนยันตัวตน (Authentication) ที่ยืนยันตัวตนของผู้ใช้บริการและผู้ให้บริการ API ที่รัดกุม มั่นคงปลอดภัย และสอดคล้องกับระดับความเสี่ยงของบริการ
- (ข) กำหนดกระบวนการบริหารจัดการข้อมูลและปัจจัยที่ใช้ในการยืนยันตัวตนอย่างปลอดภัยตลอดวงจรอายุการใช้งาน (เช่น การสร้าง การจัดการ การแสดงผล การเพิกถอน และการต่ออายุ)
- (ค) จำกัดการส่งกลับข้อมูลเฉพาะที่จำเป็นต่อการประมวลผลและการเรียกใช้งาน รวมทั้งต้องกำหนดการแสดงผลข้อผิดพลาดไม่ให้เปิดเผยข้อมูลที่สำคัญ
- (ง) กำหนดให้การสื่อสารและรับส่งข้อมูลผ่าน API ทั้งหมดเกิดขึ้นผ่านช่องทางการเข้ารหัสที่มีความมั่นคงปลอดภัย
- (จ) จัดให้มีแนวทางในการพัฒนาโปรแกรม (Secure Coding) และการตั้งค่าความมั่นคงปลอดภัยของระบบ API โดยเปิดใช้งานเฉพาะฟังก์ชันเท่าที่จำเป็น
- (ฉ) จัดให้มีการเก็บรักษาข้อมูลบันทึกเหตุการณ์ของการใช้งาน API ที่ครบถ้วนและระบุตัวตนได้
- (ช) บริหารจัดการและควบคุมทรัพยากรของระบบ API อย่างมีประสิทธิภาพ เพื่อป้องกันการหยุดชะงักของบริการ

๒.๔.๒ การสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training)

๒.๔.๒.๑ ต้องจัดทำแผนการสร้างความรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness and Training Plan) สำหรับบุคลากร รวมถึงผู้ขาย ผู้รับเหมา ผู้ให้บริการภายนอก และบุคคลภายนอกอื่นที่สามารถเข้าถึงระบบ ข้อมูล เครือข่าย หรือโครงสร้างพื้นฐาน

ที่เกี่ยวข้องกับบริการที่สำคัญ หรือมีหน้าที่หรือกิจกรรมที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์หรือความต่อเนื่องของบริการที่สำคัญ โดยกำหนดเนื้อหา รูปแบบ และระดับการสร้างความตระหนักรู้หรือการฝึกอบรมให้เหมาะสมกับบทบาทหน้าที่ ลักษณะการเข้าถึง และระดับความเสี่ยง ทั้งนี้ ไม่จำเป็นต้องครอบคลุมบุคคลภายนอกที่ไม่มีการเข้าถึงหรือไม่มีความเกี่ยวข้องที่อาจส่งผลกระทบต่อบริการที่สำคัญ โดยแผนต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) วัตถุประสงค์และขอบเขต

- กำหนดวัตถุประสงค์ของการสร้างความตระหนักรู้และการฝึกอบรม เช่น เพื่อลดความผิดพลาดของบุคลากร เพื่อปรับปรุงการแจ้งเหตุ เป็นต้น
- กำหนดบุคลากรเป้าหมาย เช่น ผู้บริหารระดับสูง บุคลากรทั่วไป บุคลากรเฉพาะทาง บุคลากรอื่น ๆ ที่เกี่ยวข้อง เป็นต้น
- กำหนดขอบเขต เช่น การดำเนินการทั้งองค์กร หรือเฉพาะที่มีความเสี่ยงสูง เป็นต้น

(ข) การกำหนดความรับผิดชอบ

(ค) กิจกรรมสร้างความตระหนักรู้และการฝึกอบรม เช่น

- การบรรยาย ณ สถานที่ หรือผ่านสื่ออิเล็กทรอนิกส์
- การสื่อสารและประชาสัมพันธ์
- เนื้อหาสำหรับการสร้างความตระหนักรู้ เช่น กฎหมาย กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนด้านความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

(ง) การวัดและประเมินผล

- การกำหนดตัวชี้วัด เช่น Phishing Test Click Rate, Training Completion Rate, Number of Reported Incidents เป็นต้น
- วิธีการวัดและประเมินผล เช่น การใช้แบบทดสอบ แบบสอบถาม การทดสอบโดยการจำลองสถานการณ์ เป็นต้น

๒.๔.๒.๒ ต้องทบทวนแผนการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าแผนยังคงเป็นปัจจุบันและสอดคล้องกับความเสี่ยง

๒.๔.๓ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

๒.๔.๓.๑ ต้องกำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะหยุดนิ่ง (Data-at-Rest) เช่น การเข้ารหัสข้อมูลส่วนบุคคลที่ถูกจัดเก็บไว้ในอุปกรณ์จัดเก็บข้อมูล

๒.๔.๓.๒ ต้องกำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะส่งผ่าน (Data-in-Transit) เช่น การส่งข้อมูลจากต้นทางไปยังปลายทางโดยใช้โพรโทคอลการสื่อสารที่มีความมั่นคงปลอดภัย

๒.๔.๓.๓ ต้องกำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลขณะถูกใช้งาน (Data-in-Use) เช่น การกำหนดสิทธิขั้นต่ำของการเข้าถึงข้อมูลที่กำลังถูกประมวลผลหรือใช้งานโดยระบบหรือผู้ใช้

๒.๔.๓.๔ มาตรการรักษาความมั่นคงปลอดภัยของข้อมูลตามข้อ ๒.๔.๓.๑ ข้อ ๒.๔.๓.๒ และข้อ ๒.๔.๓.๓ ต้องเหมาะสมกับระดับความเสี่ยงที่ประเมินได้จากการดำเนินการตามข้อ ๒.๓.๓ ซึ่งรวมถึงการพิจารณาความเสี่ยงด้านอธิปไตยของข้อมูล (Data Sovereignty) และข้อกำหนดทางกฎหมายของต่างประเทศที่อาจมีผลบังคับใช้นอกอาณาเขต (Extraterritorial Laws) ด้วย

๒.๔.๓.๕ ต้องมีการจัดเก็บ ป้องกัน ดูแลรักษา และทดสอบข้อมูลสำรอง (Backups of Data)

๒.๔.๓.๖ ต้องมีการทำลายข้อมูลที่ไม่ได้ใช้แล้วอย่างมั่นคงปลอดภัย ตามลำดับชั้นความลับ และประเภทสื่อการจัดเก็บ

๒.๔.๓.๗ สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media)

(ก) ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อ สื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แท็บเล็ต) กับระบบสารสนเทศที่ให้บริการที่สำคัญของหน่วยงาน โดยใช้ มาตรการอย่างน้อย ดังนี้

- ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ใช้เฉพาะสื่อบันทึกข้อมูลที่ได้รับอนุญาตจากหน่วยงาน และ
- ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพา ทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

(ข) ต้องเข้ารหัสข้อมูลบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓.๘ ในกรณีที่มีการใช้บริการคลาวด์ (Cloud Services) กับระบบ ข้อมูล หรือบริการ ที่อยู่ในขอบเขตของบริการที่สำคัญ หน่วยงานต้องปฏิบัติตามกฎหมาย มาตรฐาน หรือข้อกำหนดด้านการรักษา ความมั่นคงปลอดภัยคลาวด์ที่มีผลใช้บังคับตามขอบเขตที่เกี่ยวข้อง และต้องพิจารณาความเสี่ยงที่เกี่ยวข้องกับ สถานที่จัดเก็บหรือประมวลผลข้อมูล เขตอำนาจทางกฎหมาย (Jurisdiction) อธิปไตยข้อมูล (Data Sovereignty) และที่ตั้งของศูนย์ข้อมูล (Data Center Location) ตามระดับผลกระทบและความเสี่ยง อย่างเหมาะสม

หน่วยงานต้องกำหนดและทบทวนขอบเขตความรับผิดชอบร่วมกันระหว่าง หน่วยงานและผู้ให้บริการคลาวด์ (Shared Responsibility) ให้ชัดเจน รวมถึงการบริหารสิทธิ การบันทึก เหตุการณ์ การบริหารช่องโหว่ การสำรองและกู้คืนข้อมูล การตอบสนองต่อเหตุการณ์ และการคืน โอนย้าย หรือลบข้อมูลเมื่อสิ้นสุดการให้บริการ ตามขอบเขตที่เกี่ยวข้อง

๒.๔.๓.๙ ในกรณีที่มีการใช้การเข้ารหัสเพื่อคุ้มครองระบบหรือข้อมูลที่เกี่ยวข้องกับบริการที่ สำคัญ หน่วยงานต้องกำหนดกระบวนการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management) ครอบคลุมการสร้าง การจัดเก็บ การแจกจ่าย การใช้งาน การเปลี่ยน การเพิกถอน การสำรอง และการทำลาย กุญแจเข้ารหัสตามความเหมาะสม รวมทั้งกำหนดสิทธิ์ในการเข้าถึงกุญแจเข้ารหัสอย่างเหมาะสม

๒.๔.๔ การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

๒.๔.๔.๑ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(ก) ต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงานที่สอดคล้องกับ โพรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญของหน่วยงาน

ทั้งนี้ ในการจัดทำมาตรฐานดังกล่าว มาตรฐานการกำหนดค่าขั้นต่ำด้าน ความมั่นคงปลอดภัยตามวรรคหนึ่ง ต้องจัดทำโดยพิจารณาจากแหล่งอ้างอิง ที่เหมาะสมและเชื่อถือได้สำหรับระบบหรือผลิตภัณฑ์นั้น เช่น ข้อเสนอแนะหรือ

คู่มือการเสริมความมั่นคงปลอดภัย (Security Hardening Guidance) ของผู้ผลิตหรือผู้พัฒนา มาตรฐานสากล มาตรฐานหรือแนวปฏิบัติที่ได้รับการยอมรับในอุตสาหกรรม หรือข้อกำหนดของหน่วยงานที่มีอำนาจกำกับดูแล โดยคำนึงถึงการใช้งานจริง ระดับความเสี่ยง และผลกระทบต่อบริการที่สำคัญ

(ข) มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อยดังต่อไปนี้

- สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
- การแบ่งแยกหน้าที่ (Separation of Duties)
- การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
- การลบบัญชีที่ไม่ได้ใช้งาน
- การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
- การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
- การป้องกันมัลแวร์ (Malware) และ
- การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม
- การเปลี่ยนหรือปิดใช้งานบัญชี รหัสผ่าน หรือข้อมูลรับรองที่เป็นค่าเริ่มต้น (Default Credentials) ก่อนนำระบบไปใช้งานจริง
- การปิดใช้งานโพรโทคอล บริการ หรือกลไกการเข้ารหัสที่ไม่มั่นคงปลอดภัยหรือไม่จำเป็น เว้นแต่มีความจำเป็นด้านการทำงานและมีการจัดการความเสี่ยงอย่างเหมาะสม และ
- การกำหนดค่ากลไกและโพรโทคอลด้านความมั่นคงปลอดภัยให้สอดคล้องกับข้อกำหนดของระบบ ผู้ผลิตหรือผู้พัฒนา และมาตรฐานที่เกี่ยวข้องตามความเหมาะสม

(ค) ต้องตรวจสอบให้แน่ใจว่ามีการบังคับใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

(ง) ต้องทบทวนมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๔.๔.๒ การจัดการแพตช์ (Patch Management)

ต้องกำหนดและดำเนินการตามกระบวนการจัดการความมั่นคงปลอดภัยแพตช์ โดยมีรายละเอียดอย่างน้อย ดังนี้

- (ก) การจัดลำดับความสำคัญของการใช้แพตช์ความมั่นคงปลอดภัยโดยพิจารณาจากระดับความเสี่ยงที่มีผลต่อการดำเนินงานของหน่วยงาน
- (ข) การติดตามการเผยแพร่แพตช์ความมั่นคงปลอดภัยที่เกี่ยวข้องตามรายการทรัพย์สิน
- (ค) การใช้แพตช์ความมั่นคงปลอดภัยอย่างทันทั่วทั้งเพื่อลดช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ โดยเฉพาะช่องโหว่ความเสี่ยงสูงที่เปิดเผยโดยผู้ผลิต ผู้พัฒนา หรือผู้ให้บริการภายนอก ทั้งนี้ ต้องมีการตรวจสอบและทดสอบแพตช์เพื่อให้มั่นใจว่าแพตช์มีความสมบูรณ์ก่อนการใช้งาน
- (ง) การใช้มาตรการทดแทน ในกรณีที่ไม่สามารถใช้แพตช์ความมั่นคงปลอดภัยได้
- (จ) การย้อนกลับ (Roll Back) การใช้แพตช์ความมั่นคงปลอดภัยหากจำเป็น

๒.๔.๔.๓ การจัดการซอฟต์แวร์ ต้องกำหนดและดำเนินการตามกระบวนการจัดการความมั่นคงปลอดภัยซอฟต์แวร์ มีรายละเอียดอย่างน้อย ดังนี้

- (ก) การกำหนดกระบวนการเพื่อพิจารณาอนุญาตการใช้ซอฟต์แวร์ เพื่อให้มั่นใจว่าหน่วยงานใช้เฉพาะซอฟต์แวร์ที่ได้รับอนุญาตและมีความจำเป็นต่อการดำเนินงานและการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน รวมทั้งจัดทำและดูแลบัญชีรายการซอฟต์แวร์ที่ได้รับอนุญาตให้เป็นปัจจุบันอยู่เสมอ
- (ข) ทบทวนรายการซอฟต์แวร์ที่ได้รับอนุญาต อย่างน้อยทุก ๑ (หนึ่ง) ปี ทั้งนี้ การตรวจสอบครั้งแรกต้องดำเนินการให้แล้วเสร็จภายใน ๑ ปี นับจากเวลาที่สร้างรายการซอฟต์แวร์
- (ค) ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของซอฟต์แวร์ก่อนนำไปใช้งาน เช่น การตรวจสอบแหล่งที่มา (Provenance) และค่าแฮช (Hash) ของซอฟต์แวร์
- (ง) ตรวจสอบให้มั่นใจว่าคอมพิวเตอร์และดีבקเกอร์จะถูกใช้เฉพาะในกรณีที่จำเป็นและเฉพาะบนอุปกรณ์ที่ได้รับอนุญาตเท่านั้น
- (จ) หากสามารถกระทำได้ ต้องแยกชั้นแอปพลิเคชันและชั้นฐานข้อมูลออกจากกัน และทำการควบคุมความมั่นคงปลอดภัยในแต่ละชั้น
- (ฉ) การจัดการซอฟต์แวร์ที่สิ้นสุดอายุการใช้งาน (End-of-Life) หรือสิ้นสุดการสนับสนุน (End-of-Support) เพื่อบรรเทาความเสี่ยงจากช่องโหว่ที่ผู้ผลิตอุปกรณ์ดั้งเดิมหรือผู้ให้บริการภายนอกไม่สนับสนุนหรือแก้ไขให้แล้ว

๒.๔.๔.๔ การจัดการฮาร์ดแวร์ ต้องกำหนดและดำเนินการตามกระบวนการจัดการความมั่นคงปลอดภัยฮาร์ดแวร์ มีรายละเอียดอย่างน้อย ดังนี้

- (ก) การบำรุงรักษาฮาร์ดแวร์ เช่น การตรวจสอบและซ่อมบำรุงตามรอบ การตรวจสอบความพร้อมใช้งานของอุปกรณ์ด้านความมั่นคงปลอดภัยไซเบอร์
- (ข) การจัดการอุปกรณ์ที่สิ้นสุดการรับประกันหรือสิ้นสุดการผลิตและขาย (End-of-Life) หรือสิ้นสุดการสนับสนุน (End-of-Support)
- (ค) การทำลายอุปกรณ์ที่ถูกถอดออกจากระบบ

๒.๔.๔.๕ ต้องจัดทำและดำเนินการตามกระบวนการจัดการการเปลี่ยนแปลง (Change Management) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๒.๔.๔.๖ การจัดการบันทึกเหตุการณ์ (Log Management)

- (ก) ต้องกำหนดและจัดเก็บบันทึกเหตุการณ์ที่จำเป็นต่อการเฝ้าระวัง ตรวจสอบ วิเคราะห์ และสอบสวนเหตุภัยคุกคามทางไซเบอร์ของระบบสำคัญ โดยอย่างน้อยให้ครอบคลุมการพิสูจน์ตัวตนและการเข้าถึง การใช้สิทธิพิเศษ การเปลี่ยนแปลงการกำหนดค่าที่มีนัยสำคัญ เหตุการณ์ด้านความมั่นคงปลอดภัย และบันทึกจากอุปกรณ์หรือระบบรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องตามความเหมาะสม
- (ข) ต้องกำหนดระยะเวลาการเก็บรักษา การควบคุมการเข้าถึง และมาตรการป้องกันการแก้ไขหรือลบบันทึกโดยไม่ได้รับอนุญาต ให้สอดคล้องกับกฎหมายข้อกำหนด และระดับความเสี่ยง
- (ค) ตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว
- (ง) ระบบที่เกี่ยวข้องต้องมีการอ้างอิงเวลาที่ถูกต้องและสอดคล้องกันตามความเหมาะสม เพื่อสนับสนุนการเชื่อมโยงและวิเคราะห์เหตุการณ์ และ
- (จ) ต้องสร้างและจัดเก็บบันทึกข้อมูลจราจรคอมพิวเตอร์ให้เป็นไปตามกฎหมาย และประกาศที่เกี่ยวข้อง

๒.๔.๔.๗ การพัฒนาซอฟต์แวร์ที่มีความมั่นคงปลอดภัย (Secured Software Development) ต้องดำเนินการอย่างน้อย ดังนี้

- (ก) ประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของโครงการ (Security Risk Assessment)
- (ข) กำหนดข้อกำหนดของโครงการ (Terms of Reference) โดยคำนึงถึงปัจจัยความมั่นคงปลอดภัยทางไซเบอร์
- (ค) ออกแบบและพัฒนา (Design and Development) โดยคำนึงถึงความมั่นคงปลอดภัยทางไซเบอร์ เช่น การใช้แนวทางการเขียนโค้ดปลอดภัย (Secure Coding) การแบ่งแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการให้บริการออกจากกัน
- (ง) ทดสอบระบบและตรวจสอบความสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ก่อนนำไปใช้งาน
- (จ) บำรุงรักษาและเฝ้าระวังการเข้าถึงข้อมูล การใช้งานระบบ และกิจกรรมที่ผิดปกติ
- (ฉ) เมื่อเลิกใช้งาน (Disposal) ให้ทำลายข้อมูลสำคัญอย่างปลอดภัย

๒.๔.๔.๘ ส่วนขยายการรักษาความมั่นคงปลอดภัยระบบชื่อโดเมน (DNSSEC)

- (ก) ต้องเปิดใช้งานการตรวจสอบ DNSSEC (DNSSEC Validation) สำหรับตัวค้นหาชื่อโดเมน (DNS Resolver) หรือใช้วิธีการที่เทียบเท่าหรือดีกว่าในการตรวจสอบความสมบูรณ์ของข้อมูล DNS (DNS Records) เพื่อป้องกัน

การโจมตี DNS เช่น การวางยาพิษแคชของ DNS (DNS Cache Poisoning) และการปลอมแปลง DNS (DNS Spoofing)

- (ข) ต้องทำให้มั่นใจว่าทุกชื่อโดเมนที่อยู่ภายใต้การควบคุมของหน่วยงาน และที่ใช้ในการเชื่อมต่อกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งในส่วนของการดำเนินการและการให้บริการ ได้รับการลงลายเซ็น DNSSEC (DNSSEC-Signed) บนเครื่องแม่ข่าย DNS ของหน่วยงานเจ้าของโดเมน (DNS Authoritative Server)

๒.๔.๔.๙ ความพร้อมต่อการเข้ารหัสยุคหลังควอนตัม (Post-Quantum Cryptography: PQC Readiness) หน่วยงานต้องจัดทำและดูแลรักษาบัญชีระบบเข้ารหัส (Cryptography Inventory) สำหรับระบบสำคัญหรือระบบที่เกี่ยวข้องกับบริการที่สำคัญ เพื่อสนับสนุนการประเมินความเสี่ยงและการวางแผนเปลี่ยนผ่านด้านการเข้ารหัส โดยพิจารณาถึงประเภทและการใช้งานของเทคโนโลยีเข้ารหัส ความเสี่ยงจากการเปลี่ยนแปลงของเทคโนโลยีควอนตัม ความสามารถในการปรับเปลี่ยนกลไกการเข้ารหัส (Cryptographic Agility) ตลอดจนแผนงานหรือแนวทางการเปลี่ยนผ่านสู่การเข้ารหัสยุคหลังควอนตัมที่สำนักงานกำหนดหรือเผยแพร่ รวมถึงมาตรฐานสากลที่เกี่ยวข้องตามความเหมาะสม ทั้งนี้ การดำเนินการให้เป็นไปตามระดับความเสี่ยง ความพร้อมทางเทคนิค และผลกระทบต่อการให้บริการที่สำคัญ โดยอย่างน้อยต้อง

- (ก) ระบุระบบหรือองค์ประกอบที่มีการใช้การเข้ารหัส รวมถึงอัลกอริทึม โพรโทคอล และกลไกการบริหารจัดการกุญแจเข้ารหัส (Cryptographic Key Management) ที่เกี่ยวข้องตามความเหมาะสม
- (ข) ระบุวัตถุประสงค์และลักษณะการใช้การเข้ารหัส รวมถึงระบบหรือข้อมูลที่ได้รับการคุ้มครองตามความเหมาะสม
- (ค) ประเมินความเสี่ยงและความเปราะบางที่อาจเกิดขึ้นจากความก้าวหน้าของเทคโนโลยีควอนตัม โดยพิจารณาความสำคัญของระบบ อายุการใช้งาน และระยะเวลาที่ข้อมูลต้องได้รับการคุ้มครอง
- (ง) กำหนดลำดับความสำคัญและแนวทางในการเตรียมความพร้อมสำหรับการเปลี่ยนผ่านไปสู่อัลกอริทึมหรือกลไกการเข้ารหัสที่เหมาะสม โดยพิจารณา มาตรฐาน ข้อกำหนด และความพร้อมของเทคโนโลยีที่เกี่ยวข้อง และ
- (จ) ทบทวนและปรับปรุงบัญชีระบบเข้ารหัสอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ อัลกอริทึม โพรโทคอล หรือข้อกำหนดด้านการเข้ารหัสที่มีนัยสำคัญ

๒.๔.๔.๑๐ การรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์และเว็บแอปพลิเคชัน (Website and Web Application Security) ในกรณีที่เว็บไซต์หรือเว็บแอปพลิเคชันอยู่ในขอบเขตหรือเกี่ยวข้องกับบริการที่สำคัญ หน่วยงานต้องปฏิบัติตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับเว็บไซต์ พ.ศ. ๒๕๖๘ และที่แก้ไขเพิ่มเติม (ถ้ามี) ตามขอบเขตที่เกี่ยวข้อง

๒.๔.๕ การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี (Technology Infrastructure Resilience)

๒.๔.๕.๑ การแบ่งส่วนเครือข่าย (Network Segmentation)

- (ก) ต้องแบ่งส่วนสถาปัตยกรรมเครือข่ายออกเป็นกลุ่มตามระดับความมั่นคงปลอดภัยและความเสี่ยง
- (ข) ต้องจำกัดการสื่อสารระหว่างส่วนเครือข่ายที่แตกต่างกันให้เหลือเพียงเท่าที่จำเป็นสำหรับการทำงานของหน่วยงานเท่านั้น
- (ค) ต้องมีกลไกการรักษาความมั่นคงปลอดภัยเครือข่ายระหว่างส่วนเครือข่ายที่แตกต่างกัน เพื่อตรวจจับและปิดกั้นการรับส่งข้อมูลเครือข่ายที่เป็นอันตราย
- (ง) ต้องกำหนดกลไกและกระบวนการในการตัดการเชื่อมต่อกับส่วนของเครือข่ายที่ได้รับผลกระทบจากเหตุการณ์คุกคามทางไซเบอร์ (Isolation)

๒.๔.๕.๒ ป้องกันทรัพย์สินทางสารสนเทศ เช่น เครื่องแม่ข่าย อุปกรณ์เครือข่าย และระบบจัดเก็บข้อมูล จากอัคคีภัย น้ำท่วม หรือภัยจากสภาพแวดล้อมอื่น ๆ เช่น แผ่นดินไหว ไฟฟ้า อุณหภูมิหรือความชื้นผิดปกติ ระบบไฟฟ้าขัดข้อง ระบบระบายความร้อนขัดข้อง หรือเหตุการณ์ทางกายภาพอื่นที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัย ความพร้อมใช้ หรือความต่อเนื่องของระบบและบริการที่สำคัญ โดยกำหนดมาตรการป้องกันตามลักษณะของสถานที่และระดับความเสี่ยงที่เกี่ยวข้อง

๒.๔.๕.๓ แผนการสำรองข้อมูล (Backup Plan)

- (ก) ต้องจัดทำแผนการสำรองข้อมูล (Backup Plan) เพื่อให้มั่นใจว่าหน่วยงานสามารถกู้คืนข้อมูลและบริการที่สำคัญได้ ในกรณีที่เกิดความเสียหายของข้อมูลหรือการขัดข้องของระบบ โดยแผนการสำรองและกู้คืนข้อมูลต้องมีเนื้อหาอย่างน้อยดังนี้
 - ขอบเขต/รายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล
 - วิธีการ/เทคโนโลยีการสำรองข้อมูลและรูปแบบข้อมูล (Data Format)
 - ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
 - การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
 - ขั้นตอนและวิธีการกู้ข้อมูล
 - การทดสอบความสามารถในการกู้คืนข้อมูลจากอุปกรณ์สำรองข้อมูล (Restoration Test)
 - สถานที่จัดเก็บข้อมูลสำรอง
- (ข) ต้องสำรองข้อมูลเป็นระยะ ตามความถี่ที่เหมาะสมและมีความสอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) และต้องตรวจสอบให้มั่นใจว่าการสำรองข้อมูลสำเร็จทุกครั้ง
- (ค) ต้องทดสอบกระบวนการกู้คืนข้อมูลจากชุดข้อมูลสำรองเป็นระยะ เพื่อยืนยันว่าข้อมูลสามารถกู้คืนได้เมื่อจำเป็น ความถี่ในการทดสอบต้องสอดคล้องกับระดับความเสี่ยงด้านไซเบอร์ของทรัพย์สินทางสารสนเทศที่เกี่ยวข้อง
- (ง) ต้องทบทวนแผนการสำรองและกู้คืนข้อมูลอย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่าแผนดังกล่าวยังคงมีความเหมาะสมและเป็นปัจจุบัน

๒.๔.๖ การแบ่งปันข้อมูล (Information Sharing)

ต้องกำหนดกระบวนการแบ่งปันและแลกเปลี่ยนข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์ เหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ ช่องโหว่ เทคนิคการโจมตี และมาตรการป้องกันหรือบรรเทาผลกระทบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศและบริการที่สำคัญ กับหน่วยงานที่เกี่ยวข้อง

เพื่อสนับสนุนการเฝ้าระวัง การตรวจจับ การป้องกัน และการรับมือภัยคุกคามทางไซเบอร์ร่วมกัน (Collective Defense) อย่างทันทั่วทั้งที่ และลดความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นในวงกว้าง

การแบ่งปันข้อมูลต้องคำนึงถึงความถูกต้อง ความน่าเชื่อถือ ความเหมาะสมของข้อมูล ความมั่นคงปลอดภัย และข้อจำกัดในการเปิดเผยหรือใช้ข้อมูล โดยให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด ทั้งนี้ การประสานงาน การแจ้งเตือน การแบ่งปันข้อมูลแก่ผู้ได้รับผลกระทบ และการรายงานเหตุภัยคุกคามทางไซเบอร์ในกระบวนการรับมือเหตุการณ์ ให้ดำเนินการตามข้อ ๒.๖.๓

กระบวนการที่เกี่ยวข้องประกอบด้วย

๒.๔.๖.๑ การจัดตั้งกระบวนการและผู้รับผิดชอบ (Internal Process and Governance) ต้องกำหนดกระบวนการและผู้รับผิดชอบในการรวบรวม ตรวจสอบความถูกต้อง (Validation) วิเคราะห์ และคัดกรองข้อมูลภัยคุกคามทางไซเบอร์ (Threat Intelligence) ก่อนดำเนินการแบ่งปัน รวมถึงการตรวจสอบและปกปิดหรือลบข้อมูลที่มีความละเอียดอ่อน (Sanitization) ตามความเหมาะสม เพื่อให้ข้อมูลที่แบ่งปันมีความถูกต้อง น่าเชื่อถือ และไม่ก่อให้เกิดความเสี่ยงจากการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต

๒.๔.๖.๒ ประเภท รูปแบบ และเนื้อหาของข้อมูล (Information Type, Format, and Content)

- (ก) ประเภทของข้อมูล ข้อมูลที่แบ่งปันอาจประกอบด้วยข้อมูลบ่งชี้การบุกรุก (Indicators of Compromise: IoCs) เช่น ค่าแฮชของไฟล์ หมายเลขไอพี (IP Address) หรือชื่อโดเมนที่เป็นอันตราย และข้อมูลบ่งชี้พฤติกรรม การโจมตี (Indicators of Attack: IoAs) เช่น การพยายามยกระดับสิทธิ์ หรือการเคลื่อนไหวกายในเครือข่ายที่ผิดปกติ รวมถึงข้อมูลช่องโหว่และเทคนิคการโจมตีที่เกี่ยวข้อง
- (ข) รูปแบบข้อมูลทางเทคนิค ควรกำหนดรูปแบบข้อมูลที่สามารถนำไปใช้ในการวิเคราะห์ ตรวจจับ และป้องกันภัยคุกคามได้อย่างมีประสิทธิภาพ โดยอาจใช้รูปแบบที่เครื่องคอมพิวเตอร์สามารถประมวลผลได้โดยอัตโนมัติ (Machine-Readable Format) เช่น Structured Threat Information eXpression (STIX) และ Trusted Automated eXchange of Intelligence Information (TAXII) ตามความเหมาะสมและความพร้อมของหน่วยงาน
- (ค) บริบทของภัยคุกคาม ข้อมูลที่แบ่งปันควรมีรายละเอียดประกอบตามความเหมาะสม เพื่อให้ผู้รับสามารถประเมินความเสี่ยงและนำข้อมูลไปใช้ประโยชน์ได้ เช่น ภาพรวมของภัยคุกคาม กลุ่มอุตสาหกรรมที่เป็นเป้าหมาย เทคนิคและวิธีการโจมตี (Tactics, Techniques, and Procedures: TTPs) และข้อเสนอแนะในการตรวจจับ ป้องกัน หรือบรรเทาผลกระทบ (Recommended Mitigations)

๒.๔.๖.๓ ช่องทาง หลักเกณฑ์ และกรอบเวลา (Secure Channels, Classification, and Timelines)

- (ก) ช่องทางการสื่อสาร ต้องกำหนดช่องทางที่ปลอดภัยและน่าเชื่อถือสำหรับการแบ่งปันข้อมูลกับหน่วยงานกำกับดูแล หน่วยงานที่เกี่ยวข้อง และผู้ประกอบกิจการโทรคมนาคม เช่น ช่องทางสื่อสารที่มีการควบคุมการเข้าถึงระบบแลกเปลี่ยนข้อมูลที่ปลอดภัย (Secure Portal) หรือส่วนต่อประสานโปรแกรมประยุกต์ (API) ตามความเหมาะสม

- (ข) การจำแนกชั้นข้อมูล ต้องกำหนดระดับการเปิดเผยและข้อจำกัดในการนำข้อมูลที่แบ่งปันไปใช้ต่ออย่างเหมาะสม โดยอาจอ้างอิง Traffic Light Protocol (TLP) หรือหลักเกณฑ์อื่นที่สำนักงาน กสทช. ประกาศกำหนด เพื่อให้ผู้รับทราบขอบเขตในการเข้าถึง ใช้งาน และเผยแพร่ข้อมูลต่อ
- (ค) กรอบเวลาในการแบ่งปัน ต้องดำเนินการแบ่งปันข้อมูลภายในระยะเวลาที่เหมาะสมกับระดับความรุนแรง ความน่าเชื่อถือของข้อมูล ผลกระทบที่อาจเกิดขึ้น และความจำเป็นในการป้องกันหรือรับมือภัยคุกคาม หรือตามหลักเกณฑ์และวิธีการที่หน่วยงานที่มีอำนาจกำหนด

๒.๔.๖.๔ การบูรณาการข้อมูลและการตอบรับ (Integration and Feedback Loop)

- (ก) ต้องมีกระบวนการนำข้อมูลภัยคุกคามทางไซเบอร์ (Threat Intelligence) ที่ได้รับจากภายนอกมาวิเคราะห์และใช้ประกอบการปรับปรุงมาตรการเฝ้าระวัง ตรวจสอบ ป้องกัน และรับมือภัยคุกคามทางไซเบอร์ของหน่วยงานตามความเหมาะสม
- (ข) ต้องจัดให้มีกลไกการให้ข้อมูลตอบรับ (Feedback Mechanism) แก่หน่วยงานหรือผู้ส่งข้อมูลตามความเหมาะสม เช่น การแจ้งผลการนำข้อมูลไปใช้ การแจ้งข้อมูลที่อาจคลาดเคลื่อนหรือเป็นการแจ้งเตือนผิดพลาด (False Positive) หรือการเพิ่มเติมข้อมูลภัยคุกคามที่ตรวจพบ เพื่อสนับสนุนการปรับปรุงคุณภาพของข้อมูลและยกระดับความสามารถในการป้องกันภัยคุกคามร่วมกัน

๒.๔.๗ การรักษาความมั่นคงปลอดภัยโดยการออกแบบและตลอดวงจรชีวิต (Security by Design and Secure Lifecycle)

ต้องดำเนินการอย่างน้อย ดังนี้

๒.๔.๗.๑ การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยของโครงการ (Security Risk Assessment) โดยดำเนินการตามข้อ ๒.๓.๓ และพิจารณาเงื่อนไขการประเมินความเสี่ยงก่อนนำเทคโนโลยีใหม่หรือการเปลี่ยนแปลงระบบที่มีนัยสำคัญไปใช้งานตามข้อ ๒.๓.๓.๖

๒.๔.๗.๒ การกำหนดข้อกำหนดของโครงการ (Terms of Reference) โดยคำนึงถึงปัจจัยความมั่นคงปลอดภัยไซเบอร์

๒.๔.๗.๓ การออกแบบและการพัฒนา (Design and Development)

๒.๔.๗.๔ การติดตั้งใช้งานและการทดสอบ (Implementation and Assessment)

๒.๔.๗.๕ การดำเนินการและเฝ้าระวัง (Operations and Monitoring)

๒.๔.๗.๖ การเลิกใช้งาน (Disposal)

๒.๔.๗.๗ ก่อนนำระบบสำคัญหรือการเปลี่ยนแปลงระบบที่มีนัยสำคัญขึ้นใช้งานจริง (Production) หน่วยงานต้องตรวจสอบว่าข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้องได้รับการดำเนินการและทดสอบตามความเหมาะสม ช้องโหวหรือความเสี่ยงที่มีนัยสำคัญได้รับการแก้ไขหรือมีมาตรการบรรเทาและความเสี่ยงที่เหลืออยู่ได้รับการยอมรับจากผู้มีอำนาจตามที่หน่วยงานกำหนด

๒.๕ การตรวจพบ (Detect)

๒.๕.๑ การเฝ้าระวังและตรวจจับภัยคุกคามอย่างต่อเนื่อง (Continuous Security Monitoring and Threat Detection)

๒.๕.๑.๑ ต้องจัดให้มีกลไกและกระบวนการเฝ้าระวัง และตรวจจับภัยคุกคามทางไซเบอร์ รวมถึงบูรณาการข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence) และข้อมูลเชิงบริบทที่เกี่ยวข้อง และระบุภัยคุกคามทางไซเบอร์ที่อาจหลุดรอดจากมาตรการควบคุมหรือระบบตรวจจับ

๒.๕.๑.๒ ควรมีกลไกที่มีความสามารถในการค้นหาภัยคุกคามเชิงรุก (Cyber Threat Hunting) ดังต่อไปนี้

(ก) ค้นหาและตรวจสอบสิ่งบ่งชี้การบุกรุก (Indicators of Compromise: IoC) ภายในระบบสารสนเทศของหน่วยงาน โดยเฉพาะระบบที่เกี่ยวข้องกับระบบโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ข) ตรวจจับ วิเคราะห์ ติดตาม และสกัดกั้นภัยคุกคามทางไซเบอร์ที่สามารถหลบเลี่ยงมาตรการควบคุมความมั่นคงปลอดภัยที่มีอยู่

(ค) ดำเนินการปฏิบัติการค้นหาภัยคุกคามเชิงรุกสำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อย่างน้อยหนึ่งครั้งในทุกรอบระยะเวลา ๒๔ เดือน โดยควรดำเนินการครั้งแรกให้แล้วเสร็จภายใน ๑๒ เดือนนับแต่วันที่ประกาศนี้มีผลใช้บังคับ

๒.๕.๑.๓ ตรวจจับเหตุการณ์ไม่พึงประสงค์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการกิจหรือบริการที่สำคัญของหน่วยงาน ครบคลุมอย่างน้อยดังนี้

(ก) ระบบเครือข่ายและบริการเครือข่าย

(ข) สภาพแวดล้อมทางกายภาพ

(ค) กิจกรรมของบุคลากรและการใช้เทคโนโลยี

(ง) กิจกรรมและบริการของผู้ให้บริการภายนอก

(จ) ข้อมูลและสภาพแวดล้อมขณะประมวลผลของฮาร์ดแวร์และซอฟต์แวร์คอมพิวเตอร์

(ฉ) ระบบและสภาพแวดล้อมของข้อมูลสำรอง (Backup Systems and Environment)

๒.๕.๑.๔ ทบทวนกระบวนการตาม ข้อ ๒.๕.๑.๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๒.๕.๑.๕ การเฝ้าระวังและตรวจจับภัยคุกคามต้องครอบคลุมแหล่งข้อมูลและกิจกรรมที่มีนัยสำคัญต่อบริการที่สำคัญตามระดับความเสี่ยง เช่น กิจกรรมการพิสูจน์ตัวตนและการเข้าถึง การใช้บัญชีที่มีสิทธิพิเศษ การเปลี่ยนแปลงการกำหนดค่า เหตุการณ์จากระบบและอุปกรณ์เครือข่าย เหตุการณ์จากมาตรการรักษาความมั่นคงปลอดภัย และการรับส่งข้อมูลหรือพฤติกรรมที่ผิดปกติ

๒.๕.๒ การวิเคราะห์เหตุการณ์ไม่พึงประสงค์ (Adverse Event Analysis)

๒.๕.๒.๑ ตรวจวิเคราะห์เหตุการณ์ไม่พึงประสงค์ โดยครอบคลุมการดำเนินการต่อไปนี้

(ก) วิเคราะห์เหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

(ข) รวบรวมและเชื่อมโยงข้อมูลจากหลายแหล่ง และหากเป็นไปได้ควรพิจารณาใช้เทคโนโลยีการวิเคราะห์และเชื่อมโยงเหตุการณ์

(ค) ประเมินขอบเขตและผลกระทบของเหตุการณ์

- (ง) แจ้งเตือนและส่งข้อมูลไปยังผู้มีหน้าที่ตอบสนองต่อเหตุการณ์หรือเครื่องมือตอบสนองต่อเหตุการณ์
- (จ) บูรณาการข้อมูลข่าวกรองภัยคุกคามทางไซเบอร์และข้อมูลเชิงบริบทอื่น ๆ เข้ากับกระบวนการวิเคราะห์เหตุการณ์
- (ฉ) ระบุว่าภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงานหรือไม่

๒.๕.๒.๒ ทบทวนกระบวนการตามข้อ ๒.๕.๒.๑ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

๒.๖ การรับมือ (Respond)

๒.๖.๑ การจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Management)

๒.๖.๑.๑ ต้องจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนรับมือเหตุภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

- (ก) โครงสร้างทีมรับมือเหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ
- (ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และกฎหมายลำดับรองใด ๆ ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับบริการที่สำคัญ
- (ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และทีมรับมือเหตุภัยคุกคามทางไซเบอร์ รวมถึงเกณฑ์การยกระดับ/ถ่ายโอน (Escalate/Elevate) เหตุการณ์
- (ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
- (จ) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการฟื้นฟู ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน
- (ฉ) ขั้นตอนการฟื้นฟู (Recovery Process)
- (ช) ขั้นตอนการสืบสวนสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์
- (ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอกหรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ เช่น ผู้ขายสำหรับบริการด้านพิสูจน์หลักฐานทางดิจิทัล (Digital Forensics) / การฟื้นฟูและการบังคับใช้กฎหมายเพื่อดำเนินคดี
- (ณ) เกณฑ์ในการประกาศสิ้นสุดเหตุการณ์ (Incident Closure) และ
- (ญ) ขั้นตอนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๒.๖.๑.๒ ต้องดำเนินการตามแผนรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) และตรวจสอบให้แน่ใจว่าแผนรับมือเหตุการณ์คุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการที่สำคัญของหน่วยงาน

๒.๖.๑.๓ ต้องมีการคัดกรอง (Triage) เพื่อยืนยันว่าเหตุการณ์ที่ได้รับรายงานเป็นเหตุการณ์คุกคามทางไซเบอร์ (Cyber Incident) รวมทั้งจัดหมวดหมู่และลำดับความสำคัญของเหตุการณ์ โดยอาจพิจารณากระดับ/ถ่ายโอน (Escalate/Elevate) เหตุการณ์ตามความสำคัญและระดับผลกระทบตามเกณฑ์ที่กำหนดไว้

๒.๖.๑.๔ ต้องทบทวนและฝึกซ้อมแผนรับมือเหตุการณ์คุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ เพื่อให้แน่ใจว่าแผนรับมือเหตุการณ์คุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๖.๑.๕ ต้องทบทวนแผนรับมือเหตุการณ์คุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๒.๖.๒ การวิเคราะห์เหตุการณ์คุกคามทางไซเบอร์ (Incident Analysis)

๒.๖.๒.๑ ต้องวิเคราะห์เพื่อระบุลำดับเหตุการณ์ (Timeline of Events) ในระหว่างที่เหตุการณ์คุกคามทางไซเบอร์เกิดขึ้น โดยครอบคลุมตั้งแต่การตรวจพบครั้งแรกจนถึงการจำกัดขอบเขต วิเคราะห์หาสาเหตุที่แท้จริง (Root Cause) ของเหตุการณ์เพื่อทำความเข้าใจว่าช่องโหว่ (Vulnerability) หรือความบกพร่องของกระบวนการใดที่ถูกใช้ประโยชน์โดยผู้ไม่ประสงค์ดี รวมถึงตรวจสอบระบบอื่นที่อาจได้รับผลกระทบเพื่อค้นหาหลักฐานการโจมตีและร่องรอยความต่อเนื่องของเหตุการณ์คุกคามทางไซเบอร์

๒.๖.๒.๒ ต้องเก็บรวบรวมข้อมูลเหตุการณ์ ข้อมูลเมตา (เช่น IP, ชื่อผู้ใช้, วันและเวลาที่เก็บ) และบันทึกการดำเนินการที่เกิดขึ้นระหว่างการตรวจสอบและวิเคราะห์เหตุการณ์ (เช่น ใครทำอะไร เวลาใดทำอะไร) โดยต้องมีมาตรการเพื่อให้แน่ใจว่าข้อมูลและบันทึกดังกล่าวมีความน่าเชื่อถือและถูกต้อง ครบถ้วน เช่น การทำให้บันทึกไม่สามารถแก้ไขย้อนหลังได้ (Immutable)

๒.๖.๓ การสื่อสารและการรายงานในการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Incident Response Reporting and Communication)

๒.๖.๓.๑ ต้องประสานงาน แจ้งเตือนและแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์คุกคามทางไซเบอร์ ในส่วนที่เกี่ยวข้องกับบริการที่สำคัญ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการเพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบหรืออาจเกิดขึ้นได้ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญของหน่วยงาน และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

รายละเอียด แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงานและสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒.๖.๓.๒ ต้องแจ้งหรือรายงานเหตุการณ์คุกคามทางไซเบอร์ตามที่กฎหมายกำหนด

๒.๖.๓.๓ ต้องจัดทำและดำเนินการตามแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๒.๖.๓.๔ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต

(ก) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

- (ข) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
- (ค) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
- (ง) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน และ
- (จ) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิม และโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๒.๖.๓.๕ ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๒.๖.๓.๖ ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิภาพในช่วงวิกฤต อันเนื่องมาจากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์

๒.๖.๔ การบรรเทาเหตุภัยคุกคามทางไซเบอร์ (Incident Mitigation)

๒.๖.๔.๑ ต้องมีขั้นตอนและทรัพยากรที่พร้อมใช้งานเพื่อจำกัดขอบเขต (Contain) และกำจัด (Eradicate) ภัยคุกคามทางไซเบอร์ที่ตรวจพบออกจากระบบ โดยอาจใช้เทคโนโลยีอัตโนมัติ ใช้การดำเนินการโดยผู้ปฏิบัติ ใช้บริการจากผู้ให้บริการภายนอกที่เชื่อถือได้ หรือขอความช่วยเหลือจากหน่วยงานที่เกี่ยวข้องตามความจำเป็น

๒.๖.๔.๒ ต้องเฝ้าระวังอย่างต่อเนื่อง เพื่อตรวจสอบยืนยันว่าภัยคุกคามถูกจำกัดและไม่มี การแพร่กระจายไปยังส่วนอื่นของระบบ

๒.๗ การฟื้นฟู (Recover)

๒.๗.๑ แผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) และแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan: DRP)

๒.๗.๑.๑ ต้องจัดทำและดำเนินการตามแผนความต่อเนื่องทางธุรกิจและแผนฟื้นฟูจากภัยพิบัติ เพื่อให้แน่ใจว่าการกิจหรือบริการที่สำคัญของหน่วยงานสามารถดำเนินการหรือให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักของระบบสารสนเทศ ระบบและโครงสร้างพื้นฐานโทรคมนาคม หรือโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม เนื่องจากเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในรูปแบบต่าง ๆ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบถามแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตค่านิยมและการกำหนดระยะเวลาที่สำคัญ ได้แก่ ระยะเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)

ทั้งนี้ การจัดทำแผนความต่อเนื่องทางธุรกิจและแผนฟื้นฟูจากภัยพิบัติ ให้เป็นไปตามหลักเกณฑ์และวิธีการที่สำนักงานประกาศกำหนด

๒.๗.๑.๒ ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจและแผนฟื้นฟูจากภัยพิบัติ อย่างน้อยปีละ ๑ ครั้ง และประเมินประสิทธิภาพของแผนดังกล่าวต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ รวมถึงมีการทบทวนและปรับปรุงแผนตามผลการประเมินอย่างเหมาะสม

๒.๗.๒ แผนฟื้นฟูจากเหตุการณ์ความทางไซเบอร์ (Incident Recovery Plan)

๒.๗.๒.๑ ต้องจัดทำแผนฟื้นฟูเหตุการณ์ความทางไซเบอร์ (Incident Recovery Plan) เพื่อให้มั่นใจได้ว่าหน่วยงานสามารถฟื้นฟูระบบและกู้คืนข้อมูลที่ได้รับผลกระทบจากเหตุการณ์ความทางไซเบอร์ได้อย่างทันท่วงที และลดผลกระทบต่อการดำเนินตามภารกิจหรือบริการที่สำคัญของหน่วยงาน ซึ่งหน่วยงานอาจจัดทำแผนฟื้นฟูเหตุการณ์ความทางไซเบอร์แยกออกมาเป็นแผนหนึ่งหรือเป็นส่วนหนึ่งของแผนรับมือเหตุการณ์ความทางไซเบอร์ (Cybersecurity Incident Response Plan) ก็ได้ โดยต้องมีเนื้อหาอย่างน้อยดังนี้

- (ก) ระดับความสำคัญของระบบและข้อมูล เพื่อใช้จัดลำดับความเร่งด่วนในการฟื้นฟู โดยสอดคล้องกับ ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO) ของหน่วยงาน
 - (ข) บทบาทหน้าที่และความรับผิดชอบของสมาชิกในทีม
 - (ค) ขั้นตอนปฏิบัติในการฟื้นฟูระบบ
 - (ง) ขั้นตอนการทดสอบและยืนยันว่าระบบที่ฟื้นฟูมานั้นมีความถูกต้อง
 - (จ) ขั้นตอนการสื่อสารทั้งภายในและภายนอกหน่วยงานในระหว่างการฟื้นฟู รวมถึงกลไกการรายงานต่อผู้ที่เกี่ยวข้อง
- ทั้งนี้ หน่วยงานอาจดำเนินการทดสอบและฝึกซ้อมแผนฟื้นฟูเหตุการณ์ความทางไซเบอร์ร่วมกับการทดสอบหรือฝึกซ้อมแผนความต่อเนื่องทางธุรกิจและแผนฟื้นฟูจากภัยพิบัติตามข้อ ๒.๗.๑ ได้ โดยต้องครอบคลุมวัตถุประสงค์ ขั้นตอน และผลลัพธ์ที่ต้องการของแต่ละแผน รวมทั้งมีหลักฐานการทดสอบและการประเมินผลที่สามารถตรวจสอบย้อนกลับได้

๒.๗.๒.๒ ต้องทดสอบและซักซ้อมแผนฟื้นฟูเหตุการณ์ความทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง เพื่อให้มั่นใจว่ากระบวนการฟื้นฟูสามารถใช้งานได้จริง และบุคลากรที่เกี่ยวข้องมีความเข้าใจในบทบาทหน้าที่

๒.๗.๒.๓ ต้องทบทวนและปรับปรุงแผนฟื้นฟูเหตุการณ์ความทางไซเบอร์อย่างน้อยปีละหนึ่งครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ เพื่อให้แผนมีความเป็นปัจจุบันและสอดคล้องกับระดับความเสี่ยง

๒.๗.๒.๔ ต้องดำเนินการตามแผนฟื้นฟูจากเหตุการณ์ความทางไซเบอร์ (Incident Recovery Plan) อย่างน้อยดังต่อไปนี้

- (ก) ต้องยืนยันว่าภัยคุกคามถูกกำจัดออกจากระบบแล้ว (Eradicated) เพื่อที่จะส่งมอบงานจากทีมรับมือ (Respond) ไปยังทีมฟื้นฟู (Recovery) ตามขั้นตอนการเรียกใช้งานกระบวนการฟื้นฟูที่ระบุไว้ในแผนรับมือเหตุการณ์ความทางไซเบอร์
- (ข) จัดลำดับการฟื้นฟูระบบและบริการตามความสำคัญของภารกิจ (Critical Mission Functions) ของหน่วยงาน โดยอ้างอิงจากผลการวิเคราะห์ผลกระทบทางธุรกิจ (BIA) และ Recovery Time Objective (RTO)
- (ค) ตรวจสอบความถูกต้องครบถ้วน (Integrity) ของการสำรองข้อมูล (Backup) ก่อนนำมาใช้ในการกู้คืนข้อมูล
- (ง) ต้องดำเนินการฟื้นฟูระบบตามลำดับความสำคัญที่ถูกจัดลำดับตามความสำคัญของภารกิจ

- (จ) หลังจากการฟื้นฟูเสร็จสิ้น ต้องมีการตรวจสอบยืนยัน (Validation) เพื่อให้มั่นใจว่า สินทรัพย์ที่ฟื้นฟูนั้นมีความสมบูรณ์ และทำงานได้ถูกต้อง
- (ฉ) ต้องประกาศสิ้นสุดกระบวนการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (End of Incident Recovery) เพื่อยืนยันการกลับสู่สภาวะการปฏิบัติงานปกติ (Normal Operations)

๒.๗.๓ การสื่อสารระหว่างการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Communication)

๒.๗.๓.๑ ต้องสื่อสารความคืบหน้าของกิจกรรมการฟื้นฟู (เช่น ระบบใดที่ฟื้นฟูสำเร็จแล้ว ระบบใดที่อยู่ระหว่างการดำเนินการ) รวมถึงเมื่อระบบหรือบริการกลับมาใช้งานได้ปกติแล้วต้องแจ้งให้ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกทราบ

๒.๗.๓.๒ การให้ข้อมูลความคืบหน้าของกิจกรรมการฟื้นฟูกับสาธารณชน ต้องใช้วิธีการช่องทาง และข้อความ ที่ผ่านการอนุมัติจากผู้ที่มีอำนาจของหน่วยงาน

ส่วนที่ ๓ ข้อกำหนดเฉพาะ

๓.๑ ความพร้อมรับมือทางไซเบอร์ (Cyber Resilience)

หน่วยงานต้องดำเนินการตามข้อกำหนดทั่วไปในส่วนที่ ๒ เกี่ยวกับการสำรองและกู้คืนข้อมูล ความต่อเนื่องของบริการ และการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ รวมทั้งจัดให้มีมาตรการเพิ่มเติมเพื่อเสริมสร้างความสามารถในการรักษาความต่อเนื่องและฟื้นคืนบริการที่สำคัญจากเหตุภัยคุกคามทางไซเบอร์อย่างน้อยดังต่อไปนี้

๓.๑.๑ การป้องกันข้อมูลสำรองจากภัยคุกคามทางไซเบอร์

หน่วยงานต้องจัดให้มีการสำรองข้อมูล ระบบ และการกำหนดค่าที่จำเป็นต่อการกู้คืนบริการที่สำคัญ พร้อมทั้งกำหนดมาตรการป้องกันข้อมูลสำรองจากการเข้าถึง การแก้ไข การเข้ารหัส หรือการลบโดยไม่ได้รับอนุญาต รวมถึงภัยคุกคามที่อาจส่งผลกระทบต่อระบบต้นทางและข้อมูลสำรองพร้อมกัน โดยพิจารณาใช้มาตรการแยกข้อมูลสำรองทางกายภาพหรือทางตรรกะ การจัดเก็บข้อมูลสำรองแบบไม่เชื่อมต่อกับระบบต้นทาง (Offline Backup) การป้องกันการแก้ไขหรือลบข้อมูลสำรอง (Immutable Backup) หรือมาตรการอื่นที่ให้ผลลัพธ์เทียบเท่า ตามระดับความเสี่ยงและความสำคัญของบริการ

ทั้งนี้ ให้ดำเนินการร่วมกับมาตรการสำรองและกู้คืนข้อมูลตามข้อ ๒.๔.๕.๓ โดยไม่จำเป็นต้องจัดทำแผนหรือกระบวนการแยกต่างหาก หากมาตรการที่มีอยู่ครอบคลุมข้อกำหนดดังกล่าวแล้ว

๓.๑.๒ การป้องกันการบุกรุกซ้ำระหว่างการกู้คืนระบบ

ก่อนนำข้อมูลสำรองหรือระบบที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์กลับมาใช้งาน หน่วยงานต้องตรวจสอบความสมบูรณ์ ความถูกต้อง และความเหมาะสมของข้อมูลสำรองหรือระบบที่จะกู้คืน รวมทั้งดำเนินการมาตรการที่จำเป็นเพื่อลดความเสี่ยงจากการนำมัลแวร์ ช่องโหว่ การกำหนดค่าที่ไม่มั่นคงปลอดภัย หรือสภาพแวดล้อมที่ถูกบุกรุกกลับเข้าสู่ระบบที่กู้คืน

ทั้งนี้ ให้ดำเนินการร่วมกับกระบวนการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๒.๗.๒ โดยคำนึงถึงความสำคัญและความต่อเนื่องของบริการที่สำคัญ

๓.๑.๓ การรักษาความต่อเนื่องของบริการที่สำคัญ

หน่วยงานต้องกำหนดความต้องการด้านความต่อเนื่องและความพร้อมรับมือ (Resilience Requirements) ของบริการที่สำคัญ โดยคำนึงถึงผลการวิเคราะห์ผลกระทบทางธุรกิจ ระดับความเสี่ยง และการพึ่งพาระบบหรือโครงสร้างพื้นฐานที่เกี่ยวข้อง เพื่อให้สามารถรักษาความต่อเนื่องหรือฟื้นคืนบริการได้ภายในระยะเวลาที่ยอมรับได้เมื่อเกิดความขัดข้องหรือเหตุภัยคุกคามทางไซเบอร์

ทั้งนี้ ให้ดำเนินการร่วมกับมาตรการด้านความต่อเนื่องทางธุรกิจและการฟื้นฟูจากภัยพิบัติตาม ข้อ ๒.๗.๑ และมาตรการด้านการสำรองและกู้คืนข้อมูลตามข้อ ๒.๔.๕.๓ สำหรับระบบและโครงสร้างพื้นฐาน โทรคมนาคม ให้พิจารณามาตรการรองรับความขัดข้องตามข้อ ๓.๒.๖ โดยไม่จำเป็นต้องกำหนดมาตรการหรือ กระบวนการซ้ำซ้อน หากมาตรการที่มีอยู่สามารถรองรับความต้องการด้านความต่อเนื่องของบริการได้อย่าง เพียงพอ

๓.๒ ความมั่นคงปลอดภัยของระบบและโครงสร้างพื้นฐานโทรคมนาคม (Telecommunications Systems and Infrastructure Security)

หน่วยงานต้องกำหนดและดำเนินการตามมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับระบบ และโครงสร้างพื้นฐานโทรคมนาคม รวมถึงโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่เกี่ยวข้องกับบริการ ที่สำคัญ โดยคำนึงถึงลักษณะของระบบ ระดับความเสี่ยง ข้อจำกัดทางเทคนิค และผลกระทบต่อความพร้อมใช้ ความเชื่อถือได้ และความต่อเนื่องของบริการ

ทั้งนี้ ให้ดำเนินการตามข้อกำหนดทั่วไปในส่วนที่ ๒ และมาตรการเฉพาะด้านโทรคมนาคมอย่างน้อย ดังต่อไปนี้

๓.๒.๑ การประเมินความเสี่ยงและความมั่นคงปลอดภัยของระบบโทรคมนาคม

หน่วยงานต้องประเมินและจัดการความเสี่ยงของระบบและโครงสร้างพื้นฐานโทรคมนาคม รวมถึงโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม ตามข้อ ๒.๓.๓ โดยให้ครอบคลุมความเสี่ยงที่มี ลักษณะเฉพาะของระบบโทรคมนาคม เช่น การถูกควบคุมหรือสั่งการโดยไม่ได้รับอนุญาต ความขัดข้องของ ระบบบริหารจัดการโครงข่าย การเปลี่ยนแปลงค่าการทำงานที่มีนัยสำคัญ และการพึ่งพาระหว่างระบบที่อาจ ส่งผลกระทบต่อบริการที่สำคัญ

การประเมินช่องโหว่ การทดสอบความมั่นคงปลอดภัย และการติดตามจัดการช่องโหว่ ให้ดำเนินการตามข้อ ๒.๓.๔ โดยคำนึงถึงข้อจำกัดทางเทคนิคและความเสี่ยงจากการทดสอบที่อาจกระทบต่อ การให้บริการโทรคมนาคม ทั้งนี้ อาจใช้วิธีการประเมินหรือทดสอบทางเลือกที่เหมาะสมกับลักษณะของระบบ

๓.๒.๒ การควบคุมการกำหนดค่าและการเปลี่ยนแปลงระบบโทรคมนาคม (Telecommunications Configuration and Change Control) สำหรับระบบสำคัญ ระบบและโครงสร้างพื้นฐานโทรคมนาคม และ โครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม หน่วยงานต้องกำหนดและควบคุมค่าการกำหนดระบบ (Configuration) ที่มีผลต่อความพร้อมใช้ ความเชื่อถือได้ หรือความต่อเนื่องของบริการ โดยอย่างน้อยต้อง

- (ก) กำหนดค่าการกำหนดระบบที่ได้รับอนุมัติหรือค่าฐาน (Approved or Baseline Configuration)
- (ข) จำกัดสิทธิ์ในการเปลี่ยนแปลงค่าการกำหนดระบบให้เฉพาะผู้ได้รับอนุญาต
- (ค) บันทึกและสามารถตรวจสอบย้อนหลังการเปลี่ยนแปลงที่มีนัยสำคัญ
- (ง) ตรวจสอบและทดสอบผลกระทบก่อนนำการเปลี่ยนแปลงที่มีนัยสำคัญไปใช้ตามความเหมาะสม และ
- (จ) มีวิธีการย้อนกลับ (Rollback) กู้คืน หรือดำเนินการด้วยวิธีอื่นที่เหมาะสม หากการเปลี่ยนแปลงส่งผลกระทบต่อการให้บริการ

๓.๒.๓ การควบคุมการเชื่อมต่อและการแบ่งแยกเครือข่ายโทรคมนาคม

หน่วยงานต้องกำหนดมาตรการควบคุมการเชื่อมต่อระหว่างระบบและโครงสร้างพื้นฐาน โทรคมนาคม ระบบบริหารจัดการโครงข่าย ระบบสารสนเทศภายใน เครือข่ายภายนอก และระบบของ ผู้ให้บริการภายนอก ตามหน้าที่ ความจำเป็นในการดำเนินงาน และระดับความเสี่ยง

สำหรับการเชื่อมต่อที่ใช้ควบคุมหรือบริหารจัดการโครงข่ายโทรคมนาคม ต้องจำกัดการเข้าถึงทิศทางการสื่อสาร และบริการหรือโพรโทคอลที่อนุญาตให้ใช้งานตามความจำเป็น รวมถึงป้องกันการเข้าถึงหรือการสั่งการโดยไม่ได้รับอนุญาต โดยให้สอดคล้องกับมาตรการแบ่งส่วนเครือข่ายตามข้อ ๒.๔.๕.๑ และการควบคุมการเข้าถึงตามข้อ ๒.๔.๑.๓

๓.๒.๔ การควบคุมการบริหารจัดการและการสั่งการระบบโทรคมนาคม

สำหรับระบบที่ใช้ควบคุมหรือบริหารจัดการโครงข่ายโทรคมนาคม เช่น ระบบบริหารจัดการโครงข่าย (Network Management System: NMS) ระบบสนับสนุนการปฏิบัติงาน (Operations Support System: OSS) และระบบควบคุมอุปกรณ์โครงข่าย หน่วยงานต้องดำเนินการอย่างน้อย ดังต่อไปนี้

- (ก) จำกัดการเข้าถึงและการใช้สิทธิ์ในการบริหารจัดการระบบให้เฉพาะผู้ได้รับอนุญาตตามหน้าที่และความจำเป็น รวมถึงควบคุมการเข้าถึงจากผู้ให้บริการภายนอก
- (ข) ป้องกันการเปลี่ยนแปลงคำสั่งควบคุม (Control Commands) ค่าการกำหนดระบบ (Configuration Parameters) หรือค่าข้อมูลนำเข้า (Input Values) ที่มีผลต่อการทำงานของระบบโดยไม่ได้รับอนุญาต
- (ค) ควบคุม บันทึกลง และตรวจสอบย้อนหลังการใช้คำสั่งหรือการดำเนินการผ่านระบบบริหารจัดการโครงข่ายที่มีนัยสำคัญต่อการให้บริการ เพื่อให้สามารถระบุผู้ดำเนินการ ช่วงเวลา และการเปลี่ยนแปลงที่เกิดขึ้นได้ตามความเหมาะสม และ
- (ง) เฝ้าระวังและตรวจจับการเข้าถึง การสื่อสาร หรือการสั่งการที่ผิดปกติ ซึ่งอาจส่งผลกระทบต่อความพร้อมใช้ ความถูกต้องของการทำงาน หรือความต่อเนื่องของบริการที่สำคัญ รวมถึงกำหนดกลไกแจ้งเตือนและตอบสนองต่อความผิดปกติที่ตรวจพบ

ทั้งนี้ ให้ดำเนินการร่วมกับมาตรการควบคุมการเข้าถึง การกำหนดค่าระบบ การบริหารการเปลี่ยนแปลง และการเฝ้าระวังตามส่วนที่ ๒ โดยไม่จำเป็นต้องจัดทำกระบวนการแยกต่างหากหากกระบวนการที่มีอยู่ครอบคลุมข้อกำหนดดังกล่าวแล้ว

๓.๒.๕ การป้องกันและบรรเทาการโจมตีที่มุ่งทำให้บริการไม่พร้อมใช้งาน (DoS/DDoS Protection)

สำหรับระบบและโครงสร้างพื้นฐานโทรคมนาคมที่ให้บริการหรือเชื่อมต่อกับเครือข่ายภายนอก หน่วยงานต้องจัดให้มีกลไกในการตรวจจับและบรรเทาการโจมตีที่มุ่งทำให้บริการไม่พร้อมใช้งาน (Denial-of-Service: DoS) หรือการโจมตีแบบกระจาย (Distributed Denial-of-Service: DDoS) ตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ

ทั้งนี้ ต้องกำหนดขั้นตอนการตอบสนองและการประสานงานกับผู้ให้บริการโครงข่าย ผู้ให้บริการภายนอก หรือหน่วยงานที่เกี่ยวข้องตามความเหมาะสม เพื่อจำกัดผลกระทบและสนับสนุนการฟื้นคืนบริการได้อย่างทันท่วงที

๓.๒.๖ ความทนทานและการรองรับความขัดข้องของระบบโทรคมนาคม (Telecommunications System Resilience)

หน่วยงานต้องกำหนดมาตรการหรือกลไกเพื่อให้ระบบและโครงสร้างพื้นฐานโทรคมนาคมที่เกี่ยวข้องกับบริการที่สำคัญสามารถรองรับความขัดข้องหรือเหตุภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม เช่น การสลับไปใช้ระบบสำรอง (Failover) การทำงานในสถานะที่ปลอดภัย (Fail-Safe) หรือการดำเนินงานด้วยวิธีทดแทน

ทั้งนี้ ต้องคำนึงถึงลักษณะของระบบ ความปลอดภัยของการดำเนินงาน ผลการวิเคราะห์ผลกระทบทางธุรกิจ และความต่อเนื่องของบริการที่สำคัญ โดยให้สอดคล้องกับมาตรการด้านความต่อเนื่องทางธุรกิจและการฟื้นฟูจากภัยพิบัติตามข้อ ๒.๗.๑ และมาตรการด้านการสำรองและกู้คืนข้อมูลตามข้อ ๒.๔.๕.๓ ตามความเหมาะสม

๓.๒.๗ ความมั่นคงปลอดภัยและความพร้อมใช้ของโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม (Telecommunications Supporting Infrastructure Security and Resilience)

สำหรับโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่มีนัยสำคัญต่อบริการที่สำคัญ เช่น ระบบจ่ายและสำรองพลังงาน ระบบระบายความร้อน และระบบตรวจวัดหรือควบคุมสภาพแวดล้อม หน่วยงานต้องดำเนินการอย่างน้อย ดังต่อไปนี้

- (ก) ระบุองค์ประกอบและการพึ่งพาที่มีผลต่อความพร้อมใช้และความต่อเนื่องของบริการที่สำคัญ
- (ข) กำหนดค่าหรือเกณฑ์การทำงานที่ยอมรับได้ (Operating Thresholds) และเฝ้าระวังสถานะหรือความผิดปกติของระบบตามความเหมาะสม รวมถึงจัดให้มีกลไกแจ้งเตือนและตอบสนองเมื่อพบความผิดปกติที่อาจส่งผลกระทบต่อบริการที่สำคัญ
- (ค) ดำเนินการบำรุงรักษาและทดสอบการทำงานตามระยะเวลาที่กำหนด
- (ง) จัดให้มีความทนทาน ความซ้ำซ้อน (Redundancy) หรือแนวทางทดแทนตามระดับความสำคัญและผลการวิเคราะห์ผลกระทบทางธุรกิจ เพื่อลดความเสี่ยงจากความขัดข้องขององค์ประกอบหรือการพึ่งพาจุดเดียว (Single Point of Failure) ที่อาจส่งผลกระทบต่อบริการที่สำคัญ และ
- (จ) ป้องกันการเข้าถึง การควบคุม การสั่งการ หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต ในกรณีที่ระบบดังกล่าวสามารถบริหารจัดการหรือควบคุมผ่านระบบดิจิทัลหรือเครือข่าย โดยคำนึงถึงความปลอดภัยของบุคลากร อุปกรณ์ และความต่อเนื่องของบริการที่สำคัญ

ทั้งนี้ ให้ดำเนินการร่วมกับมาตรการด้านการบริหารทรัพย์สิน การควบคุมการเข้าถึง การเฝ้าระวังและความทนทานของโครงสร้างพื้นฐานตามส่วนที่ ๒ โดยไม่จำเป็นต้องจัดทำกระบวนการแยกต่างหากหากมาตรการที่มีอยู่ครอบคลุมข้อกำหนดดังกล่าวแล้ว

๓.๒.๘ การรักษาความมั่นคงปลอดภัยของการเชื่อมต่อโครงข่ายและโครงสร้างพื้นฐานโทรคมนาคมภายในประเทศและระหว่างประเทศ (Domestic and International Telecommunications Interconnection and Infrastructure Security)

ในกรณีที่หน่วยงานมีระบบหรือโครงสร้างพื้นฐานที่เกี่ยวข้องกับการเชื่อมต่อโครงข่ายโทรคมนาคมระหว่างผู้ประกอบการ หรือการเชื่อมต่อระหว่างประเทศ เช่น ระบบเชื่อมต่อโครงข่าย (Interconnection) ระบบประตูสื่อสารระหว่างประเทศ (International Gateway) หรือระบบและโครงสร้างพื้นฐานที่เกี่ยวข้องกับเคเบิลใต้น้ำ (Submarine Cable) และระบบดังกล่าวมีนัยสำคัญต่อบริการที่สำคัญ หน่วยงานต้องพิจารณาความเสี่ยงและกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสม โดยอย่างน้อยให้ครอบคลุม

- (ก) การระบุขอบเขตการเชื่อมต่อ ระบบที่เกี่ยวข้อง และการพึ่งพาผู้ประกอบการหรือผู้ให้บริการภายนอกที่มีนัยสำคัญ
- (ข) การควบคุมการเข้าถึง การเชื่อมต่อ และการบริหารจัดการระบบที่เกี่ยวข้อง เพื่อป้องกันการเข้าถึงหรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต
- (ค) การเฝ้าระวังความผิดปกติที่อาจส่งผลกระทบต่อความพร้อมใช้ ความเชื่อถือได้ หรือความต่อเนื่องของบริการ และ

(ง) การกำหนดกลไกการประสานงาน การตอบสนองต่อเหตุการณ์ และแนวทางรองรับความ
ขัดข้องร่วมกับผู้ประกอบกิจการหรือผู้ให้บริการที่เกี่ยวข้องตามความเหมาะสม
ทั้งนี้ ให้ดำเนินการตามระดับความเสี่ยงและความรับผิดชอบของหน่วยงาน โดยไม่จำเป็นต้อง
กำหนดมาตรการซ้ำกับข้อกำหนดทั่วไปหรือมาตรการเฉพาะอื่นที่ครอบคลุมอยู่แล้ว

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อการทำงานของบริการที่สำคัญและความมั่นคงของประเทศ

สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ (สำนักงาน กสทช.) ในฐานะหน่วยงานควบคุมหรือกำกับดูแลหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม จึงจัดทำกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ เพื่อกำหนดหลักการ ขอบเขต คำนิยาม และกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้เหมาะสมกับลักษณะของบริการ ระบบ โครงข่าย และโครงสร้างพื้นฐานโทรคมนาคม

กรอบมาตรฐานฉบับนี้มุ่งเน้นการบริหารจัดการตามระดับความเสี่ยง (Risk-based Approach) การรักษาความพร้อมใช้และความเชื่อถือได้ของบริการ (Service Availability and Reliability) การรักษาความต่อเนื่องของบริการ (Service Continuity) และความสามารถในการรับมือและฟื้นคืนจากเหตุภัยคุกคามทางไซเบอร์ (Cyber Resilience) โดยอ้างอิงหลักการและมาตรฐานสากลที่เกี่ยวข้อง

ทั้งนี้ กรอบมาตรฐานฉบับนี้ให้ใช้ร่วมกับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม ซึ่งกำหนดข้อกำหนดและแนวทางดำเนินการเพื่อให้บรรลุผลลัพธ์ด้านความมั่นคงปลอดภัยไซเบอร์ตามกรอบมาตรฐานฉบับนี้

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีการให้บริการโทรคมนาคมซึ่งอยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. ให้มีแนวทางการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์อย่างเป็นระบบ สอดคล้องกับระดับความเสี่ยง ความสำคัญของระบบและบริการ และผลกระทบที่อาจเกิดขึ้น

๒.๒ เพื่อกำหนดกรอบการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้ครอบคลุมการกำกับดูแล (Govern) การระบุ (Identify) การป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการฟื้นคืน (Recover) โดยมุ่งรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ตลอดจนความเชื่อถือได้ (Reliability) และความต่อเนื่องของบริการ (Service Continuity) ที่สำคัญ

๒.๓ เพื่อใช้เป็นกรอบอ้างอิงสำหรับการจัดทำและการนำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปใช้ รวมถึงสนับสนุนการกำกับดูแล การประเมินความเสี่ยง การติดตาม และการปรับปรุงการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานอย่างต่อเนื่อง

๓. ขอบเขตการใช้

๓.๑ กรอบมาตรฐานฉบับนี้ใช้กับผู้รับใบอนุญาตประกอบกิจการโทรคมนาคมซึ่งเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคมที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยหลักเกณฑ์ ลักษณะ หน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมาย การควบคุมและกำกับดูแล และที่แก้ไขเพิ่มเติมหรือใช้แทนในภายหลัง โดยครอบคลุมภารกิจหรือบริการที่สำคัญ (Critical Services) ดังต่อไปนี้

- (๑) บริการโทรศัพท์ประจำที่ภายในประเทศ (Fixed-line)
- (๒) บริการโทรศัพท์เคลื่อนที่ภายในประเทศ (Mobile)
- (๓) บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ (Internet)
- (๔) บริการโทรคมนาคมระหว่างประเทศผ่านโครงข่ายภาคพื้นดินและภาคพื้นน้ำ

๓.๒ การนำกรอบมาตรฐานฉบับนี้ไปใช้ ให้ครอบคลุมระบบสารสนเทศ ระบบและโครงข่ายโทรคมนาคม ข้อมูล ซอฟต์แวร์ เฟิร์มแวร์ อุปกรณ์ แพลตฟอร์ม ระบบบริหารจัดการ ระบบสนับสนุน การปฏิบัติงาน โครงสร้างพื้นฐานทางกายภาพและทางวิศวกรรม บุคลากร กระบวนการ ผู้ให้บริการภายนอก และการพึ่งพาอื่น เท่าที่เกี่ยวข้องกับหรืออาจส่งผลกระทบต่อการให้บริการที่สำคัญตามข้อ ๓.๑

๓.๓ การกำหนดขอบเขตของระบบ ทรัพย์สิน และองค์ประกอบที่ต้องนำกรอบมาตรฐานไปใช้ **ให้หน่วยงานเป็นผู้พิจารณาและกำหนดขอบเขตดังกล่าว** โดยพิจารณาตามความสัมพันธ์และการพึ่งพาของ องค์ประกอบดังกล่าวต่อการให้บริการที่สำคัญ ระดับความเสี่ยง และผลกระทบที่อาจเกิดขึ้นต่อความมั่นคง ปลอดภัย ความพร้อมใช้ ความเชื่อถือได้ หรือความต่อเนื่องของบริการ ทั้งนี้ การที่ระบบหรือองค์ประกอบใด อยู่ภายในหน่วยงานมิได้หมายความว่าระบบหรือองค์ประกอบนั้นจะอยู่ภายใต้ขอบเขตของกรอบมาตรฐาน ฉบับนี้โดยอัตโนมัติ หากไม่มีความเกี่ยวข้องหรือไม่มีผลกระทบต่อการให้บริการที่สำคัญตามข้อ ๓.๑

หน่วยงานต้องจัดทำและเก็บรักษาข้อมูลขอบเขตที่กำหนด พร้อมเหตุผลและหลักฐาน ประกอบตามความเหมาะสม เพื่อให้สามารถตรวจสอบได้ โดยไม่จำเป็นต้องเสนอขอบเขตดังกล่าวให้สำนักงาน กสทช. หรือสำนักงานให้ความเห็นชอบล่วงหน้า เว้นแต่กฎหมาย ประกาศ หรือหลักเกณฑ์ที่มีผลใช้บังคับ จะกำหนดไว้เป็นอย่างอื่น

๓.๔ ในกรณีที่ระบบ เทคโนโลยี หรือบริการที่อยู่ในขอบเขตตามข้อ ๓.๑ ถึงข้อ ๓.๓ อยู่ภายใต้ กฎหมาย มาตรฐาน หรือข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เฉพาะที่มีผลใช้บังคับ หน่วยงาน ต้องปฏิบัติตามกฎหมาย มาตรฐาน หรือข้อกำหนดดังกล่าวร่วมกับกรอบมาตรฐานและประมวลแนวทางปฏิบัติ ที่เกี่ยวข้อง

๔. คำนิยาม

คำศัพท์	ความหมาย
พระราชบัญญัติ	พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
สำนักงาน	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
สำนักงาน กสทช.	สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ

คำศัพท์	ความหมาย
กรอบมาตรฐาน	กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
ประมวลแนวปฏิบัติ	ประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
โพรไฟล์ของหน่วยงาน	กลไกที่ใช้สำหรับการอธิบายสถานะการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
โพรไฟล์ของกลุ่มหน่วยงาน	โพรไฟล์ของกลุ่มหน่วยงานที่มีลักษณะภารกิจหรือบริการใกล้เคียงกันจัดทำขึ้นตามข้อตกลงร่วมกัน หรือที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดขึ้น
หน่วยงาน	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่มีภารกิจหรือให้บริการด้านโทรคมนาคม ซึ่งอยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล และที่แก้ไขเพิ่มเติมหรือใช้แทนในภายหลัง
บริการที่สำคัญ (Critical Service)	ภารกิจหรือบริการที่สำคัญของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติว่าด้วยหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล และที่แก้ไขเพิ่มเติมหรือใช้แทนในภายหลัง เฉพาะในส่วนของการให้บริการโทรคมนาคมที่อยู่ภายใต้การควบคุมหรือกำกับดูแลของสำนักงาน กสทช. ตามขอบเขตที่กำหนดไว้ในกรอบมาตรฐานฉบับนี้
ระบบสำคัญ (Critical System)	ระบบ โครงข่าย ทรัพยากรสิน กระบวนการ หรือองค์ประกอบที่จำเป็นต่อการให้บริการที่สำคัญ หรือซึ่งหากเกิดการหยุดชะงัก ความเสียหาย การทำงานผิดปกติ หรือการถูกควบคุมโดยมิชอบ อาจส่งผลกระทบต่ออย่างมีนัยสำคัญต่อการให้บริการที่สำคัญ
การกำกับดูแล	การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ตามหลักการควบคุม กำกับ และตรวจสอบ
การระบุ	การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพยากรสินและชีวิตร่างกายของบุคคล ทั้งนี้ให้ครอบคลุมถึงการระบุความเสี่ยงต่อระบบควบคุมหรืออุปกรณ์เทคโนโลยีปฏิบัติการ และข้อมูลอื่นที่เกี่ยวข้องกับระบบควบคุมหรืออุปกรณ์ดังกล่าว
การป้องกัน	มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น
การรับมือ	มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

คำศัพท์	ความหมาย
การฟื้นฟู	มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์
มาตรการทดแทน (Compensating Controls)	มาตรการควบคุมทางเลือกที่หน่วยงานนำมาใช้เพื่อลดความเสี่ยง ในกรณีที่ไม่สามารถดำเนินการตามมาตรการควบคุมตามที่กำหนดไว้ในประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศด้านการให้บริการโทรคมนาคม โดยมาตรการทดแทนต้องสามารถปกป้องระบบหรือหน่วยงานได้ในระดับที่เทียบเท่าหรือใกล้เคียงกับมาตรการควบคุมตามที่กำหนดดังกล่าว
เทคโนโลยีสารสนเทศ (Information Technology: IT)	บริการ อุปกรณ์ หรือระบบที่เชื่อมต่อถึงกัน (รวมถึงระบบย่อยของอุปกรณ์) ซึ่งหน่วยงานใช้ในการดำเนินการเพื่อการได้มา การจัดเก็บ การวิเคราะห์ การประเมินผล การปรับเปลี่ยน การจัดการ การเคลื่อนย้าย การควบคุม การแสดงผล การสับเปลี่ยน และการรับส่งข้อมูลหรือสารสนเทศโดยอัตโนมัติ โดยให้หมายรวมถึงอุปกรณ์หรือบริการที่หน่วยงานใช้โดยตรง และที่ถูกใช้โดยผู้รับจ้างภายใต้สัญญาจ้างกับหน่วยงานด้วย เทคโนโลยีสารสนเทศครอบคลุมถึงคอมพิวเตอร์ อุปกรณ์ประกอบ (เช่น อุปกรณ์ถ่ายภาพ อุปกรณ์นำเข้า อุปกรณ์ส่งออก และอุปกรณ์จัดเก็บข้อมูล) ที่จำเป็นต่อการรักษาความมั่นคงปลอดภัยและการเฝ้าระวัง) อุปกรณ์ต่อพ่วงที่ออกแบบให้ควบคุมโดยหน่วยประมวลผลกลางของคอมพิวเตอร์ ซอฟต์แวร์ เฟิร์มแวร์ บริการต่าง ๆ (รวมถึงบริการประมวลผลแบบคลาวด์ บริการช่วยเหลือด้านเทคนิค (Help-desk) หรือบริการที่ต้องใช้ผู้เชี่ยวชาญเฉพาะด้านที่สนับสนุนในทุกช่วงของวงจรชีวิตของอุปกรณ์หรือบริการ) ตลอดจนทรัพยากรที่เกี่ยวข้อง อย่างไรก็ตาม เทคโนโลยีสารสนเทศไม่รวมถึงอุปกรณ์ใด ๆ ที่ผู้รับจ้างจัดหามาใช้ประกอบการดำเนินงาน โดยที่สัญญาจ้างไม่ได้กำหนดให้ต้องใช้อุปกรณ์นั้น
ระบบและโครงสร้างพื้นฐานโทรคมนาคม (Telecommunications Systems and Infrastructure)	ระบบ โครงข่าย อุปกรณ์ ซอฟต์แวร์ แพลตฟอร์ม และโครงสร้างพื้นฐานทางเทคนิคที่ใช้ในการให้บริการ ควบคุม บริหารจัดการ หรือสนับสนุนการให้บริการที่สำคัญด้านโทรคมนาคม รวมถึงองค์ประกอบที่เกี่ยวข้องเท่าที่มีความจำเป็นต่อการให้บริการที่สำคัญ
โครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคม (Telecommunications Supporting Infrastructure)	ระบบ อุปกรณ์ และโครงสร้างพื้นฐานทางเทคนิค ทางกายภาพ หรือทางวิศวกรรมที่สนับสนุนการดำเนินงานของระบบและโครงสร้างพื้นฐานโทรคมนาคมที่จำเป็นต่อการให้บริการที่สำคัญ รวมถึงระบบจ่ายและสำรองพลังงาน ระบบระบายความร้อน ระบบตรวจวัดและควบคุมสภาพแวดล้อม ระบบป้องกันอัคคีภัย และระบบสนับสนุนอื่นที่มีลักษณะเทียบเท่า
การยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)	กระบวนการยืนยันตัวตนโดยใช้ปัจจัยการยืนยันตัวตนตั้งแต่สองปัจจัยขึ้นไปจากต่างประเภทกัน เช่น สิ่งที่คุณใช้งานทราบ (Knowledge Factor) สิ่งที่คุณใช้งานครอบครอง (Possession Factor) หรือคุณลักษณะเฉพาะของคุณใช้งาน (Inherence Factor) เพื่อเพิ่มความมั่นคงปลอดภัยในการเข้าถึงระบบหรือบริการ ตัวอย่างเช่น การใช้รหัสผ่านร่วมกับรหัสยืนยันแบบใช้ครั้งเดียว (One-Time

คำศัพท์	ความหมาย
	Password: OTP) ผ่านอุปกรณ์หรือแอปพลิเคชันที่ผูกกับผู้ใช้งาน การใช้รหัสผ่านร่วมกับอุปกรณ์ยืนยันตัวตนทางกายภาพ (Security Key) หรือการใช้ปัจจัยชีวมิติร่วมกับอุปกรณ์ยืนยันตัวตนที่รองรับมาตรฐานที่เหมาะสม ทั้งนี้ การใช้ปัจจัยหลายรายการจากประเภทเดียวกันไม่ถือเป็นการยืนยันตัวตนแบบหลายปัจจัย
ผู้ให้บริการภายนอก (External Service Provider)	บุคคลหรือนิติบุคคลภายนอกที่ให้บริการ สนับสนุน พัฒนา ดำเนินงาน หรือบำรุงรักษาระบบ ข้อมูล โครงข่าย หรือทรัพยากรที่เกี่ยวข้องกับการให้บริการที่สำคัญ หรือสามารถเข้าถึงทรัพยากรดังกล่าว รวมถึงผู้รับจ้างช่วงหรือผู้ให้บริการช่วงต่อตามขอบเขตที่เกี่ยวข้อง
ความเสี่ยงด้านห่วงโซ่อุปทาน (Supply Chain Risk)	ความเสี่ยงที่เกิดจากหรือเกี่ยวข้องกับผู้ผลิต ผู้พัฒนา ผู้ให้บริการภายนอก ผู้รับจ้าง คู่ค้า ฮาร์ดแวร์ ซอฟต์แวร์ ส่วนประกอบ หรือบริการที่หน่วยงานพึ่งพา ซึ่งอาจส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยไซเบอร์หรือการให้บริการที่สำคัญ
การบริหารช่องโหว่ (Vulnerability Management)	กระบวนการอย่างต่อเนื่องในการระบุ รับทราบ ประเมิน จัดลำดับความสำคัญ แก้ไขหรือบรรเทา ติดตาม และทบทวนช่องโหว่ โดยพิจารณาตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้น
การเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD)	กระบวนการในการรับแจ้ง คัดกรอง ตรวจสอบ ประเมินผลกระทบ ประสานการแก้ไขหรือบรรเทา ติดตามผล และสื่อสารหรือเปิดเผยข้อมูลเกี่ยวกับช่องโหว่อย่างเหมาะสมระหว่างผู้เกี่ยวข้อง
การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	กระบวนการที่มุ่งลดหรือจัดช่องทางการโจมตีของผู้ไม่ประสงค์ดี ด้วยการอุดช่องโหว่ของระบบและปิดใช้งานบริการที่ไม่จำเป็น
คอมไพเลอร์ (Compiler)	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
ความพร้อมรับมือทางไซเบอร์ (Cyber Resilience)	ความสามารถของหน่วยงานในการดำเนินงานหรือให้บริการได้อย่างต่อเนื่องภายใต้เหตุภัยคุกคามทางไซเบอร์ หรือสถานะที่ไม่พึงประสงค์ที่กระทบต่อระบบ เทคโนโลยีสารสนเทศหรือระบบเทคโนโลยีปฏิบัติการของหน่วยงาน รวมถึงความสามารถในการคาดการณ์ การต้านทาน การฟื้นฟู และการปรับตัวให้กลับสู่ระดับการดำเนินงานตามปกติได้อย่างเหมาะสม
เครื่องแม่ข่ายบันทึกข้อมูล (Data Historian Server)	เครื่องแม่ข่ายฐานข้อมูลแบบรวมศูนย์ที่รองรับการวิเคราะห์ข้อมูลโดยใช้เทคนิคทางสถิติสำหรับการควบคุมกระบวนการ
ดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator)	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้หน่วยงานมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

คำศัพท์	ความหมาย
ทรัพย์สินสารสนเทศ (Information Asset)	ข้อมูล และทรัพยากรหรือองค์ประกอบต่าง ๆ ที่เกี่ยวข้องกับการสร้าง การจัดเก็บ การประมวลผล การส่งผ่าน หรือการปกป้องข้อมูลดังกล่าว ซึ่งมีคุณค่าหรือมีความสำคัญต่อการดำเนินงานของหน่วยงาน ทั้งนี้รวมถึงแต่ไม่จำกัดเพียง ระบบสารสนเทศ ระบบคอมพิวเตอร์ ฮาร์ดแวร์ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย สื่อบันทึกข้อมูล เอกสาร และบุคลากรที่เกี่ยวข้อง
แพตช์ (Patch)	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ
ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite)	ประเภทและระดับของความเสี่ยงในภาพรวมที่หน่วยงานพร้อมที่จะยอมรับ เพื่อให้บรรลุวัตถุประสงค์เชิงกลยุทธ์หรือเป้าหมายของหน่วยงาน
ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO)	ระยะเวลาเป้าหมายในการกู้คืนระบบและบริการที่หยุดชะงัก ให้สามารถกลับมาดำเนินงานในระดับความสามารถขั้นต่ำที่ยอมรับได้ โดยระยะเวลาดังกล่าวไม่เกิน ระยะเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (MTPD)
ระยะเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD)	ระยะเวลาสูงสุดที่หน่วยงานยังสามารถยอมรับผลกระทบจากการหยุดชะงักของบริการได้
ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)	ช่วงเวลาสูงสุดของข้อมูลย้อนหลังที่หน่วยงานสามารถยอมรับให้สูญหายได้ โดยวัดจากช่วงเวลาก่อนเกิดเหตุจนถึงจุดเวลาที่ข้อมูลสามารถถูกกู้คืน และกิจกรรมที่หยุดชะงักสามารถกลับมาดำเนินการได้
อธิปไตยทางข้อมูล (Data Sovereignty)	หลักการที่ข้อมูลดิจิทัลอยู่ภายใต้กฎหมายและอำนาจการกำกับดูแลของประเทศที่ข้อมูลนั้นถูกจัดเก็บหรือประมวลผล ไม่ว่าผู้เป็นเจ้าของข้อมูลหรือผู้ให้บริการระบบหรือบริการดิจิทัลจะตั้งอยู่ที่ใดก็ตาม ซึ่งหมายความว่ากฎหมายของประเทศที่ข้อมูลนั้นอยู่มีอำนาจเหนือข้อมูลนั้น และรัฐบาลของประเทศนั้นมีสิทธิ์ในการเข้าถึงหรือควบคุมข้อมูลได้ตามกฎหมาย การรักษาอธิปไตยข้อมูลเป็นสิ่งจำเป็นสำหรับภาครัฐ เพื่อปกป้องข้อมูลสำคัญของชาติ เช่น ข้อมูลด้านความมั่นคง ข้อมูลส่วนบุคคลของประชาชน และข้อมูลเชิงยุทธศาสตร์จากการถูกควบคุมโดยกฎหมายต่างชาติ

๕. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ฉบับนี้ เป็นการประยุกต์ใช้หลักการตามมาตรฐานและแนวปฏิบัติที่เป็นที่ยอมรับในระดับสากล รวมถึง The NIST Cybersecurity Framework (CSF) 2.0 ซึ่งเป็นกรอบมาตรฐานที่ใช้ได้กับเทคโนโลยีสารสนเทศและการสื่อสาร (ICT) ทุกประเภท ไม่ว่าจะเป็นเทคโนโลยีสารสนเทศ (Information Technology) อินเทอร์เน็ตทุกสรรพสิ่ง (Internet of Things) และ

เทคโนโลยีปฏิบัติการ (Operational Technology) โดยกรอบมาตรฐานประกอบด้วย ๓ องค์ประกอบหลักดังต่อไปนี้

ก) แกนหลักของกรอบมาตรฐาน (Core) เป็นองค์ประกอบหลักที่ใช้อธิบายการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน โดยมีโครงสร้างของแกนหลักตามลำดับชั้นอันประกอบด้วยการดำเนินการ (Functions) และหมวดหมู่ (Categories) ซึ่งระบุรายละเอียดผลลัพธ์การดำเนินการในแต่ละด้าน เพื่อให้บุคลากรทุกระดับของหน่วยงาน ตั้งแต่ผู้บริหารไปจนถึงผู้ปฏิบัติงานมีความเข้าใจในทิศทางเดียวกัน

ข) โปรไฟล์ของหน่วยงาน (Organizational Profile) เป็นกลไกสำหรับการอธิบายสถานะการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ตามแกนหลักของกรอบมาตรฐานทั้งสถานะในปัจจุบัน และสถานะเป้าหมาย (Target)

ค) ระดับการดำเนินการ (Tier) เป็นแนวทางสำหรับการระบุระดับความสามารถในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ซึ่งสามารถนำไปปรับใช้กับโปรไฟล์ของหน่วยงานได้

๕.๑ แกนหลักของกรอบมาตรฐาน (Core) ประกอบไปด้วยการดำเนินการ (Functions) ๖ ด้าน ดังแสดงในภาพด้านล่าง



หน่วยงานต้องดำเนินการในทุกด้านควบคู่กันไป เนื่องจากล้วนมีบทบาทสำคัญต่อการป้องกันและรับมือเหตุภัยคุกคามทางไซเบอร์ โดยที่การกักกันดูแล (Govern) การระบุ (Identify) และการป้องกัน (Protect) จะเป็นการดำเนินการเชิงรุกที่เน้นไปที่การป้องกันและการเตรียมพร้อม ในขณะที่การตรวจพบ (Detect) การรับมือ (Respond) และการฟื้นฟู (Recover) จะเป็นการดำเนินการเมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้น ดังนั้นหน่วยงานต้องดำเนินการด้านการกักกันดูแล การระบุ และการป้องกันอย่างต่อเนื่อง เพื่อให้มีความพร้อมในการดำเนินการด้านการรับมือเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นได้ตลอดเวลา

๕.๑.๑ การกักกันดูแล (Govern) เป็นการดำเนินการที่เกี่ยวข้องกับการกำหนดยุทธศาสตร์ ความคาดหวัง และนโยบายการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ทั้งนี้รวมถึงการสื่อสาร และการกำกับติดตามการดำเนินการให้เป็นไปตามที่กำหนด

ผลการดำเนินการในด้านการกักกันดูแลจะทำให้หน่วยงานสามารถดำเนินการและจัดลำดับความสำคัญของผลการดำเนินการทั้ง ๕ ด้านที่เหลือ เพื่อให้สอดคล้องกับภารกิจของหน่วยงานและความคาดหวังของผู้มีส่วนได้ส่วนเสีย นอกจากนี้ การดำเนินการด้านการกักกันดูแลมีความสำคัญอย่างยิ่งต่อการบูรณาการการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ให้เข้ากับยุทธศาสตร์การจัดการความเสี่ยงในภาพรวมของหน่วยงาน (Enterprise Risk Management: ERM)

การดำเนินการด้านการกำกับดูแลครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๑.๑ บริบทของหน่วยงาน (Organizational Context)

๕.๑.๑.๒ กลยุทธ์ในการจัดการความเสี่ยง (Risk Management Strategy)

๕.๑.๑.๓ บทบาทหน้าที่ ความรับผิดชอบ และอำนาจหน้าที่ (Roles, Responsibilities, and Authorities)

๕.๑.๑.๔ นโยบาย (Policy)

๕.๑.๑.๕ การจัดการความเสี่ยงในห่วงโซ่อุปทานความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Supply Chain Risk Management)

๕.๑.๒ การระบุ (Identify) เป็นการดำเนินการที่เกี่ยวข้องกับการทำความเข้าใจความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่หน่วยงานต้องเผชิญอยู่ในปัจจุบัน การระบุทรัพย์สินสารสนเทศของหน่วยงาน (เช่น ข้อมูล ฮาร์ดแวร์ ซอฟต์แวร์ ระบบต่าง ๆ อาคารสถานที่ บริการ และบุคลากร) ตลอดจนระบุผู้จัดหาสินค้าและผู้ให้บริการภายนอก รวมถึงความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง จะช่วยให้หน่วยงานสามารถกำหนดลำดับความสำคัญของการดำเนินการให้สอดคล้องกับยุทธศาสตร์การจัดการความเสี่ยง และความจำเป็นต่อภารกิจของหน่วยงานที่กำหนดไว้ภายใต้การดำเนินการด้านการกำกับดูแล (Govern) นอกจากนี้ การระบุความเสี่ยงยังครอบคลุมไปถึงการระบุโอกาสในการปรับปรุงนโยบาย แผน กระบวนการ ขั้นตอน และแนวปฏิบัติต่าง ๆ ที่เกี่ยวข้องกับการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อใช้เป็นข้อมูลสนับสนุนการดำเนินการทั้งหกด้าน

การดำเนินการด้านการระบุความเสี่ยงครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๒.๑ การบริหารทรัพย์สินและวงจรชีวิตเทคโนโลยี (Asset and Technology Lifecycle Management)

๕.๑.๒.๒ การกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ

๕.๑.๒.๓ การประเมินความเสี่ยง (Risk Assessment)

๕.๑.๒.๔ การบริหารช่องโหว่และการประเมินความมั่นคงปลอดภัย (Vulnerability Management and Security Assessment)

๕.๑.๒.๕ การรับแจ้ง การจัดการ และการเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD)

๕.๑.๓ การป้องกัน (Protect) เป็นการดำเนินการที่มุ่งเน้นไปที่การนำมาตรการป้องกันมาใช้เพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่ทรัพย์สินสารสนเทศของหน่วยงาน ภายหลังจากที่ได้ระบุและจัดลำดับความสำคัญตามระดับความเสี่ยงของทรัพย์สินสารสนเทศแล้ว โดยมีเป้าหมายเพื่อลดความน่าจะเป็นหรือผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

การดำเนินการด้านการป้องกันครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๓.๑ การจัดการอัตลักษณ์ การยืนยันตัวตน และการควบคุมการเข้าถึง (Identity Management, Authentication, and Access Controls)

๕.๑.๓.๒ การสร้างความตระหนักรู้และการฝึกอบรม (Awareness and Training)

๕.๑.๓.๓ การรักษาความมั่นคงปลอดภัยของข้อมูล (Data Security)

๕.๑.๓.๔ การรักษาความมั่นคงปลอดภัยของแพลตฟอร์ม (Platform Security)

๕.๑.๓.๕ การเสริมสร้างความพร้อมรับมือของโครงสร้างพื้นฐานทางเทคโนโลยี (Technology Infrastructure Resilience)

๕.๑.๓.๖ การแบ่งปันข้อมูล (Information Sharing)

๕.๑.๓.๗ การรักษาความมั่นคงปลอดภัยโดยการออกแบบและตลอดวงจรชีวิต (Security by Design and Secure Lifecycle)

๕.๑.๔ การตรวจพบ (Detect) เป็นการดำเนินการที่เกี่ยวข้องกับการเฝ้าระวัง การตรวจพบ และการวิเคราะห์ความเป็นไปได้ของการโจมตีทางไซเบอร์หรือการถูกเจาะระบบ การดำเนินการในด้านนี้ช่วยให้หน่วยงานสามารถตรวจจับและวิเคราะห์ความผิดปกติ ตัวบ่งชี้การถูกเจาะระบบ (Indicators of Compromise) รวมถึงเหตุการณ์ที่อาจก่อให้เกิดความเสียหาย ได้อย่างทันท่วงที ซึ่งเป็นพื้นฐานสำคัญต่อการตอบสนองและการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ

การดำเนินการด้านการตรวจพบครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๔.๑ การเฝ้าระวังและตรวจจับภัยคุกคามอย่างต่อเนื่อง (Continuous Security Monitoring and Threat Detection)

๕.๑.๔.๒ การวิเคราะห์เหตุการณ์ที่ไม่พึงประสงค์ (Adverse Event Analysis)

๕.๑.๕ การรับมือ (Respond) เป็นการดำเนินการภายหลังจากตรวจพบเหตุภัยคุกคามทางไซเบอร์โดยมุ่งเน้นไปที่การระงับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

การดำเนินการด้านการรับมือครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๕.๑ การจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Management)

๕.๑.๕.๒ การวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Incident Analysis)

๕.๑.๕.๓ การสื่อสารและการรายงานในการรับมือเหตุภัยคุกคามทางไซเบอร์ (Incident Response Reporting and Communication)

๕.๑.๕.๔ การบรรเทาเหตุภัยคุกคามทางไซเบอร์ (Incident Mitigation)

๕.๑.๕.๕ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๕.๑.๖ การฟื้นฟู (Recover) เป็นการดำเนินการที่มุ่งเน้นการกู้คืนและฟื้นฟูทรัพยากรสารสนเทศ รวมถึงการดำเนินงานที่ได้รับผลกระทบจากเหตุภัยคุกคามทางไซเบอร์ ให้กลับสู่ภาวะปกติโดยเร็ว ทั้งนี้ เพื่อลดผลกระทบจากเหตุภัยคุกคามทางไซเบอร์

การดำเนินการด้านการฟื้นฟูครอบคลุมหมวดหมู่ต่าง ๆ ดังนี้

๕.๑.๖.๑ แผนความต่อเนื่องทางธุรกิจและแผนฟื้นฟูจากภัยพิบัติ (Business Continuity Plan: BCP and Disaster Recovery Plan: DRP)

๕.๑.๖.๒ แผนฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Plan)

๕.๑.๖.๓ การสื่อสารระหว่างการฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ (Incident Recovery Communication)

๕.๒ โพรไฟล์ของหน่วยงาน (Organizational Profile) เป็นกลไกสำหรับการอธิบายสถานะการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ตามแกนหลักของกรอบมาตรฐานทั้งสถานะปัจจุบัน และสถานะเป้าหมาย (Target)

โพรไฟล์ของหน่วยงานที่สอดคล้องกับภารกิจหรือบริการ ความคาดหวังของผู้มีส่วนได้ส่วนเสีย สถานการณ์ภัยคุกคามทางไซเบอร์ และข้อกำหนดของหน่วยงาน จะช่วยให้หน่วยงานสามารถจัดลำดับความสำคัญของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามกรอบมาตรฐานทั้ง ๖ ด้านได้อย่างเหมาะสมและมีประสิทธิภาพเพิ่มมากขึ้น นอกจากนี้ หน่วยงานยังสามารถใช้โพรไฟล์ของหน่วยงานเป็นเครื่องมือในการทำความเข้าใจ การปรับใช้ และการสื่อสารเกี่ยวกับผลการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานได้ โดยโพรไฟล์ของหน่วยงานประกอบไปด้วย

๕.๒.๑ โปรไฟล์ปัจจุบัน (Current Profile) สะท้อนถึงผลการดำเนินการตามแกนหลักของกรอบมาตรฐานที่หน่วยงานดำเนินการอยู่ในปัจจุบัน พร้อมทั้งระดับของการดำเนินการ (Tier)

๕.๒.๒ โปรไฟล์เป้าหมาย (Target Profile) สะท้อนถึงผลการดำเนินการตามแกนหลักของกรอบมาตรฐานที่หน่วยงานเลือกและจะให้ความสำคัญ เพื่อใช้เป็นเป้าหมายในการดำเนินการตามกรอบมาตรฐาน ทั้งนี้ การกำหนดโปรไฟล์เป้าหมายเป็นการวางทิศทาง การปรับปรุงเพื่อยกระดับขีดความสามารถทางไซเบอร์ โดยได้พิจารณาถึงการเปลี่ยนแปลงที่อาจเกิดขึ้นในอนาคต เช่น การประกาศข้อกำหนดใหม่ หรือการนำเทคโนโลยีใหม่มาปรับใช้

สำนักงานอาจจัดทำแนวปฏิบัติสำหรับจัดทำโปรไฟล์ของหน่วยงานให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการดำเนินการ

ขั้นตอนการจัดทำโปรไฟล์ของหน่วยงาน

การจัดทำโปรไฟล์ของหน่วยงาน เป็นกระบวนการเปรียบเทียบระหว่างโปรไฟล์ปัจจุบัน (หรือผลการประเมินการดำเนินการในปัจจุบัน) กับโปรไฟล์เป้าหมายที่หน่วยงานมุ่งหวังจะบรรลุ เพื่อวิเคราะห์และระบุช่องว่างระหว่างโปรไฟล์ทั้งสอง จากนั้นจัดทำแผนปฏิบัติการเพื่อพัฒนาและปรับปรุงการดำเนินงานให้เป็นไปตามเป้าหมาย กระบวนการนี้ช่วยให้หน่วยงานสามารถยกระดับและปรับปรุงโปรไฟล์เป้าหมายให้มีความเหมาะสมและสอดคล้องกับสถานการณ์ในการประเมินครั้งต่อไป การจัดทำโปรไฟล์ของหน่วยงานมีขั้นตอนดังนี้

ขั้นตอนที่ ๑ กำหนดขอบเขตในการจัดทำโปรไฟล์ของหน่วยงาน (Scope the Organizational Profile)

กำหนดขอบเขตในการจัดทำโปรไฟล์ โดยคำนึงถึงความสอดคล้องกับวัตถุประสงค์เชิงภารกิจของหน่วยงาน ความคาดหวังของผู้มีส่วนได้ส่วนเสีย สถานการณ์ภัยคุกคามทางไซเบอร์ และข้อกำหนดหรือกฎหมายที่เกี่ยวข้องกับหน่วยงาน ทั้งนี้ หน่วยงานอาจจัดทำโปรไฟล์ในภาพรวมของหน่วยงานเพียงโปรไฟล์เดียว หรือจัดทำโปรไฟล์เฉพาะด้านสำหรับกระบวนการหรือระบบสารสนเทศสำคัญ (เช่น กระบวนการตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ ระบบการเงินของหน่วยงาน ระบบที่ให้บริการแก่ประชาชนเป็นจำนวนมาก) ก็ได้ ดังนั้น หน่วยงานหนึ่งอาจจัดทำโปรไฟล์จำนวนหนึ่งโปรไฟล์หรือหลายโปรไฟล์ก็ได้ ทั้งนี้ ขึ้นกับขอบเขตและวัตถุประสงค์ที่ต้องการ

ในการกำหนดขอบเขตดังกล่าว หน่วยงานควรพิจารณาประเด็นสำคัญ ดังตัวอย่างต่อไปนี้

- ก) วัตถุประสงค์หลักของการจัดทำโปรไฟล์ของหน่วยงาน
- ข) ขอบเขตของโปรไฟล์ควรครอบคลุมทั้งหน่วยงาน หรือเฉพาะบางส่วน เช่น เฉพาะส่วนงาน เฉพาะระบบสารสนเทศสำคัญ เฉพาะข้อมูลสารสนเทศของหน่วยงาน เฉพาะทรัพย์สินที่เป็นเทคโนโลยี หรือเฉพาะผลิตภัณฑ์และบริการ
- ค) ประเภทของภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงต่อหน่วยงาน ช่องโหว่ การโจมตี และมาตรการป้องกัน
- ง) บุคคลหรือทีมงานที่รับผิดชอบในการจัดทำ ทบทวน และนำไปใช้ดำเนินการจริง
- จ) บุคคลหรือกลุ่มบุคคลที่มีหน้าที่กำหนดความคาดหวังและเป้าหมายในการดำเนินการ เพื่อให้บรรลุผลลัพธ์ตามโปรไฟล์เป้าหมาย

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดขอบเขตในการจัดทำโปรไฟล์ให้ครอบคลุมภารกิจหรือบริการตามประกาศคณะกรรมการการรักษา

ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง หลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๘ ซึ่งอยู่ในความรับผิดชอบของหน่วยงาน เป็นอย่างน้อย

ขั้นตอนที่ ๒ รวบรวมข้อมูลที่จำเป็นสำหรับการจัดทำโพรไฟล์ (Gather the Information Needed to Prepare the Organizational Profile)

รวบรวมข้อมูลที่เกี่ยวข้อง ให้เพียงพอต่อการประเมินสถานะการดำเนินการของหน่วยงาน เช่น

- ก) นโยบายหรือยุทธศาสตร์ของหน่วยงาน
- ข) ลำดับความสำคัญและทรัพยากรที่ต้องใช้ในการจัดการความเสี่ยง
- ค) ผลการประเมินความเสี่ยงระดับหน่วยงาน
- ง) ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)
- จ) ข้อกำหนด มาตรฐาน และแนวทางปฏิบัติด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
- ฉ) เทคโนโลยีที่เกี่ยวข้อง
- ช) บทบาทและหน้าที่ของผู้ที่เกี่ยวข้องในการดำเนินการ

แหล่งข้อมูลที่ใช้ในการจัดทำโพรไฟล์อาจแตกต่างกันไปตามวัตถุประสงค์การใช้งานขอบเขตของโพรไฟล์ และระดับความละเอียดของข้อมูลที่ต้องการ โดยทั่วไปแล้ว ข้อมูลดังกล่าวอาจมาจากหลายแหล่ง รวมถึง โพรไฟล์ของกลุ่มหน่วยงาน (Community Profile) ซึ่งอาจเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กลุ่มหน่วยงานที่มีลักษณะภารกิจหรือบริการใกล้เคียงกันจัดทำขึ้นตามข้อตกลงร่วมกัน หรือที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดขึ้น

ขั้นตอนที่ ๓ สร้างโพรไฟล์ของหน่วยงาน (Create the Organizational Profile)

หน่วยงานดำเนินการสร้างโพรไฟล์ของหน่วยงาน ดังต่อไปนี้

- ก) นำข้อมูลที่ได้รวบรวมไว้ตามขั้นตอนที่ ๒ มาพิจารณาถึงความสอดคล้องกับการดำเนินการตามขอบเขตในการจัดทำโพรไฟล์ที่หน่วยงานได้เลือกไว้ในขั้นตอนที่ ๑ และใช้ข้อมูลดังกล่าวประกอบการจัดทำโพรไฟล์ปัจจุบัน
- ข) จัดทำหรือพิจารณาโพรไฟล์ปัจจุบัน และประเมินความเสี่ยงทางไซเบอร์ที่อาจเกิดขึ้น
- ค) นำโพรไฟล์ของกลุ่มหน่วยงานที่เกี่ยวข้องมาเป็นข้อกำหนดขั้นต่ำในการจัดทำโพรไฟล์เป้าหมายของหน่วยงาน โดยอาจปรับเพิ่มระดับการดำเนินการ (Tier) หมวดหมู่ย่อย (Subcategories) การอ้างอิงข้อมูลสนับสนุน (Informative References) หรือแนวทางปฏิบัติเฉพาะของหน่วยงาน ให้สอดคล้องกับผลการประเมินความเสี่ยงในข้อ ข) รวมถึงนโยบาย ระเบียบ และข้อกำหนดของหน่วยงาน ที่เกี่ยวข้องด้วย ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หน่วยงานดังกล่าวต้องจัดทำโพรไฟล์เป้าหมายให้เป็นไปตามโพรไฟล์ของกลุ่มหน่วยงาน (Community Profile) ที่หน่วยงานควบคุมหรือกำกับดูแลของตนกำหนดเป็นอย่างน้อย
- ง) สื่อสารเป้าหมายการดำเนินการไปยังผู้ที่มีส่วนเกี่ยวข้อง พร้อมทั้งกำหนดตัวชี้วัด
- จ) ควบคุมและติดตามให้เป็นไปตามเป้าหมาย และปรับปรุงโพรไฟล์เป้าหมายเป็นระยะ

ขั้นตอนที่ ๔ วิเคราะห์ช่องว่างระหว่างโปรไฟล์ปัจจุบันและโปรไฟล์เป้าหมาย และจัดทำแผนปฏิบัติการ (Analyze the Gaps between the Current and Target Profiles and Create an Action Plan)

วิเคราะห์ความแตกต่างระหว่างโปรไฟล์ปัจจุบันและโปรไฟล์เป้าหมาย ทั้งในด้านบุคลากร กระบวนการ และเทคโนโลยี เพื่อระบุช่องว่าง (Gap) ที่ต้องดำเนินการปรับปรุง จากนั้นนำผลการวิเคราะห์ดังกล่าวมาใช้จัดทำแผนปฏิบัติการ (Action Plan) เพื่อกำหนดแนวทางและลำดับความสำคัญของการดำเนินการปรับปรุงและยกระดับการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้บรรลุตามเป้าหมายที่กำหนดไว้อย่างเหมาะสมและคุ้มค่า

ในการจัดทำแผนปฏิบัติการ หน่วยงานควรคำนึงถึงปัจจัยสำคัญ เช่น ภารกิจหลักของหน่วยงาน ผลประโยชน์ที่คาดว่าจะได้รับ ความเสี่ยงที่อาจเกิดขึ้น ความคุ้มค่าของการดำเนินการ และทรัพยากรที่จำเป็น เช่น บุคลากรและงบประมาณ ทั้งนี้ แผนปฏิบัติการอาจอยู่ในรูปแบบของแผนดำเนินงานและเป้าหมาย (Plan of Action and Milestones) หรือแผนปฏิบัติการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำแผนการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗ โดยต้องระบุรายการที่หน่วยงานต้องดำเนินการเพื่อปิดช่องว่าง พร้อมแนวทางการดำเนินการที่ชัดเจน

แผนปฏิบัติการควรประกอบด้วยข้อมูลสำคัญ ดังนี้

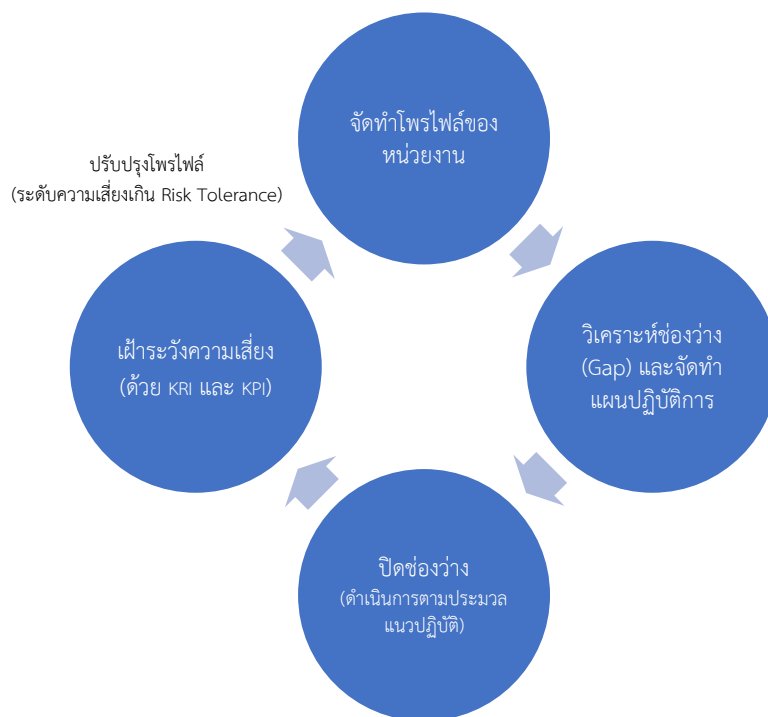
- ก) แนวทางการดำเนินการปรับปรุง
- ข) ระดับความสำคัญ
- ค) ผู้รับผิดชอบหลัก
- ง) กำหนดการปรับปรุง
- จ) ทรัพยากรที่ต้องใช้

ในกรณีที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องจัดทำแผนปฏิบัติการเพื่อปรับปรุงการดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้บรรลุระดับการดำเนินการ (Tier) ที่หน่วยงานควบคุมหรือกำกับดูแลของตนกำหนดไว้ในโปรไฟล์ของกลุ่มหน่วยงาน (Community Profile) ภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลดังกล่าวกำหนดด้วย

ขั้นตอนที่ ๕ ดำเนินการตามแผนปฏิบัติการ และปรับปรุงสถานะความมั่นคงปลอดภัยไซเบอร์ (Implement the Action Plan and Update the Organizational Profile)

ดำเนินการตามแผนปฏิบัติการที่ได้จัดทำไว้ในขั้นตอนที่ ๔ โดยดำเนินการตามข้อกำหนดในประมวลแนวปฏิบัติ ไม่ว่าจะเป็นการกำหนดนโยบาย การวางกระบวนการทำงาน หรือการใช้เครื่องมืออัตโนมัติ เพื่อผลักดันให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานบรรลุตามโปรไฟล์เป้าหมายภายในระยะเวลาที่กำหนด

หน่วยงานอาจใช้โปรไฟล์ของหน่วยงาน (Organizational Profile) ในการติดตามความก้าวหน้าของการดำเนินการตามแผนปฏิบัติการ นอกจากนี้ หน่วยงานสามารถใช้ดัชนีชี้วัดผลการดำเนินงาน (Key Performance Indicators: KPI) และดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicators: KRI) เพื่อเฝ้าระวังความเสี่ยงและประเมินประสิทธิภาพของมาตรการควบคุมที่นำมาใช้ หากพบความเสี่ยงที่เกินระดับความเสี่ยงสูงสุดที่ยอมรับได้ (Risk Tolerance) หน่วยงานควรดำเนินการปรับปรุงแผนปฏิบัติการโปรไฟล์ของหน่วยงาน หรือระดับความเสี่ยงสูงสุดที่ยอมรับได้ให้เหมาะสม



๕.๓ โปรไฟล์ของกลุ่มหน่วยงานที่มีลักษณะภารกิจหรือบริการใกล้เคียงกัน (Community Profile)

โปรไฟล์ของกลุ่มหน่วยงานที่มีลักษณะภารกิจหรือบริการใกล้เคียงกัน (Community Profile) คือ โปรไฟล์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีลักษณะเป็นข้อกำหนดขั้นต่ำ (Baseline) ของภาคส่วน ที่หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่ได้รับมอบหมายกำหนดขึ้นสำหรับหน่วยงานภายใต้ การควบคุมหรือกำกับดูแลหรือหน่วยงานสมาชิกที่มีลักษณะภารกิจหรือบริการใกล้เคียงกัน โดยมีวัตถุประสงค์ เพื่อให้กลุ่มหน่วยงานดังกล่าวนำไปใช้เป็นแนวทางในการจัดทำโปรไฟล์เป้าหมายของตนให้สอดคล้องกับ ทิศทางที่หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่ได้รับมอบหมายกำหนด

หน่วยงานควบคุมหรือกำกับดูแลหรือหน่วยงานที่ได้รับมอบหมายจัดทำโปรไฟล์ของกลุ่ม หน่วยงานที่มีลักษณะภารกิจหรือบริการใกล้เคียงกัน (Community Profile) ตามวงจรชีวิตของโปรไฟล์ (Profile Lifecycle) ซึ่งประกอบด้วย ๔ ขั้นตอนหลัก ได้แก่

ก) การวางแผน (Plan)

กำหนดกลุ่มหน่วยงานเป้าหมาย (หรือกลุ่มหน่วยงานที่มีลักษณะภารกิจหรือบริการ ใกล้เคียงกัน) เพื่อจัดทำโปรไฟล์เฉพาะสำหรับกลุ่มหน่วยงานดังกล่าว พร้อมทั้งระบุ ผู้มีส่วนร่วม หน่วยงานอื่นที่เกี่ยวข้อง ตลอดจนมาตรฐานหรือข้อกำหนดเฉพาะของกลุ่ม หน่วยงานเป้าหมาย เพื่อใช้เป็นแนวทางในการกำหนดประเด็นและเนื้อหาที่จะบรรจุไว้ใน โปรไฟล์ของกลุ่มหน่วยงาน

ข) การพัฒนา (Develop)

ดำเนินการจัดลำดับความสำคัญของการดำเนินการตามแกนหลักของกรอบมาตรฐาน (Core) และจัดทำร่างโปรไฟล์ของกลุ่มหน่วยงาน (Community Profile) จากนั้น นำร่าง โปรไฟล์ดังกล่าวไปรับฟังความคิดเห็นจากกลุ่มหน่วยงานเป้าหมายตาม ก) ก่อนประกาศใช้ โปรไฟล์ของกลุ่มหน่วยงานอย่างเป็นทางการ

ค) การนำไปใช้ (Use)

กำหนดแนวทางความร่วมมือ การส่งเสริม และการประสานงาน เพื่อให้กลุ่มหน่วยงานเป้าหมายนำโพรไฟล์ที่ได้พัฒนาขึ้นในข้อ ข) ไปใช้ให้เกิดประสิทธิภาพสูงสุด พร้อมทั้งประเมินสถานะการดำเนินการตามโพรไฟล์ของกลุ่มหน่วยงานเป้าหมาย

ง) การบำรุงรักษา (Maintain)

ประเมินความสำเร็จของการนำโพรไฟล์ของกลุ่มหน่วยงานไปใช้ในทางปฏิบัติ รวมถึงรวบรวมข้อเสนอแนะเพื่อพิจารณาการเปลี่ยนแปลงที่จำเป็น เพื่อนำไปทบทวนและปรับปรุงโพรไฟล์ให้สอดคล้องกับภัยคุกคามทางไซเบอร์ เทคโนโลยี หรือข้อกำหนดทางกฎหมายที่เปลี่ยนแปลงไป

๕.๔ ระดับการดำเนินการ (Tier)

หน่วยงานสามารถเลือกระดับการดำเนินการ (Tier) ในการจัดทำโพรไฟล์ปัจจุบันและโพรไฟล์เป้าหมาย โดยระดับการดำเนินการดังกล่าวจะสะท้อนถึงระดับความเข้มแข็งของการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และสะท้อนถึงมุมมองของหน่วยงานที่มีต่อความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และกระบวนการจัดการความเสี่ยงดังกล่าว

ระดับการดำเนินการสะท้อนถึงการดำเนินการในแต่ละระดับ เริ่มตั้งแต่การดำเนินการแบบไม่เป็นทางการ ไปสู่แนวทางที่มีความชัดเจนตัว อ้างอิงตามความเสี่ยง และมีการปรับปรุงอย่างต่อเนื่อง โดยระดับการดำเนินการมี ๔ ระดับ ดังนี้

ระดับที่ ๑: ดำเนินการบางส่วน (Partial)

ระดับที่ ๒: ดำเนินการโดยอ้างอิงความเสี่ยง (Risk Informed)

ระดับที่ ๓: ดำเนินการตามมาตรฐาน และครอบคลุมทั้งหน่วยงาน (Repeatable)

ระดับที่ ๔: ดำเนินการปรับเปลี่ยนตามสถานการณ์ที่เปลี่ยนแปลง (Adaptive)

ระดับการดำเนินการ (Tier) ถูกออกแบบมาเพื่อส่งเสริมกระบวนการบริหารจัดการความเสี่ยงของหน่วยงานที่มีอยู่เดิม ไม่ใช่เพื่อใช้ทดแทนแนวทางหรือระเบียบวิธีการจัดการความเสี่ยงที่มีอยู่ โดยหน่วยงานอาจใช้ระดับการดำเนินการเป็นเกณฑ์อ้างอิง (Benchmark) สำหรับการสื่อสารภายในหน่วยงาน เพื่อให้เกิดความเข้าใจร่วมกันในแนวทางการบริหารจัดการความเสี่ยง

หน่วยงานควรส่งเสริมให้การดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับที่สูงขึ้น โดยเฉพาะเมื่อพิจารณาแล้วว่ามีปัจจัยความเสี่ยงเพิ่มขึ้น เช่น อัตราการเกิดเหตุภัยคุกคามทางไซเบอร์ที่สูงขึ้น ข้อบังคับตามกฎหมายที่เข้มข้นขึ้น หรือเมื่อผลการวิเคราะห์ความคุ้มค่าของการลงทุน (Cost-benefit Analysis) ชี้ให้เห็นว่า มีความคุ้มค่าในการลงทุนเพื่อยกระดับการดำเนินการ

๖. หลักการประยุกต์ใช้กรอบมาตรฐานและประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การนำกรอบมาตรฐานและประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปประยุกต์ใช้ ให้หน่วยงานดำเนินการตามหลักการดังต่อไปนี้

๖.๑ การบริหารจัดการตามระดับความเสี่ยง (Risk-based Approach)

หน่วยงานต้องกำหนดและดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์โดยพิจารณาจากระดับความเสี่ยง ความสำคัญของบริการ ลักษณะของระบบและโครงสร้างพื้นฐาน ภัยคุกคาม ช่องโหว่ การพึ่งพาระบบหรือผู้ให้บริการภายนอก และผลกระทบที่อาจเกิดขึ้นต่อการให้บริการที่สำคัญ

การเลือกใช้มาตรการควบคุมต้องสอดคล้องกับผลการประเมินความเสี่ยง และต้องมีการทบทวนเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญของระบบ เทคโนโลยี ภัยคุกคาม สภาพแวดล้อม การให้บริการ หรือข้อกำหนดที่เกี่ยวข้อง

๖.๒ หลักความได้สัดส่วน (Proportionality)

การกำหนดมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องมีความเหมาะสมและได้สัดส่วนกับระดับความเสี่ยง ความสำคัญของระบบหรือบริการ และผลกระทบที่อาจเกิดขึ้น โดยคำนึงถึงความเป็นไปได้ทางเทคนิค ผลกระทบต่อการดำเนินงาน ความพร้อมใช้ ความเชื่อถือได้ และความต่อเนื่องของบริการ

หน่วยงานไม่จำเป็นต้องนำมาตรการในระดับเดียวกันไปใช้กับทุกระบบหรือทุกองค์ประกอบ หากสามารถแสดงให้เห็นได้ว่ามาตรการที่เลือกใช้มีความเหมาะสมกับระดับความเสี่ยงและสามารถบรรลุผลลัพธ์ด้านความมั่นคงปลอดภัยที่กำหนดได้

๖.๓ ความเป็นกลางทางเทคโนโลยี (Technology Neutrality)

การจัดทำและการประยุกต์ใช้กรอบมาตรฐานและประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้เป็นไปตามกฎหมาย กฎ ระเบียบ ประกาศ และข้อกำหนดที่เกี่ยวข้องโดยสำนักงาน กสทช. ยึดหลักความเป็นกลางทางเทคโนโลยี (Technology Neutrality) และพิจารณาอ้างอิงมาตรฐานสากล มาตรฐานที่ได้รับการยอมรับ และแนวปฏิบัติที่เกี่ยวข้องกับอุตสาหกรรมโทรคมนาคม เพื่อประกอบการกำหนดกรอบและข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างเหมาะสม

การกำหนดกรอบและข้อกำหนดดังกล่าวมุ่งเน้นผลลัพธ์ด้านความมั่นคงปลอดภัย (Security Outcomes) โดยไม่กำหนดหรือผูกพันกับผลิตภัณฑ์ ผู้ผลิต หรือเทคโนโลยีใดเป็นการเฉพาะ ทั้งนี้ หน่วยงานสามารถเลือกใช้เทคโนโลยี สถาปัตยกรรม หรือวิธีการที่เหมาะสมกับบริบทของตน ภายใต้กฎหมาย กฎ ระเบียบ ประกาศ ข้อกำหนด และระดับความเสี่ยงที่เกี่ยวข้อง

๖.๔ การใช้มาตรการทดแทน (Compensating Controls)

ในกรณีที่ข้อกำหนดมิได้กำหนดวิธีการหรือมาตรการเฉพาะที่ต้องดำเนินการ และหน่วยงานไม่สามารถนำมาตรการควบคุมที่กำหนดหรือแนะนำไปใช้ได้ เนื่องจากข้อจำกัดด้านเทคนิค สถาปัตยกรรมของระบบ ความต่อเนื่องของบริการ หรือเหตุผลอันสมควรอื่น หน่วยงานอาจกำหนดมาตรการทดแทน (Compensating Controls) โดยต้องประเมินความเสี่ยงและแสดงให้เห็นว่ามาตรการดังกล่าวสามารถลดความเสี่ยงหรือให้ผลลัพธ์ด้านความมั่นคงปลอดภัยในระดับที่เหมาะสม

การใช้มาตรการทดแทนต้องไม่ขัดหรือหลีกเลี่ยงกฎหมาย กฎ ระเบียบ ประกาศ หรือข้อกำหนดที่มีผลใช้บังคับ และต้องมีการบันทึกเหตุผล ผลการประเมินความเสี่ยง มาตรการที่นำมาใช้ และเงื่อนไขหรือระยะเวลาในการทบทวนอย่างเหมาะสม

๖.๕ การรักษาความต่อเนื่องและความเชื่อถือได้ของบริการ (Service Continuity and Reliability)

การดำเนินมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ต้องคำนึงถึงความสมดุลระหว่างการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้ (Availability) ตลอดจนความเชื่อถือได้ (Reliability) และความต่อเนื่องของบริการ (Service Continuity)

มาตรการด้านความมั่นคงปลอดภัยไซเบอร์ที่นำมาใช้ต้องไม่ก่อให้เกิดความเสี่ยงหรือผลกระทบต่อการให้บริการที่สำคัญโดยไม่เหมาะสม และต้องคำนึงถึงความสามารถในการฟื้นคืนจากเหตุการณ์ (Cyber Resilience) ตามระดับความสำคัญของระบบหรือบริการ

๖.๖ การใช้หลักฐานและความสามารถในการตรวจสอบ (Evidence-based and Verifiable Implementation)

หน่วยงานต้องสามารถแสดงหลักฐานที่เหมาะสมเพื่อยืนยันการดำเนินการตามกรอบมาตรฐานและประมวลแนวทางปฏิบัติ รวมถึงผลลัพธ์ของมาตรการที่นำมาใช้ โดยหลักฐานดังกล่าวต้องมีความเพียงพอเหมาะสม เป็นปัจจุบัน และสามารถตรวจสอบย้อนกลับได้ตามความเหมาะสม

การประเมินความสอดคล้องให้พิจารณาทั้งการมีอยู่ของมาตรการ (Design) การนำมาตรการไปใช้ (Implementation) และประสิทธิผลของมาตรการ (Effectiveness) ตามระดับความเสี่ยงและความสำคัญของระบบหรือบริการ

ข้อแนะนำเพิ่มเติมประกอบการปฏิบัติตาม
ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ด้านการให้บริการโทรคมนาคม
ฉบับวันที่ XX ตุลาคม ๒๕๖๙

หลักการใช้อ้างอิงเพิ่มเติม

ข้อแนะนำเพิ่มเติมฉบับนี้จัดทำขึ้นเพื่อสนับสนุนการนำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปประยุกต์ใช้ให้เหมาะสมกับลักษณะของระบบ เทคโนโลยี ระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ โดยมุ่งส่งเสริมการนำแนวปฏิบัติที่ดี (Good Practices) และแนวทางด้านความมั่นคงปลอดภัยไซเบอร์ที่ได้รับการยอมรับมาประยุกต์ใช้ตามบริบทของแต่ละหน่วยงาน

ข้อแนะนำในเอกสารฉบับนี้มีข้อกำหนดขั้นต่ำที่หน่วยงานทุกแห่งต้องดำเนินการในลักษณะเดียวกัน เว้นแต่จะมีกฎหมาย กฎ ระเบียบ ประกาศ หรือข้อกำหนดอื่นที่ใช้บังคับกำหนดไว้เป็นการเฉพาะ ทั้งนี้ หน่วยงานควรพิจารณานำข้อแนะนำที่เกี่ยวข้องไปประยุกต์ใช้ตามความเหมาะสม โดยคำนึงถึงระดับความเสี่ยง ความสำคัญของระบบ ความพร้อมทางเทคโนโลยี ความเป็นไปได้ในการดำเนินงาน และความจำเป็นในการรักษาความมั่นคงปลอดภัยและความต่อเนื่องของบริการที่สำคัญ

การเลือกใช้เทคโนโลยี ผลิตภัณฑ์ สถาปัตยกรรม หรือมาตรการควบคุมตามข้อแนะนำเพิ่มเติมฉบับนี้ควรพิจารณาจากผลลัพธ์ด้านความมั่นคงปลอดภัยที่ต้องการ (Security Outcomes) โดยหน่วยงานอาจเลือกใช้มาตรการหรือกลไกอื่นที่ให้ระดับการป้องกันหรือผลลัพธ์ด้านความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่าได้

ภาพรวมข้อแนะนำเพิ่มเติม

ข้อแนะนำเพิ่มเติมฉบับนี้แบ่งแนวทางการรักษาความมั่นคงปลอดภัยไซเบอร์ออกเป็น ๑๓ เรื่อง ครอบคลุมความมั่นคงปลอดภัยและความทนทานของระบบและโครงสร้างพื้นฐานโทรคมนาคม การรักษาความมั่นคงปลอดภัยของบริการโทรคมนาคมที่สำคัญ ตลอดจนแนวทางด้านความมั่นคงปลอดภัยขั้นสูงที่ควรพิจารณาเพิ่มเติมให้เหมาะสมกับพัฒนาการของเทคโนโลยี ลักษณะของภัยคุกคาม และระดับความเสี่ยงของแต่ละหน่วยงาน ดังนี้

ลำดับ	เรื่อง	ขอบเขตโดยสรุป
๑	ความมั่นคงและความทนทานของระบบและโครงสร้างพื้นฐานโทรคมนาคม	การวิเคราะห์ความล้มเหลวและผลกระทบต่อบริการ (Service Failure and Impact Analysis) การลดจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure) ความซ้ำซ้อน (Redundancy) การแบ่งแยกเครือข่าย (Network Segmentation) การปกป้องส่วนบริหารจัดการ (Management Plane) และการตรวจจับความผิดปกติ (Anomaly Detection)
๒	ความมั่นคงปลอดภัยสำหรับเครือข่าย 5G และเครือข่ายโทรคมนาคมยุคใหม่	สถาปัตยกรรมการให้บริการ (Service-Based Architecture: SBA) การแบ่งเครือข่ายเสมือน (Network Slicing) การจำลองฟังก์ชันเครือข่าย (Network Functions Virtualization: NFV) เครือข่ายที่กำหนดด้วยซอฟต์แวร์ (Software-Defined Networking: SDN) และ

ลำดับ	เรื่อง	ขอบเขตโดยสรุป
		ระบบอัตโนมัติและการประสานการทำงาน (Automation and Orchestration)
๓	ความมั่นคงปลอดภัยสำหรับบริการโทรศัพท์ประจำที่และบริการเสียง	การรักษาความมั่นคงปลอดภัยของระบบส่งสัญญาณ (Signaling Security) การป้องกันการสื่อสารผ่านระบบโทรศัพท์ประจำที่และระบบเสียงผ่านโครงข่ายไอพี (Voice over IP: VoIP) การป้องกันการทุจริตด้านบริการโทรศัพท์ (Telecommunications/Voice Fraud) และความทนทานของบริการเสียง
๔	ความมั่นคงปลอดภัยสำหรับบริการอินเทอร์เน็ตบรอดแบนด์ประจำที่	การรักษาความมั่นคงปลอดภัยของการกำหนดเส้นทาง (Routing Security) การป้องกันการปลอมแปลงที่อยู่ต้นทาง (Anti-Spoofing) การป้องกันการโจมตีแบบปฏิเสธการให้บริการ (DoS/DDoS Protection) การรักษาความมั่นคงปลอดภัยของระบบชื่อโดเมน (DNS Security) และการเฝ้าระวังโครงข่าย
๕	ความมั่นคงปลอดภัยสำหรับบริการโทรคมนาคมระหว่างประเทศและโครงข่ายเคเบิล	การรักษาความมั่นคงปลอดภัยของเกตเวย์ระหว่างประเทศ (International Gateway) สถานีเคเบิลใต้น้ำ (Cable Landing Station) สถานีเชื่อมต่อภาคพื้นดิน (Terrestrial Gateway) ความหลากหลายของผู้ให้บริการและเส้นทาง (Provider and Path Diversity) และความต่อเนื่องของการเชื่อมต่อระหว่างประเทศ
๖	สถาปัตยกรรมแบบไม่เชื่อถือโดยปริยายและการปกป้องส่วนบริหารจัดการ	สถาปัตยกรรมแบบไม่เชื่อถือโดยปริยาย (Zero Trust Architecture) การตรวจสอบอย่างชัดแจ้ง (Verify Explicitly) การให้สิทธิ์เท่าที่จำเป็น (Least Privilege) การตั้งสมมติฐานว่าการละเมิดอาจเกิดขึ้นแล้ว (Assume Breach) การบริหารสิทธิ์ระดับสูง (Privileged Access Management) และการประเมินสถานะความมั่นคงปลอดภัยของอุปกรณ์ (Device Posture Assessment)
๗	ความทนทานต่อแรนซัมแวร์และการสำรองและกู้คืนข้อมูลขั้นสูง	ความทนทานต่อแรนซัมแวร์ (Ransomware Resilience) การปกป้องและแยกสภาพแวดล้อมของข้อมูลสำรอง การสำรองข้อมูลแบบไม่สามารถแก้ไขได้ (Immutable Backup) หรือแบบแยกออกจากระบบ (Offline Backup) การทดสอบการกู้คืน (Recovery Testing) และการกู้คืนจากเหตุการณ์ทางไซเบอร์ (Cyber Recovery)
๘	ความมั่นคงปลอดภัยของห่วงโซ่อุปทานและองค์ประกอบซอฟต์แวร์	การบริหารความเสี่ยงของผู้ผลิตและผู้ให้บริการ (Supplier/Vendor Risk) ข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์ (Software Component Information) ซอฟต์แวร์แบบเปิดเผยรหัสต้นฉบับ (Open-source Software) การบริหารวงจรชีวิต (Lifecycle Management) การบริหารช่องโหว่ และการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย (Security Assurance)
๙	ความมั่นคงปลอดภัยของบริการคลาวด์และบริการภายนอก	การกำหนดความรับผิดชอบร่วมกัน (Shared Responsibility) สถานที่จัดเก็บและประมวลผลข้อมูล (Data and Processing Location) เขตอำนาจทางกฎหมาย (Jurisdiction) การควบคุมกฎแฉเข้ารหัส

ลำดับ	เรื่อง	ขอบเขตโดยสรุป
		(Cryptographic Key Control) ความเสี่ยงจากการกระจุกตัวของกา รพึ่งพา (Concentration Risk) ความสามารถในการเคลื่อนย้ายระบบ และข้อมูล (Portability) และแผนการยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy)
๑๐	ความมั่นคงปลอดภัย ของระบบ ปัญญาประดิษฐ์	การประเมินความเสี่ยงของปัญญาประดิษฐ์ (AI Risk Assessment) การปกป้องข้อมูลและแบบจำลอง (Data and Model Security) การ ป้องกันการชักนำคำสั่งโดยมิชอบ (Prompt Injection) การจำกัดสิทธิ์ ของระบบปัญญาประดิษฐ์ การกำกับดูแลโดยมนุษย์ (Human Oversight) กลไกสำรอง (Fallback) และการทดสอบความมั่นคง ปลอดภัยของระบบปัญญาประดิษฐ์
๑๑	ความคล่องตัวทางการ เข้ารหัสและการเตรียม ความพร้อมต่อ เทคโนโลยีควอนตัม	การจัดทำข้อมูลการใช้เทคโนโลยีการเข้ารหัส (Cryptographic Inventory) ความคล่องตัวทางการเข้ารหัส (Cryptographic Agility) การประเมินการพึ่งพากลไกการเข้ารหัส (Cryptographic Dependency) ความเสี่ยงจากเทคโนโลยีควอนตัม และการเตรียม ความพร้อมสำหรับการเข้ารหัสหลังยุคควอนตัม (Post-Quantum Cryptography: PQC)
๑๒	การตรวจจับภัยคุกคาม ขั้นสูง ข่าวกองภัย คุกคาม และการ แลกเปลี่ยนข้อมูล	การตรวจจับความผิดปกติและพฤติกรรม (Behavioral and Anomaly Detection) การตรวจจับภัยคุกคามในระดับเครือข่าย (Network- based Threat Detection) ข่าวกองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI) ข้อมูลบ่งชี้การบุกรุก (Indicators of Compromise: IOC) รูปแบบพฤติกรรมของผู้โจมตี (Tactics, Techniques and Procedures: TTP) การค้นหาภัยคุกคามเชิงรุก (Threat Hunting) และการแลกเปลี่ยนข้อมูลภัยคุกคาม
๑๓	การออกแบบระบบ อย่างมั่นคงปลอดภัย และการให้ความเชื่อมั่น ด้านความมั่นคง ปลอดภัย	ความมั่นคงปลอดภัยโดยการออกแบบ (Secure by Design) ความ มั่นคงปลอดภัยโดยค่าเริ่มต้น (Secure by Default) ขอบเขตความ เชื่อถือ (Trust Boundaries) การทดสอบความมั่นคงปลอดภัย การให้ ความเชื่อมั่นจากบุคคลภายนอก (Independent Security Assurance) รากฐานความเชื่อถือเป็นฮาร์ดแวร์ (Hardware Root of Trust) หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า และการรักษาความ มั่นคงปลอดภัยตลอดวงจรชีวิต (Lifecycle Security)

การนำข้อเสนอแนะเพิ่มเติมไปประยุกต์ใช้

ข้อเสนอแนะเพิ่มเติมทั้ง ๑๓ เรื่องนี้ได้มีระดับความจำเป็นหรือความเหมาะสมเท่ากันสำหรับทุกหน่วยงาน
ทุกระบบ หรือทุกบริการ หน่วยงานควรพิจารณาเลือกนำข้อเสนอแนะที่เกี่ยวข้องไปประยุกต์ใช้ตามลักษณะของ
บริการ เทคโนโลยี ระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ
โดยคำนึงถึงความพร้อมทางเทคโนโลยี ความเป็นไปได้ในการดำเนินงาน และความต่อเนื่องของบริการ ทั้งนี้
หน่วยงานอาจเลือกใช้มาตรการ กลไก หรือเทคโนโลยีอื่นที่ให้ผลลัพธ์ด้านความมั่นคงปลอดภัย (Security
Outcomes) เทียบเท่าหรือสูงกว่าได้ตามความเหมาะสม

๑. ข้อเสนอแนะด้านความมั่นคงและความทนทานของระบบและโครงสร้างพื้นฐานโทรคมนาคม

๑.๑ การวิเคราะห์ความล้มเหลวและผลกระทบต่อบริการ

หน่วยงานควรพิจารณาวิเคราะห์ความล้มเหลวและผลกระทบต่อบริการ (Service Failure and Impact Analysis) สำหรับระบบและโครงสร้างพื้นฐานโทรคมนาคม รวมถึงโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่มีความสำคัญ เพื่อระบุเหตุการณ์หรือสภาวะที่อาจทำให้ระบบไม่สามารถให้บริการได้ตามที่กำหนด และประเมินผลกระทบที่อาจเกิดขึ้นต่อความพร้อมใช้งาน (Availability) ความน่าเชื่อถือ (Reliability) ความต่อเนื่องของบริการ (Service Continuity) และคุณภาพการให้บริการ (Quality of Service)

การวิเคราะห์ดังกล่าวควรพิจารณาความสัมพันธ์และการพึ่งพาหาระหว่างระบบ (System and Service Dependencies) รวมถึงความล้มเหลวที่อาจเกิดขึ้นจากระบบเทคโนโลยีสารสนเทศ ระบบโทรคมนาคม ระบบบริหารจัดการเครือข่าย ระบบสนับสนุนการปฏิบัติงาน และโครงสร้างพื้นฐานสนับสนุนที่เกี่ยวข้อง

๑.๒ การลดจุดล้มเหลวเพียงจุดเดียวและการเพิ่มความทนทานของระบบ

สำหรับระบบหรือองค์ประกอบที่มีความสำคัญสูงต่อบริการที่สำคัญ หน่วยงานควรพิจารณาระบบและลดจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure: SPOF) และจัดให้มีกลไกที่เหมาะสมเพื่อรักษาความต่อเนื่องของบริการเมื่อองค์ประกอบหลักเกิดความขัดข้องหรือไม่สามารถใช้งานได้

กลไกดังกล่าวอาจรวมถึงการจัดให้มีระบบหรืออุปกรณ์สำรอง (Redundancy) การสลับไปใช้ระบบสำรอง (Failover) การกระจายเส้นทาง (Path Diversity) การกำหนดเส้นทางใหม่ (Rerouting) หรือการลดระดับการให้บริการอย่างเหมาะสม (Graceful Degradation) เพื่อให้สามารถรักษาบริการที่มีความสำคัญสูงไว้ได้ในระหว่างเกิดเหตุการณ์ผิดปกติ

๑.๓ การแบ่งแยกเครือข่ายและขอบเขตความเชื่อถือ

หน่วยงานควรพิจารณาแบ่งแยกเครือข่าย (Network Segmentation) หรือกำหนดขอบเขตความเชื่อถือ (Trust Boundaries) ระหว่างส่วนของระบบที่มีหน้าที่ ระดับความสำคัญ หรือระดับความเสี่ยงแตกต่างกัน โดยอาจพิจารณาแบ่งแยกระหว่างเครือข่ายหรือส่วนที่เกี่ยวข้องกับการให้บริการแก่ผู้ใช้ (Service/User Plane) ส่วนควบคุมการทำงานของเครือข่าย (Control Plane) และส่วนบริหารจัดการระบบและเครือข่าย (Management Plane) ตามลักษณะสถาปัตยกรรมของระบบ

การเชื่อมต่อระหว่างเครือข่ายหรือขอบเขตดังกล่าวควรได้รับการควบคุมตามหลักสิทธิ์เท่าที่จำเป็น (Least Privilege) และอนุญาตเฉพาะการสื่อสารที่จำเป็นต่อการปฏิบัติงาน โดยพิจารณาใช้มาตรการควบคุมการเข้าถึง การกรองการสื่อสาร และการเฝ้าระวังที่เหมาะสมกับระดับความเสี่ยง

๑.๔ การปกป้องส่วนบริหารจัดการระบบและเครือข่าย

หน่วยงานควรให้ความสำคัญเป็นพิเศษกับการปกป้องส่วนบริหารจัดการระบบและเครือข่าย (Management Plane) เนื่องจากการเข้าถึงส่วนดังกล่าวโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อระบบหรือบริการที่สำคัญ

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาใช้เครือข่ายบริหารจัดการที่แยกจากเครือข่ายทั่วไป (Dedicated or Segregated Management Network) การเข้าถึงผ่านเครื่องกลางที่ได้รับการเสริมความมั่นคงปลอดภัย (Hardened Jump Host/Bastion Host) การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) การจำกัดสิทธิ์ของผู้ดูแลระบบ และการบันทึกกิจกรรมการบริหารจัดการที่มีนัยสำคัญ

๑.๕ ความมั่นคงและความทนทานของโครงสร้างพื้นฐานสนับสนุน

หน่วยงานควรพิจารณาความเสี่ยงจากโครงสร้างพื้นฐานสนับสนุนบริการโทรคมนาคมที่อาจส่งผลกระทบต่อบริการที่สำคัญ เช่น ระบบจ่ายไฟฟ้า ระบบไฟฟ้าสำรอง ระบบทำความเย็น ระบบควบคุมและตรวจวัดสภาพแวดล้อม ระบบป้องกันและระงับอัคคีภัย และระบบสนับสนุนอื่นที่เกี่ยวข้อง

สำหรับโครงสร้างพื้นฐานสนับสนุนที่มีความสำคัญสูง ควรพิจารณาจัดให้มีการเฝ้าระวังสถานะการบำรุงรักษาและทดสอบตามระยะเวลาที่เหมาะสม ตลอดจนความซ้ำซ้อน (Redundancy) หรือแนวทางการทำงานทดแทน เพื่อช่วยลดโอกาสที่ความล้มเหลวของระบบสนับสนุนจะส่งผลกระทบต่อบริการที่สำคัญหยุดชะงัก

๑.๖ การเฝ้าระวังความผิดปกติของระบบและการสื่อสาร

หน่วยงานควรพิจารณาเฝ้าระวังและวิเคราะห์การทำงานของระบบ รวมถึงการสื่อสารระหว่างเครือข่ายหรือขอบเขตความเชื่อถือที่มีความสำคัญ เพื่อสนับสนุนการตรวจจับพฤติกรรมหรือเหตุการณ์ที่เบี่ยงเบนจากสภาวะการทำงานปกติ (Anomalous Behavior)

ในกรณีที่เหมาะสม หน่วยงานอาจกำหนดค่าฐานอ้างอิงของพฤติกรรมปกติ (Behavioral Baseline) เพื่อช่วยตรวจจับเหตุการณ์ เช่น การเชื่อมต่อที่ไม่ได้รับอนุญาต การใช้โปรโตคอลที่ผิดปกติ การเปลี่ยนแปลงรูปแบบการสื่อสาร หรือปริมาณข้อมูลที่เบี่ยงเบนอย่างมีนัยสำคัญ ทั้งนี้ ควรกำหนดกระบวนการตรวจสอบและตอบสนองต่อการแจ้งเตือนตามระดับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ

๒. ข้อเสนอแนะด้านความมั่นคงปลอดภัยสำหรับเครือข่าย 5G และเครือข่ายโทรคมนาคมยุคใหม่

ข้อเสนอแนะในส่วนนี้ใช้สำหรับหน่วยงานที่มีการใช้งานเครือข่าย 5G หรือเทคโนโลยีเครือข่ายโทรคมนาคมยุคใหม่ที่มีลักษณะสถาปัตยกรรมและการทำงานที่เกี่ยวข้อง โดยหน่วยงานควรพิจารณานำข้อเสนอแนะไปประยุกต์ใช้ตามสถาปัตยกรรมของระบบ ระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ

๒.๑ ความมั่นคงปลอดภัยของสถาปัตยกรรมแบบบริการ

สำหรับระบบที่ใช้สถาปัตยกรรมแบบบริการ (Service-Based Architecture: SBA) หรือมีการสื่อสารระหว่างองค์ประกอบของระบบผ่านส่วนต่อประสานโปรแกรมประยุกต์ (Application Programming Interface: API) หน่วยงานควรพิจารณามาตรการด้านความมั่นคงปลอดภัยที่เหมาะสมตลอดวงจรการใช้งานของ API

๒.๑.๑ การพิสูจน์ตัวตนและการกำหนดสิทธิ์

หน่วยงานควรพิจารณาจัดให้มีการพิสูจน์ตัวตน (Authentication) และการกำหนดสิทธิ์ (Authorization) สำหรับการสื่อสารระหว่างฟังก์ชันเครือข่าย (Network Functions) หรือองค์ประกอบของระบบที่เกี่ยวข้อง โดยใช้กลไกที่ได้รับการยอมรับและเหมาะสมกับสถาปัตยกรรมของระบบ

ในกรณีที่มีการใช้มาตรฐาน OAuth 2.0 หรือกลไกในลักษณะเดียวกัน ควรกำหนดขอบเขตสิทธิ์ (Scope) อายุของข้อมูลรับรองหรือโทเคน (Credential/Token Lifetime) และการจัดการข้อมูลรับรองให้เหมาะสมกับระดับความเสี่ยง

๒.๑.๒ การปกป้องการสื่อสาร

การสื่อสารที่มีความสำคัญระหว่างฟังก์ชันเครือข่ายหรือผ่าน API ควรได้รับการปกป้องความลับและความถูกต้องครบถ้วนของข้อมูลระหว่างการรับส่ง (Data in Transit) โดยใช้โปรโตคอลการเข้ารหัสที่มีความมั่นคงปลอดภัยและยังได้รับการสนับสนุน

หน่วยงานควรมีแนวทางในการบริหารใบรับรองดิจิทัล (Digital Certificate) กุญแจเข้ารหัส (Cryptographic Key) และการปรับเปลี่ยนโพรโทคอลหรือชุดการเข้ารหัสเมื่อเทคโนโลยีที่ใช้อยู่ไม่เหมาะสมหรือไม่ปลอดภัยอีกต่อไป

๒.๑.๓ การปกป้อง API

หน่วยงานควรพิจารณาใช้มาตรการปกป้อง API ตามระดับความเสี่ยง เช่น การตรวจสอบคำขอ การจำกัดอัตราการเรียกใช้ (Rate Limiting) การควบคุมสิทธิ์ การตรวจสอบข้อมูลนำเข้า (Input Validation) การบันทึกเหตุการณ์ และการตรวจจับพฤติกรรมการเรียกใช้ที่ผิดปกติ

อาจพิจารณาใช้ API Gateway หรือกลไกที่ให้ความสามารถเทียบเท่า เพื่อบังคับใช้นโยบายด้านความมั่นคงปลอดภัยอย่างสอดคล้องกัน โดยเฉพาะ API ที่มีความสำคัญต่อการควบคุมหรือบริหารจัดการเครือข่าย

๒.๒ ความมั่นคงปลอดภัยของการแบ่งส่วนเครือข่าย

สำหรับเครือข่ายที่ใช้การแบ่งส่วนเครือข่าย (Network Slicing) หน่วยงานควรพิจารณาความเสี่ยงที่เกิดจากการใช้ทรัพยากร โครงสร้างพื้นฐาน หรือองค์ประกอบร่วมกันระหว่าง Network Slices โดยคำนึงถึงความแตกต่างของระดับความสำคัญและข้อกำหนดด้านความมั่นคงปลอดภัยของแต่ละ Slice

๒.๒.๑ การแยกทรัพยากรและขอบเขตความเชื่อถือ

หน่วยงานควรพิจารณากำหนดมาตรการเพื่อรักษาการแยกจากกันของ Network Slices (Slice Isolation) ตามระดับความเสี่ยง โดยครอบคลุมการแยกด้านการสื่อสาร การเข้าถึง ทรัพยากร การบริหารจัดการ และข้อมูลที่เกี่ยวข้อง

ในกรณีที่มีการใช้ทรัพยากรร่วมกัน ควรประเมินความเสี่ยงที่เหตุการณ์หรือการถูกโจมตีใน Slice หนึ่งอาจส่งผลกระทบต่อ Slice อื่น (Cross-Slice Impact) และจัดให้มีมาตรการลดความเสี่ยงที่เหมาะสม

๒.๒.๒ การประเมินความมั่นคงปลอดภัยระหว่าง Network Slices

สำหรับ Network Slices ที่มีความสำคัญสูง หน่วยงานควรพิจารณาประเมินหรือทดสอบประสิทธิภาพของการแบ่งแยก (Isolation Effectiveness) เป็นระยะ และเมื่อมีการเปลี่ยนแปลงสถาปัตยกรรมหรือการกำหนดค่าที่มีนัยสำคัญ

การประเมินอาจรวมถึงการทดสอบเจาะระบบระหว่าง Network Slices (Inter-Slice Penetration Testing) หรือวิธีการประเมินอื่นที่เหมาะสม โดยกำหนดขอบเขต วิธีการ และมาตรการควบคุมความเสี่ยงจากการทดสอบอย่างชัดเจน

๒.๒.๓ การเฝ้าระวัง Network Slices

หน่วยงานควรพิจารณาเฝ้าระวังเหตุการณ์และพฤติกรรมที่ผิดปกติที่อาจส่งผลต่อการแบ่งแยก Network Slices รวมถึงการเข้าถึงข้าม Slice การใช้ทรัพยากรผิดปกติ การเปลี่ยนแปลงการกำหนดค่าที่ไม่ได้รับอนุญาต และเหตุการณ์ที่อาจทำให้ผลกระทบแพร่กระจายจาก Slice หนึ่งไปยัง Slice อื่น

๒.๓ ความมั่นคงปลอดภัยของระบบเครือข่ายเสมือนและเครือข่ายที่ควบคุมด้วยซอฟต์แวร์

สำหรับระบบที่ใช้เทคโนโลยีการจำลองฟังก์ชันเครือข่าย (Network Functions Virtualisation: NFV) เครือข่ายที่ควบคุมด้วยซอฟต์แวร์ (Software-Defined Networking: SDN) ฟังก์ชันเครือข่ายเสมือน (Virtual Network Function: VNF) หรือฟังก์ชันเครือข่ายแบบ Cloud-native (Cloud-native Network Function: CNF) หน่วยงานควรพิจารณาความเสี่ยงจากการรวมศูนย์การควบคุม การใช้โครงสร้างพื้นฐานร่วมกัน และการพึ่งพาซอฟต์แวร์หรือแพลตฟอร์มที่เกี่ยวข้อง

๒.๓.๑ การเสริมความมั่นคงปลอดภัยขององค์ประกอบ

หน่วยงานควรพิจารณาการเสริมความมั่นคงปลอดภัยของระบบ (System Hardening) สำหรับองค์ประกอบที่เกี่ยวข้อง เช่น VNF, CNF, Hypervisor, Container Platform, Orchestration Platform และ SDN Controller ตามลักษณะของสถาปัตยกรรมที่ใช้

ควรปิดหรือจำกัดบริการ ฟังก์ชัน พอร์ต บัญชี และส่วนเชื่อมต่อที่ไม่จำเป็น รวมทั้งบริหารการกำหนดค่าระบบและช่องโหว่ตามแนวทางที่เหมาะสมกับผลิตภัณฑ์และระดับความเสี่ยง

๒.๓.๒ การแบ่งแยก Management Plane

หน่วยงานควรพิจารณาแบ่งแยกส่วนบริหารจัดการ (Management Plane) ออกจากส่วนให้บริการหรือส่วนข้อมูลผู้ใช้ (Service/User Plane) ตามความเหมาะสม และจำกัดการเข้าถึง Management Plane เฉพาะบุคคล อุปกรณ์ ระบบ และช่องทางที่ได้รับอนุญาต

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณามาตรการเพิ่มเติม เช่น การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) การบริหารสิทธิ์ผู้ดูแลระบบ (Privileged Access Management: PAM) และการบันทึกกิจกรรมที่มีสิทธิ์ระดับสูง (Privileged Activity Logging)

๒.๓.๓ การปกป้องระบบควบคุมและระบบ Orchestration

เนื่องจากระบบควบคุมและระบบจัดการทรัพยากรแบบอัตโนมัติอาจมีสิทธิ์ในการเปลี่ยนแปลงองค์ประกอบของเครือข่ายในวงกว้าง หน่วยงานควรพิจารณากำหนดมาตรการปกป้อง SDN Controller, Orchestrator และ Management Platform เป็นระบบที่มีความสำคัญสูงตามระดับผลกระทบที่อาจเกิดขึ้น ควรพิจารณาจำกัดสิทธิ์การบริหารจัดการ ตรวจสอบความถูกต้องของการเปลี่ยนแปลง บันทึกกิจกรรมที่มีนัยสำคัญ และจัดให้มีกลไกการกู้คืนหรือย้อนกลับการเปลี่ยนแปลง (Rollback) ในกรณีที่มีการเปลี่ยนแปลงส่งผลกระทบต่อความมั่นคงปลอดภัยหรือความต่อเนื่องของบริการ

๒.๔ ความมั่นคงปลอดภัยของระบบอัตโนมัติและการจัดการเครือข่าย

ในกรณีที่หน่วยงานใช้ระบบอัตโนมัติ (Automation) หรือระบบจัดการและประสานการทำงาน (Management and Orchestration) เพื่อกำหนดค่า จัดสรรทรัพยากร ปรับเปลี่ยนเส้นทาง หรือดำเนินการอื่นที่อาจส่งผลกระทบต่อบริการที่สำคัญ ควรพิจารณาความเสี่ยงที่เกิดจากความผิดพลาดของระบบอัตโนมัติ การกำหนดค่าที่ไม่ถูกต้อง การใช้สิทธิ์โดยไม่ได้รับอนุญาต หรือการถูกโจมตีผ่านระบบควบคุมดังกล่าว

สำหรับการเปลี่ยนแปลงที่อาจมีผลกระทบสูง ควรพิจารณาจัดให้มีกลไกตรวจสอบก่อนนำไปใช้ (Pre-deployment Validation) การกำหนดขอบเขตการเปลี่ยนแปลง การติดตามผลหลังการเปลี่ยนแปลง และแนวทางย้อนกลับ (Rollback) หรือคืนค่าระบบเมื่อเกิดความผิดปกติ

๒.๕ การประเมินความมั่นคงปลอดภัยสำหรับเทคโนโลยีเครือข่ายใหม่

เมื่อมีการนำเทคโนโลยี สถาปัตยกรรม หรือความสามารถใหม่มาใช้ในเครือข่ายโทรคมนาคม หน่วยงานควรพิจารณาประเมินความเสี่ยงด้านความมั่นคงปลอดภัยก่อนนำไปใช้งานกับระบบหรือบริการที่สำคัญ โดยเฉพาะกรณีที่เทคโนโลยีดังกล่าวทำให้เกิดการเปลี่ยนแปลงต่อ Trust Boundary การบริหารตัวตนและสิทธิ์ การเชื่อมต่อกับบุคคลภายนอก การใช้โครงสร้างพื้นฐานร่วมกัน หรือความสามารถในการควบคุมระบบจากระยะไกล

การประเมินควรคำนึงถึงความสามารถในการเฝ้าระวัง การตอบสนองต่อเหตุการณ์ การกู้คืนระบบ และความพร้อมของผู้ผลิตหรือผู้ให้บริการในการสนับสนุนด้านความมั่นคงปลอดภัยตลอดอายุการใช้งานของเทคโนโลยีนั้น

๓. ข้อเสนอแนะด้านความมั่นคงปลอดภัยสำหรับบริการโทรศัพท์ประจำที่และบริการเสียง

ข้อเสนอแนะในส่วนนี้ใช้สำหรับระบบและโครงข่ายที่เกี่ยวข้องกับบริการโทรศัพท์ประจำที่และบริการเสียง รวมถึงระบบโทรศัพท์แบบดั้งเดิม ระบบโทรศัพท์บนเครือข่ายไอพี (Voice over Internet Protocol: VoIP) ระบบสัญญาณ (Signaling System) และระบบสนับสนุนที่เกี่ยวข้อง โดยหน่วยงานควรพิจารณานำข้อเสนอแนะไปประยุกต์ใช้ตามเทคโนโลยีที่ใช้กัน ระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ

๓.๑ การปกป้องระบบสัญญาณ

ระบบสัญญาณ (Signaling System) เป็นองค์ประกอบสำคัญต่อการควบคุมและให้บริการโทรคมนาคม การถูกเข้าถึง ใช้งาน หรือเปลี่ยนแปลงโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อความลับของข้อมูล ความถูกต้องของการให้บริการ การฉ้อโกง หรือความพร้อมใช้งานของบริการ

หน่วยงานจึงควรพิจารณามาตรการปกป้องระบบสัญญาณให้เหมาะสมกับเทคโนโลยีและสถาปัตยกรรมที่ใช้กัน

๓.๑.๑ การปกป้องระบบ SS7

สำหรับระบบที่ยังมีการใช้งานระบบสัญญาณหมายเลข ๗ (Signaling System No. 7: SS7) หน่วยงานควรพิจารณาใช้กลไกที่สามารถตรวจสอบ กรอง และตรวจจับข้อความสัญญาณที่ผิดปกติหรือไม่ได้รับอนุญาต เช่น ระบบป้องกันสำหรับ SS7 (SS7 Firewall) หรือกลไกที่ให้ความสามารถด้านความมั่นคงปลอดภัยเทียบเท่า

การกำหนดมาตรการควรพิจารณาความเสี่ยงที่เกี่ยวข้อง เช่น การเข้าถึงข้อมูลสมาชิกโดยไม่ได้รับอนุญาต การติดตามตำแหน่ง การดักจับข้อความ การเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องกับผู้ใช้บริการ และการใช้ระบบสัญญาณเพื่อสนับสนุนการฉ้อโกงหรือการโจมตีระบบโทรคมนาคม

๓.๑.๒ การปกป้องระบบสัญญาณแบบ IP

สำหรับระบบที่ใช้โพรโทคอลสัญญาณบนเครือข่ายไอพี เช่น Session Initiation Protocol (SIP) หน่วยงานควรพิจารณามาตรการสำหรับการพิสูจน์ตัวตน การควบคุมสิทธิ์ การตรวจสอบความถูกต้องของข้อความสัญญาณ การจำกัดการเชื่อมต่อ และการตรวจจบบรูปแบบการใช้งานที่ผิดปกติ

หน่วยงานอาจพิจารณาใช้ตัวควบคุมขอบเขตการสื่อสาร (Session Border Controller: SBC) หรือกลไกที่ให้ความสามารถเทียบเท่า เพื่อสนับสนุนการควบคุมการสื่อสาร การปกป้องระบบสัญญาณ การซ่อนโครงสร้างเครือข่ายภายใน (Topology Hiding) และการลดความเสี่ยงจากการโจมตีที่มุ่งทำให้บริการไม่พร้อมใช้งาน

๓.๒ การปกป้องการสื่อสารของบริการเสียง

สำหรับบริการเสียงที่รับส่งผ่านเครือข่ายไอพี หน่วยงานควรพิจารณาปกป้องทั้งข้อมูลส่วนควบคุมหรือสัญญาณ (Signaling) และข้อมูลเสียงหรือสื่อที่รับส่ง (Media) ตามระดับความเสี่ยงและความเหมาะสมของระบบ

๓.๒.๑ การปกป้องข้อมูลระหว่างการรับส่ง

หน่วยงานควรพิจารณาใช้กลไกการเข้ารหัสที่เหมาะสมเพื่อปกป้องความลับและความถูกต้องครบถ้วนของข้อมูลระหว่างการรับส่ง (Data in Transit) โดยเฉพาะการสื่อสารที่มีความสำคัญหรือมีความเสี่ยงต่อการถูกดักจับหรือเปลี่ยนแปลงข้อมูล

สำหรับระบบ VoIP อาจพิจารณาใช้ Transport Layer Security (TLS) เพื่อป้องกันการรับส่งข้อมูลสัญญาณ และ Secure Real-time Transport Protocol (SRTP) หรือกลไกที่ให้ระดับการป้องกันเทียบเท่าเพื่อปกป้องข้อมูลเสียง ตามความสามารถและข้อจำกัดของระบบที่ใช้กัน

๓.๒.๒ การบริหารกุญแจและข้อมูลรับรอง

ในกรณีที่มีการใช้การเข้ารหัส หน่วยงานควรพิจารณากระบวนการบริหารกุญแจเข้ารหัสและข้อมูลรับรอง (Cryptographic Key and Credential Management) ให้ครอบคลุมวงจรชีวิตที่เกี่ยวข้อง รวมถึงการสร้าง การแจกจ่าย การจัดเก็บ การใช้งาน การเปลี่ยนหรือหมุนเวียน การเพิกถอน และการทำลาย เมื่อหมดความจำเป็น

ควรหลีกเลี่ยงการใช้โปรโตคอล กลไกการเข้ารหัส หรือชุดการเข้ารหัสที่ไม่ปลอดภัยหรือไม่ได้รับการสนับสนุนอีกต่อไป โดยคำนึงถึงความเข้ากันได้และผลกระทบต่อความต่อเนื่องของบริการ

๓.๓ การป้องกันการฉ้อโกงที่เกี่ยวข้องกับบริการโทรศัพท์และบริการเสียง

หน่วยงานควรพิจารณาความเสี่ยงจากการฉ้อโกงที่เกี่ยวข้องกับบริการโทรศัพท์และบริการเสียง (Telecommunications and Voice Fraud) ซึ่งอาจเกิดจากการเข้าถึงบัญชี ระบบ หรือบริการโดยไม่ได้รับอนุญาต การปลอมแปลงข้อมูล การใช้บริการผิดวัตถุประสงค์ หรือการใช้ช่องโหว่ของระบบและกระบวนการให้บริการ

๓.๓.๑ การตรวจจับพฤติกรรมผิดปกติ

หน่วยงานควรพิจารณาใช้ข้อมูลและรูปแบบพฤติกรรมการใช้งานที่เหมาะสมเพื่อสนับสนุนการตรวจจับความผิดปกติ เช่น ปริมาณการโทรที่เพิ่มขึ้นผิดปกติ การโทรไปยังปลายทางที่มีความเสี่ยงสูง การเปลี่ยนแปลงรูปแบบการใช้งานอย่างมีนัยสำคัญ หรือกิจกรรมที่แตกต่างจากพฤติกรรมปกติของบัญชีหรือบริการ

อาจพิจารณาใช้การวิเคราะห์พฤติกรรม (Behavioral Analytics) หรือระบบตรวจจับการฉ้อโกง (Fraud Detection System) ตามความเหมาะสม โดยควรกำหนดเกณฑ์การแจ้งเตือนและกระบวนการตรวจสอบเพื่อช่วยลดผลการแจ้งเตือนที่ผิดพลาด (False Positive)

๓.๓.๒ การตอบสนองต่อเหตุการณ์ที่อาจเป็นการฉ้อโกง

เมื่อพบกิจกรรมที่มีความเสี่ยงสูง หน่วยงานควรพิจารณามาตรการตอบสนองที่เหมาะสม เช่น การขอการยืนยันเพิ่มเติม การจำกัดธุรกรรมหรือการใช้งานบางประเภท การระงับการใช้งานชั่วคราว หรือการส่งต่อเหตุการณ์เพื่อให้ผู้รับผิดชอบตรวจสอบ

ในกรณีที่ใช้กลไกอัตโนมัติเพื่อระงับหรือจำกัดบริการ ควรพิจารณาผลกระทบที่อาจเกิดขึ้นต่อผู้ใช้บริการที่ขบด้วยกฎหมาย และจัดให้มีกระบวนการตรวจสอบหรือคืนสถานะบริการอย่างเหมาะสม

๓.๔ การป้องกันการโจมตีที่มุ่งทำให้บริการเสียงไม่พร้อมใช้งาน

หน่วยงานควรพิจารณาความเสี่ยงจากการโจมตีที่มุ่งทำให้ระบบโทรศัพท์หรือบริการเสียงไม่สามารถให้บริการได้ เช่น การส่งคำขอหรือข้อความสัญญาณในปริมาณสูง การใช้ทรัพยากรของระบบจนเกินขีดความสามารถ หรือการโจมตีต่อองค์ประกอบที่เป็นจุดสำคัญของบริการ

มาตรการที่พิจารณาอาจรวมถึงการจำกัดอัตราการใช้งาน (Rate Limiting) การควบคุมจำนวนการเชื่อมต่อ การกรองทราฟฟิกที่ผิดปกติ การจัดสรรทรัพยากรอย่างเหมาะสม การแบ่งแยกระบบ และการจัดให้มีกลไกสำรองหรือการกระจายภาระการให้บริการ

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาทดสอบความสามารถในการรักษาบริการภายใต้สภาวะที่มีปริมาณการใช้งานสูงหรือเกิดเหตุการณ์ผิดปกติ โดยการทดสอบต้องได้รับการวางแผนและควบคุมเพื่อไม่ให้ส่งผลกระทบต่อบริการจริงโดยไม่เหมาะสม

๓.๕ การเฝ้าระวังและบันทึกเหตุการณ์ที่เกี่ยวข้องกับบริการเสียง

หน่วยงานควรพิจารณาจัดเก็บและวิเคราะห์ข้อมูลเหตุการณ์ที่มีความสำคัญต่อความมั่นคงปลอดภัยของบริการโทรศัพท์และบริการเสียง เช่น เหตุการณ์การพิสูจน์ตัวตน การเข้าถึงระบบ การเปลี่ยนแปลงการกำหนดค่า เหตุการณ์จากระบบสัญญาณ และเหตุการณ์ที่ระบบตรวจจับว่าอาจเกี่ยวข้องกับการโจมตีหรือการฉ้อโกง

ข้อมูลดังกล่าวควรได้รับการปกป้องจากการเข้าถึง การเปลี่ยนแปลง หรือการลบโดยไม่ได้รับอนุญาต และควรสามารถนำมาใช้สนับสนุนการวิเคราะห์เหตุการณ์ การตอบสนองต่อเหตุการณ์ และการตรวจสอบย้อนหลังได้ โดยคำนึงถึงข้อกำหนดทางกฎหมายและการคุ้มครองข้อมูลที่เกี่ยวข้อง

๔. ข้อเสนอแนะด้านความมั่นคงปลอดภัยสำหรับบริการอินเทอร์เน็ตบรอดแบนด์ประจำที่

บริการอินเทอร์เน็ตบรอดแบนด์ประจำที่ (Fixed-line Broadband Internet Services) มีการพึ่งพาโครงสร้างพื้นฐานเครือข่าย ระบบกำหนดเส้นทาง ระบบชื่อโดเมน และการเชื่อมต่อกับเครือข่ายภายนอก ซึ่งความผิดปกติหรือการถูกโจมตีต้องก่อประกอบดังกล่าอาจส่งผลกระทบต่อผู้ใช้บริการเป็นวงกว้าง

หน่วยงานจึงควรพิจารณามาตรการด้านความมั่นคงปลอดภัยที่ครอบคลุมความถูกต้องของการกำหนดเส้นทาง ความพร้อมใช้งานของเครือข่าย การป้องกันการปลอมแปลงข้อมูลต้นทาง และความมั่นคงปลอดภัยของระบบชื่อโดเมน ตามระดับความเสี่ยงและความสำคัญของบริการ

๔.๑ การรักษาความมั่นคงปลอดภัยของการกำหนดเส้นทาง

หน่วยงานควรพิจารณาความเสี่ยงด้านการกำหนดเส้นทาง (Routing Security) ที่อาจส่งผลให้การรับส่งข้อมูลถูกเปลี่ยนเส้นทาง ผิดเส้นทาง หรือไม่สามารรถเข้าถึงปลายทางได้ตามปกติ รวมถึงเหตุการณ์จากการประกาศเส้นทางที่ผิดพลาดหรือไม่ได้รับอนุญาต (Route Leak/Route Hijacking)

๔.๑.๑ แนวปฏิบัติด้าน Routing Security

หน่วยงานควรพิจารณากำหนดและดำเนินการด้าน Routing Security ที่เหมาะสม เช่น การควบคุมการประกาศเส้นทาง การกรองข้อมูล Routing การตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากเครือข่ายอื่น และการเฝ้าระวังการเปลี่ยนแปลงของเส้นทางที่มีนัยสำคัญ

หน่วยงานอาจพิจารณาแนวปฏิบัติที่ได้รับการยอมรับในอุตสาหกรรม เช่น แนวทาง Mutually Agreed Norms for Routing Security (MANRS) หรือแนวปฏิบัติอื่นที่ให้ผลลัพธ์ด้านความมั่นคงปลอดภัยเทียบเท่า เพื่อใช้ประกอบการกำหนดมาตรการที่เหมาะสมกับเครือข่ายของหน่วยงาน

๔.๑.๒ การตรวจสอบความถูกต้องของการประกาศเส้นทาง

หน่วยงานควรพิจารณาใช้กลไกสำหรับเพิ่มความเชื่อมั่นต่อความถูกต้องของการประกาศเส้นทาง เช่น Resource Public Key Infrastructure (RPKI) และการตรวจสอบแหล่งกำเนิดของเส้นทาง (Route Origin Validation: ROV) หรือกลไกอื่นที่ได้รับการยอมรับและให้ผลลัพธ์ด้านความมั่นคงปลอดภัยเทียบเท่า

การนำกลไกดังกล่าวมาใช้ควรคำนึงถึงผลกระทบต่อการให้บริการ การจัดการกรณีข้อมูลไม่ถูกต้องหรือไม่สมบูรณ์ และกระบวนการตอบสนองเมื่อพบการประกาศเส้นทางที่ผิดปกติ

๔.๑.๓ การเฝ้าระวังความผิดปกติของเส้นทาง

หน่วยงานควรพิจารณาเฝ้าระวังเหตุการณ์ด้าน Routing ที่อาจส่งผลกระทบต่อบริการที่สำคัญ เช่น การเปลี่ยนแปลงเส้นทางอย่างผิดปกติ การประกาศ Prefix จากแหล่งที่ไม่คาดหมาย การเปลี่ยนแปลง Reachability อย่างมีนัยสำคัญ หรือเหตุการณ์ที่อาจบ่งชี้ถึง Route Leak หรือ Route Hijacking

เมื่อพบเหตุการณ์ที่มีนัยสำคัญ ควรมีกระบวนการตรวจสอบ ประสานงาน และตอบสนองกับ ผู้ให้บริการหรือเครือข่ายที่เกี่ยวข้องตามความเหมาะสม

๔.๒ การป้องกันการปลอมแปลงหมายเลขที่อยู่อินเทอร์เน็ต

หน่วยงานควรพิจารณามาตรการป้องกันการปลอมแปลงหมายเลขที่อยู่อินเทอร์เน็ตต้นทาง (IP Source Address Spoofing) เพื่อช่วยลดความเสี่ยงที่โครงข่ายของหน่วยงานหรือผู้ใช้บริการจะถูกนำไปใช้เป็น แหล่งกำเนิดหรือส่วนหนึ่งของการโจมตีต่อระบบอื่น

๔.๒.๑ การกรองข้อมูลตามแหล่งกำเนิด

หน่วยงานควรพิจารณาใช้กลไกการกรองข้อมูลตามหมายเลขที่อยู่อินเทอร์เน็ตต้นทาง (Source Address Validation/Filtering) ในตำแหน่งที่เหมาะสมของเครือข่าย โดยพิจารณาตามลักษณะ สถาปัตยกรรม รูปแบบการกำหนดเส้นทาง และผลกระทบต่อบริการ

แนวปฏิบัติ เช่น Best Current Practice 38 (BCP 38) หรือแนวทางที่ให้ผลลัพธ์เทียบเท่า อาจนำมาใช้เป็นข้อมูลประกอบการออกแบบและกำหนดมาตรการดังกล่าว

๔.๒.๒ การป้องกันการใช้โครงข่ายเป็นแหล่งโจมตี

หน่วยงานควรพิจารณากลไกในการตรวจจับหรือจำกัดกิจกรรมที่อาจบ่งชี้ว่าระบบหรือผู้ใช้ ภายในโครงข่ายกำลังถูกใช้เป็นแหล่งกำเนิดของการโจมตี เช่น ปริมาณทราฟฟิกที่ผิดปกติ การใช้หมายเลขที่อยู่ อินเทอร์เน็ตต้นทางที่ไม่สอดคล้องกับเครือข่าย หรือรูปแบบการสื่อสารที่อาจเกี่ยวข้องกับการโจมตีแบบสะท้อน หรือขยายผล (Reflection/Amplification Attack)

๔.๓ การป้องกันและบรรเทาการโจมตีแบบปฏิเสธการให้บริการ

หน่วยงานควรพิจารณาความสามารถในการตรวจจับ ป้องกัน และบรรเทาการโจมตีแบบปฏิเสธการ ให้บริการ (Denial-of-Service: DoS) และการโจมตีแบบปฏิเสธการให้บริการแบบกระจาย (Distributed Denial-of-Service: DDoS) ให้เหมาะสมกับขนาดของเครือข่าย ลักษณะบริการ ระดับความเสี่ยง และ ผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ

๔.๓.๑ ความสามารถในการตรวจจับและบรรเทาการโจมตี

หน่วยงานควรพิจารณาจัดให้มีความสามารถในการตรวจจับและบรรเทาทราฟฟิกที่ผิดปกติใน ตำแหน่งที่เหมาะสม เช่น Core Network, Edge Network หรือจุดเชื่อมต่อกับเครือข่ายภายนอก โดยอาจใช้ กลไกภายในของหน่วยงาน บริการจากผู้ให้บริการภายนอก หรือรูปแบบผสมผสานตามความเหมาะสม

การออกแบบควรคำนึงถึงความสามารถในการรองรับปริมาณการโจมตี ความต่อเนื่องของ บริการ และความเสี่ยงจากการที่มาตรการบรรเทาการโจมตีอาจส่งผลกระทบต่อทราฟฟิกที่ชอบด้วยกฎหมาย

๔.๓.๒ การเตรียมความพร้อมในการตอบสนองต่อ DDoS

หน่วยงานควรพิจารณาจัดทำแนวทางหรือขั้นตอนการตอบสนองต่อเหตุการณ์ DDoS โดย กำหนดบทบาทและช่องทางการประสานงานกับผู้เกี่ยวข้อง เช่น ผู้ให้บริการเชื่อมต่ออินเทอร์เน็ต ผู้ให้บริการ DDoS Mitigation หรือหน่วยงานที่เกี่ยวข้อง

สำหรับบริการที่มีความสำคัญสูง ควรพิจารณาทดสอบความพร้อมของกระบวนการและกลไก การบรรเทาการโจมตีเป็นระยะ โดยการทดสอบต้องได้รับการวางแผนและควบคุมเพื่อมิให้ส่งผลกระทบต่อ บริการจริงโดยไม่เหมาะสม

๔.๔ การรักษาความมั่นคงปลอดภัยของระบบชื่อโดเมน

ระบบชื่อโดเมน (Domain Name System: DNS) เป็นองค์ประกอบสำคัญต่อการให้บริการ อินเทอร์เน็ต ความผิดปกติ การถูกเปลี่ยนแปลงข้อมูล หรือการใช้ DNS เป็นส่วนหนึ่งของการโจมตีอาจส่ง ผลกระทบต่อผู้ใช้บริการและความพร้อมใช้งานของบริการในวงกว้าง

๔.๔.๑ การตรวจสอบความถูกต้องของข้อมูล DNS

สำหรับระบบที่ให้บริการ DNS Resolver หน่วยงานควรพิจารณาการตรวจสอบความถูกต้องของข้อมูลด้วยส่วนขยายด้านความมั่นคงปลอดภัยของระบบชื่อโดเมน (Domain Name System Security Extensions: DNSSEC) ตามความเหมาะสม เพื่อช่วยลดความเสี่ยงจากการปลอมแปลงหรือแก้ไขข้อมูล DNS เช่น DNS Cache Poisoning

ในกรณีที่หน่วยงานบริหารจัดการ Authoritative DNS ที่เกี่ยวข้องกับบริการที่สำคัญ ควรพิจารณาความเหมาะสมในการใช้ DNSSEC และมาตรการปกป้องภัยจากแฮกเกอร์และกระบวนการบริหารจัดการที่เกี่ยวข้อง

๔.๔.๒ การลดความเสี่ยงจาก DNS Amplification

หน่วยงานควรพิจารณากำหนดค่า DNS Server เพื่อลดความเสี่ยงจากการถูกนำไปใช้เป็นส่วนหนึ่งของการโจมตีแบบสะท้อนหรือขยายผล (DNS Reflection/Amplification Attack)

มาตรการอาจรวมถึงการจำกัดการให้บริการ Recursive DNS เฉพาะผู้ใช้หรือเครือข่ายที่ได้รับอนุญาต การจำกัดอัตราการตอบสนอง (Response Rate Limiting: RRL) การลดการตอบสนองที่ไม่จำเป็น และการเฝ้าระวังปริมาณคำขอหรือรูปแบบการใช้งานที่ผิดปกติ

๔.๔.๓ ความทนทานและความพร้อมใช้งานของ DNS

สำหรับ DNS ที่มีความสำคัญต่อบริการ หน่วยงานควรพิจารณาการกระจายองค์ประกอบหรือจุดให้บริการเพื่อลดความเสี่ยงจากจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure) และจัดให้มีการสามารถในการเฝ้าระวังและตอบสนองเมื่อ DNS ไม่สามารถให้บริการได้ตามปกติ

๔.๕ การเฝ้าระวังและประสานงานเหตุการณ์ด้านความมั่นคงปลอดภัยของอินเทอร์เน็ต

หน่วยงานควรพิจารณานำข้อมูลจากระบบที่เกี่ยวข้อง เช่น Routing, DNS, DDoS Protection, Network Security และ Network Management มาวิเคราะห์ร่วมกัน เพื่อสนับสนุนการตรวจจับเหตุการณ์ที่อาจส่งผลกระทบต่อบริการอินเทอร์เน็ตเป็นวงกว้าง

ในกรณีที่เหตุการณ์เกี่ยวข้องกับเครือข่ายหรือผู้ให้บริการหลายฝ่าย หน่วยงานควรมีกระบวนการและช่องทางการประสานงานที่เหมาะสม เพื่อสนับสนุนการแลกเปลี่ยนข้อมูลทางเทคนิค การตรวจสอบสาเหตุ การจำกัดผลกระทบ และการฟื้นคืนบริการ

๕. ข้อเสนอแนะด้านความมั่นคงปลอดภัยสำหรับบริการโทรคมนาคมระหว่างประเทศและโครงข่ายเคเบิล

บริการโทรคมนาคมระหว่างประเทศ รวมถึงโครงข่ายเคเบิลภาคพื้นดินและเคเบิลใต้น้ำ เป็นองค์ประกอบสำคัญในการเชื่อมต่อโครงข่ายโทรคมนาคมของประเทศกับโครงข่ายระหว่างประเทศ ความขัดข้อง การถูกโจมตี หรือความเสียหายต่อองค์ประกอบดังกล่าวอาจส่งผลกระทบต่อความพร้อมใช้งาน ความต่อเนื่อง และคุณภาพของบริการโทรคมนาคมในวงกว้าง

หน่วยงานจึงควรพิจารณาความมั่นคงปลอดภัยทั้งด้านไซเบอร์ ด้านกายภาพ และด้านความทนทานของโครงข่าย โดยคำนึงถึงการพึ่งพาหาระหว่างระบบ เส้นทางการเชื่อมต่อ ผู้ให้บริการภายนอก และโครงสร้างพื้นฐานสนับสนุนที่เกี่ยวข้อง

๕.๑ การรักษาความมั่นคงปลอดภัยทางกายภาพของสถานีและโครงสร้างพื้นฐานที่สำคัญ

สำหรับสถานีเคเบิลใต้น้ำ (Cable Landing Station) สถานีหรือจุดเชื่อมต่อโครงข่ายภาคพื้นดิน (Terrestrial Gateway) และสถานที่ที่มีองค์ประกอบสำคัญต่อบริการโทรคมนาคมระหว่างประเทศ หน่วยงานควรพิจารณากำหนดระดับการควบคุมทางกายภาพให้เหมาะสมกับสำคัญของสถานที่และผลกระทบที่อาจเกิดขึ้นหากระบบถูกเข้าถึง ทำลาย ครอบงำ หรือหยุดชะงัก

๕.๑.๑ การควบคุมการเข้าถึงพื้นที่สำคัญ

หน่วยงานควรพิจารณากำหนดพื้นที่ควบคุมและมาตรการควบคุมการเข้าออกตามระดับความสำคัญของพื้นที่ โดยอาจประกอบด้วยการพิสูจน์ตัวตน การกำหนดสิทธิ์ การบันทึกการเข้าออก การควบคุมผู้มาติดต่อหรือผู้รับจ้าง การตรวจจับการบุกรุก และการเฝ้าระวังพื้นที่ตามความเหมาะสม

สำหรับพื้นที่ที่มีความสำคัญสูง ควรพิจารณาใช้การป้องกันหลายชั้น (Layered Physical Security) เพื่อลดความเสี่ยงจากการเข้าถึงองค์ประกอบสำคัญโดยไม่ได้รับอนุญาต

๕.๑.๒ การปกป้องจุดเชื่อมต่อและเส้นทางทางกายภาพ

หน่วยงานควรพิจารณาความเสี่ยงต่อจุดเชื่อมต่อ สายสัญญาณ ห้องเชื่อมต่อ อุปกรณ์ส่งสัญญาณ และองค์ประกอบทางกายภาพอื่นที่มีความสำคัญ รวมถึงความเสี่ยงจากการตัด การทำลาย การรบกวน การเข้าถึงโดยไม่ได้รับอนุญาต และภัยธรรมชาติ

มาตรการป้องกันควรกำหนดตามลักษณะของสถานที่ ความเป็นไปได้ในการเข้าถึง และผลกระทบต่อบริการหากองค์ประกอบดังกล่าวไม่สามารถใช้งานได้

๕.๒ ความทนทานของโครงข่ายและความหลากหลายของเส้นทาง

หน่วยงานควรพิจารณาความเสี่ยงจากการพึ่งพาผู้ให้บริการ เส้นทาง จุดเชื่อมต่อ หรือองค์ประกอบใดองค์ประกอบหนึ่งมากเกินไป ซึ่งอาจก่อให้เกิดจุดล้มเหลวเพียงจุดเดียว (Single Point of Failure) หรือความล้มเหลวร่วมกัน (Common Cause Failure)

๕.๒.๑ ความหลากหลายของผู้ให้บริการและเส้นทาง

สำหรับบริการที่มีความสำคัญสูง หน่วยงานควรพิจารณาความหลากหลายของผู้ให้บริการและเส้นทางในการเชื่อมต่อ (Provider and Path Diversity) ตามระดับความเสี่ยง เพื่อช่วยลดผลกระทบจากความขัดข้องของผู้ให้บริการ เส้นทาง หรือระบบเชื่อมต่อใดระบบหนึ่ง

การพิจารณาความหลากหลายของเส้นทางไม่ควรพิจารณาเฉพาะเส้นทางในเชิงตรรกะ (Logical Path) แต่ควรพิจารณาความสัมพันธ์ของเส้นทางทางกายภาพ (Physical Path) และโครงสร้างพื้นฐานที่อาจใช้ร่วมกันด้วย เพื่อหลีกเลี่ยงกรณีที่เส้นทางซึ่งดูเหมือนแยกจากกันในทางตรรกะยังคงพึ่งพาโครงสร้างพื้นฐานทางกายภาพเดียวกัน

๕.๒.๒ การทดสอบกลไกการสลับเส้นทางและการกู้คืน

หน่วยงานควรพิจารณาทดสอบกลไกการสลับเส้นทาง (Failover/Rerouting) และกระบวนการกู้คืนบริการเป็นระยะตามระดับความสำคัญของระบบ เพื่อให้มั่นใจว่ากลไกสำรองสามารถทำงานได้เมื่อเส้นทางหลักไม่สามารถให้บริการได้

การทดสอบควรคำนึงถึงผลกระทบต่อบริการจริง และควรมีแผนย้อนกลับ (Rollback Plan) หรือมาตรการรองรับในกรณีที่การทดสอบก่อให้เกิดผลกระทบที่ไม่คาดหมาย

๕.๓ การเฝ้าระวังการเชื่อมต่อระหว่างประเทศ

หน่วยงานควรพิจารณาเฝ้าระวังสถานะและความผิดปกติของการเชื่อมต่อระหว่างประเทศ เพื่อให้สามารถตรวจพบเหตุการณ์ที่อาจส่งผลกระทบต่อความพร้อมใช้งาน ความถูกต้องของเส้นทาง หรือคุณภาพของบริการได้อย่างเหมาะสม

๕.๓.๑ การเฝ้าระวัง Routing และ Reachability

หน่วยงานควรพิจารณาติดตามการเปลี่ยนแปลงของข้อมูล Routing และ Reachability ที่มีนัยสำคัญ โดยเฉพาะเหตุการณ์ที่อาจบ่งชี้ถึงการประกาศเส้นทางผิดปกติ (Route Anomaly) การรั่วไหลของเส้นทาง (Route Leak) หรือการยึดครองเส้นทางโดยไม่ได้รับอนุญาต (Route Hijacking)

ในกรณีที่พบเหตุการณ์ผิดปกติ ควรมีกระบวนการตรวจสอบและช่องทางการประสานงานกับ ผู้ให้บริการหรือเครือข่ายที่เกี่ยวข้อง เพื่อสนับสนุนการจำกัดผลกระทบและการฟื้นคืนบริการ

๕.๓.๒ การเฝ้าระวังความพร้อมใช้งานและคุณภาพการเชื่อมต่อ

หน่วยงานควรพิจารณาติดตามตัวชี้วัดที่เหมาะสมกับบริการ เช่น ความพร้อมใช้งาน (Availability) ความหน่วง (Latency) การสูญหายของข้อมูลระหว่างการรับส่ง (Packet Loss) หรือการเปลี่ยนแปลงของปริมาณการรับส่งข้อมูลที่มีนัยสำคัญ เพื่อสนับสนุนการตรวจพบความผิดปกติและการ วิเคราะห์ผลกระทบต่อบริการ

๕.๔ การปกป้องข้อมูลระหว่างการรับส่ง

หน่วยงานควรพิจารณาความเสี่ยงต่อความลับและความถูกต้องครบถ้วนของข้อมูลที่ได้รับส่งผ่าน โครงข่ายโทรคมนาคมระหว่างประเทศ โดยเฉพาะข้อมูลหรือการเชื่อมต่อที่มีความสำคัญและมีความเสี่ยงต่อ การถูกดักจับ เปลี่ยนแปลง หรือเข้าถึงโดยไม่ได้รับอนุญาต

๕.๔.๑ การเข้ารหัสการเชื่อมต่อที่มีความสำคัญ

หน่วยงานควรพิจารณาใช้การเข้ารหัส (Encryption) สำหรับการเชื่อมต่อที่มีความสำคัญตาม ระดับความเสี่ยงและความเหมาะสมทางเทคนิค โดยอาจดำเนินการในระดับแอปพลิเคชัน ระดับเครือข่าย ระดับลิงก์ (Link Layer) หรือระดับอื่นที่เหมาะสมกับสถาปัตยกรรมของระบบ

สำหรับการเชื่อมต่อระหว่างอุปกรณ์หรือสถานีที่มีความสำคัญ อาจพิจารณาใช้เทคโนโลยี เช่น MAC Security (MACsec) การเข้ารหัสในระดับ Optical Layer หรือกลไกอื่นที่ให้ระดับการป้องกันเทียบเท่า โดยไม่ถือว่าเทคโนโลยีดังกล่าวเป็นข้อกำหนดสำหรับทุกระบบ

๕.๔.๒ การบริหารกุญแจเข้ารหัส

ในกรณีที่ใช้การเข้ารหัส หน่วยงานควรพิจารณาการบริหารกุญแจเข้ารหัส (Cryptographic Key Management) ที่เหมาะสมกับความสำคัญของระบบ โดยครอบคลุมการสร้าง การแจกจ่าย การจัดเก็บ การใช้งาน การเปลี่ยนหรือหมุนเวียน การเพิกถอน และการทำลายกุญแจเมื่อหมดความจำเป็น

๕.๕ ความพร้อมต่อเหตุขัดข้องและความเสียหายของโครงข่ายเคเบิล

หน่วยงานควรพิจารณาจัดเตรียมแนวทางรองรับกรณีที่เส้นทางเคเบิลหรือสถานีที่เกี่ยวข้องไม่สามารถ ให้บริการได้จากเหตุการณ์ทางไซเบอร์ ความขัดข้องทางเทคนิค ภัยธรรมชาติ อุบัติเหตุ หรือความเสียหายทาง กายภาพ

๕.๕.๑ การวิเคราะห์สถานการณ์ความเสียหาย

ควรพิจารณาสถานการณ์ที่อาจส่งผลกระทบต่อบริการ เช่น การขาดของเคเบิล การสูญเสีย เส้นทางหลายเส้นพร้อมกัน ความขัดข้องของ Cable Landing Station หรือ Terrestrial Gateway การ สูญเสียระบบไฟฟ้าหรือระบบทำความเย็น และความขัดข้องของผู้ให้บริการที่มีการพึ่งพาสูง

ผลการวิเคราะห์ควรนำมาใช้ประกอบการกำหนดความต้องการด้านความซ้ำซ้อน เส้นทาง สำรอง การฟื้นคืนบริการ และการประสานงานกับหน่วยงานหรือผู้ให้บริการที่เกี่ยวข้อง

๕.๕.๒ การประสานงานเมื่อเกิดเหตุ

หน่วยงานควรพิจารณาจัดเตรียมข้อมูลการติดต่อ ขั้นตอนการยกระดับเหตุ (Escalation) และ ช่องทางการประสานงานกับผู้ให้บริการเคเบิล ผู้ให้บริการเชื่อมต่อ ผู้ให้บริการโครงสร้างพื้นฐาน และ ผู้เกี่ยวข้องอื่นที่จำเป็นต่อการตอบสนองและฟื้นคืนบริการ

สำหรับเหตุการณ์ที่อาจส่งผลกระทบในวงกว้าง ควรพิจารณากระบวนการแลกเปลี่ยนข้อมูล สถานการณ์และการประสานการดำเนินงานอย่างเหมาะสม โดยคำนึงถึงข้อกำหนดด้านการรายงานเหตุการณ์ที่ ใช้บังคับ

๕.๖ ความทนทานของโครงสร้างพื้นฐานสนับสนุน

สถานีและจุดเชื่อมต่อที่มีความสำคัญต่อบริการโทรคมนาคมระหว่างประเทศควรพิจารณาความพร้อมของระบบสนับสนุน เช่น ระบบจ่ายและสำรองพลังงาน ระบบทำความเย็น ระบบตรวจวัดและควบคุมสภาพแวดล้อม ระบบป้องกันและระงับอัคคีภัย และระบบสื่อสารที่จำเป็นต่อการปฏิบัติงาน

สำหรับองค์ประกอบที่มีความสำคัญสูง ควรพิจารณาความซ้ำซ้อน (Redundancy) ระยะเวลาที่ระบบสำรองสามารถรองรับการทำงาน การเผื่อสำรองสถานะ และการทดสอบระบบสำรองเป็นระยะ เพื่อช่วยลดความเสี่ยงที่ความขัดข้องของระบบสนับสนุนจะทำให้บริการหลักหยุดชะงัก

๖. ข้อเสนอแนะด้านสถาปัตยกรรมแบบไม่เชื่อถือโดยปริยายและการปกป้องส่วนบริหารจัดการ (Zero Trust Architecture and Management Plane Security)

หน่วยงานควรพิจารณาประยุกต์ใช้หลักการสถาปัตยกรรมแบบไม่เชื่อถือโดยปริยาย (Zero Trust Architecture: ZTA) สำหรับระบบและบริการที่มีความสำคัญ โดยเฉพาะระบบที่มีการเข้าถึงจากหลายเครือข่าย มีผู้ให้บริการภายนอก มีการบริหารจัดการจากระยะไกล หรือมีความเสี่ยงจากการใช้สิทธิ์ระดับสูง

การประยุกต์ใช้ควรพิจารณาตามระดับความเสี่ยงและบริบทของหน่วยงาน โดยไม่จำเป็นต้องนำเทคโนโลยีหรือสถาปัตยกรรมรูปแบบเดียวกันมาใช้กับทุกระบบ

๖.๑ การตรวจสอบอย่างชัดเจนก่อนอนุญาตให้เข้าถึง (Verify Explicitly)

หน่วยงานควรพิจารณาตรวจสอบและประเมินเงื่อนไขที่เกี่ยวข้องก่อนอนุญาตให้ผู้ใช้ อุปกรณ์ ระบบ หรือบริการเข้าถึงทรัพยากรที่มีความสำคัญ โดยไม่อาศัยเพียงตำแหน่งของเครือข่ายหรือการอยู่ในเครือข่ายขององค์กรเป็นเหตุให้เกิดความเชื่อถือโดยอัตโนมัติ

การพิจารณาอาจครอบคลุมข้อมูล เช่น

- (ก) ตัวตนและสิทธิ์ของผู้ใช้หรือระบบ
- (ข) สถานะความน่าเชื่อถือของอุปกรณ์ (Device Posture)
- (ค) ตำแหน่งและบริบทของการเชื่อมต่อ
- (ง) ระดับความเสี่ยงของกิจกรรมที่ร้องขอ และ
- (จ) ข้อมูลพฤติกรรมหรือเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

๖.๒ การกำหนดสิทธิ์เท่าที่จำเป็น (Least Privilege)

หน่วยงานควรพิจารณาจำกัดสิทธิ์ในการเข้าถึงระบบ ข้อมูล และฟังก์ชันให้เท่าที่จำเป็นต่อการปฏิบัติงาน โดยเฉพาะบัญชีที่มีสิทธิ์ระดับสูง บัญชีสำหรับผู้ให้บริการภายนอก และบัญชีที่ใช้ในการบริหารจัดการระบบสำคัญ

สำหรับกิจกรรมที่มีความเสี่ยงสูง อาจพิจารณาใช้กลไก เช่น

- การให้สิทธิ์เฉพาะช่วงเวลาที่เป็น (Just-in-Time Access)
- การให้สิทธิ์เฉพาะงานหรือวัตถุประสงค์ (Just-Enough Access)
- การอนุมัติสิทธิ์ก่อนใช้งาน
- การเพิกถอนสิทธิ์โดยอัตโนมัติเมื่อสิ้นสุดระยะเวลาหรือภารกิจ

๖.๓ การออกแบบโดยสมมติว่าการบุกรุกอาจเกิดขึ้นได้ (Assume Breach)

หน่วยงานควรพิจารณาออกแบบระบบและเครือข่ายภายใต้สมมติฐานว่าผู้โจมตีอาจสามารถเข้าถึงบางส่วนของระบบได้ เพื่อจำกัดโอกาสที่การถูกบุกรุกในระบบหนึ่งจะขยายผลไปยังระบบอื่น

มาตรการที่อาจนำมาพิจารณา ได้แก่ การแบ่งแยกเครือข่าย (Network Segmentation) การแบ่งแยกขอบเขตความเชื่อถือ (Trust Boundary) การควบคุมการเคลื่อนที่ภายในเครือข่าย (Lateral Movement) และการเฝ้าระวังพฤติกรรมที่ผิดปกติ

๖.๔ การปกป้องส่วนบริหารจัดการระบบและเครือข่าย

หน่วยงานควรพิจารณากำหนดมาตรการด้านความมั่นคงปลอดภัยที่เข้มงวดสำหรับส่วนบริหารจัดการระบบและเครือข่าย (Management Plane) เนื่องจากการเข้าถึงส่วนดังกล่าวโดยไม่ได้รับอนุญาตอาจส่งผลกระทบต่อระบบหรือบริการที่สำคัญ

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณามาตรการอย่างน้อยดังนี้

(ก) แยก Management Network ออกจากเครือข่ายทั่วไปตามความเหมาะสม

(ข) จำกัดการเข้าถึงเฉพาะบุคคล อุปกรณ์ และช่องทางที่ได้รับอนุญาต

(ค) ใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA)

(ง) พิจารณาใช้ Privileged Access Management (PAM) หรือกลไกที่ให้ผลลัพธ์เทียบเท่า

(จ) บันทึกกิจกรรมการบริหารจัดการที่มีนัยสำคัญ และ

(ฉ) มีช่องทางการเข้าถึงสำรองที่มีความมั่นคงปลอดภัยสำหรับการกู้คืนระบบเมื่อช่องทางหลักไม่สามารถใช้งานได้

๖.๕ การบริหารสิทธิ์ผู้ดูแลระบบและบัญชีที่มีสิทธิ์สูง

บัญชีที่มีสิทธิ์สูงควรได้รับการบริหารจัดการแยกจากบัญชีใช้งานทั่วไปตามความเหมาะสม และควรมีมาตรการลดความเสี่ยงจากการถูกขโมยข้อมูลรับรองหรือการใช้สิทธิ์ในทางที่ไม่เหมาะสม

หน่วยงานอาจพิจารณา:

(ก) แยกบัญชีสำหรับการบริหารระบบออกจากบัญชีใช้งานทั่วไป

(ข) หลีกเลี่ยงการใช้บัญชีที่มีสิทธิ์สูงสำหรับงานประจำทั่วไป

(ค) ใช้ Credential Vault หรือกลไกที่มีความสามารถเทียบเท่า

(ง) จำกัดอายุและระยะเวลาการใช้งานข้อมูลรับรอง

(จ) บันทึกหรือเฝ้าระวังเซสชันที่มีสิทธิ์สูง (Privileged Session Monitoring/Recording) ตามความเหมาะสม และ

(ฉ) ทบทวนสิทธิ์และบัญชีที่มีสิทธิ์สูงเป็นระยะ

๖.๖ การประเมินสถานะความน่าเชื่อถือของอุปกรณ์ (Device Posture Assessment)

สำหรับการเข้าถึงระบบสำคัญ โดยเฉพาะจากระยะไกลหรือจากอุปกรณ์ที่ไม่ได้อยู่ภายใต้การควบคุมโดยตรง หน่วยงานควรพิจารณาประเมินสถานะของอุปกรณ์ก่อนอนุญาตให้เข้าถึงปัจจัยที่อาจนำมาพิจารณา ได้แก่ สถานะการอัปเดตระบบปฏิบัติการและแพตช์ การมีมาตรการป้องกันมัลแวร์ สถานะการเข้ารหัสอุปกรณ์ การกำหนดค่าความมั่นคงปลอดภัย และสถานะของซอฟต์แวร์ที่จำเป็นต่อการป้องกันระบบ

ในกรณีที่อุปกรณ์ไม่เป็นไปตามเงื่อนไขที่กำหนด หน่วยงานอาจพิจารณาจำกัดระดับการเข้าถึง กักแยกอุปกรณ์ (Quarantine) หรือกำหนดขั้นตอนแก้ไขก่อนอนุญาตให้เข้าถึงระบบที่มีความสำคัญ

๖.๗ การเฝ้าระวังและประเมินสิทธิ์อย่างต่อเนื่อง (Continuous Access Evaluation)

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาให้การอนุญาตเข้าถึงมิได้เป็นการตัดสินใจเพียงครั้งเดียว ณ เวลาที่เข้าสู่ระบบ แต่สามารถทบทวนหรือปรับเปลี่ยนสิทธิ์ตามความเสี่ยงหรือบริบทที่เปลี่ยนแปลงระหว่างการใช้งาน

ตัวอย่างเหตุการณ์ที่อาจนำมาประกอบการพิจารณา ได้แก่ การเปลี่ยนแปลงตำแหน่งหรืออุปกรณ์ การตรวจพบพฤติกรรมที่ผิดปกติ การยกระดับความเสี่ยงของบัญชี หรือการตรวจพบเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

๖.๘ การนำ Zero Trust ไปใช้กับผู้ให้บริการภายนอก

ในกรณีที่ผู้ให้บริการภายนอกสามารถเข้าถึงระบบสำคัญ หน่วยงานควรพิจารณาใช้หลักการ Zero Trust เพื่อจำกัดสิทธิ์ ขอบเขต เวลา และช่องทางการเข้าถึงให้เท่าที่จำเป็น

ควรหลีกเลี่ยงการเปิดช่องทาง Remote Access แบบถาวรโดยไม่จำเป็น และควรมีการทบทวนหรือเพิกถอนสิทธิ์เมื่อหมดความจำเป็น รวมทั้งบันทึกกิจกรรมที่มีนัยสำคัญเพื่อให้สามารถตรวจสอบย้อนหลังได้

๗. ข้อเสนอแนะด้านความทนทานต่อแรนซัมแวร์และการสำรองและกู้คืนข้อมูลขั้นสูง (Ransomware Resilience and Advanced Backup and Recovery)

หน่วยงานควรพิจารณาเสริมสร้างความสามารถในการป้องกัน รับมือ และฟื้นคืนระบบจากการโจมตีด้วยแรนซัมแวร์ (Ransomware) และเหตุการณ์ทางไซเบอร์ที่อาจส่งผลให้ข้อมูล ระบบหลัก หรือระบบสำรองถูกเข้ารหัส ถูกทำลาย ถูกเปลี่ยนแปลง หรือไม่สามารถใช้งานได้

การกำหนดมาตรการควรพิจารณาจากระดับความสำคัญของระบบ ผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) วัตถุประสงค์ระยะเวลาในการกู้คืน (Recovery Time Objective: RTO) วัตถุประสงค์จุดกู้คืนข้อมูล (Recovery Point Objective: RPO) และระยะเวลาสูงสุดที่ยอมรับได้ของการหยุดชะงัก (Maximum Tolerable Period of Disruption: MTPD) รวมถึงรูปแบบภัยคุกคามที่เกี่ยวข้อง

๗.๑ การประยุกต์ใช้แนวทางการสำรองข้อมูลแบบ 3-2-1-1-0

สำหรับระบบและข้อมูลที่มีความสำคัญสูง หน่วยงานควรพิจารณาประยุกต์ใช้หลักการสำรองข้อมูลแบบ 3-2-1-1-0 หรือแนวทางอื่นที่ให้ระดับความสามารถในการป้องกันและกู้คืนข้อมูลเทียบเท่า โดยมีแนวคิดประกอบด้วย

- (ก) มีข้อมูลอย่างน้อย ๓ ชุด ซึ่งรวมข้อมูลที่ใช้งานจริงและข้อมูลสำรอง
- (ข) จัดเก็บข้อมูลโดยใช้สื่อหรือรูปแบบการจัดเก็บที่แตกต่างกันอย่างเหมาะสม
- (ค) มีข้อมูลสำรองอย่างน้อย ๑ ชุดที่แยกจากสถานที่หรือสภาพแวดล้อมหลัก
- (ง) มีข้อมูลสำรองอย่างน้อย ๑ ชุดที่เป็นแบบออฟไลน์ (Offline) ไม่สามารถเปลี่ยนแปลงได้ตามช่วงเวลาที่กำหนด (Immutable) หรือได้รับการแยกออกจากระบบหลักด้วยมาตรการที่ให้ระดับการป้องกันเทียบเท่า และ
- (จ) ตรวจสอบและทดสอบข้อมูลสำรองเพื่อลดข้อผิดพลาดที่อาจทำให้ไม่สามารถนำข้อมูลกลับมาใช้ในการกู้คืนได้

การใช้หลักการดังกล่าวควรปรับให้เหมาะสมกับลักษณะระบบ ปริมาณข้อมูล สถาปัตยกรรมการให้บริการ และข้อจำกัดในการดำเนินงานของหน่วยงาน

๗.๒ การปกป้องระบบสำรองจากการโจมตี

หน่วยงานควรพิจารณาออกแบบระบบสำรองโดยคำนึงถึงกรณีที่ผู้โจมตีสามารถเข้าถึงระบบหลักหรือได้รับสิทธิ์ระดับสูงแล้ว และอาจพยายามค้นหา เปลี่ยนแปลง เข้ารหัส หรือลบข้อมูลสำรองเพื่อขัดขวางการกู้คืนระบบ

มาตรการที่อาจนำมาพิจารณา ได้แก่

- (ก) การแยกสิทธิ์ในการบริหารระบบสำรองออกจากสิทธิ์ในการบริหารระบบหลัก
- (ข) การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) สำหรับการบริหารระบบสำรอง
- (ค) การจำกัดการเชื่อมต่อระหว่าง Production Environment และ Backup Environment
- (ง) การใช้ข้อมูลสำรองที่ไม่สามารถเปลี่ยนแปลงได้ตามเวลาที่กำหนด (Immutable Backup)
- (จ) การจัดเก็บข้อมูลสำรองแบบออฟไลน์ (Offline Backup) หรือแยกออกจากระบบหลัก (Isolated Backup) ตามระดับความเสี่ยง และ
- (ฉ) การบันทึกและเฝ้าระวังกิจกรรมที่เกี่ยวข้องกับการลบ เปลี่ยนแปลง หรือบริหารข้อมูลสำรอง

๗.๓ การแยกข้อมูลสำรองและสภาพแวดล้อมการสำรอง

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาลดความเป็นไปได้ที่เหตุการณ์เดียวจะส่งผลกระทบต่อทั้งระบบหลักและข้อมูลสำรองพร้อมกัน โดยพิจารณาการแยกในด้านที่เหมาะสม เช่น เครือข่าย บัญชีผู้ดูแลระบบ ระบบยืนยันตัวตน แพลตฟอร์มจัดเก็บข้อมูล สถานที่ หรือขอบเขตการบริหารจัดการ การแยกดังกล่าวควรพิจารณาถึงความเสี่ยงจากการใช้ข้อมูลรับรอง (Credential) หรือระบบบริหารจัดการร่วมกัน ซึ่งอาจทำให้ผู้โจมตีที่สามารถควบคุม Production Environment สามารถขยายผลไปยัง Backup Environment ได้

๗.๔ การทดสอบความสามารถในการกู้คืน

หน่วยงานควรพิจารณาทดสอบการกู้คืนระบบและข้อมูล (Recovery Testing) เป็นระยะตามระดับความสำคัญและความเสี่ยง โดยไม่ควรจำกัดเพียงการตรวจสอบว่าข้อมูลสำรองถูกสร้างขึ้นสำเร็จ แต่ควรประเมินว่าสามารถนำข้อมูลสำรองมาใช้ฟื้นคืนระบบและบริการได้จริงภายในระยะเวลาที่กำหนด

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาทดสอบการกู้คืนแบบครบวงจร (End-to-End Recovery Testing) ซึ่งอาจครอบคลุม

- (ก) การเรียกคืนข้อมูลจาก Backup Repository
- (ข) การติดตั้งหรือสร้างระบบที่จำเป็นขึ้นใหม่
- (ค) การคืนค่าการกำหนดระบบและการเชื่อมต่อ
- (ง) การตรวจสอบความถูกต้องครบถ้วนของข้อมูลและระบบ
- (จ) การตรวจสอบการทำงานของบริการหลังการกู้คืน และ
- (ฉ) การประเมินว่าสามารถบรรลุ RTO และ RPO ที่กำหนดไว้ได้หรือไม่

๗.๕ การตรวจสอบความน่าเชื่อถือก่อนนำระบบกลับมาให้บริการ

ภายหลังเหตุการณ์ทางไซเบอร์ หน่วยงานควรพิจารณาตรวจสอบความน่าเชื่อถือและความถูกต้องครบถ้วนของระบบและข้อมูลก่อนนำกลับเข้าสู่สภาพแวดล้อมการให้บริการจริง (Production Environment) เพื่อลดความเสี่ยงจากการนำองค์ประกอบที่ถูกบุกรุกกลับเข้าสู่ระบบ

การตรวจสอบอาจครอบคลุมมัลแวร์ กลไกที่ผู้โจมตีใช้เพื่อกดการเข้าถึงระบบ (Persistence Mechanism) บัญชีหรือข้อมูลรับรองที่อาจถูกละเมิด การเปลี่ยนแปลงการกำหนดค่าที่ไม่ได้รับอนุญาต และช่องโหว่ที่เป็นสาเหตุหรือเกี่ยวข้องกับเหตุการณ์

ในกรณีที่ไม่สามารถสร้างความเชื่อมั่นต่อสถานะของระบบเดิมได้อย่างเพียงพอ ควรพิจารณาการสร้างระบบขึ้นใหม่จากแหล่งที่เชื่อถือได้ (Trusted Source) แทนการกู้คืนระบบเดิมโดยตรง

๗.๖ สภาพแวดล้อมสำหรับการกู้คืนที่มีความมั่นคงปลอดภัย

สำหรับระบบที่มีความสำคัญสูง หน่วยงานอาจพิจารณาจัดเตรียมสภาพแวดล้อมสำหรับการกู้คืนที่มีความมั่นคงปลอดภัย (Clean Recovery Environment) หรือความสามารถในการสร้างสภาพแวดล้อมดังกล่าวเมื่อเกิดเหตุ เพื่อใช้ตรวจสอบ กู้คืน และทดสอบระบบก่อนเชื่อมต่อกลับเข้าสู่ Production Environment

สภาพแวดล้อมดังกล่าวควรได้รับการแยกและควบคุมอย่างเหมาะสม เพื่อป้องกันไม่ให้ภัยคุกคามจากระบบที่ถูกบุกรุกแพร่กระจายเข้าสู่ระบบที่กำลังกู้คืน

๗.๗ การกำหนดลำดับความสำคัญในการกู้คืนบริการ

หน่วยงานควรพิจารณากำหนดลำดับความสำคัญในการกู้คืนระบบและบริการ (Recovery Prioritization) โดยอ้างอิงจากผลการวิเคราะห์ผลกระทบทางธุรกิจ ความสัมพันธ์และการพึ่งพาหาระบบ รวมถึงความสำคัญของบริการต่อผู้ใช้บริการและโครงสร้างพื้นฐานที่เกี่ยวข้อง

การกำหนดลำดับการกู้คืนควรคำนึงถึงระบบที่จำเป็นต่อการกู้คืนระบบอื่นด้วย เช่น ระบบพิสูจน์ตัวตน ระบบชื่อโดเมน ระบบบริหารจัดการเครือข่าย ระบบจัดการกฎแฉเข้ารหัส ระบบบันทึกเหตุการณ์ และโครงสร้างพื้นฐานสนับสนุนที่เกี่ยวข้อง

๗.๘ การเตรียมความพร้อมสำหรับการกู้คืนจากเหตุการณ์ทางไซเบอร์

หน่วยงานควรพิจารณาสถานการณ์ที่ระบบปกติซึ่งใช้ในการบริหารจัดการและกู้คืนอาจไม่สามารถเชื่อถือหรือใช้งานได้ภายหลังเหตุการณ์ทางไซเบอร์ และจัดเตรียมข้อมูล เครื่องมือ และช่องทางที่จำเป็นสำหรับการกู้คืนไว้ล่วงหน้าตามความเหมาะสม

ข้อมูลดังกล่าวอาจประกอบด้วยแผนผังระบบและเครือข่าย รายการทรัพย์สิน การกำหนดค่าที่จำเป็น ข้อมูลติดต่อฉุกเฉิน ขั้นตอนการกู้คืน และข้อมูลอื่นที่จำเป็นต่อการนำบริการกลับมาใช้งาน โดยควรจัดเก็บในรูปแบบที่สามารถเข้าถึงได้แม้ระบบหลักไม่สามารถใช้งานได้

๗.๙ การฝึกซ้อมสถานการณ์ Ransomware และ Cyber Recovery

สำหรับระบบหรือบริการที่มีความสำคัญสูง หน่วยงานควรพิจารณาฝึกซ้อมสถานการณ์ที่ Production Environment และระบบสำรองบางส่วนถูกโจมตีพร้อมกัน เพื่อประเมินความสามารถในการตัดสินใจ ประสานงาน กักกันระบบ กู้คืนข้อมูล และนำบริการกลับมาให้บริการอย่างปลอดภัย

การฝึกซ้อมอาจดำเนินการในรูปแบบการฝึกซ้อมบนโต๊ะ (Tabletop Exercise) การทดสอบทางเทคนิค หรือการทดสอบการกู้คืนแบบจำลองตามระดับความเสี่ยงและความเหมาะสม โดยควรนำผลการฝึกซ้อมมาปรับปรุงแผน ขั้นตอน และมาตรการที่เกี่ยวข้อง

๘. ข้อเสนอแนะด้านความมั่นคงปลอดภัยของห่วงโซ่อุปทานและองค์ประกอบซอฟต์แวร์ (Supply Chain and Software Component Security)

หน่วยงานควรพิจารณาการวัดการบริหารความเสี่ยงด้านห่วงโซ่อุปทาน (Supply Chain Risk) สำหรับผลิตภัณฑ์ ระบบ ซอฟต์แวร์ บริการ และผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการที่สำคัญ โดยคำนึงถึงความเสี่ยงตลอดวงจรชีวิต ตั้งแต่การออกแบบ การจัดหา การพัฒนา การติดตั้ง การใช้งาน การบำรุงรักษา การปรับปรุง ไปจนถึงการยกเลิกการใช้งาน

การดำเนินการควรพิจารณาตามระดับความสำคัญของระบบ ระดับการเข้าถึงของผู้ผลิตหรือผู้ให้บริการ การพึ่งพาองค์ประกอบหรือบริการจากภายนอก ความสามารถในการตรวจสอบและแก้ไขช่องโหว่ ตลอดจนผลกระทบที่อาจเกิดขึ้นหากผลิตภัณฑ์หรือบริการดังกล่าวถูกโจมตี มีช่องโหว่ ไม่สามารถให้บริการ หรือไม่ได้รับการสนับสนุนอีกต่อไป

๘.๑ การจำแนกและประเมินความสำคัญของผู้ผลิตและผู้ให้บริการ

หน่วยงานควรพิจารณาจำแนกผู้ผลิต ผู้จำหน่าย ผู้รับจ้าง และผู้ให้บริการภายนอกตามระดับความสำคัญและความเสี่ยง (Supplier/Vendor Criticality) เพื่อกำหนดระดับการประเมิน การควบคุม และการติดตามที่เหมาะสม

การพิจารณาอาจครอบคลุม

- (ก) ความสำคัญของผลิตภัณฑ์หรือบริการต่อบริการที่สำคัญ
- (ข) ระดับการเข้าถึงระบบ ข้อมูล เครือข่าย หรือสถานที่ของหน่วยงาน
- (ค) ระดับสิทธิ์ในการบริหารจัดการหรือเปลี่ยนแปลงระบบ
- (ง) การพึ่งพาผู้ผลิต ผู้ให้บริการ เทคโนโลยี หรือองค์ประกอบจากภายนอก
- (จ) ความสามารถในการเปลี่ยนหรือทดแทนผลิตภัณฑ์หรือผู้ให้บริการ และ
- (ฉ) ผลกระทบที่อาจเกิดขึ้นหากผู้ผลิตหรือผู้ให้บริการถูกโจมตี หยุดให้บริการ หรือไม่สามารถให้การสนับสนุนได้

สำหรับผู้ผลิตหรือผู้ให้บริการที่มีความสำคัญสูง หน่วยงานควรพิจารณาใช้กระบวนการประเมินและติดตามความเสี่ยงที่เหมาะสมกับระดับความสำคัญดังกล่าว

๘.๒ ข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์

สำหรับผลิตภัณฑ์หรือซอฟต์แวร์ที่มีความสำคัญสูง หน่วยงานควรพิจารณาขอหรือจัดให้มีข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์ (Software Components) ในระดับที่เพียงพอต่อการประเมินและบริหารความเสี่ยง โดยคำนึงถึงความสำคัญของระบบ ลักษณะการใช้งาน และความเสี่ยงที่เกี่ยวข้อง

ข้อมูลดังกล่าวอาจครอบคลุมองค์ประกอบจากบุคคลภายนอก (Third-party Components) ซอฟต์แวร์แบบเปิดเผยรหัสต้นฉบับ (Open-source Software) เวอร์ชันที่ใช้งาน สถานะการสนับสนุน และข้อมูลที่จำเป็นต่อการระบุและประเมินผลกระทบจากช่องโหว่ที่เกี่ยวข้อง

การขอข้อมูลควรคำนึงถึงความจำเป็นและระดับความเสี่ยง และไม่ควรกำหนดให้ผู้ผลิตหรือผู้ให้บริการเปิดเผยข้อมูลที่เป็นความลับทางการค้า รายละเอียดทางเทคนิค หรือข้อมูลอื่นเกินกว่าที่จำเป็นต่อการประเมินและบริหารความเสี่ยง

๘.๓ การบริหารข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์

สำหรับระบบที่มีความสำคัญสูงหรือมีการพึ่งพาสองส่วนประกอบซอฟต์แวร์จากหลายแหล่ง หน่วยงานควรพิจารณาจัดให้มี ข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์ (Software Component Information) ในระดับที่เพียงพอต่อการประเมินและบริหารความเสี่ยง เพื่อสนับสนุนการระบุองค์ประกอบ การติดตามช่องโหว่ การประเมินผลกระทบ และการดำเนินการเมื่อมีการเปิดเผยช่องโหว่ใหม่

ข้อมูลดังกล่าวควรสามารถเชื่อมโยงกับผลิตภัณฑ์ ระบบ หรือซอฟต์แวร์ที่เกี่ยวข้องได้อย่างเหมาะสม และอาจครอบคลุมข้อมูลเกี่ยวกับชื่อและประเภทขององค์ประกอบ เวอร์ชัน ผู้ผลิตหรือผู้ดูแลรักษา สถานะการสนับสนุน ตลอดจนข้อมูลอื่นที่จำเป็นต่อการติดตามและประเมินความเสี่ยง ทั้งนี้ ระดับรายละเอียดของข้อมูลควรพิจารณาตามความสำคัญของระบบและระดับความเสี่ยง

หน่วยงานควรพิจารณากำหนดกระบวนการปรับปรุงข้อมูลเมื่อซอฟต์แวร์หรือองค์ประกอบมีการเปลี่ยนแปลง และกำหนดผู้รับผิดชอบในการนำข้อมูลดังกล่าวไปใช้ร่วมกับกระบวนการบริหารช่องโหว่ (Vulnerability Management) และการบริหารความเสี่ยง (Risk Management)

การมีข้อมูลเกี่ยวกับองค์ประกอบซอฟต์แวร์ไม่ควรถือเป็นหลักฐานโดยตัวมันเองว่าผลิตภัณฑ์หรือซอฟต์แวร์มีความมั่นคงปลอดภัย แต่ควรใช้เป็นข้อมูลประกอบการประเมินและบริหารความเสี่ยงร่วมกับมาตรการอื่นที่เกี่ยวข้อง

๘.๔ การบริหารความเสี่ยงจากองค์ประกอบภายนอกและซอฟต์แวร์แบบเปิดเผยรหัสต้นฉบับ

หน่วยงานควรพิจารณาความเสี่ยงจากองค์ประกอบของบุคคลภายนอก (Third-party Components) และซอฟต์แวร์แบบเปิดเผยรหัสต้นฉบับ (Open-source Software) ที่เป็นส่วนหนึ่งของระบบที่มีความสำคัญ โดยเฉพาะองค์ประกอบที่มีสิทธิ์สูง เชื่อมต่อกับเครือข่าย หรือถูกนำไปใช้ร่วมกันในหลายระบบ

ควรพิจารณาความสามารถในการระบุเวอร์ชัน ติดตามช่องโหว่ ประเมินผลกระทบ และปรับปรุงหรือทดแทนองค์ประกอบเมื่อพบความเสี่ยงที่มีนัยสำคัญ

หากองค์ประกอบไม่ได้รับการดูแล ไม่มีการปรับปรุงด้านความมั่นคงปลอดภัย หรือไม่สามารถแก้ไขช่องโหว่ได้ภายในระยะเวลาที่เหมาะสม หน่วยงานควรพิจารณามาตรการลดความเสี่ยง การทดแทนองค์ประกอบ หรือมาตรการควบคุมชดเชย (Compensating Controls) ตามระดับความเสี่ยง

๘.๕ การบริหารวงจรชีวิตและการสิ้นสุดการสนับสนุน

หน่วยงานควรพิจารณาติดตามสถานะวงจรชีวิตของผลิตภัณฑ์ ซอฟต์แวร์ เฟิร์มแวร์ และองค์ประกอบที่มีความสำคัญ รวมถึงการสิ้นสุดการจำหน่าย การสิ้นสุดการสนับสนุน หรือการสิ้นสุดอายุการใช้งานตามที่ผู้ผลิตหรือผู้ให้บริการกำหนด

สำหรับระบบที่กำลังเข้าสู่หรือพ้นระยะการสนับสนุน หน่วยงานควรพิจารณาจัดทำแผนปรับปรุงทดแทน หรือย้ายระบบ (Migration) ตามระดับความเสี่ยงและผลกระทบต่อบริการ

หากยังไม่สามารถทดแทนหรือปรับปรุงระบบได้ ควรพิจารณาประเมินความเสี่ยงเพิ่มเติมและใช้มาตรการควบคุมชดเชย เช่น การจำกัดการเชื่อมต่อ การแบ่งแยกระบบ การลดสิทธิ์การเข้าถึง หรือการเพิ่มการเฝ้าระวังตามความเหมาะสม

๘.๖ ความสามารถในการบริหารและเปิดเผยช่องโหว่

สำหรับผู้ผลิตหรือผู้ให้บริการที่เกี่ยวข้องกับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาความสามารถในการรับแจ้ง ประเมิน แก้ไข และสื่อสารข้อมูลเกี่ยวกับช่องโหว่ของผลิตภัณฑ์หรือบริการ

อาจพิจารณาความสามารถของผู้ผลิตหรือผู้ให้บริการในการจัดเตรียมแพตช์ (Patch) การปรับปรุงด้านความมั่นคงปลอดภัย (Security Update) หรือมาตรการลดความเสี่ยงในกรณีที่ยังไม่สามารถแก้ไขช่องโหว่ได้ รวมถึงการมีช่องทางรับแจ้งช่องโหว่และกระบวนการเปิดเผยช่องโหว่อย่างประสานงาน (Coordinated Vulnerability Disclosure: CVD) ตามความเหมาะสม

๘.๗ ข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดหาและสัญญา

สำหรับผลิตภัณฑ์หรือบริการที่มีความสำคัญสูง หน่วยงานควรพิจารณากำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในการจัดหา สัญญา หรือข้อตกลงที่เกี่ยวข้อง ให้เหมาะสมกับระดับความเสี่ยงและลักษณะของผลิตภัณฑ์หรือบริการ

ข้อกำหนดอาจครอบคลุมการแจ้งช่องโหว่ที่มีนัยสำคัญ การจัดเตรียมแพตช์หรือมาตรการลดความเสี่ยง การแจ้งการสิ้นสุดการสนับสนุน การแจ้งและประสานงานเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย การควบคุมการเข้าถึงระบบของบุคคลภายนอก และความร่วมมือในการตรวจสอบหรือประเมินความมั่นคงปลอดภัยตามความเหมาะสม

ทั้งนี้ ควรกำหนดเฉพาะข้อมูลและหลักฐานที่จำเป็นและเพียงพอต่อการประเมินความเสี่ยงและการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย โดยไม่กำหนดให้ผู้ผลิตหรือผู้ให้บริการเปิดเผยข้อมูลเกินความจำเป็น

๘.๘ การใช้ผลการประเมินหรือหลักฐานการให้ความเชื่อมั่นจากภายนอก

สำหรับผลิตภัณฑ์ ระบบ หรือบริการที่มีความสำคัญสูง หน่วยงานอาจพิจารณาผลการประเมิน การทดสอบ การรับรอง หรือหลักฐานการให้ความเชื่อมั่นจากบุคคลภายนอก (Independent Security Assessment /Assurance) เพื่อใช้เป็นข้อมูลประกอบการประเมินความเสี่ยง

สำหรับผลิตภัณฑ์หรืออุปกรณ์โทรคมนาคม อาจพิจารณากรอบหรือโครงการประเมินด้านความมั่นคงปลอดภัยที่ได้รับการยอมรับในอุตสาหกรรมและเหมาะสมกับประเภทผลิตภัณฑ์ เช่น GSMA Network Equipment Security Assurance Scheme (NESAS) หรือแนวทางอื่นที่ให้ระดับการประเมินหรือการให้ความเชื่อมั่นที่เหมาะสม

ผลการประเมินหรือการรับรองจากภายนอกไม่ควรใช้ทดแทนการประเมินความเสี่ยงของหน่วยงาน เนื่องจากขอบเขต สภาพแวดล้อม การกำหนดค่า และรูปแบบการใช้งานจริงอาจแตกต่างจากขอบเขตที่ได้รับการประเมิน

๘.๙ การบริหารความเสี่ยงจากการพึ่งพาผู้ผลิตหรือผู้ให้บริการ

สำหรับระบบหรือบริการที่มีความสำคัญสูง หน่วยงานควรพิจารณาความเสี่ยงจากการพึ่งพาผู้ผลิต ผู้ให้บริการ เทคโนโลยี แพลตฟอร์ม หรือองค์ประกอบภายนอกที่มีนัยสำคัญ โดยเฉพาะกรณีที่มีการเปลี่ยนหรือทดแทนทำได้ยาก หรืออาจส่งผลกระทบต่อความต่อเนื่องของบริการ

หน่วยงานอาจพิจารณาความสามารถในการเปลี่ยนหรือทดแทนผลิตภัณฑ์หรือผู้ให้บริการ การย้ายระบบ (Migration) การส่งออกข้อมูลและการกำหนดค่า การเข้าถึงเอกสารและข้อมูลที่จำเป็นต่อการบริหารระบบ ตลอดจนมาตรการรองรับกรณีที่ผู้ผลิตหรือผู้ให้บริการหลักไม่สามารถให้การสนับสนุนได้

การบริหารความเสี่ยงดังกล่าว ไม่จำเป็นต้องหมายถึงการใช้ผู้ผลิตหรือผู้ให้บริการหลายรายในทุก ระบบ แต่ควรทำให้หน่วยงานสามารถประเมินการพึ่งพาและมีแนวทางรองรับความเสี่ยงที่เหมาะสม

๘.๑๐ การติดตามความเสี่ยงด้านห่วงโซ่อุปทานตลอดวงจรชีวิต

หน่วยงานควรพิจารณาทบทวนความเสี่ยงด้านห่วงโซ่อุปทานตลอดระยะเวลาที่ผลิตภัณฑ์ ระบบ หรือบริการถูกใช้งาน โดยไม่จำกัดเฉพาะขั้นตอนการจัดหา

การทบทวนอาจพิจารณาข้อมูลเกี่ยวกับช่องโหว่ เหตุการณ์ด้านความมั่นคงปลอดภัย การเปลี่ยนแปลงองค์ประกอบซอฟต์แวร์ การเปลี่ยนแปลงสถานะการสนับสนุน การเปลี่ยนแปลงผู้ผลิตหรือผู้ให้บริการ และข้อมูลภัยคุกคามที่เกี่ยวข้อง

เมื่อพบการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อระดับความเสี่ยงอย่างมีนัยสำคัญ หน่วยงานควรพิจารณาประเมินความเสี่ยงและปรับมาตรการควบคุมให้เหมาะสม

๙. ข้อเสนอแนะด้านความมั่นคงปลอดภัยของบริการคลาวด์และบริการภายนอก (Cloud and External Service Security)

หน่วยงานควรพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยที่เกิดจากการใช้บริการคลาวด์ (Cloud Services) บริการที่มีการประมวลผลหรือจัดเก็บข้อมูลภายนอกหน่วยงาน และบริการจากผู้ให้บริการภายนอกที่มีความสำคัญต่อบริการที่สำคัญ โดยคำนึงถึงรูปแบบการให้บริการ สถาปัตยกรรม ความรับผิดชอบร่วมกันที่ตั้งและเขตอำนาจทางกฎหมายของข้อมูลและระบบ ตลอดจนความสามารถในการเปลี่ยนหรือยุติการใช้บริการ

การประเมินและกำหนดมาตรการควรพิจารณาตามระดับความสำคัญของระบบและข้อมูล ลักษณะการพึ่งพาผู้ให้บริการ ผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ และข้อกำหนดทางกฎหมายหรือข้อกำหนดด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

๙.๑ การกำหนดขอบเขตความรับผิดชอบร่วมกัน (Shared Responsibility)

หน่วยงานควรพิจารณากำหนดขอบเขตความรับผิดชอบระหว่างหน่วยงานกับผู้ให้บริการคลาวด์หรือผู้ให้บริการภายนอกให้ชัดเจน โดยครอบคลุมหน้าที่ด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับระบบและบริการที่ใช้งาน

ประเด็นที่ควรพิจารณาอาจรวมถึง

- (ก) การบริหารตัวตนและสิทธิ์เข้าถึง
- (ข) การกำหนดค่าและเสริมความมั่นคงปลอดภัยของระบบ
- (ค) การบริหารช่องโหว่และการปรับปรุงระบบ
- (ง) การบันทึกและเฝ้าระวังเหตุการณ์
- (จ) การสำรองและกู้คืนข้อมูล
- (ฉ) การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย และ
- (ช) การคืน โอนย้าย ลบ หรือทำลายข้อมูลเมื่อสิ้นสุดการให้บริการ

หน่วยงานควรหลีกเลี่ยงการสมมติว่าความรับผิดชอบด้านความมั่นคงปลอดภัยทั้งหมดถูกโอนไปยังผู้ให้บริการเพียงเพราะมีการใช้บริการคลาวด์หรือบริการจากภายนอก

๙.๒ สถานที่จัดเก็บและประมวลผลข้อมูล

หน่วยงานควรพิจารณาสถานที่จัดเก็บข้อมูล (Data Location) และสถานที่ประมวลผลข้อมูล (Processing Location) สำหรับระบบหรือข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เพื่อประเมินผลกระทบด้านกฎหมาย ความมั่นคงปลอดภัย ความต่อเนื่องของบริการ และความสามารถในการกำกับดูแลข้อมูล

การพิจารณาควรครอบคลุมสถานที่หลัก สถานที่สำรอง สถานที่ที่กู้คืนจากภัยพิบัติ รวมถึงสถานที่ที่ผู้ให้บริการหรือผู้รับช่วงบริการอาจประมวลผลหรือเข้าถึงข้อมูลตามขอบเขตที่เกี่ยวข้อง

๙.๓ เขตอำนาจทางกฎหมายและอธิปไตยข้อมูล

หน่วยงานควรพิจารณาความเสี่ยงจากเขตอำนาจทางกฎหมาย (Jurisdiction) ที่เกี่ยวข้องกับข้อมูลระบบ และผู้ให้บริการ รวมถึงกรณีที่ผู้ให้บริการหรือบริษัทในเครืออยู่ภายใต้กฎหมายของประเทศอื่นซึ่งอาจมีผลต่อการเข้าถึง เปิดเผย หรือโอนข้อมูล

สำหรับข้อมูลหรือระบบที่มีความสำคัญสูง ควรพิจารณาประเด็นอธิปไตยข้อมูล (Data Sovereignty) ร่วมกับลักษณะของข้อมูล การเข้ารหัส การควบคุมกุญแจเข้ารหัส ข้อกำหนดทางกฎหมาย และความสามารถในการควบคุมการเข้าถึงข้อมูล

ทั้งนี้ การพิจารณา Data Sovereignty ไม่จำเป็นต้องหมายถึงการกำหนดให้ข้อมูลทุกประเภทหรือศูนย์ข้อมูลทุกแห่งต้องตั้งอยู่ภายในประเทศไทย เว้นแต่กฎหมายหรือข้อกำหนดที่ใช้บังคับกำหนดไว้เป็นการเฉพาะ

๙.๔ การบริหารกุญแจเข้ารหัสและการควบคุมข้อมูล

สำหรับระบบหรือข้อมูลที่มีความสำคัญสูง หน่วยงานควรพิจารณาว่าใครเป็นผู้ควบคุมกุญแจเข้ารหัส (Cryptographic Key Control) และผู้ใดสามารถเข้าถึง ใช้ เปลี่ยน หรือเพิกถอนกุญแจดังกล่าวได้

อาจพิจารณารูปแบบการบริหารกุญแจ เช่น กุญแจที่ผู้ให้บริการบริหารจัดการ กุญแจที่ลูกค้าบริหารจัดการ (Customer-Managed Keys) หรือกลไกอื่นที่ให้การควบคุมเหมาะสมกับความเสี่ยงและข้อกำหนดของระบบ

การเลือกใช้รูปแบบดังกล่าวควรพิจารณาความสมดุลระหว่างระดับการควบคุม ความซับซ้อนในการบริหารจัดการ ความสามารถในการกู้คืน และผลกระทบต่อความต่อเนื่องของบริการ

๙.๕ การบริหารความเสี่ยงจากการพึ่งพาผู้ให้บริการรายเดียว (Concentration Risk)

หน่วยงานควรพิจารณาความเสี่ยงจากการพึ่งพาผู้ให้บริการคลาวด์ ผู้ให้บริการแพลตฟอร์ม หรือผู้ให้บริการภายนอกรายเดียว โดยเฉพาะกรณีที่บริการจำนวนมากหรือระบบที่มีความสำคัญสูงพึ่งพาผู้ให้บริการเดียวกัน

การประเมินอาจพิจารณา

(ก) จำนวนและความสำคัญของระบบที่พึ่งพาผู้ให้บริการรายเดียว

(ข) ผลกระทบหากผู้ให้บริการเกิดเหตุขัดข้องเป็นเวลานาน

(ค) ความสามารถในการย้ายระบบหรือข้อมูล

(ง) ความพร้อมของทางเลือกหรือบริการทดแทน และ

(จ) การพึ่งพาบริการย่อยหรือผู้รับช่วงบริการของผู้ให้บริการหลัก

การบริหารความเสี่ยงดังกล่าวไม่จำเป็นต้องหมายถึงการใช้ Multi-cloud ในทุกกรณี แต่ควรทำให้หน่วยงานเข้าใจระดับการพึ่งพาและมีแนวทางรองรับที่เหมาะสม

๙.๖ ความสามารถในการเคลื่อนย้ายระบบและข้อมูล (Portability)

หน่วยงานควรพิจารณาความสามารถในการเคลื่อนย้ายข้อมูล การกำหนดค่า และระบบที่สำคัญไปยังสภาพแวดล้อมอื่น หากมีความจำเป็นจากเหตุผลด้านความมั่นคงปลอดภัย ความต่อเนื่องของบริการ การเปลี่ยนแปลงเชิงพาณิชย์ หรือการยุติบริการ

ควรพิจารณารูปแบบข้อมูล การพึ่งพาบริการเฉพาะของผู้ให้บริการ การกำหนดค่าที่จำเป็น เอกสารทางเทคนิค และระยะเวลาที่ต้องใช้ในการย้ายระบบหรือข้อมูล

๙.๗ แผนการยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy)

สำหรับบริการคลาวด์หรือบริการภายนอกที่มีความสำคัญสูง หน่วยงานควรพิจารณาจัดทำแผนการยุติหรือเปลี่ยนผู้ให้บริการ (Exit Strategy) ไว้ล่วงหน้า เพื่อช่วยลดผลกระทบหากไม่สามารถใช้บริการเดิมต่อไปได้

แผนดังกล่าวอาจครอบคลุม

(ก) วิธีการส่งออกและตรวจสอบความครบถ้วนของข้อมูล

(ข) การย้ายระบบและการกำหนดค่า

(ค) การโอนหรือเปลี่ยนแปลงกุญแจเข้ารหัสและข้อมูลรับรอง

(ง) การจัดการสิทธิ์ของผู้ให้บริการเดิม

(จ) การลบหรือทำลายข้อมูลที่เหลืออยู่ในระบบของผู้ให้บริการ และ

(ฉ) การตรวจสอบว่ากระบวนการเปลี่ยนผ่านไม่ส่งผลกระทบต่อความต่อเนื่องของบริการเกินระดับที่ยอมรับได้

๙.๘ การลดความเสี่ยงจากการผูกติดกับผู้ให้บริการ (Vendor Lock-in Risk)

หน่วยงานควรพิจารณาความเสี่ยงจากการใช้เทคโนโลยี รูปแบบข้อมูล ส่วนเชื่อมต่อ หรือบริการที่ทำให้การเปลี่ยนหรือย้ายไปยังผู้ให้บริการรายอื่นทำได้ยากหรือมีต้นทุนสูงอย่างมีนัยสำคัญ

สำหรับระบบที่มีความสำคัญสูง อาจพิจารณาการใช้อนุกรมมาตรฐานเปิด (Open Standards) รูปแบบข้อมูลที่สามารถส่งออกได้ API ที่มีเอกสารรองรับ หรือวิธีการอื่นที่ช่วยรักษาความสามารถในการเคลื่อนย้ายและบริหารระบบโดยไม่พึ่งพาผู้ให้บริการเดิมเกินความจำเป็น

อย่างไรก็ตาม การลด Vendor Lock-in ไม่ควรตีความว่าองค์กรต้องหลีกเลี่ยงการใช้ความสามารถเฉพาะของผู้ให้บริการทั้งหมด แต่ควรประเมินความเสี่ยงและผลกระทบจากการพึ่งพาดังกล่าวอย่างเหมาะสม

๙.๙ การบริหารผู้รับช่วงบริการ (Subcontractor/Subprocessor Risk)

หน่วยงานควรพิจารณาความเสี่ยงจากผู้รับช่วงบริการหรือผู้ให้บริการต่อเนื่องในห่วงโซ่ของผู้ให้บริการหลัก โดยเฉพาะผู้ที่สามารถเข้าถึง ประมวลผล หรือจัดเก็บข้อมูล หรือสนับสนุนระบบที่มีความสำคัญ

อาจพิจารณาความสามารถของผู้ให้บริการหลักในการระบุและกำกับดูแลผู้รับช่วงบริการ การแจ้งเมื่อมีการเปลี่ยนแปลงผู้รับช่วงบริการ และการทำให้ข้อกำหนดด้านความมั่นคงปลอดภัยที่สำคัญถูกส่งต่อไปยังผู้รับช่วงบริการตามความเหมาะสม

๙.๑๐ การเฝ้าระวังและตรวจสอบบริการคลาวด์อย่างต่อเนื่อง

หน่วยงานควรพิจารณาเฝ้าระวังสถานะด้านความมั่นคงปลอดภัยของบริการคลาวด์และบริการภายนอกตลอดระยะเวลาที่ใช้งาน มิใช่จำกัดเฉพาะการประเมินก่อนจัดซื้อหรือเริ่มใช้บริการ

ข้อมูลที่น่านำมาพิจารณา ได้แก่

(ก) เหตุการณ์ด้านความมั่นคงปลอดภัย

(ข) การเปลี่ยนแปลงบริการหรือสถาปัตยกรรมที่มีนัยสำคัญ

(ค) ช่องโหว่หรือประกาศด้านความมั่นคงปลอดภัย

(ง) ผลการประเมินหรือรายงาน Assurance ที่เกี่ยวข้อง

(จ) การเปลี่ยนแปลงสถานที่ประมวลผลข้อมูลหรือผู้รับช่วงบริการ และ

(ฉ) การเปลี่ยนแปลงที่อาจส่งผลกระทบต่อปฏิบัติตามข้อกำหนดของหน่วยงาน

เมื่อพบการเปลี่ยนแปลงที่มีนัยสำคัญ ควรพิจารณาทบทวนความเสี่ยงและมาตรการควบคุมที่เกี่ยวข้อง

๙.๑๑ ความต่อเนื่องและการกู้คืนบริการคลาวด์

หน่วยงานควรพิจารณาความสามารถในการกู้คืนระบบและข้อมูลเมื่อบริการคลาวด์หรือบริการภายนอกเกิดความขัดข้อง โดยไม่ควรอาศัยเพียงสมมติฐานว่าผู้ให้บริการจะสามารถกู้คืนระบบได้ตามความต้องการของหน่วยงานโดยอัตโนมัติ

ควรพิจารณาให้ Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) ของบริการคลาวด์สอดคล้องกับความต้องการของบริการที่สำคัญ รวมทั้งพิจารณาการทดสอบการกู้คืนและความพร้อมของข้อมูลสำรองตามระดับความเสี่ยง

๑๐. ข้อเสนอแนะด้านความมั่นคงปลอดภัยของระบบปัญญาประดิษฐ์ (Artificial Intelligence Security)

หน่วยงานที่นำระบบปัญญาประดิษฐ์ (Artificial Intelligence: AI) มาใช้กับระบบ กระบวนการ หรือบริการที่สำคัญ ควรพิจารณาความเสี่ยงด้านความมั่นคงปลอดภัยที่อาจเกิดขึ้นตลอดวงจรชีวิตของ AI ตั้งแต่การจัดหา การพัฒนา การฝึกหรือปรับแต่ง การทดสอบ การนำไปใช้งาน การเชื่อมต่อกับระบบอื่น การเฝ้าระวัง ไปจนถึงการยกเลิกการใช้งาน

ระดับของมาตรการควรพิจารณาตามวัตถุประสงค์การใช้งาน ระดับความเป็นอิสระในการตัดสินใจ (Autonomy) สิทธิ์ที่ AI สามารถใช้ ผลกระทบที่อาจเกิดขึ้นต่อระบบหรือบริการที่สำคัญ และความสามารถของบุคลากรในการตรวจสอบ แทรกแซง หรือยกเลิกการทำงานของ AI

๑๐.๑ การจำแนกการใช้งาน AI ตามความเสี่ยง

หน่วยงานควรพิจารณาจำแนกการใช้งาน AI ตามระดับความเสี่ยงและผลกระทบ เพื่อกำหนดมาตรการด้านความมั่นคงปลอดภัยที่เหมาะสม โดยอาจพิจารณา

- (ก) ความสำคัญของระบบหรือบริการที่ AI เกี่ยวข้อง
- (ข) ลักษณะข้อมูลที่ AI สามารถเข้าถึงหรือประมวลผล
- (ค) สิทธิ์ของ AI ในการเข้าถึง เปลี่ยนแปลง หรือสั่งการระบบ
- (ง) ระดับความเป็นอิสระของ AI ในการดำเนินการ
- (จ) ความสามารถของบุคลากรในการตรวจสอบหรือยับยั้งผลลัพธ์ และ
- (ฉ) ผลกระทบต่อความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และความต่อเนื่องของบริการ หาก AI ทำงานผิดพลาดหรือถูกโจมตี

AI ที่ใช้เพียงเพื่อสนับสนุนงานทั่วไปควรสามารถกำหนดมาตรการที่แตกต่างจาก AI ที่สามารถสั่งการหรือเปลี่ยนแปลงระบบเครือข่ายและบริการที่สำคัญได้

๑๐.๒ การปกป้องข้อมูลที่ใช้กับ AI

หน่วยงานควรพิจารณาปกป้องข้อมูลที่ใช้ในการพัฒนา ฝึก ปรับแต่ง ทดสอบ และใช้งาน AI ตามระดับความสำคัญและความเสี่ยงของข้อมูล โดยคำนึงถึงความลับ ความถูกต้องครบถ้วน แหล่งที่มา และสิทธิ์ในการเข้าถึงข้อมูล

สำหรับ AI ที่เกี่ยวข้องกับระบบหรือบริการที่สำคัญ ควรพิจารณาความเสี่ยงจากข้อมูลที่ถูกเปลี่ยนแปลงหรือปนเปื้อน (Data Poisoning) ข้อมูลที่ไม่เหมาะสมกับวัตถุประสงค์การใช้งาน และการนำข้อมูลที่มีความอ่อนไหวเข้าสู่ระบบ AI โดยไม่ได้รับอนุญาต

๑๐.๓ การปกป้องแบบจำลองและองค์ประกอบของระบบ AI

หน่วยงานควรพิจารณาปกป้องแบบจำลอง AI (AI Model) การกำหนดค่า คำสั่งระบบ (System Instructions) ข้อมูลรับรอง ส่วนเชื่อมต่อ และองค์ประกอบอื่นที่มีความสำคัญจากการเข้าถึง เปลี่ยนแปลง คัดลอก หรือใช้งานโดยไม่ได้รับอนุญาต

สำหรับแบบจำลองหรือองค์ประกอบที่ได้รับจากบุคคลภายนอก ควรพิจารณาแหล่งที่มา เวอร์ชัน การเปลี่ยนแปลงที่มีนัยสำคัญ สถานะการสนับสนุน และข้อมูลด้านความมั่นคงปลอดภัยที่เพียงพอต่อการประเมินความเสี่ยง

ทั้งนี้ ไม่จำเป็นต้องกำหนดให้ผู้ให้บริการเปิดเผยรายละเอียดภายในของแบบจำลองทั้งหมด หากสามารถให้ข้อมูลเพียงพอต่อการประเมินความเสี่ยง การให้ความเชื่อมั่น และการควบคุมการเปลี่ยนแปลงได้

๑๐.๔ การป้องกันการชักนำหรือควบคุม AI โดยไม่เหมาะสม

สำหรับระบบ AI ที่รับข้อมูลหรือคำสั่งจากผู้ใช้ ระบบภายนอก หรือแหล่งข้อมูลที่ไม่สามารถเชื่อถือได้ทั้งหมด หน่วยงานควรพิจารณาความเสี่ยงจากการชักนำให้ AI ดำเนินการนอกเหนือจากวัตถุประสงค์หรือข้อจำกัดที่กำหนด เช่น Prompt Injection, Indirect Prompt Injection หรือการใช้ข้อมูลที่จัดทำขึ้นเพื่อหลอกล่อมาตรการควบคุม

มาตรการที่พิจารณาอาจครอบคลุมการตรวจสอบข้อมูลนำเข้า การจำกัดสิทธิ์ของ AI การแยกข้อมูล que ที่เชื่อถือได้ออกจากข้อมูลภายนอก การตรวจสอบผลลัพธ์ก่อนนำไปใช้กับระบบสำคัญ และการควบคุมเครื่องมือหรือระบบที่ AI สามารถเรียกใช้งาน

๑๐.๕ การจำกัดสิทธิ์และขอบเขตการดำเนินการของ AI

ระบบ AI ไม่ควรได้รับสิทธิ์ในการเข้าถึงหรือควบคุมระบบเกินกว่าที่จำเป็นต่อวัตถุประสงค์การใช้งาน โดยเฉพาะ AI Agent หรือระบบที่สามารถเรียกใช้เครื่องมือ โปรแกรม ส่วนเชื่อมต่อ หรือคำสั่งเพื่อดำเนินการกับระบบอื่น

หน่วยงานควรพิจารณาหลักสิทธิ์เท่าที่จำเป็น (Least Privilege) การจำกัดขอบเขตการดำเนินการ (Action Scope) และการแยกสิทธิ์ระหว่างการอ่านข้อมูล การเสนอแนะ การเปลี่ยนแปลง และการสั่งการ ระบบจริงสำหรับการดำเนินการที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบหรือบริการที่สำคัญ ควรพิจารณาให้มีการอนุมัติหรือการตรวจสอบโดยบุคลากรก่อนดำเนินการตามระดับความเสี่ยง

๑๐.๖ การกำกับดูแลโดยมนุษย์และความสามารถในการแทรกแซง (Human Oversight and Intervention)

สำหรับ AI ที่สามารถมีผลต่อการกำหนดค่า การควบคุม การรักษาความมั่นคงปลอดภัย หรือความต่อเนื่องของระบบและบริการที่สำคัญ หน่วยงานควรพิจารณาจัดให้มีระดับการกำกับดูแลโดยมนุษย์ (Human Oversight) ที่เหมาะสมกับความเสี่ยง

บุคลากรที่เกี่ยวข้องควรมีข้อมูลเพียงพอที่จะเข้าใจผลลัพธ์หรือการดำเนินการที่สำคัญ และสามารถยืนยัน ปฏิเสธ ระบุ หรือยกเลิกการดำเนินการได้เมื่อจำเป็น

การกำกับดูแลดังกล่าวไม่จำเป็นต้องหมายถึงการอนุมัติโดยมนุษย์สำหรับการดำเนินการ แต่ควรสอดคล้องกับระดับความเสี่ยง ความสามารถของระบบ และผลกระทบที่อาจเกิดขึ้น

๑๐.๗ กลไกสำรองและการกลับไปใช้กระบวนการที่เชื่อถือได้ (Fallback and Override)

สำหรับระบบที่พึ่งพา AI ในการสนับสนุนบริการที่สำคัญ หน่วยงานควรพิจารณาความสามารถในการลดระดับ ระบุ หรือแยก AI ออกจากกระบวนการเมื่อ AI ทำงานผิดปกติ ถูกโจมตี หรือไม่สามารถให้ผลลัพธ์ที่มีความน่าเชื่อถือเพียงพออาจพิจารณากลไกสำรอง (Fallback Mechanism) กระบวนการดำเนินงานแบบไม่พึ่งพา AI การควบคุมโดยบุคลากร หรือวิธีการอื่นที่สามารถรักษาการให้บริการในระดับที่ยอมรับได้

การออกแบบควรหลีกเลี่ยงสถานการณ์ที่ความล้มเหลวของ AI เพียงองค์ประกอบเดียวทำให้ไม่สามารถควบคุมหรือกู้คืนบริการที่สำคัญได้

๑๐.๘ การบันทึกและตรวจสอบการดำเนินการของ AI

สำหรับ AI ที่สามารถดำเนินการหรือมีอิทธิพลต่อระบบที่มีความสำคัญ หน่วยงานควรพิจารณาจัดเก็บข้อมูลที่เพียงพอต่อการตรวจสอบย้อนหลัง โดยคำนึงถึงความเหมาะสมและข้อจำกัดของเทคโนโลยี

ข้อมูลอาจครอบคลุมตัวตนของผู้ใช้หรือระบบที่ร้องขอการดำเนินการ เวอร์ชันของแบบจำลองหรือระบบ AI ข้อมูลหรือคำสั่งที่มีนัยสำคัญ ผลลัพธ์ การเรียกใช้เครื่องมือหรือระบบภายนอก การอนุมัติของบุคลากร และการเปลี่ยนแปลงที่เกิดขึ้นกับระบบ

การบันทึกควรคำนึงถึงการคุ้มครองข้อมูลที่มีความอ่อนไหว และไม่ควรจัดเก็บข้อมูลทั้งหมดโดยไม่มีวัตถุประสงค์หรือความจำเป็นที่ชัดเจน

๑๐.๙ การทดสอบความมั่นคงปลอดภัยของระบบ AI

สำหรับ AI ที่มีความสำคัญสูง หน่วยงานควรพิจารณาทดสอบความมั่นคงปลอดภัยก่อนนำไปใช้งาน และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ โดยพิจารณาสถานการณ์ที่สัมพันธ์กับลักษณะการใช้งานจริง

การทดสอบอาจครอบคลุมการพยายามหลีกเลี่ยงข้อจำกัดของระบบ การจัดการข้อมูลนำเข้า การเข้าถึงข้อมูลหรือเครื่องมือโดยไม่ได้รับอนุญาต การสร้างผลลัพธ์ที่อาจนำไปสู่การดำเนินการที่ไม่ปลอดภัย และความสามารถของมาตรการควบคุมในการจำกัดผลกระทบ

สำหรับระบบที่มีความเสี่ยงสูง อาจพิจารณาการทดสอบเชิงรุก (Adversarial Testing/AI Red Teaming) ตามความเหมาะสม โดยกำหนดขอบเขตและมาตรการควบคุมเพื่อไม่ให้เกิดการทดสอบส่งผลกระทบต่อระบบจริง

๑๐.๑๐ การเฝ้าระวังประสิทธิผลและการเปลี่ยนแปลงของ AI

หน่วยงานควรพิจารณาเฝ้าระวัง AI หลังจากนำไปใช้งาน เพื่อให้สามารถตรวจพบการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยหรือความน่าเชื่อถือของผลลัพธ์

สำหรับระบบที่เกี่ยวข้อง อาจพิจารณาการเปลี่ยนแปลงของข้อมูล (Data Drift) การเปลี่ยนแปลงพฤติกรรมหรือประสิทธิผลของแบบจำลอง (Model/Performance Drift) การเพิ่มขึ้นของผลลัพธ์ที่ผิดปกติ การเปลี่ยนแปลงแหล่งข้อมูล และการเปลี่ยนแปลงแบบจำลองหรือบริการ AI จากผู้ให้บริการภายนอก

เมื่อพบการเปลี่ยนแปลงที่มีนัยสำคัญ ควรพิจารณาทบทวนความเสี่ยง ทดสอบระบบเพิ่มเติม หรือปรับมาตรการควบคุมตามความเหมาะสม

๑๐.๑๑ การใช้บริการ AI จากภายนอก

ในกรณีที่ใช้แบบจำลอง แพลตฟอร์ม หรือบริการ AI จากผู้ให้บริการภายนอก หน่วยงานควรพิจารณาความเสี่ยงด้านข้อมูล การเข้าถึง การเปลี่ยนแปลงบริการ การพึ่งพาผู้ให้บริการ และความสามารถในการตอบสนองต่อเหตุการณ์

ควรมีข้อมูลเพียงพอต่อการประเมินความเสี่ยงและการควบคุมการเปลี่ยนแปลง เช่น ขอบเขตการใช้ข้อมูลของหน่วยงาน สถานที่หรือรูปแบบการประมวลผลตามที่เกี่ยวข้อง การเก็บรักษาข้อมูล การใช้ข้อมูลเพื่อพัฒนาหรือปรับปรุงบริการ การเปลี่ยนแปลงแบบจำลองหรือความสามารถที่มีนัยสำคัญ และมาตรการด้านความมั่นคงปลอดภัยที่เกี่ยวข้อง

ทั้งนี้ ไม่ควรกำหนดให้ผู้ให้บริการเปิดเผยรายละเอียดของแบบจำลอง อัลกอริทึม หรือทรัพย์สินทางปัญญาทั้งหมด หากข้อมูลดังกล่าวไม่จำเป็นต่อการประเมินและบริหารความเสี่ยง

๑๐.๑๒ การบริหารการเปลี่ยนแปลงของระบบ AI

หน่วยงานควรพิจารณาให้การเปลี่ยนแปลงที่มีนัยสำคัญของระบบ AI อยู่ภายใต้กระบวนการบริหารการเปลี่ยนแปลง (Change Management) ตามระดับความเสี่ยง โดยเฉพาะการเปลี่ยนแบบจำลอง เวอร์ชัน แหล่งข้อมูล การเชื่อมต่อ เครื่องมือ สิทธิ์ หรือระดับความเป็นอิสระของระบบ

ก่อนนำการเปลี่ยนแปลงที่มีนัยสำคัญไปใช้กับระบบหรือบริการที่สำคัญ ควรพิจารณาประเมินผลกระทบ ทดสอบมาตรการควบคุม และจัดเตรียมความสามารถในการย้อนกลับ (Rollback) หรือใช้กระบวนการสำรองหากผลการเปลี่ยนแปลงไม่เป็นไปตามที่คาดหวัง

๑๑. ข้อเสนอแนะด้านความคล่องตัวทางการเข้ารหัสและการเตรียมความพร้อมต่อเทคโนโลยีควอนตัม (Cryptographic Agility and Quantum-Readiness)

หน่วยงานควรพิจารณาความเสี่ยงที่เกิดจากการเปลี่ยนแปลงของเทคโนโลยีการเข้ารหัส (Cryptography) รวมถึงความเสี่ยงที่กลไก อัลกอริทึม โพรโทคอล หรือขนาดกุญแจที่ใช้งานอยู่ในปัจจุบันอาจไม่เหมาะสมหรือไม่สามารถให้ระดับการป้องกันที่เพียงพอในอนาคต

สำหรับระบบและข้อมูลที่มีความสำคัญ หน่วยงานควรพิจารณาความสามารถในการระบุเทคโนโลยีการเข้ารหัสที่ใช้งาน ประเมินการพึ่งพา และเปลี่ยนผ่านไปยังกลไกที่เหมาะสมเมื่อมีความจำเป็น โดยคำนึงถึงความต่อเนื่องของบริการ ความเข้ากันได้ของระบบ และความเสี่ยงที่เกี่ยวข้อง

๑๑.๑ การจัดทำข้อมูลเกี่ยวกับการใช้เทคโนโลยีการเข้ารหัส

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาจัดให้มีข้อมูลเกี่ยวกับการใช้เทคโนโลยีการเข้ารหัสในระดับที่เพียงพอต่อการประเมินและบริหารความเสี่ยง

ข้อมูลดังกล่าวอาจครอบคลุม

- (ก) ระบบ บริการ หรือข้อมูลที่มีการใช้การเข้ารหัส
- (ข) วัตถุประสงค์ของการเข้ารหัส เช่น การปกป้องข้อมูลระหว่างการรับส่งหรือข้อมูลที่จัดเก็บ
- (ค) โพรโทคอลและกลไกการเข้ารหัสที่มีนัยสำคัญ
- (ง) ระบบบริหารกุญแจและใบรับรองดิจิทัลที่เกี่ยวข้อง
- (จ) ผลกระทบหรือบริการภายนอกที่มีการพึ่งพากลไกการเข้ารหัส และ
- (ฉ) ข้อจำกัดที่อาจมีผลต่อการเปลี่ยนหรือปรับปรุงเทคโนโลยีการเข้ารหัส

การจัดทำข้อมูลดังกล่าวไม่จำเป็นต้องเป็นทะเบียนแยกต่างหาก หากหน่วยงานสามารถใช้ข้อมูลจาก Asset Inventory, Configuration Management หรือระบบบริหารจัดการอื่นที่มีอยู่เพื่อให้ได้ข้อมูลเพียงพอต่อการบริหารความเสี่ยง

๑๑.๒ ความคล่องตัวทางการเข้ารหัส (Cryptographic Agility)

หน่วยงานควรพิจารณาความสามารถของระบบในการเปลี่ยน ปรับปรุง หรือยกเลิกการใช้กลไกการเข้ารหัสที่ไม่เหมาะสม โดยไม่ก่อให้เกิดผลกระทบต่อบริการที่สำคัญเกินระดับที่ยอมรับได้

สำหรับระบบที่มีวงจรชีวิตยาวหรือมีความสำคัญสูง ควรพิจารณาความสามารถในการเปลี่ยน อัลกอริทึม โพรโทคอล ใบรับรอง กุญแจ หรือองค์ประกอบด้านการเข้ารหัส โดยหลีกเลี่ยงการออกแบบที่ผูกติดกับกลไกการเข้ารหัสเพียงรูปแบบเดียวโดยไม่สามารถเปลี่ยนแปลงได้อย่างเหมาะสม

๑๑.๓ การประเมินการพึ่งพาเทคโนโลยีการเข้ารหัส

หน่วยงานควรพิจารณาความสัมพันธ์และการพึ่งพาระหว่างระบบที่ใช้เทคโนโลยีการเข้ารหัส โดยเฉพาะระบบที่ต้องทำงานร่วมกับอุปกรณ์ ซอฟต์แวร์ ผู้ให้บริการ หรือโครงข่ายภายนอก

การประเมินควรช่วยให้สามารถระบุได้ว่าการเปลี่ยนแปลงกลไกการเข้ารหัสในองค์ประกอบหนึ่ง อาจส่งผลกระทบต่อระบบหรือบริการอื่นอย่างไร รวมถึงข้อจำกัดด้านความเข้ากันได้ (Interoperability) ประสิทธิภาพ และความต่อเนื่องของบริการ

๑๑.๔ การติดตามความเหมาะสมของเทคโนโลยีการเข้ารหัส

หน่วยงานควรพิจารณาติดตามการเปลี่ยนแปลงของมาตรฐาน แนวปฏิบัติ ช่องโหว่ และข้อค้นพบที่อาจมีผลต่อความเหมาะสมของเทคโนโลยีการเข้ารหัสที่ใช้งานอยู่

เมื่อพบว่าอัลกอริทึม โพรโทคอล หรือกลไกที่ใช้งานไม่สามารถให้ระดับการป้องกันที่เหมาะสมอีกต่อไป หน่วยงานควรพิจารณาความเสี่ยง ผลกระทบ และแผนการเปลี่ยนผ่าน (Migration) ตามความสำคัญของระบบและข้อมูล

๑๑.๕ การประเมินความเสี่ยงจากเทคโนโลยีควอนตัม

สำหรับข้อมูลและระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาผลกระทบที่อาจเกิดขึ้นจากความก้าวหน้าของเทคโนโลยีควอนตัมต่อกลไกการเข้ารหัสที่ใช้งาน โดยเฉพาะข้อมูลที่ต้องรักษาความลับเป็นระยะเวลานาน

การประเมินควรพิจารณาระยะเวลาที่ข้อมูลจำเป็นต้องได้รับการปกป้อง อายุการใช้งานของระบบ และระยะเวลาที่ต้องใช้ในการเปลี่ยนหรือปรับปรุงเทคโนโลยีการเข้ารหัส เพื่อช่วยกำหนดลำดับความสำคัญในการเตรียมความพร้อม

๑๑.๖ ความเสี่ยงจากการจัดเก็บข้อมูลเข้ารหัสเพื่อถอดรหัสในอนาคต (Harvest Now, Decrypt Later)

สำหรับข้อมูลที่มีความลับสูงและจำเป็นต้องรักษาความลับเป็นระยะเวลานาน หน่วยงานควรพิจารณาความเสี่ยงที่ผู้ไม่ประสงค์ดีอาจเก็บรวบรวมข้อมูลที่ถูกเข้ารหัสไว้ในปัจจุบัน เพื่อพยายามถอดรหัสในอนาคตเมื่อมีเทคโนโลยีหรือความสามารถที่เพียงพอ

การประเมินความเสี่ยงดังกล่าวควรพิจารณาพร้อมกับอายุความลับของข้อมูล (Confidentiality Lifetime) ลักษณะของข้อมูล ช่องทางการรับส่ง และผลกระทบหากข้อมูลถูกเปิดเผยในอนาคต

ทั้งนี้ ไม่จำเป็นต้องถือว่าข้อมูลทุกประเภทมีความเสี่ยงในระดับเดียวกัน

๑๑.๗ การเตรียมความพร้อมสำหรับการเปลี่ยนผ่านไปสู่กลไกการเข้ารหัสรุ่นใหม่

สำหรับระบบหรือข้อมูลที่ผลการประเมินระบุว่ามีความเสี่ยงในระยะยาว หน่วยงานควรพิจารณาเตรียมความพร้อมสำหรับการเปลี่ยนผ่านไปสู่กลไกการเข้ารหัสรุ่นใหม่ รวมถึงการเข้ารหัสที่ออกแบบให้สามารถรับมือกับภัยคุกคามจากคอมพิวเตอร์ควอนตัม (Post-Quantum Cryptography: PQC) เมื่อมีความเหมาะสม

การเตรียมความพร้อมอาจครอบคลุมการระบุระบบที่ได้รับผลกระทบ การประเมินความสามารถของผลิตภัณฑ์และผู้ให้บริการ การทดสอบความเข้ากันได้และประสิทธิภาพ การวางแผน Migration และการประเมินผลกระทบต่อระบบหรือบริการที่เกี่ยวข้อง

การนำ PQC มาใช้ควรพิจารณาตามความพร้อมของมาตรฐาน เทคโนโลยี ระบบนิเวศ และความเสี่ยงของหน่วยงาน โดยไม่ควรเร่งเปลี่ยนระบบที่มีความสำคัญโดยปราศจากการทดสอบผลกระทบอย่างเหมาะสม

๑๑.๘ การพิจารณารูปแบบการเปลี่ยนผ่าน

ในช่วงการเปลี่ยนผ่าน หน่วยงานอาจพิจารณากลไกหรือสถาปัตยกรรมที่สามารถรองรับเทคโนโลยีการเข้ารหัสเดิมและเทคโนโลยีรุ่นใหม่ร่วมกัน (Hybrid Approach) ในกรณีที่มีความเหมาะสมและได้รับการสนับสนุนจากมาตรฐานหรือเทคโนโลยีที่เกี่ยวข้อง

การเลือกรูปแบบการเปลี่ยนผ่านควรพิจารณาความมั่นคงปลอดภัย ความเข้ากันได้ ประสิทธิภาพ ความซับซ้อนในการบริหารจัดการ และความสามารถในการย้อนกลับหากเกิดปัญหา

ทั้งนี้ ไม่ควรกำหนด Hybrid Approach เป็นรูปแบบบังคับสำหรับทุกระบบ

๑๑.๙ การพิจารณาความพร้อมของผู้ผลิตและผู้ให้บริการ

สำหรับระบบที่มีความสำคัญและมีวงจรชีวิตยาว หน่วยงานควรพิจารณาความสามารถของผู้ผลิตหรือผู้ให้บริการในการสนับสนุนการเปลี่ยนแปลงด้านการเข้ารหัสในอนาคต

ในการจัดหาหรือทบทวนผลิตภัณฑ์ หน่วยงานอาจขอข้อมูลเกี่ยวกับความสามารถในการปรับปรุง โปรโตคอล อัลกอริทึม การบริหารกุญแจหรือใบรับรอง และแนวทางการสนับสนุนการเปลี่ยนผ่านเมื่อกลไกการเข้ารหัสที่ใช้งานไม่เหมาะสมอีกต่อไป

การขอข้อมูลควรมุ่งให้ได้ ข้อมูลเพียงพอต่อการประเมินความเสี่ยงและความสามารถในการเปลี่ยนผ่าน โดยไม่กำหนดให้ผู้ผลิตเปิดเผยรายละเอียดทางเทคนิคหรือทรัพย์สินทางปัญญาเกินความจำเป็น

๑๑.๑๐ การวางแผนและทดสอบการเปลี่ยนผ่าน

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาจัดลำดับความสำคัญและวางแผนการเปลี่ยนผ่านด้านการเข้ารหัสล่วงหน้า โดยเฉพาะระบบที่มีวงจรชีวิตยาว เปลี่ยนแปลงได้ยาก หรือมีการพึ่งพาระบบอื่นจำนวนมาก

ก่อนนำกลไกการเข้ารหัสใหม่ไปใช้กับระบบจริง ควรพิจารณาทดสอบความเข้ากันได้ ประสิทธิภาพ ความสามารถในการบริหารกฎแฉและใบรับรอง ผลกระทบต่อระบบที่เกี่ยวข้อง และความสามารถในการกู้คืนหรือย้อนกลับหากการเปลี่ยนแปลงไม่เป็นไปตามที่คาดหวัง

๑๒. ข้อเสนอแนะด้านการตรวจจับภัยคุกคามขั้นสูง ข่าวกองภัยคุกคาม และการแลกเปลี่ยนข้อมูล (Advanced Threat Detection, Threat Intelligence and Information Sharing)

หน่วยงานควรพิจารณากระดับความสามารถในการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อระบบหรือบริการที่สำคัญ โดยนำข้อมูลจากระบบ เครือข่าย เหตุการณ์ด้านความมั่นคงปลอดภัย และข่าวกองภัยคุกคาม (Threat Intelligence) มาใช้ประกอบการวิเคราะห์ตามระดับความเสี่ยงและความเหมาะสม

การดำเนินการควรมุ่งให้หน่วยงานสามารถตรวจพบพฤติกรรมหรือกิจกรรมที่มีนัยสำคัญได้อย่างเหมาะสม แม้กิจกรรมดังกล่าวอาจไม่ตรงกับรูปแบบหรือข้อมูลบ่งชี้การโจมตีที่ทราบอยู่ก่อนแล้ว และควรสามารถนำข้อมูลที่ตรวจพบไปสนับสนุนการตอบสนองต่อเหตุการณ์ การบริหารความเสี่ยง และการปรับปรุงมาตรการป้องกัน

๑๒.๑ การตรวจจับความผิดปกติและพฤติกรรมที่มีความเสี่ยง

สำหรับระบบหรือเครือข่ายที่มีความสำคัญสูง หน่วยงานควรพิจารณาความสามารถในการตรวจจับพฤติกรรมหรือกิจกรรมที่แตกต่างจากสภาวะปกติ (Behavioral/Anomaly Detection) โดยอาศัยข้อมูลที่เหมาะสมกับลักษณะของระบบ

ข้อมูลที่น่ามาวิเคราะห์ ได้แก่

- (ก) การพิสูจน์ตัวตนและการใช้สิทธิ์
- (ข) การสื่อสารระหว่างระบบและเครือข่าย
- (ค) การเปลี่ยนแปลงการกำหนดค่าที่มีนัยสำคัญ
- (ง) การใช้บัญชีหรือสิทธิ์ระดับสูง
- (จ) การเชื่อมต่อกับระบบหรือปลายทางที่ไม่คาดหวัง และ
- (ฉ) การเปลี่ยนแปลงของปริมาณ รูปแบบ หรือพฤติกรรมการรับส่งข้อมูล

การตรวจจับควรพิจารณาบริบทของระบบและบริการ เพื่อลดการแจ้งเตือนที่ผิดพลาดและช่วยให้สามารถจัดลำดับความสำคัญของเหตุการณ์ได้อย่างเหมาะสม

๑๒.๒ การตรวจจับภัยคุกคามในระดับเครือข่าย

สำหรับเครือข่ายที่มีความสำคัญสูง หน่วยงานอาจพิจารณาความสามารถในการตรวจจับและวิเคราะห์กิจกรรมด้านเครือข่าย (Network-based Threat Detection) เพื่อสนับสนุนการตรวจพบการเชื่อมต่อหรือพฤติกรรมที่อาจไม่สามารถตรวจพบได้จากข้อมูลของระบบปลายทางเพียงอย่างเดียว

การดำเนินการอาจพิจารณาข้อมูลการเชื่อมต่อ รูปแบบกราฟฟิค ข้อมูลจากโปรโตคอล หรือข้อมูลอื่นที่เหมาะสมกับสถาปัตยกรรมและเทคโนโลยีที่ใช้

สำหรับระบบโทรคมนาคม อาจพิจารณาการวิเคราะห์ที่เข้าใจลักษณะของโปรโตคอลหรือการสื่อสารที่เกี่ยวข้อง (Protocol-aware Analysis) ตามความเหมาะสม โดยไม่จำเป็นต้องกำหนดผลิตภัณฑ์หรือเทคโนโลยีเฉพาะ

๑๒.๓ การใช้ข่าวกรองภัยคุกคาม

หน่วยงานควรพิจารณานำข่าวกรองภัยคุกคาม (Cyber Threat Intelligence: CTI) ที่เกี่ยวข้องและเชื่อถือได้มาใช้สนับสนุนการป้องกัน ตรวจสอบ วิเคราะห์ และตอบสนองต่อภัยคุกคาม

ข่าวกรองภัยคุกคามอาจประกอบด้วยข้อมูลเกี่ยวกับผู้คุกคาม รูปแบบและวิธีการโจมตี ช่องโหว่ โครงสร้างพื้นฐานที่เกี่ยวข้องกับการโจมตี หรือข้อมูลบ่งชี้การบุกรุก โดยควรประเมินความเกี่ยวข้อง ความน่าเชื่อถือ ความทันเวลา และบริบทของข้อมูลก่อนนำไปใช้

หน่วยงานไม่ควรถือว่าข้อมูล Threat Intelligence ทุกแหล่งมีความน่าเชื่อถือหรือมีความเกี่ยวข้องในระดับเดียวกัน

๑๒.๔ การใช้ข้อมูลบ่งชี้และพฤติกรรมของผู้โจมตี

หน่วยงานควรพิจารณาใช้ทั้งข้อมูลบ่งชี้การบุกรุก (Indicators of Compromise: IOC) และข้อมูลเกี่ยวกับกลยุทธ์ เทคนิค และกระบวนการของผู้โจมตี (Tactics, Techniques and Procedures: TTP) ตามความเหมาะสม

IOC สามารถช่วยสนับสนุนการตรวจจับเหตุการณ์ที่มีข้อมูลบ่งชี้ที่ทราบอยู่แล้ว ขณะที่การวิเคราะห์ TTP และพฤติกรรมสามารถช่วยเพิ่มความสามารถในการตรวจจับกิจกรรมที่อาจมีการเปลี่ยนแปลงรายละเอียดทางเทคนิคเพื่อหลีกเลี่ยงการตรวจจับ

หน่วยงานควรพิจารณานำข้อมูลดังกล่าวไปใช้ในการปรับปรุงกฎการตรวจจับ กรณีการใช้งานด้านการเฝ้าระวัง (Detection Use Cases) และกระบวนการตอบสนองต่อเหตุการณ์ตามความเหมาะสม

๑๒.๕ การค้นหาภัยคุกคามเชิงรุก (Threat Hunting)

สำหรับระบบหรือบริการที่มีความสำคัญสูง หน่วยงานอาจพิจารณาดำเนินการค้นหาภัยคุกคามเชิงรุก (Threat Hunting) เพื่อค้นหาหลักฐานหรือพฤติกรรมที่อาจบ่งชี้ถึงการบุกรุกซึ่งยังไม่ได้รับการตรวจพบจากกลไกการแจ้งเตือนตามปกติ

การดำเนินการควรอาศัยสมมติฐานหรือข้อมูลที่มีเหตุผลรองรับ เช่น ข่าวกรองภัยคุกคาม เหตุการณ์ที่เคยเกิดขึ้น ช่องโหว่ที่มีความสำคัญ หรือ TTP ที่เกี่ยวข้องกับระบบและเทคโนโลยีของหน่วยงาน

ผลจาก Threat Hunting ควรถูกนำมาใช้เพื่อปรับปรุงความสามารถในการตรวจจับ การตอบสนอง และมาตรการป้องกันที่เกี่ยวข้อง

๑๒.๖ การเชื่อมโยงข้อมูลจากหลายแหล่ง

หน่วยงานควรพิจารณาความสามารถในการนำข้อมูลจากแหล่งต่าง ๆ มาวิเคราะห์ร่วมกัน เพื่อเพิ่มบริบทและลดข้อจำกัดจากการพิจารณาเหตุการณ์แต่ละรายการแยกจากกัน

ข้อมูลอาจมาจากระบบบริหารเหตุการณ์และข้อมูลด้านความมั่นคงปลอดภัย (Security Information and Event Management: SIEM) ระบบเครือข่าย ระบบปลายทาง ระบบบริหารตัวตน ระบบคลาวด์ ระบบโทรคมนาคม หรือแหล่งข้อมูลภัยคุกคามภายนอก

ทั้งนี้ ไม่จำเป็นต้องกำหนดให้ข้อมูลทั้งหมดถูกรวบรวมไว้ในแพลตฟอร์มเดียว หากหน่วยงานสามารถเชื่อมโยงและใช้ข้อมูลที่เป็นต่อการตรวจจับและวิเคราะห์เหตุการณ์ได้อย่างมีประสิทธิภาพ

๑๒.๗ การแลกเปลี่ยนข้อมูลภัยคุกคาม

หน่วยงานควรพิจารณาแลกเปลี่ยนข้อมูลภัยคุกคามและข้อมูลเหตุการณ์ด้านความมั่นคงปลอดภัยกับหน่วยงานหรือกลุ่มที่เกี่ยวข้อง เมื่อการแลกเปลี่ยนดังกล่าวสามารถช่วยลดความเสี่ยงหรือสนับสนุนการป้องกันและตอบสนองต่อภัยคุกคามได้

ข้อมูลที่แลกเปลี่ยนควรมีขอบเขตที่เหมาะสม ถูกต้องเพียงพอต่อวัตถุประสงค์ และคำนึงถึงข้อจำกัดด้านกฎหมาย การรักษาความลับ การคุ้มครองข้อมูล และความอ่อนไหวของข้อมูลด้านความมั่นคงปลอดภัย

ก่อนแลกเปลี่ยนข้อมูล หน่วยงานควรพิจารณาการจำแนกข้อมูล การลดหรือปกปิดข้อมูลที่ไม่จำเป็น และข้อจำกัดในการนำข้อมูลไปใช้หรือเปิดเผยต่อ

๑๒.๘ รูปแบบและกลไกสำหรับการแลกเปลี่ยนข้อมูล

ในกรณีที่มีการแลกเปลี่ยนข้อมูลภัยคุกคามระหว่างระบบหรือระหว่างหน่วยงานเป็นประจำ อาจพิจารณาใช้รูปแบบข้อมูลและกลไกที่สามารถสนับสนุนการแลกเปลี่ยนข้อมูลอย่างมีโครงสร้างและสามารถทำงานร่วมกันได้ (Interoperability)

มาตรฐานหรือกลไก เช่น Structured Threat Information Expression (STIX) และ Trusted Automated Exchange of Intelligence Information (TAXII) อาจนำมาใช้ตามความเหมาะสม หรืออาจใช้รูปแบบอื่นที่สามารถสนับสนุนวัตถุประสงค์ในการแลกเปลี่ยนข้อมูลได้อย่างมีประสิทธิภาพ

ทั้งนี้ ไม่ควรกำหนด STIX/TAXII เป็นรูปแบบบังคับสำหรับการแลกเปลี่ยนข้อมูลทุกกรณี

๑๒.๙ การตรวจสอบและยืนยันข้อมูลก่อนนำไปใช้

ก่อนนำข้อมูลภัยคุกคามจากภายนอกไปใช้เพื่อบล็อก จำกัดการเข้าถึง หรือดำเนินมาตรการที่อาจส่งผลกระทบต่อบริการ หน่วยงานควรพิจารณาความน่าเชื่อถือ แหล่งที่มา ความทันเวลา และบริบทของข้อมูล

สำหรับการดำเนินการที่อาจส่งผลกระทบต่อบริการที่สำคัญหรือผู้ใช้บริการจำนวนมาก ควรพิจารณามาตรการป้องกันการดำเนินการจากข้อมูลที่ผิดพลาดหรือหมกมุ่น รวมถึงความสามารถในการตรวจสอบและย้อนกลับการดำเนินการเมื่อจำเป็น

๑๒.๑๐ การใช้ระบบอัตโนมัติในการตรวจจับและตอบสนอง

หน่วยงานอาจพิจารณาใช้ระบบอัตโนมัติในการประมวลผลข้อมูลภัยคุกคาม การจัดลำดับความสำคัญของเหตุการณ์ หรือการดำเนินมาตรการตอบสนอง เพื่อช่วยลดระยะเวลาในการตรวจจับและตอบสนองต่อภัยคุกคาม

สำหรับการดำเนินการอัตโนมัติที่อาจส่งผลกระทบอย่างมีนัยสำคัญต่อระบบหรือบริการ ควรกำหนดขอบเขต เงื่อนไข และมาตรการควบคุมที่เหมาะสม รวมถึงความสามารถในการระงับหรือย้อนกลับการดำเนินการ

ระดับการกำกับดูแลโดยบุคลากรควรสอดคล้องกับความเสี่ยงและผลกระทบที่อาจเกิดขึ้นจากการดำเนินการอัตโนมัติ

๑๒.๑๑ การนำผลการตรวจจับกลับไปปรับปรุงมาตรการป้องกัน

หน่วยงานควรพิจารณานำผลจากการตรวจจับเหตุการณ์ Threat Hunting การวิเคราะห์ Threat Intelligence และบทเรียนจากเหตุการณ์ที่เกิดขึ้น มาใช้ปรับปรุงมาตรการป้องกันและความสามารถในการตรวจจับอย่างต่อเนื่อง

การปรับปรุงอาจครอบคลุมกฎการตรวจจับ การกำหนดค่าระบบ การแบ่งแยกเครือข่าย การควบคุมสิทธิ์ การบริหารช่องโหว่ ขั้นตอนการตอบสนอง และการฝึกอบรมบุคลากรที่เกี่ยวข้อง

๑๓. ข้อเสนอแนะด้านการออกแบบระบบอย่างมั่นคงปลอดภัยและการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย (Secure by Design and Security Assurance)

หน่วยงานควรพิจารณานำหลักการความมั่นคงปลอดภัยโดยการออกแบบ (Secure by Design) และความมั่นคงปลอดภัยโดยค่าเริ่มต้น (Secure by Default) มาใช้กับระบบ เครือข่าย ซอฟต์แวร์ อุปกรณ์ และบริการที่มีความสำคัญ โดยพิจารณาความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการกำหนดความต้องการ การออกแบบ การจัดหา การพัฒนา การติดตั้ง การทดสอบ การใช้งาน การบำรุงรักษา การเปลี่ยนแปลง จนถึงการยกเลิกการใช้งาน

ระดับของมาตรการและการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย (Security Assurance) ควรสอดคล้องกับระดับความเสี่ยง ความสำคัญของระบบ และผลกระทบที่อาจเกิดขึ้นต่อบริการที่สำคัญ โดยไม่จำเป็นต้องกำหนดมาตรการหรือระดับการทดสอบเดียวกันสำหรับทุกระบบ

๑๓.๑ ความมั่นคงปลอดภัยโดยการออกแบบ (Secure by Design)

หน่วยงานควรพิจารณาความต้องการด้านความมั่นคงปลอดภัยตั้งแต่ขั้นตอนการออกแบบหรือกำหนดความต้องการของระบบ แทนการเพิ่มมาตรการด้านความมั่นคงปลอดภัยภายหลังจากนำระบบไปใช้งานแล้ว

การออกแบบอาจพิจารณาหลักการ เช่น

(ก) การให้สิทธิ์เท่าที่จำเป็น (Least Privilege)

(ข) การแบ่งแยกหน้าที่และส่วนประกอบที่มีระดับความเชื่อถือแตกต่างกัน

(ค) การลดพื้นผิวการโจมตี (Attack Surface)

(ง) การป้องกันความล้มเหลวขององค์ประกอบเดียวไม่ให้เกิดผลกระทบต่อระบบโดยรวม

(จ) การรองรับการตรวจจับ ตอบสนอง และกู้คืนเมื่อเกิดเหตุ และ

(ฉ) การพิจารณาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาความเสี่ยงและข้อกำหนดด้านความมั่นคงปลอดภัยตั้งแต่ก่อนการจัดหาหรือพัฒนาระบบ

๑๓.๒ ความมั่นคงปลอดภัยโดยค่าเริ่มต้น (Secure by Default)

หน่วยงานควรพิจารณาให้ระบบหรือผลิตภัณฑ์ถูกกำหนดค่าเริ่มต้นในลักษณะที่ลดความเสี่ยงจากการใช้งานโดยไม่จำเป็นต้องพึ่งพาการปรับแต่งจำนวนมากภายหลัง

อาจพิจารณา

(ก) ปิดบริการ ฟังก์ชัน พอร์ต หรือส่วนเชื่อมต่อที่ไม่จำเป็น

(ข) จำกัดสิทธิ์เริ่มต้นให้อยู่ในระดับที่จำเป็น

(ค) หลีกเลี่ยงบัญชีหรือข้อมูลรับรองเริ่มต้นที่ไม่ปลอดภัย

(ง) เปิดใช้กลไกด้านความมั่นคงปลอดภัยที่จำเป็นตามระดับความเสี่ยง และ

(จ) กำหนดค่าการบันทึกเหตุการณ์และการปรับปรุงระบบให้เหมาะสมกับลักษณะการใช้งาน

ทั้งนี้ ค่าเริ่มต้นของผู้ผลิตไม่ควรถูกถือว่าเหมาะสมกับบริบทของหน่วยงานโดยอัตโนมัติ แต่ควรได้รับการทบทวนตามความเสี่ยงและสถาปัตยกรรมของระบบ

๑๓.๓ การกำหนดขอบเขตความเชื่อถือในการออกแบบระบบ (Trust Boundaries)

สำหรับระบบที่มีความสำคัญสูง หน่วยงานควรพิจารณาระบุขอบเขตความเชื่อถือ (Trust Boundaries) ระหว่างองค์ประกอบ ผู้ใช้ ระบบ เครือข่าย และบริการที่มีระดับความเชื่อถือหรือความสำคัญแตกต่างกัน

การออกแบบควรพิจารณาควบคุมการสื่อสารและการเข้าถึงข้าม Trust Boundary ตามความจำเป็น รวมถึงการพิสูจน์ตัวตน การอนุญาต การตรวจสอบข้อมูล การบันทึกเหตุการณ์ และการเฝ้าระวังตามระดับความเสี่ยง

การอยู่ภายในเครือข่ายหรือสถานที่ของหน่วยงานเพียงอย่างเดียวไม่ควรถูกใช้เป็นเหตุผลในการให้ความเชื่อถือโดยอัตโนมัติ

๑๓.๔ การออกแบบเพื่อลดผลกระทบเมื่อเกิดการละเมิด

สำหรับระบบที่มีความสำคัญ หน่วยงานควรพิจารณาออกแบบให้สามารถจำกัดขอบเขตและผลกระทบเมื่อองค์ประกอบใดองค์ประกอบหนึ่งถูกโจมตีหรือถูกควบคุมโดยไม่ได้รับอนุญาต

อาจพิจารณาการแบ่งแยกระบบ การจำกัดสิทธิ์ การจำกัดการเคลื่อนที่ภายในระบบ (Lateral Movement) การแยกส่วนบริหารจัดการ การป้องกันการแพร่กระจายของเหตุการณ์ และความสามารถในการแยกองค์ประกอบที่ได้รับผลกระทบออกจากระบบโดยไม่ทำให้บริการทั้งหมดหยุดชะงักโดยไม่จำเป็น

๑๓.๕ การสร้างรากฐานความเชื่อถือของระบบ

สำหรับระบบหรืออุปกรณ์ที่มีความสำคัญสูง หน่วยงานอาจพิจารณากลไกที่ช่วยสร้างและตรวจสอบความเชื่อถือของอุปกรณ์ ซอฟต์แวร์ และกระบวนการเริ่มต้นระบบ เพื่อช่วยป้องกันการเปลี่ยนแปลงโดยไม่ได้รับอนุญาตและสนับสนุนการปกป้องข้อมูลสำคัญ

กลไกดังกล่าวอาจรวมถึงรากฐานความเชื่อถือในฮาร์ดแวร์ (Hardware Root of Trust) หรือกลไกที่ให้ระดับความเชื่อมั่นเทียบเท่า เพื่อสนับสนุนการปกป้องกฎแฉเข้ารหัส การตรวจสอบความถูกต้องของซอฟต์แวร์หรือเฟิร์มแวร์ หรือการยืนยันความน่าเชื่อถือของอุปกรณ์

การเลือกใช้กลไกดังกล่าวควรพิจารณาจากผลลัพธ์ด้านความมั่นคงปลอดภัยที่ต้องการ และไม่ควรถูกกำหนดเทคโนโลยี ผู้ผลิต หรือสถาปัตยกรรมเฉพาะโดยไม่จำเป็น

๑๓.๖ การทดสอบความมั่นคงปลอดภัยตามระดับความเสี่ยง

หน่วยงานควรพิจารณากำหนดระดับและรูปแบบการทดสอบความมั่นคงปลอดภัยให้เหมาะสมกับความสำคัญและความเสี่ยงของระบบ

การทดสอบอาจประกอบด้วยการทบทวนการกำหนดค่า การประเมินช่องโหว่ การทดสอบเจาะระบบ (Penetration Testing) การทดสอบส่วนเชื่อมต่อและ API การทดสอบการแบ่งแยกระบบ หรือการทดสอบสถานการณ์การโจมตีตามความเหมาะสม

สำหรับระบบที่มีความสำคัญสูง ควรพิจารณาทดสอบเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญหรือเมื่อมีข้อมูลที่แสดงว่ารูปแบบภัยคุกคามหรือความเสี่ยงเปลี่ยนแปลงอย่างมีนัยสำคัญ

การทดสอบควรกำหนดขอบเขต วิธีการ และมาตรการป้องกันผลกระทบต่อบริการจริงอย่างเหมาะสม

๑๓.๗ การให้ความเชื่อมั่นจากบุคคลภายนอก (Independent Security Assurance)

สำหรับระบบ ผลิตภัณฑ์ หรือบริการที่มีความสำคัญสูง หน่วยงานอาจพิจารณาใช้การประเมิน การทดสอบ การรับรอง หรือหลักฐานจากบุคคลภายนอกที่มีความเหมาะสม เพื่อสนับสนุนการให้ความเชื่อมั่นด้านความมั่นคงปลอดภัย

การเลือกใช้หลักฐานควรพิจารณาขอบเขต วิธีการ ระยะเวลาที่ทำการประเมิน เวอร์ชันของผลิตภัณฑ์ และความสอดคล้องกับสภาพแวดล้อมการใช้งานจริง

ผลการรับรองหรือการประเมินจากภายนอกไม่ควรถูกใช้แทนการประเมินความเสี่ยงของหน่วยงาน เนื่องจากการกำหนดค่า การเชื่อมต่อ และสภาพแวดล้อมการใช้งานจริงอาจแตกต่างจากขอบเขตที่ได้รับการประเมิน

๑๓.๘ การออกแบบเพื่อรองรับการปรับปรุงด้านความมั่นคงปลอดภัย

ระบบที่มีวงจรชีวิตยาวควรได้รับการพิจารณาความสามารถในการปรับปรุงซอฟต์แวร์ เฟิร์มแวร์ การกำหนดค่า ไบรร์รอง และองค์ประกอบด้านความมั่นคงปลอดภัยที่เกี่ยวข้องตลอดอายุการใช้งาน

กระบวนการปรับปรุงควรสามารถตรวจสอบความถูกต้องและแหล่งที่มาของการปรับปรุง รวมถึงพิจารณาความสามารถในการย้อนกลับหรือกู้คืนในกรณีที่การปรับปรุงก่อให้เกิดปัญหา

สำหรับระบบที่ไม่สามารถปรับปรุงได้โดยง่าย ควรพิจารณาข้อจำกัดดังกล่าวเป็นส่วนหนึ่งของการประเมินความเสี่ยงตั้งแต่ขั้นตอนการจัดหาหรือออกแบบระบบ

๑๓.๙ การออกแบบเพื่อรองรับการเฝ้าระวังและการตรวจสอบ

ระบบที่มีความสำคัญควรได้รับการออกแบบให้สามารถสร้างและจัดเตรียมข้อมูลที่เพียงพอต่อการเฝ้าระวัง ตรวจสอบ วิเคราะห์เหตุการณ์ และสนับสนุนการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัย ควรพิจารณาความสามารถในการบันทึกเหตุการณ์ที่สำคัญ การระบุตัวตนหรือระบบที่ดำเนินกิจกรรม การบันทึกการเปลี่ยนแปลงที่มีนัยสำคัญ และการเชื่อมโยงข้อมูลกับระบบเฝ้าระวังของหน่วยงานตามความเหมาะสม

การออกแบบดังกล่าวควรคำนึงถึงความสมดุลระหว่างความต้องการด้านการตรวจสอบ ปริมาณข้อมูล ประสิทธิภาพของระบบ การรักษาความลับ และข้อกำหนดด้านการคุ้มครองข้อมูล

๑๓.๑๐ การบริหารความมั่นคงปลอดภัยตลอดวงจรชีวิต

หน่วยงานควรพิจารณาความมั่นคงปลอดภัยตลอดวงจรชีวิตของระบบ ตั้งแต่การกำหนดความต้องการ การออกแบบ การจัดหา การพัฒนา การติดตั้ง การใช้งาน การบำรุงรักษา การเปลี่ยนแปลง จนถึงการยกเลิกการใช้งาน

เมื่อระบบมีการเปลี่ยนแปลงที่มีนัยสำคัญ ควรพิจารณาว่าข้อสมมติด้านความมั่นคงปลอดภัย สถาปัตยกรรม Trust Boundary การพึ่งพาระบบอื่น และมาตรการควบคุมที่กำหนดไว้เดิมยังคงเหมาะสมหรือไม่

เมื่อยกเลิกระบบ ควรพิจารณาการเพิกถอนสิทธิ์และข้อมูลรับรอง การจัดการกุญแจเข้ารหัส การลบหรือทำลายข้อมูล การยกเลิกการเชื่อมต่อ และการจัดการอุปกรณ์หรือสื่อบันทึกข้อมูลตามระดับความเสี่ยง

๑๓.๑๑ การนำผลการประเมินกลับไปปรับปรุงการออกแบบ

หน่วยงานควรพิจารณานำผลจากการประเมินความเสี่ยง การทดสอบความมั่นคงปลอดภัย เหตุการณ์ที่เกิดขึ้น การบริหารช่องโหว่ และบทเรียนจากการดำเนินงานกลับไปใช้ในการปรับปรุงข้อกำหนด สถาปัตยกรรม การกำหนดค่า และการออกแบบระบบ

สำหรับระบบที่มีวงจรชีวิตยาว การทบทวนดังกล่าวช่วยให้หลัก Secure by Design ไม่จำกัดอยู่เฉพาะการออกแบบครั้งแรก แต่สามารถปรับให้เหมาะสมกับเทคโนโลยี ภัยคุกคาม และสภาพแวดล้อมที่เปลี่ยนแปลงไป