กรมการขนส่งทางราง
Department of Rail Transport

ประมวลแนวปฏิบัติ กรอบมาตรฐานและมาตรฐานขั้นต่ำ ด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับผู้ให้บริการขนส่งทางราง

โครงการจ้างที่ปรึกษาพัฒนาแนวการกำกับดูแลผู้ให้บริการขนส่งทางรางและจัดทำมาตรการความมั่นคงปลอดภัยไซเบอร์
ของกรมการขนส่งทางรางตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

มกราคม ๒๕๖๙

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบ หรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพและไปในทิศทางเดียวกัน

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานควบคุมหรือกำกับดูแล จึงจัดทำกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง แนวทางการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๘

๑.๒ วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกรอบการดำเนินการด้านการรักษาความมั่นคงปลอดภัยสารสนเทศให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

๑.๓ ขอบเขต

เอกสารฉบับนี้ครอบคลุมตามกรอบและวิธีปฏิบัติสำหรับด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๔ มาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๔ คำนิยาม

ลำดับ	คำนิยาม	ความหมาย
๑.	ขร.	กรมการขนส่งทางราง
๒.	คณะกรรมการ	คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๓.	กกม.	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
๔.	สกมช.	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
๕.	หน่วยงานผู้ให้บริการขนส่งทางราง	ผู้ให้บริการขนส่งทางรางที่อยู่ภายใต้การควบคุมและกำกับดูแลของกรมการขนส่งทางรางตามกฎหมายกำหนด

ลำดับ	คำนิยาม	ความหมาย
๖.	บริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง	บริการ หรือระบบงานที่เกี่ยวข้องกับบริการของผู้ให้บริการขนส่งทางรางในฐานะหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามกฎหมายกำหนดภายใต้ภารกิจ หรือบริการที่สำคัญ ๔ บริการ ดังนี้ ๑. บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง ๒. บริการที่เกี่ยวข้องกับการส่งสัญญาณ การสื่อสารและการส่งข้อมูล ๓. บริการขายตั๋วและสำรองที่นั่ง ๔. บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแลและเก็บข้อมูล
๗.	ดัชนีชี้วัดความเสี่ยงที่สำคัญ	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคตและเตรียมมาตรการการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย
๘.	คอมไพเลอร์ (Compiler)	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรม เป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๙.	แพตซ์ (Patch)	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟต์แวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟต์แวร์ ผู้พัฒนาซอฟต์แวร์หลายรายได้เผยแพร่แพตซ์ (Patch) ออกมาเป็นระยะ เช่น บริษัท Microsoft มีการเผยแพร่แพตซ์ (Patch) ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๑๐.	Recovery Time Objective (RTO)	ระยะเวลาในการกู้คืนระบบ
๑๑.	Recovery Point Objective (RPO)	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๑๒.	Maximum Tolerance Period of Disruption (MTPD)	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น เมื่อเกิดภัยคุกคามขึ้นหน่วยงานต้องแก้ไขให้ระบบกลับมาใช้งานได้ภายในระยะเวลาที่เร็วที่สุดแต่ต้องไม่เกินระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักได้

ลำดับ	คำนิยาม	ความหมาย
๑๓.	ผู้ใช้งาน	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานผู้ให้บริการขนส่งทางราง
๑๔.	บุคคลภายนอก	บุคคลจากหน่วยงานภายนอกที่เข้ามาดำเนินการอย่างใดอย่างหนึ่งกับหน่วยงานซึ่งเกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เช่น เข้ามาประชุม เข้ามาปฏิบัติงานร่วม เป็นต้น
๑๕.	หน่วยงานภายนอก	หน่วยงานภายนอกที่หน่วยงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๑๖.	ผู้ให้บริการภายนอก (Service Provider, Third-Party Provider, Outsource)	นิติบุคคลอื่นซึ่งเข้าทำสัญญารับจัดการงานที่โดยปกติหน่วยงานผู้ให้บริการขนส่งทางรางต้องดำเนินการเอง รวมถึงผู้ที่เข้าทำสัญญาช่วง เพื่อรับช่วงจัดการงานนั้น ๆ ทุกช่วง
๑๗.	สิทธิ์ของผู้ใช้งาน	สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๑๘.	ผู้ดูแลระบบ	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
๑๙.	สินทรัพย์	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่าคุณค่าสำหรับหน่วยงาน
๒๐.	การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การขออนุญาต การกำหนดสิทธิ์ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
๒๑.	ความมั่นคงปลอดภัยด้านสารสนเทศ	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของระบบเทคโนโลยีสารสนเทศ
๒๒.	ภัยคุกคาม	สาเหตุที่ทำให้เกิดเหตุไม่พึงประสงค์ที่มีผลเสียหายต่อหน่วยงานผู้ให้บริการขนส่งทางราง
๒๓.	ช่องโหว่	จุดอ่อนของทรัพย์สิน หรือมาตรการ ที่ภัยคุกคามสามารถใช้ประโยชน์ในการทำให้เกิดความเสียหาย
๒๔.	สื่อบันทึกข้อมูล	สิ่งที่ใช้จัดเก็บข้อมูล ชุดคำสั่ง และสารสนเทศอื่น ๆ เช่น USB drive, SD Card, Memory stick, เทป, CD/DVD, Removable drive, External Hard disk, Flash memory และหน่วยความจำของอุปกรณ์ Router หรือ Switch เป็นต้น

ลำดับ	คำนิยาม	ความหมาย
๒๕.	ทรัพย์สิน	ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) ระบบเครือข่ายคอมพิวเตอร์ ระบบสารสนเทศและข้อมูลสารสนเทศ หรือสิ่งอื่นใดที่มีคุณค่าสำหรับงานด้านเทคโนโลยีสารสนเทศ
๒๖.	ความเสี่ยง	เหตุการณ์ที่มีโอกาสเกิดขึ้นได้และทำให้เกิดความเสียหายต่อสินทรัพย์สารสนเทศขององค์กร เช่น ไวรัสทำให้ข้อมูลเสียหาย ข้อมูลสำคัญถูกเข้าถึงโดยไม่ได้รับอนุญาต หน้าเว็บไซต์ถูกเปลี่ยนแปลงแก้ไขซึ่งอาจทำให้องค์กรเสียชื่อเสียง
๒๗.	ISO/IEC ๒๗๐๐๑	มาตรฐานระบบการจัดการความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System หรือ ISMS)
๒๘.	NIST Cybersecurity Framework	กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)
๒๙.	มาตรฐาน IEC ๖๒๔๔๓	กรอบมาตรฐานความมั่นคงปลอดภัยทางไซเบอร์ของระบบควบคุมอุตสาหกรรม (Industrial Automation and Control Systems: IACS)

บทที่ ๒
กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework)

รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑.๑ บทนำ

NIST Cybersecurity Framework (CSF) เป็นมาตรฐานที่พัฒนาโดยสถาบันมาตรฐานและเทคโนโลยีแห่งชาติของสหรัฐอเมริกา (National Institute of Standards and Technology - NIST) โดยมีวัตถุประสงค์ เพื่อช่วยให้องค์กรสามารถบริหารจัดการความเสี่ยงด้านไซเบอร์ได้อย่างมีประสิทธิภาพ CSF ถูกออกแบบให้ยืดหยุ่น และสามารถนำไปประยุกต์ใช้ได้กับองค์กรทุกประเภท ไม่ว่าจะเป็นภาครัฐ เอกชน หรือองค์กรที่ต้องการเพิ่มความมั่นคงปลอดภัยของระบบสารสนเทศ

รูปที่ ๒ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบไปด้วย ๖ หัวข้อ

๒.๑.๒ หลักการของมาตรฐาน

หลักการสำคัญที่ใช้เป็นแนวทางในการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ โดยแบ่งออกเป็น ๖ ฟังก์ชันหลัก ได้แก่

๑. การกำกับดูแล (Government)

ซึ่งเน้นย้ำถึงความสำคัญของการกำกับดูแลและความเป็นผู้นำในการบริหารจัดการความเสี่ยงด้านไซเบอร์ในระดับองค์กร โดยมีองค์ประกอบ ดังนี้

- บริบทขององค์กร (Organizational Context) เป็นการทำความเข้าใจสภาพแวดล้อม วัตถุประสงค์ และความต้องการขององค์กรที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- กลยุทธ์การบริหารความเสี่ยง (Risk Management Strategy) เป็นการกำหนดแนวทางและเป้าหมายในการจัดการความเสี่ยงด้านไซเบอร์
- บทบาท ความรับผิดชอบ และอำนาจหน้าที่ (Roles, Responsibilities, and Authorities) เป็นการกำหนดผู้รับผิดชอบและขอบเขตอำนาจที่ชัดเจน
- นโยบาย (Policy) ต้องจัดทำนโยบายและแนวปฏิบัติที่เกี่ยวข้องกับความมั่นคงปลอดภัยทางไซเบอร์
- การกำกับดูแล (Oversight) ต้องมีการตรวจสอบและประเมินผลการดำเนินงานด้านความมั่นคงปลอดภัยอย่างต่อเนื่อง
- การบริหารจัดการความเสี่ยงในห่วงโซ่อุปทาน (Cybersecurity Supply Chain Risk Management - C-SCRM) โดยกำหนดการจัดการความเสี่ยงที่มาจากผู้ให้บริการและบุคคลที่สามในห่วงโซ่อุปทาน

๒. การระบุ (Identify)

มุ่งเน้นที่การทำความเข้าใจและระบุความเสี่ยงด้านไซเบอร์ขององค์กร ซึ่งประกอบด้วย

- การบริหารจัดการสินทรัพย์ (Asset Management) โดยจัดให้มีการระบุและจัดประเภทสินทรัพย์ที่สำคัญขององค์กร (เช่น ระบบ ข้อมูล บุคลากร)
- สภาพแวดล้อมทางธุรกิจ (Business Environment) ซึ่งเป็นการทำความเข้าใจบทบาทของความมั่นคงปลอดภัยไซเบอร์ในการสนับสนุนการดำเนินงานขององค์กร
- การบริหารความเสี่ยง (Risk Assessment) โดยกำหนดให้มีการประเมินความเสี่ยงและช่องโหว่ด้านความมั่นคงปลอดภัย
- การบริหารจัดการความเสี่ยงห่วงโซ่อุปทาน (Supply Chain Risk Management) การระบุและประเมินความเสี่ยงที่เกี่ยวข้องกับผู้ให้บริการและบุคคลที่สาม

๓. การป้องกัน (Protect)

ฟังก์ชันนี้ครอบคลุมการพัฒนากำหนดและดำเนินกิจกรรมป้องกันเพื่อจำกัดหรือยับยั้งผลกระทบที่อาจเกิดจากเหตุการณ์ด้านความมั่นคงปลอดภัย ประกอบด้วย

- การบริหารจัดการข้อมูล (Data Security) โดยจัดให้มีการป้องกันข้อมูลสำคัญจากการเข้าถึง การใช้งาน การเปิดเผย การขัดขวาง การแก้ไข หรือการทำลายโดยไม่ได้รับอนุญาต
- การควบคุมการเข้าถึง (Identity Management, Authentication, and Access Control) เป็นการบริหารจัดการตัวตน การยืนยันตัวตน และการควบคุมการเข้าถึงระบบและข้อมูล
- การป้องกันระบบและข้อมูล (Protective Technology) โดยการนำเทคโนโลยีและมาตรการป้องกันต่างๆ มาใช้ (เช่น ไฟร์วอลล์ การเข้ารหัส ซอฟต์แวร์ป้องกันมัลแวร์)
- การอบรมและสร้างความตระหนัก (Awareness and Training) โดยการให้ความรู้แก่บุคลากรเกี่ยวกับภัยคุกคามและการปฏิบัติงานที่ปลอดภัยจากภัยคุกคามทางไซเบอร์
- กระบวนการป้องกัน (Protective Processes) โดยกำหนดและดำเนินการตามกระบวนการที่ช่วยป้องกันเหตุการณ์ด้านความมั่นคงปลอดภัย

๔. การตรวจจับ (Detect)

ฟังก์ชันนี้เน้นที่การพัฒนากิจกรรมเพื่อระบุการเกิดเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ให้ทันท่วงที ประกอบด้วย

- การตรวจสอบความผิดปกติและเหตุการณ์ (Anomalies and Events) โดยจัดให้มีการตรวจจับกิจกรรมที่ผิดปกติหรือเหตุการณ์ด้านความมั่นคงปลอดภัยทางไซเบอร์
- การตรวจสอบความปลอดภัย (Security Continuous Monitoring) โดยจัดให้มีการเฝ้าระวังระบบและเครือข่ายอย่างต่อเนื่อง
- กระบวนการตรวจจับ (Detection Processes) โดยกำหนดและดำเนินการตามกระบวนการ เพื่อตรวจจับภัยคุกคาม

๕. การตอบสนอง (Respond)

ฟังก์ชันนี้มุ่งเน้นที่การพัฒนากิจกรรมเพื่อดำเนินการเมื่อตรวจพบเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วย

- การวางแผนการตอบสนอง (Response Planning) โดยจัดให้มีทำแผนการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์
- การสื่อสาร (Communication) โดยการสื่อสารข้อมูลที่เกี่ยวข้องกับเหตุการณ์ไปยังผู้มีส่วนได้ส่วนเสีย
- การวิเคราะห์ (Analysis) โดยดำเนินการวิเคราะห์เหตุการณ์ เพื่อทำความเข้าใจสาเหตุและขอบเขตของผลกระทบ
- การลดผลกระทบ (Mitigation) โดยดำเนินการตามมาตรการควบคุมขององค์กรเพื่อลดผลกระทบของเหตุการณ์

- การปรับปรุง (Improvements) โดยการนำบทเรียนจากเหตุการณ์ภัยคุกคามทางไซเบอร์มาดำเนินการปรับปรุงกระบวนการและมาตรการป้องกันที่อยู่ปัจจุบันเพื่อป้องกันการเกิดซ้ำ

๖. การกู้คืน (Recover)

ฟังก์ชันนี้เน้นที่การพัฒนากิจกรรมเพื่อฟื้นฟูระบบและบริการที่ได้รับผลกระทบจากเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งประกอบด้วย

- การวางแผนการกู้คืน (Recovery Planning) โดยดำเนินการจัดทำแผนการกู้คืนระบบและข้อมูลจากภัยคุกคามทางไซเบอร์
- การปรับปรุง (Improvements) โดยนำบทเรียนจากการกู้คืนไปปรับปรุงแผนและความสามารถในการฟื้นตัว
- การสื่อสาร (Communications) จัดให้มีการสื่อสารสถานะการกู้คืนกับผู้มีส่วนได้ส่วนเสียรับทราบเป็นระยะ

๒.๒ กรอบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS)

๒.๒.๑ บทนำ (Introduction)

ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานสากลสำหรับการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS) ที่ออกแบบมาเพื่อช่วยให้องค์กรสามารถปกป้องข้อมูลสำคัญจากภัยคุกคามทางไซเบอร์ และลดความเสี่ยงจากการรั่วไหลของข้อมูล ระบบนี้เป็นโครงสร้างที่ช่วยให้องค์กรสามารถวางแผน ดำเนินการ ตรวจสอบ และปรับปรุงมาตรการรักษาความปลอดภัยของข้อมูลอย่างต่อเนื่อง โดยสามารถนำไปใช้ได้กับทุกประเภทขององค์กร ไม่ว่าจะเป็นภาครัฐ ภาคเอกชน หรือองค์กรที่เกี่ยวข้องกับข้อมูลที่มีความอ่อนไหวสูง

รูปที่ ๓ กรอบมาตรฐานการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS)

๒.๒.๒ หลักการของ ISO/IEC ๒๗๐๐๑:๒๐๒๒ (Key Principles)

หลักการสำคัญของมาตรฐาน ISO/IEC ๒๗๐๐๑ อิงตามหลักการสำคัญของความมั่นคงปลอดภัยสารสนเทศที่เรียกว่า CIA Triad ได้แก่

๑. การรักษาความลับของข้อมูล (Confidentiality)

- การป้องกันไม่ให้ข้อมูลถูกเข้าถึง แก้ไข หรือเปิดเผยโดยบุคคลที่ไม่ได้รับอนุญาต เพื่อรักษาความปลอดภัยและลดความเสี่ยงจากการรั่วไหลของข้อมูล

๒. ความถูกต้องครบถ้วนของข้อมูล (Integrity)

- การป้องกันข้อมูลจากการถูกแก้ไข ดัดแปลง หรือทำลายโดยไม่ได้รับอนุญาต เพื่อให้มั่นใจว่าข้อมูลยังคงถูกต้องและน่าเชื่อถือ

๓. ความพร้อมใช้งานของข้อมูล (Availability)

- การทำให้ข้อมูลสามารถเข้าถึงและใช้งานได้อย่างต่อเนื่อง เมื่อต้องการโดยไม่มีการหยุดชะงักหรือสูญหาย

๒.๒.๓ ข้อกำหนดของ ISO/IEC ๒๗๐๐๑:๒๐๒๒ (Requirements)

ข้อกำหนดใน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ถูกแบ่งออกเป็นส่วนต่าง ๆ ดังนี้

๑. บริบทขององค์กร (Context of the Organization)

- การทำความเข้าใจบริบทภายในและภายนอกที่อาจมีผลกระทบต่อ ISMS
- การระบุและทำความเข้าใจความต้องการของผู้มีส่วนได้ส่วนเสีย
- การกำหนดขอบเขตของ ISMS

๒. ความเป็นผู้นำ (Leadership)

- การสนับสนุนจากผู้บริหารระดับสูงในเรื่องการจัดการ ISMS
- การกำหนดนโยบายความมั่นคงปลอดภัยของข้อมูล
- การมอบหมายบทบาท ความรับผิดชอบ และอำนาจหน้าที่

๓. การวางแผน (Planning)

- การระบุความเสี่ยง และโอกาสที่เกี่ยวข้องกับ ISMS
- การกำหนดวัตถุประสงค์ และเป้าหมายด้านความมั่นคงปลอดภัยของข้อมูล
- การวางแผน เพื่อจัดการความเสี่ยงและโอกาส

๔. การสนับสนุน (Support)

- การจัดหาทรัพยากรที่เพียงพอสำหรับ ISMS
- การฝึกอบรม และสร้างความตระหนักในองค์กร
- การสื่อสารที่มีประสิทธิภาพเกี่ยวกับ ISMS

๕. การดำเนินงาน (Operation)

- การวางแผนและควบคุมกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยของข้อมูล
- การประเมินและจัดการความเสี่ยงด้านความมั่นคงปลอดภัยของข้อมูล
- การจัดการเปลี่ยนแปลงที่มีผลกระทบต่อ ISMS

๖. การประเมินผลการปฏิบัติงาน (Performance Evaluation)

- การติดตาม วัดผล และประเมินผลการปฏิบัติงานของ ISMS
- การตรวจสอบภายใน (Internal Audit)
- การทบทวนโดยผู้บริหาร (Management Review)

๗. การปรับปรุง (Improvement)

- การแก้ไขปัญหาและการปรับปรุงอย่างต่อเนื่องของ ISMS
- การดำเนินการแก้ไขเมื่อมีความไม่สอดคล้อง

รูปที่ ๔ มาตรการควบคุม (Annex A) ตามมาตรฐาน ISO/IEC ๒๗๐๐๑: ๒๐๒๒

๒.๒.๔ ข้อกำหนดภาคผนวก (Annex A Controls)

Annex A ใน ISO/IEC ๒๗๐๐๑:๒๐๒๒ ประกอบด้วย ๙๓ ข้อควบคุม (Controls) แบ่งออกเป็น ๔ หมวดใหญ่ ดังนี้

๑. A.๕ มาตรการควบคุมเชิงองค์กร (Organizational Controls) จำนวน ๓๗ ข้อ

- A.๕.๑ : นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ
- A.๕.๒ : บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ
- A.๕.๓ : การแบ่งงานและหน้าที่ความรับผิดชอบ
- A.๕.๔ : หน้าที่ความรับผิดชอบของผู้บริหาร
- A.๕.๕ : การติดต่อหน่วยงานผู้มีอำนาจ
- A.๕.๖ : การติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษ
- A.๕.๗ : ข้อมูลวิเคราะห์เชิงลึกด้านภัยคุกคาม
- A.๕.๘ : ความมั่นคงปลอดภัยสารสนเทศในการบริการโครงการ
- A.๕.๙ : บัญชีทะเบียนข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ
- A.๕.๑๐ : การใช้งานข้อมูลและทรัพย์สินที่เกี่ยวข้องอื่น ๆ อย่างเหมาะสม
- A.๕.๑๑ : การคืนทรัพย์สิน

- A.๕.๑๒ : การจัดหมวดหมู่ของสารสนเทศ
- A.๕.๑๓ : การทำป้ายชี้บ่งสารสนเทศ
- A.๕.๑๔ : การถ่ายโอนข้อมูล
- A.๕.๑๕ : การควบคุมการเข้าถึง
- A.๕.๑๖ : การบริหารจัดการพิสูจน์ตัวตน
- A.๕.๑๗ : ข้อมูลในการพิสูจน์ตัวตน
- A.๕.๑๘ : สิทธิ์การเข้าถึง
- A.๕.๑๙ : ความมั่นคงปลอดภัยสารสนเทศในความสัมพันธ์กับผู้ให้บริการภายนอก
- A.๕.๒๐ : การระบุความมั่นคงปลอดภัยสารสนเทศในข้อตกลงของผู้ให้บริการภายนอก
- A.๕.๒๑ : การจัดการด้านความมั่นคงปลอดภัยสารสนเทศในห่วงโซ่อุปทานเทคโนโลยีสารสนเทศและการสื่อสาร
- A.๕.๒๒ : การติดตาม การทบทวน และการเปลี่ยนแปลงการจัดการบริการของผู้ให้บริการภายนอก
- A.๕.๒๓ : ความมั่นคงปลอดภัยสารสนเทศสำหรับการใช้บริการคลาวด์
- A.๕.๒๔ : การวางแผนและการเตรียมการ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- A.๕.๒๕ : การประเมินและการตัดสินใจต่อเหตุการณ์ด้านความมั่นคงปลอดภัย
- A.๕.๒๖ : การตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- A.๕.๒๗ : การเรียนรู้จากเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ
- A.๕.๒๘ : การเก็บรวบรวมหลักฐาน
- A.๕.๒๙ : ความมั่นคงปลอดภัยสารสนเทศระหว่างการหยุดชะงัก
- A.๕.๓๐ : ความพร้อมด้าน ICT เพื่อความต่อเนื่องทางธุรกิจ
- A.๕.๓๑ : กฎหมาย ข้อกำหนดทางกฎหมาย ระเบียบข้อบังคับ และข้อผูกพันตามสัญญา
- A.๕.๓๒ : สิทธิในทรัพย์สินทางปัญญา
- A.๕.๓๓ : การป้องกันบันทึก
- A.๕.๓๔ : ความเป็นส่วนตัวและการปกป้องข้อมูลส่วนบุคคล
- A.๕.๓๕ : การทบทวนด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นอิสระ
- A.๕.๓๖ : การปฏิบัติตามนโยบาย กฎระเบียบ และมาตรฐานด้านความมั่นคงปลอดภัย
- A.๕.๓๗ : เอกสารขั้นตอนการปฏิบัติงาน

๒. A.๖ มาตรการด้านบุคลากร (People Controls) จำนวน ๘ ข้อ

- A.๖.๑ : การคัดกรอง
- A.๖.๒ : ข้อตกลงและเงื่อนไขการจ้างงาน
- A.๖.๓ : ความตระหนัก การให้ความรู้ และการฝึกอบรมด้านความมั่นคงปลอดภัย
- A.๖.๔ : กระบวนการทางวินัย

- A.๖.๕ : ความรับผิดชอบหลังการสิ้นสภาพหรือการเปลี่ยนแปลงการจ้างงาน
- A.๖.๖ : ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ
- A.๖.๗ : การปฏิบัติงานจากระยะไกล
- A.๖.๘ : การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๓. A.๗ มาตรการด้านกายภาพ (Physical Controls) จำนวน ๑๔ ข้อ

- A.๗.๑ : อาณาเขตความมั่นคงปลอดภัยทางกายภาพ
- A.๗.๒ : การเข้า-ออกพื้นที่
- A.๗.๓ : ความมั่นคงปลอดภัยของสำนักงาน ห้องทำงาน และสิ่งอำนวยความสะดวก
- A.๗.๔ : การเฝ้าติดตามความมั่นคงปลอดภัยทางกายภาพ
- A.๗.๕ : การป้องกันภัยคุกคามทางกายภาพและสภาพแวดล้อม
- A.๗.๖ : การปฏิบัติงานในบริเวณที่ต้องรักษาความมั่นคงปลอดภัย
- A.๗.๗ : การจัดเก็บโต๊ะทำงาน และจัดการหน้าจอ
- A.๗.๘ : การจัดวางและการป้องกันอุปกรณ์
- A.๗.๙ : ความมั่นคงปลอดภัยของทรัพย์สินที่ใช้งานนอกสำนักงาน
- A.๗.๑๐ : สื่อบันทึกข้อมูล
- A.๗.๑๑ : ระบบสาธารณูปโภคสนับสนุน
- A.๗.๑๒ : ความมั่นคงปลอดภัยของการเดินสาย
- A.๗.๑๓ : การบำรุงรักษาอุปกรณ์
- A.๗.๑๔ : การจำหน่ายหรือนำอุปกรณ์มาใช้ซ้ำอย่างมั่นคงปลอดภัย

๔. A.๘ มาตรการด้านเทคโนโลยี (Technological Controls) จำนวน ๓๔ ข้อ

- A.๘.๑ : อุปกรณ์ปลายทางของผู้ใช้
- A.๘.๒ : สิทธิพิเศษในการเข้าถึง
- A.๘.๓ : การจำกัดการเข้าถึงสารสนเทศ
- A.๘.๔ : การเข้าถึงซอร์สโค้ด
- A.๘.๕ : การพิสูจน์ตัวตนอย่างมั่นคงปลอดภัย
- A.๘.๖ : การบริหารจัดการขีดความสามารถ
- A.๘.๗ : การป้องกันจากโปรแกรมไม่พึงประสงค์
- A.๘.๘ : การบริหารจัดการช่องโหว่ทางเทคนิค
- A.๘.๙ : การจัดการองค์ประกอบ
- A.๘.๑๐ : การลบข้อมูล
- A.๘.๑๑ : การปิดบังข้อมูล
- A.๘.๑๒ : การป้องกันข้อมูลรั่วไหล
- A.๘.๑๓ : การสำรองข้อมูล

- A.๘.๑๔ : อุปกรณ์สำรองของสิ่งอำนวยความสะดวกในการประมวลผลสารสนเทศ
- A.๘.๑๕ : การบันทึกล็อก
- A.๘.๑๖ : การเฝ้าติดตามกิจกรรม
- A.๘.๑๗ : การตั้งค่านาฬิกาให้ตรงกัน
- A.๘.๑๘ : การใช้งานโปรแกรมยูทิลิตี้ที่ได้รับสิทธิพิเศษ
- A.๘.๑๙ : การติดตั้งซอฟต์แวร์บนระบบปฏิบัติการ
- A.๘.๒๐ : ความมั่นคงปลอดภัยของเครือข่าย
- A.๘.๒๑ : ความมั่นคงปลอดภัยของบริการเครือข่าย
- A.๘.๒๒ : การแบ่งแยกเครือข่าย
- A.๘.๒๓ : การกรองเว็บ
- A.๘.๒๔ : การเข้ารหัสข้อมูล
- A.๘.๒๕ : วงจรชีวิตการพัฒนาอย่างมั่นคงปลอดภัย
- A.๘.๒๖ : ข้อกำหนดด้านความมั่นคงปลอดภัยของแอปพลิเคชัน
- A.๘.๒๗ : สถาปัตยกรรมระบบและหลักการทางวิศวกรรมที่มั่นคงปลอดภัย
- A.๘.๒๘ : การเขียนชุดคำสั่งอย่างมั่นคงปลอดภัย
- A.๘.๒๙ : การทดสอบความมั่นคงปลอดภัยในการพัฒนาและการยอมรับ
- A.๘.๓๐ : การพัฒนาโดยหน่วยงานภายนอก
- A.๘.๓๑ : การแบ่งแยกสภาพแวดล้อมของการพัฒนา การทดสอบ และการทำงานจริง
- A.๘.๓๒ : การบริหารจัดการการเปลี่ยนแปลง
- A.๘.๓๓ : ข้อมูลในการทดสอบ
- A.๘.๓๔ : การปกป้องระบบสารสนเทศระหว่างการทดสอบในการตรวจประเมิน

ISO/IEC ๒๗๐๐๑ เป็นมาตรฐานที่ช่วยให้องค์กรสามารถบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศได้อย่างมีประสิทธิภาพ ลดความเสี่ยงทางไซเบอร์ และเพิ่มความน่าเชื่อถือให้กับองค์กร การนำมาตรฐานนี้มาใช้ จะช่วยให้สามารถควบคุมความเสี่ยง ปกป้องข้อมูล และปฏิบัติตามข้อกำหนดด้านกฎหมายและกฎระเบียบได้อย่างมีประสิทธิภาพ

๒.๓ กรอบมาตรฐานเฉพาะสำหรับการรักษาความปลอดภัยทางไซเบอร์ระบบขนส่งทางราง (Cybersecurity in Railway)

๒.๓.๑ มาตรฐาน IEC ๖๒๔๔๓

หลักการของมาตรฐาน IEC ๖๒๔๔๓

มาตรฐาน IEC ๖๒๔๔๓ ได้รับการออกแบบมา เพื่อเป็นแนวทางสำหรับการรักษาความปลอดภัยไซเบอร์ โดยยึดหลักการสำคัญที่เน้นเรื่องการป้องกันภัยคุกคาม และการบริหารจัดการความเสี่ยงในระบบอุตสาหกรรมที่ซับซ้อนและเชื่อมต่อเครือข่ายหลายส่วน

๑. หลักการพื้นฐาน (Foundation Principles)

๑) การระบุตัวตนและการพิสูจน์ตัวตน (Identification and Authentication Control)

- ควบคุมการเข้าถึงระบบโดยใช้วิธีการยืนยันตัวตนที่เชื่อถือได้ เช่น รหัสผ่าน, Token หรือ การยืนยันตัวตนทางชีวมิติ (Biometric Authentication)

๒) การควบคุมการใช้งาน (Use Control)

- กำหนดสิทธิ์การเข้าถึงและการใช้งานตามบทบาทหรือหน้าที่ เพื่อลดความเสี่ยงจากการเข้าถึงข้อมูลหรือระบบที่ไม่ได้รับอนุญาต

๓) ความสมบูรณ์ของระบบ (System Integrity)

- มุ่งเน้นการป้องกันการเปลี่ยนแปลงข้อมูล หรือกระบวนการโดยไม่ได้รับอนุญาต เพื่อรักษาความถูกต้องและความน่าเชื่อถือของระบบ

๔) การรักษาความลับของข้อมูล (Data Confidentiality)

- ปกป้องข้อมูลสำคัญและข้อมูลส่วนตัวไม่ให้ถูกเข้าถึง หรือเปิดเผยโดยไม่ได้รับอนุญาต

๕) การจำกัดการไหลของข้อมูล (Restricted Data Flow)

- ควบคุมการส่งผ่านข้อมูลระหว่างระบบหรือเครือข่าย เพื่อป้องกันการรั่วไหลหรือการโจมตีที่เกิดจากช่องโหว่ของระบบ

๖) การตอบสนองต่อเหตุการณ์ (Timely Response to Events)

- กำหนดกระบวนการที่สามารถตอบสนองต่อเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยไซเบอร์ ได้อย่างทันท่วงที

๗) ความพร้อมใช้งาน (Resource Availability)

- รักษาความพร้อมใช้งานของระบบและทรัพยากรสำคัญ เพื่อให้ระบบสามารถดำเนินการได้ต่อเนื่อง

๒. หลักการเกี่ยวกับกระบวนการและการบริหารจัดการ (Process and Management Principles)

๑) ความรับผิดชอบร่วมกัน

- เจ้าของสินทรัพย์ (Asset Owners) ผู้ให้บริการ (Service Providers) และผู้พัฒนาซอฟต์แวร์ ต้องทำงานร่วมกันเพื่อรักษาความปลอดภัยของระบบ

๒) การประเมินความเสี่ยง

- ใช้กระบวนการประเมินความเสี่ยงในการกำหนดมาตรการควบคุม และระดับความปลอดภัยที่เหมาะสม

๓) วงจรชีวิตที่ปลอดภัย (Secure Lifecycle)

- การพัฒนา การบำรุงรักษา และการรื้อถอนระบบต้องคำนึงถึงความปลอดภัยในทุกขั้นตอน

๔) การจัดการเหตุการณ์ (Incident Management)

- มีกระบวนการแจ้งเตือน การตอบสนองและการกู้คืนระบบหลังเกิดเหตุการณ์ทางไซเบอร์

๓. หลักการทางเทคนิค (Technical Principles)

๑) โซนและช่องทาง (Zones and Conduits)

- ระบบ IACS ถูกแบ่งออกเป็นโซนที่มีระดับความเสี่ยงคล้ายกัน และการสื่อสารระหว่างโซน จะใช้ช่องทางที่มีการควบคุม

๒) การเข้ารหัสข้อมูล

- ใช้การเข้ารหัส เพื่อปกป้องข้อมูลสำคัญที่ถูกส่งผ่านระหว่างส่วนต่าง ๆ ของระบบ

๓) การตรวจจับและตอบสนองต่อภัยคุกคาม

- ใช้ระบบตรวจจับเหตุการณ์ (IDS) และการป้องกันเหตุการณ์ (IPS) เพื่อลดผลกระทบจากการโจมตี

๔) การควบคุมการเข้าถึงระยะไกล (Remote Access Control)

- จำกัดการเข้าถึงจากระยะไกลเฉพาะที่จำเป็น พร้อมใช้การยืนยันตัวตนหลายชั้น

๔. ข้อกำหนดของมาตรฐาน

มาตรฐานนี้ กำหนดแนวทางและข้อกำหนดต่าง ๆ สำหรับ

๑) หมวดทั่วไป (General)

ให้คำจำกัดความ คำศัพท์ และแนวคิดเบื้องต้น เพื่อสร้างความเข้าใจที่สอดคล้องกันระหว่างผู้ใช้งานมาตรฐาน

- **IEC/TS ๖๒๔๔๓-๑-๑**

กำหนดคำศัพท์ แนวคิด และโมเดลสำหรับการรักษาความปลอดภัยของ Industrial Automation and Control Systems (IACS) ซึ่งถูกนำไปใช้ตลอดทั้งชุดมาตรฐานนี้ โดยเฉพาะอย่างยิ่งได้มีการกำหนด ข้อกำหนดพื้นฐาน ๗ ข้อ (Foundation Requirements - FRs) ดังนี้ การควบคุมการระบุตัวตนและการพิสูจน์ตัวตน (FR๑), การควบคุมการใช้งาน (FR๒), ความสมบูรณ์ของระบบ (FR๓), การรักษาความลับของข้อมูล (FR๔), การจำกัดการไหลของข้อมูล (FR๕), การตอบสนองต่อเหตุการณ์อย่างทันท่วงที (FR๖) และความพร้อมใช้งานของทรัพยากร (FR๗)

- **IEC/TS ๖๒๔๔๓-๑-๒**
  รวมถึงการนิยามคำศัพท์ และตัวย่อที่ใช้ในมาตรฐาน IEC ๖๒๔๔๓

๒) หมวดนโยบายและกระบวนการ (Policies and Procedures)

มุ่งเน้นข้อกำหนดด้านการบริหารจัดการและการดำเนินการ เพื่อให้มั่นใจว่าระบบได้รับการปกป้องจากภัยคุกคาม

- **IEC ๖๒๔๔๓-๒-๑**

กำหนดข้อกำหนดสำหรับโปรแกรมความปลอดภัยของเจ้าของสินทรัพย์ (Asset Owner) ใน Industrial Automation and Control Systems (IACS) และให้คำแนะนำเกี่ยวกับวิธีการพัฒนาและปรับปรุงโปรแกรมความปลอดภัย โดยองค์ประกอบของโปรแกรมความปลอดภัย IACS ที่อธิบายไว้ในมาตรฐานนี้ ครอบคลุมถึงความสามารถด้านความปลอดภัยที่จำเป็นสำหรับการดำเนินงาน IACS อย่างปลอดภัย ซึ่งส่วนใหญ่เกี่ยวข้องกับนโยบาย ขั้นตอน วิธีปฏิบัติ และบุคลากร

- **IEC/IS ๖๒๔๔๓-๒-๒ Ed.๒**

กำหนดกรอบงานและวิธีการสำหรับการประเมินการป้องกัน IACS โดยอิงตามแนวคิดของระดับความปลอดภัยทางเทคนิค (Technical Security Level) และความพร้อมของกระบวนการที่เกี่ยวข้อง โดยแนวคิดของระดับการป้องกัน (Protection Level) เป็นการจัดระดับความปลอดภัยที่รวมมาตรการทางเทคนิคและองค์กร เพื่อแสดงถึงความครอบคลุมของโปรแกรมความปลอดภัย

- **IEC/TR ๖๒๔๔๓-๒-๓**

นิยามกระบวนการจัดการแพตช์ (Patch Management) ในสภาพแวดล้อม IACS โดยเฉพาะ

  - กำหนดรูปแบบสำหรับการแลกเปลี่ยนข้อมูลเกี่ยวกับแพตช์ความปลอดภัยระหว่างเจ้าของสินทรัพย์ (Asset Owners) และผู้ผลิตผลิตภัณฑ์ (Product Suppliers)
  - กำหนดกิจกรรมที่เกี่ยวข้องกับการพัฒนา และให้ข้อมูลแพตช์โดยผู้ผลิต รวมถึงการติดตั้งแพตช์ โดยเจ้าของสินทรัพย์ รูปแบบการแลกเปลี่ยนข้อมูลและกิจกรรมต่าง ๆ ที่กำหนดไว้ในมาตรฐานนี้ ใช้สำหรับแพตช์ที่เกี่ยวข้องกับความปลอดภัย แต่ยังสามารถปรับใช้กับแพตช์หรือการอัปเดตที่ไม่เกี่ยวข้องกับความปลอดภัยได้เช่นกัน

- **IEC ๖๒๔๔๓-๒-๔**

กำหนดข้อกำหนดสำหรับความสามารถด้านความปลอดภัยของผู้ให้บริการ IACS (Service Providers) ซึ่งพวกเขาสามารถนำเสนอให้กับเจ้าของสินทรัพย์ในระหว่างการผสานรวม (Integration) และการบำรุงรักษา (Maintenance) ของระบบอัตโนมัติ (Automation Solution) โดยบางความสามารถอ้างอิงมาตรการความปลอดภัยที่นิยามไว้ใน IEC ๖๒๔๔๓-๓-๓ ซึ่งผู้ให้บริการต้องมั่นใจว่าระบบอัตโนมัตินั้นสนับสนุนมาตรการเหล่านี้

๓) หมวดระบบ (System)

ครอบคลุมข้อกำหนดสำหรับการออกแบบดำเนินงานและการรักษาความปลอดภัยในระดับระบบ

- **IEC/TR ๖๒๔๔๓-๓-๑**

ให้การประเมินปัจจุบันเกี่ยวกับเครื่องมือด้านความปลอดภัยทางไซเบอร์ (Cybersecurity Tools), มาตรการป้องกัน (Mitigation Counter-measures) และเทคโนโลยีที่สามารถนำไปใช้ได้อย่างมีประสิทธิภาพใน Industrial Automation and Control Systems (IACS) ที่ใช้เทคโนโลยีทางอิเล็กทรอนิกส์ ในการควบคุมและตรวจสอบอุตสาหกรรมและโครงสร้างพื้นฐานที่สำคัญหลาย ๆ แห่ง โดยเอกสารนี้ อธิบายประเภทของเทคโนโลยีที่เกี่ยวข้องกับระบบควบคุมที่มุ่งเน้นความปลอดภัยทางไซเบอร์, ประเภทของผลิตภัณฑ์ที่มีในแต่ละประเภท, ข้อดีและข้อเสียของการใช้ผลิตภัณฑ์เหล่านั้นในสภาพแวดล้อม IACS อัตโนมัติ, การเปรียบเทียบกับภัยคุกคามที่คาดการณ์และช่องโหว่ที่ทราบ และที่สำคัญที่สุด คือ คำแนะนำเบื้องต้นและแนวทางการใช้ผลิตภัณฑ์เทคโนโลยีความปลอดภัยทางไซเบอร์หรือมาตรการป้องกันเหล่านี้

- **IEC ๖๒๔๔๓-๓-๒**

กำหนดข้อกำหนดสำหรับการประเมินความเสี่ยงเพื่อแบ่งแยกระบบ IACS (ซึ่งเป็นระบบที่กำลังพิจารณา) ออกเป็นโซนและช่องทาง (Conduits) โดยโซนคือการจัดกลุ่มของทรัพย์สินที่มีความเสี่ยงคล้ายกันในขณะที่การสื่อสารระหว่างโซนจะทำผ่านสิ่งที่เรียกว่า “ช่องทาง” (Conduits) ช่องทางเหล่านี้อาจถูกแมปกับการสื่อสารด้วยโปรโตคอลเครือข่ายในระบบระหว่างสองโซน เอกสารนี้ยังได้กำหนดข้อกำหนดสำหรับการประเมินความเสี่ยงในรายละเอียดของแต่ละโซนและช่องทาง และการกำหนดเป้าหมายระดับความปลอดภัย (Security Level Target - SL-T) ตามภัยคุกคามและความเสี่ยง

- **IEC ๖๒๔๔๓-๓-๓**

ให้ข้อกำหนดทางเทคนิคที่เกี่ยวข้องกับระบบควบคุม (SRs) ซึ่งเชื่อมโยงกับข้อกำหนดพื้นฐาน ๗ ข้อ (FRs) โดยเฉพาะการกำหนดข้อกำหนดสำหรับระดับความปลอดภัยของความสามารถของระบบควบคุม ข้อกำหนดเหล่านี้มีเป้าหมายที่จะนำไปใช้ร่วมกับโซน และช่องทางที่กำหนดไว้สำหรับระบบที่กำลังพิจารณา เพื่อกำหนดความสามารถด้านความปลอดภัยที่เหมาะสมในระดับระบบควบคุม

๔) หมวดส่วนประกอบ (Component)

มุ่งเน้นข้อกำหนดสำหรับส่วนประกอบทางเทคนิค เช่น อุปกรณ์ ซอฟต์แวร์ และระบบย่อย

- **IEC ๖๒๔๔๓-๔-๑**

กำหนดข้อกำหนดกระบวนการสำหรับการพัฒนาผลิตภัณฑ์ที่ปลอดภัยที่ใช้ใน Industrial Automation and Control Systems (IACS) โดยเฉพาะการกำหนดวงจรชีวิตการพัฒนาที่ปลอดภัย (Secure Development Life-cycle) เพื่อการพัฒนาและบำรุงรักษาผลิตภัณฑ์ที่ปลอดภัย ซึ่งกระบวนการนี้มุ่งเน้นที่การสร้างผลิตภัณฑ์ที่สามารถรักษาความปลอดภัยในระยะยาว

- **IEC ๖๒๔๔๓-๔-๒**

กำหนดข้อกำหนดทางเทคนิคด้านความปลอดภัยทางไซเบอร์สำหรับส่วนประกอบต่าง ๆ เช่น อุปกรณ์ฝังตัว (Embedded Devices), ส่วนประกอบเครือข่าย (Network Components), ส่วนประกอบโฮสต์ (Host Components) และแอปพลิเคชันซอฟต์แวร์ที่ถูกกำหนดไว้ใน IEC ๖๒๔๔๓-๓-๓

๒.๓.๒ มาตรฐาน TS ๕๐๗๐๑

หลักการของมาตรฐาน TS ๕๐๗๐๑

มาตรฐาน TS ๕๐๗๐๑ มีจุดประสงค์เพื่อให้แนวทางและข้อกำหนดเกี่ยวกับการป้องกันและการตอบสนองต่อภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในระบบรถไฟ ซึ่งรวมถึงการปกป้องข้อมูลที่สำคัญ การรักษาความปลอดภัยในระบบการควบคุม และการสื่อสารรวมถึงการลดความเสี่ยงจากการโจมตีทางไซเบอร์ที่อาจส่งผลกระทบต่อการดำเนินงานและความปลอดภัยของผู้โดยสาร พัฒนาโดยอ้างอิงจากมาตรฐาน IEC ๖๒๔๔๓ บนหลักการสำคัญที่ช่วยเพิ่มความปลอดภัยทางไซเบอร์ในระบบขนส่งทางราง โดยมีแนวทางดังนี้

๑) การประเมินภัยคุกคามและความเสี่ยง (Threat and Risk Assessment)

มาตรฐานนี้กำหนดให้ต้องมีการประเมินภัยคุกคามที่อาจเกิดขึ้นในระบบขนส่งทางรางอย่างสม่ำเสมอ โดยใช้วิธีการต่าง ๆ เช่น Risk Matrix หรือ Quantitative Risk Assessment เพื่อให้สามารถจัดลำดับความสำคัญของความเสี่ยงได้อย่างมีประสิทธิภาพและเพื่อวางแผนและดำเนินการในการป้องกันหรือบรรเทาผลกระทบจากภัยคุกคามที่อาจเกิดขึ้นจากการโจมตีทางไซเบอร์ โดยดำเนินการกำหนดกระบวนการสำหรับการระบุ, ประเมิน, จัดการภัยคุกคาม และความเสี่ยงทางไซเบอร์ในระบบขนส่งทางราง และครอบคลุมการระบุช่องโหว่ที่อาจเกิดขึ้นในระบบขนส่งทางราง เช่น การโจมตีจากภายนอก (DDoS) หรือจากภายใน เช่น พนักงานที่มีสิทธิ์เข้าถึงระบบ รวมถึงการประเมินผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานในระบบขนส่งทางราง โดยพิจารณาผลกระทบเชิงฟังก์ชัน และ ความน่าจะเป็นของภัยคุกคามเพื่อลดความเสี่ยงโดยรวม

๒) การปกป้องฟังก์ชันสำคัญ (Protection of Critical Functions)

มาตรฐานให้ความสำคัญกับการรักษาความปลอดภัยของฟังก์ชันที่สำคัญในระบบขนส่งทางราง เช่นระบบควบคุมสัญญาณ การชำระเงินอิเล็กทรอนิกส์ และระบบควบคุมการเดินรถ ซึ่งรวมถึงการใช้เทคโนโลยีที่ช่วยปกป้องข้อมูลและฟังก์ชัน โดยใช้มาตรการทางเทคนิค เช่น การเข้ารหัสข้อมูลที่ส่งผ่านระบบขนส่งทางราง การตรวจสอบสิทธิ์ผู้ใช้และแนะนำมาตรการเชิงป้องกัน เช่น การแบ่งส่วนเครือข่าย (Network Segmentation) เพื่อแยกระบบสำคัญออกจากเครือข่ายภายนอกและป้องกันการเข้าถึงข้อมูลสำคัญหรือการทำลายระบบจากภัยคุกคาม

๓) การควบคุมการเข้าถึง (Access Control)

มาตรฐานกำหนดให้ระบบขนส่งทางราง ต้องมีการควบคุมการเข้าถึงที่มีประสิทธิภาพ ซึ่งจะช่วยป้องกันการเข้าถึงข้อมูลหรือฟังก์ชันที่สำคัญจากบุคคลที่ไม่ได้รับอนุญาต โดยให้ใช้เทคโนโลยีที่สามารถตรวจสอบตัวบุคคลได้อย่างเข้มงวด เช่น Multi-Factor Authentication (MFA) หรือการตรวจสอบสิทธิ์การเข้าถึง และเน้นการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากผู้ไม่หวังดี โดยการควบคุมสิทธิ์ตามบทบาท (Role-Based Access Control)

๔) การตรวจติดตามและการตอบสนองต่อเหตุการณ์ (Monitoring and Incident Response)

ในกรณีที่เกิดการโจมตีทางไซเบอร์หรือเหตุการณ์ไม่ปกติ ระบบต้องมีการเตรียมพร้อมในการตอบสนองอย่างรวดเร็ว รวมถึงการติดตามสถานการณ์ การตรวจสอบเหตุการณ์ที่เกิดขึ้น และการดำเนินการฟื้นฟูระบบอย่างรวดเร็ว โดยต้องมีแผนการฟื้นฟูหลังจากเหตุการณ์ (Disaster Recovery Plan) ที่มีประสิทธิภาพและทันเวลา โดยต้องมีแผนการตอบสนองต่อเหตุการณ์ไซเบอร์ที่ชัดเจน เช่น การแจ้งเตือนภัย การหยุดใช้ระบบที่ถูกโจมตี และการฟื้นฟูระบบหลังเหตุการณ์ไซเบอร์ เพื่อป้องกันการกระทบต่อการเดินรถในระบบขนส่งทางราง

๕) การทดสอบและการประเมินความปลอดภัย (Testing and Security Assessment)

มาตรฐานนี้ยังกำหนดให้มีการทดสอบระบบและทำการประเมินความปลอดภัยอย่างต่อเนื่อง เพื่อให้มั่นใจได้ว่ามาตรการด้านความปลอดภัยที่ใช้ในระบบขนส่งทางราง สามารถตอบสนองต่อภัยคุกคามที่อาจเกิดขึ้น และระบบยังคงทำงานได้ตามที่คาดหวัง

๖) การติดตามและการตรวจสอบ (Monitoring and Auditing)

ระบบต้องมีเครื่องมือสำหรับการติดตามและตรวจสอบการทำงานของระบบในระยะยาว เพื่อสามารถตรวจจับเหตุการณ์ที่ไม่ปกติหรือการโจมตีทางไซเบอร์ได้ทันท่วงที โดยต้องมีการตรวจติดตามความปลอดภัยในแบบเรียลไทม์ โดยการจัดทำบันทึก (Logging) และการวิเคราะห์เหตุการณ์ (Incident Analysis) เพื่อปรับปรุงระบบในอนาคต รวมถึงจัดทำรายงานที่ช่วยให้สามารถติดตามผลกระทบจากเหตุการณ์และดำเนินการแก้ไขหรือปรับปรุงมาตรการความปลอดภัยได้อย่างมีประสิทธิภาพ

๒.๓.๓ มาตรฐาน EN ๕๐๑๒๘

หลักการของมาตรฐาน EN ๕๐๑๒๘

มาตรฐาน EN ๕๐๑๒๘ เป็นหนึ่งในมาตรฐานที่สำคัญสำหรับอุตสาหกรรมระบบขนส่งทางราง (Railway Applications) โดยมุ่งเน้นที่กระบวนการพัฒนาซอฟต์แวร์สำหรับระบบที่เกี่ยวข้องกับความปลอดภัย (Safety-Critical Systems) เช่น ระบบสัญญาณ ระบบควบคุมการเดินรถ และระบบตรวจสอบสถานะการทำงานของรถไฟ โดบ EN ๕๐๑๒๘ เป็นมาตรฐานที่จัดทำขึ้นโดยคณะกรรมการมาตรฐานวิศวกรรมไฟฟ้าแห่งยุโรป (European Committee for Electrotechnical Standardization: CENELEC) เพื่อรับรองว่าซอฟต์แวร์ที่พัฒนาสำหรับระบบขนส่งทางรางมีคุณภาพสูงและสอดคล้องกับมาตรฐานความปลอดภัยมาตรฐานนี้ เน้นการกำหนดขั้นตอน กระบวนการ และแนวทางปฏิบัติที่ชัดเจน เพื่อพัฒนาซอฟต์แวร์ให้มีความน่าเชื่อถือ ลดโอกาสเกิดความผิดพลาด และลดความเสี่ยงต่อชีวิตและทรัพย์สินในกรณีที่ระบบล้มเหลว ดังนี้

๑) การจัดการความเสี่ยง (Risk Management)

มาตรฐาน EN ๕๐๑๒๘ ให้ความสำคัญกับการจัดการความเสี่ยงที่เกี่ยวข้องกับการพัฒนาซอฟต์แวร์ โดยกำหนดให้มีการระบุ วิเคราะห์ และประเมินความเสี่ยงอย่างรอบคอบในทุกขั้นตอนของวงจรการพัฒนาซอฟต์แวร์ ซึ่งรวมถึงการวิเคราะห์อันตราย (Hazard Analysis) เพื่อระบุปัจจัยเสี่ยงที่อาจก่อให้เกิดปัญหาความปลอดภัย พร้อมทั้งกำหนด ระดับความสมบูรณ์ของความปลอดภัย (Safety Integrity Level: SIL) ที่เหมาะสมในแต่ละฟังก์ชัน โดยแบ่งออกเป็นระดับความปลอดภัย (SIL) ออกเป็น ๕ ระดับตั้งแต่ SIL ๐ ถึง SIL ๔ โดย SIL ๔ เป็นระดับความเสี่ยงสูงสุด และกำหนดข้อกำหนดที่เข้มงวดมากขึ้นตามระดับ SIL ที่สูงขึ้น

๒) กระบวนการพัฒนาซอฟต์แวร์ (Software Development Process)

กระบวนการพัฒนาต้องถูกออกแบบให้มีโครงสร้างและสามารถตรวจสอบย้อนกลับได้ (Traceability) โดยต้องเริ่มจากการระบุความต้องการทางฟังก์ชันและความปลอดภัยของระบบอย่างละเอียด การออกแบบระบบต้องคำนึงถึงความปลอดภัยของผู้ใช้งาน ลดความเสี่ยงจากความผิดพลาดที่อาจเกิดขึ้นในการทำงานของระบบ การลดความซับซ้อน และในการพัฒนาโค้ด ควรเลือกใช้วิธีที่เหมาะสม และพัฒนาอย่างถูกขั้นตอน เพื่อให้มั่นใจว่าจะทำงานได้อย่างถูกต้องในทุกสภาพแวดล้อม เช่น

- ภาษาโปรแกรมแนะนำให้ใช้ภาษาโปรแกรมที่มีความน่าเชื่อถือสูง เช่น C หรือ C++ และหลีกเลี่ยงการใช้ภาษาโปรแกรมที่ไม่เหมาะสม
- การออกแบบซอฟต์แวร์ ใช้เทคนิคการออกแบบซอฟต์แวร์ที่ช่วยลดความซับซ้อนและเพิ่มความน่าเชื่อถือ เช่น การออกแบบแบบโมดูลาร์
- การตรวจสอบโค้ด ดำเนินการตรวจสอบโค้ดอย่างละเอียดเพื่อหาข้อผิดพลาด
- การทดสอบ ใช้เทคนิคการทดสอบต่าง ๆ เช่น การทดสอบแบบ White-box และ Black-box เพื่อให้ครอบคลุมการทำงานของซอฟต์แวร์

๓) การประกันคุณภาพซอฟต์แวร์ (Software Quality Assurance)

มาตรฐานนี้ เน้นการสร้างระบบบริหารจัดการคุณภาพที่ครอบคลุมทุกขั้นตอน ตั้งแต่การกำหนดความต้องการไปจนถึงการส่งมอบ โดยต้องมีการกำหนดแผนการประกันคุณภาพซอฟต์แวร์ (Quality Assurance Plan) ที่ครอบคลุมทุกขั้นตอนของกระบวนการพัฒนา กำหนดให้มีการตรวจสอบและติดตามกระบวนการพัฒนาซอฟต์แวร์ เพื่อให้แน่ใจว่าเป็นไปตามแผน รวมถึงจัดทำและเก็บรักษาเอกสารที่เกี่ยวข้องกับซอฟต์แวร์อย่างเป็นระบบ เช่น การเก็บข้อมูลการตรวจสอบและรายงานการทดสอบ เพื่อให้มั่นใจได้ว่าซอฟต์แวร์จะตอบสนองต่อความต้องการด้านความปลอดภัยและประสิทธิภาพ

๔) การทดสอบและการตรวจสอบ (Testing and Verification)

มาตรฐาน EN ๕๐๑๒๘ กำหนดให้มีการทดสอบซอฟต์แวร์ในหลายระดับ เช่น การทดสอบหน่วย (Unit Testing) การทดสอบระบบ (System Testing) และการทดสอบการทำงานร่วมกัน (Integration Testing) พร้อมทั้งต้องใช้เทคนิคการทดสอบที่ครอบคลุม เช่น การทดสอบแบบ White-box, Black-box และการทดสอบตามเส้นทาง (Path Testing) เพื่อระบุข้อผิดพลาดและช่องโหว่ในระบบอย่างละเอียด

๕) การจัดการการเปลี่ยนแปลงและการบำรุงรักษา (Change Management and Maintenance)

การบริหารจัดการเปลี่ยนแปลงในซอฟต์แวร์เป็นส่วนสำคัญในการรับมือกับความต้องการที่เปลี่ยนแปลงในอนาคต ซึ่งควรกำหนดให้มีการบันทึกและติดตามการเปลี่ยนแปลงทุกครั้ง รวมถึงการบำรุงรักษาซอฟต์แวร์อย่างต่อเนื่องในระยะยาว เช่น การแก้ไขข้อผิดพลาด การอัปเดตฟังก์ชันและการปรับปรุงระบบเพื่อรับมือกับเทคโนโลยีใหม่ ๆ และต้องมีการติดตามผลการทำงานของซอฟต์แวร์หลังการใช้งานและมีแผนการแก้ไขปัญหาหรืออัปเดตตามความจำเป็น เพื่อให้มั่นใจว่ายังคงรักษาความปลอดภัยของระบบได้ตามมาตรฐาน

๖) การควบคุมการเข้าถึงและความปลอดภัย (Access Control and Security)

ซอฟต์แวร์ในระบบขนส่งทางรางต้องมีมาตรการควบคุมการเข้าถึงที่รัดกุม โดยกำหนดให้ผู้ที่เกี่ยวข้องต้องมีสิทธิ์เฉพาะที่เหมาะสมต่อบทบาทหน้าที่ รวมถึงใช้เทคโนโลยีการเข้ารหัสข้อมูลและการตรวจสอบสิทธิ์ผู้ใช้งานเพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๔ มาตรฐาน IEC ๖๓๔๕๒

หลักการของมาตรฐาน IEC ๖๓๔๕๒

มาตรฐาน IEC ๖๓๔๕๒ มุ่งเน้นการรักษาความปลอดภัยไซเบอร์ในระบบขนส่งทางราง โดยพัฒนาขึ้นเพื่อให้ความสำคัญกับการประเมินและจัดการความเสี่ยงทางไซเบอร์ในทุกขั้นตอนของวงจรชีวิตระบบขนส่งทางราง ตั้งแต่การออกแบบ การสร้าง การใช้งาน และการบำรุงรักษา มาตรฐานนี้ถือเป็นส่วนขยายของ TS ๕๐๗๐๑ ซึ่งเน้นการควบคุมความปลอดภัยไซเบอร์ในระดับการดำเนินงาน และการบำรุงรักษาระบบขนส่งทางราง โดยมาตรฐาน IEC ๖๓๔๕๒ จะขยายข้อกำหนดเหล่านี้ ไปยังการปรับปรุงระบบและการตอบสนองต่อภัยคุกคามทางไซเบอร์ในเชิงลึกมากยิ่งขึ้น

๑) การประเมินความเสี่ยง (Risk Assessment)

การประเมินความเสี่ยงจากภัยคุกคามทางไซเบอร์ในระบบขนส่งทางรางเป็นขั้นตอนที่สำคัญเพื่อให้มั่นใจว่าระบบขนส่งทางรางที่ออกแบบ หรือกำลังพัฒนาอยู่จะสามารถรับมือกับภัยคุกคามที่อาจเกิดขึ้นได้ทุกด้าน ตั้งแต่การออกแบบ การสร้าง ไปจนถึงการดำเนินงานและการบำรุงรักษา โดยต้องทำการประเมินภัยคุกคามครอบคลุมทุกระดับของระบบขนส่งทางราง ตั้งแต่โครงสร้างพื้นฐานจนถึงฟังก์ชันการทำงานที่สำคัญ และในทุกกระบวนการที่เกี่ยวข้องกับระบบขนส่งทางราง เพื่อที่เราจะสามารถคัดเลือกมาตรการป้องกัน และควบคุมที่เหมาะสมตามลำดับความสำคัญของความเสี่ยงนั้น ๆ ซึ่งอาจใช้เครื่องมือ เช่น Risk Matrix และ Quantitative Risk Assessment เพื่อช่วยในการตัดสินใจ และวางแผนในการลดความเสี่ยงที่อาจเกิดขึ้นได้

๒) การออกแบบที่ปลอดภัย (Secure Design)

การออกแบบระบบขนส่งทางรางที่ปลอดภัยจากภัยคุกคามทางไซเบอร์ จะต้องเริ่มต้นตั้งแต่ขั้นตอนแรกของการพัฒนา โดยใช้หลักการการออกแบบที่เน้นความปลอดภัยเป็นสำคัญ เช่น การเลือกใช้เทคโนโลยีที่สามารถป้องกันข้อมูลจากการโจมตี เช่น การเข้ารหัสข้อมูล และการควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด โดยการออกแบบจะต้องรองรับมาตรการป้องกันที่หลากหลาย รวมถึงระบบ Redundancy และ Fail-safe Mechanisms เพื่อให้ระบบขนส่งทางรางสามารถฟื้นตัว และทำงานได้ในกรณีที่เกิดการโจมตีหรือเหตุการณ์ไม่ปกติขึ้น

๓) การควบคุมการเข้าถึง (Access Control)

ระบบขนส่งทางรางต้องมีการควบคุมการเข้าถึงระบบขนส่งทางรางและข้อมูลที่สำคัญ โดยเฉพาะในพื้นที่ที่มีความเสี่ยงสูง เช่น ศูนย์ควบคุมการเดินรถหรือเครือข่ายที่เชื่อมต่อระหว่างสถานีต่าง ๆ เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าถึงข้อมูลหรือระบบที่สำคัญได้ โดยควรมีการตรวจสอบสิทธิ์การเข้าถึงด้วยระบบ Multi-Factor Authentication (MFA) เพื่อเพิ่มความปลอดภัย อีกทั้งต้องมีการตรวจสอบการเปลี่ยนแปลงสิทธิ์การเข้าถึง (Privilege Escalation) เพื่อป้องกันไม่ให้มีการเข้าถึงที่ไม่เหมาะสมหรือไม่ได้รับอนุญาต

๔) การตรวจจับและตอบสนองต่อเหตุการณ์ (Detection and Response)

ระบบต้องสามารถตรวจจับการโจมตี หรือเหตุการณ์ที่ไม่ปกติในทุกระบบที่สำคัญ เช่น ระบบควบคุมการเดินรถหรือการสื่อสารระหว่างสถานีและศูนย์ควบคุมได้อย่างรวดเร็วและแม่นยำ เพื่อให้สามารถตอบสนองต่อเหตุการณ์ได้ทันท่วงที โดยต้องมีการติดตั้งระบบการตรวจจับที่มีประสิทธิภาพ เช่น ระบบ SIEM (Security Information and Event Management) ที่สามารถรวบรวมข้อมูลจากทุกจุดที่มีความเสี่ยงเพื่อทำการวิเคราะห์เหตุการณ์และจัดการภัยคุกคามให้เร็วที่สุด รวมถึงต้องมีแผนการฟื้นฟู

หลังเหตุการณ์ (Disaster Recovery) และมีระบบที่สามารถจัดทำรายงานเหตุการณ์ไซเบอร์ เพื่อการติดตามและป้องกันในอนาคต เพื่อให้สามารถกลับสู่สภาพการทำงานปกติได้ในเวลาอันสั้น

๕) การประกันความปลอดภัยในระยะยาว (Long-term Security Assurance)

เพื่อให้ระบบขนส่งทางรางสามารถคงความปลอดภัยจากภัยคุกคามทางไซเบอร์ได้ในระยะยาว จำเป็นต้องมีการทบทวนและปรับปรุงมาตรการด้านความปลอดภัยอย่างต่อเนื่อง ตลอดอายุการใช้งานของระบบ เนื่องจากเทคโนโลยีและภัยคุกคามมีการพัฒนาและเปลี่ยนแปลงอย่างรวดเร็ว รวมถึงใช้เครื่องมือการสแกนช่องโหว่ (Vulnerability Scanning Tools) และการประเมินระบบเป็นระยะสามารถช่วยให้เราตรวจพบจุดอ่อนหรือช่องโหว่ใหม่ ๆ ที่อาจเกิดขึ้นในระบบได้ และทำการปรับปรุงหรืออัปเดตมาตรการที่จำเป็นเพื่อรักษาความปลอดภัยของระบบ

๖) การรายงานและการติดตาม (Reporting and Monitoring)

การติดตามและรายงานจะต้องมีระบบการติดตามและรายงานความปลอดภัยที่สามารถตรวจสอบและติดตามความเสี่ยงที่เกิดขึ้นในระบบขนส่งทางราง เช่น การตรวจสอบการโจมตีไซเบอร์หรือเหตุการณ์ไม่ปกติในเครือข่ายการสื่อสาร และต้องมีกระบวนการรายงานที่ชัดเจน เพื่อให้สามารถนำข้อมูลการติดตามไปใช้ในการปรับปรุงมาตรการรักษาความปลอดภัยได้อย่างมีประสิทธิภาพ รวมถึงจัดให้มีการสร้าง Incident Database ที่เก็บข้อมูลเกี่ยวกับเหตุการณ์ที่ผ่านมา เพื่อให้สามารถเรียนรู้จากเหตุการณ์ที่ผ่านมาและพัฒนามาตรการป้องกันในอนาคต

บทที่ ๓
การกำหนดคุณลักษณะความมั่นคงปลอดภัยทางไซเบอร์ และมาตรฐานขั้นต่ำ ด้านความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง

๓.๑ แนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง

การกำหนดคุณลักษณะความมั่นคงปลอดภัยทางไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง มีขั้นตอนดังต่อไปนี้

๑. รวบรวมข้อมูล และกำหนดประเภทข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศของผู้ให้บริการขนส่งทางราง

๑.๑) หน่วยงานเจ้าของข้อมูล/เจ้าของระบบของผู้ให้บริการขนส่งทางราง ดำเนินการระบุประเภทของ***ข้อมูลที่เกี่ยวข้องในแต่ละกระบวนการงานหลัก และกระบวนการย่อยของแต่ละหน่วยงาน***

๑.๒) หน่วยงานเจ้าของข้อมูล/เจ้าของระบบของผู้ให้บริการขนส่งทางราง จัดทำบัญชีข้อมูลและจัดประเภทของข้อมูลตามตัวอย่างใน ***ภาคผนวก ๑***

๑.๓) หน่วยงานเจ้าของข้อมูล/เจ้าของระบบของผู้ให้บริการขนส่งทางราง ดำเนินการระบุระบบสารสนเทศ และข้อมูลที่ถูกนำเข้า จัดเก็บ ประมวลผล และเป็นผลลัพธ์ (Output) ของระบบสารสนเทศ

๒. กำหนดระดับผลกระทบ

๒.๑) หน่วยงานเจ้าของข้อมูล/เจ้าของระบบของผู้ให้บริการขนส่งทางราง ดำเนินการประเมินระดับผลกระทบในด้านความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ตามตัวอย่างตารางที่ ๓ เกณฑ์การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น

๒.๒) หน่วยงานเจ้าของข้อมูล/เจ้าของระบบของผู้ให้บริการขนส่งทางราง ดำเนินการบันทึกระดับผลกระทบของข้อมูลแต่ละประเภท

ตารางที่ ๑ ตัวอย่างขั้นตอนการระบุประเภทข้อมูล

ประเภทข้อมูล	ระดับผลกระทบเบื้องต้นในด้านต่าง ๆ		
	ความลับ	ความถูกต้องครบถ้วน	สภาพพร้อมใช้งาน
หมวดการขนส่ง			
- ข้อมูลผู้โดยสาร	ต่ำ	กลาง	สูง
- ข้อมูลการชำระเงิน	สูง	สูง	กลาง
- ข้อมูลโปรโมชั่นและส่วนลด	ต่ำ	ต่ำ	ต่ำ
- ข้อมูลติดต่อผู้โดยสาร	สูง	สูง	สูง
- ข้อมูลตารางเวลาเดินรถ	กลาง	สูง	สูง
- ข้อมูลตำแหน่งรถไฟแบบเรียลไทม์	กลาง	สูง	สูง
- ข้อมูลเซ็นเซอร์ตรวจจับสิ่งกีดขวาง	ต่ำ	ต่ำ	ต่ำ

๓. ขั้นตอนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางราง

๓.๑) ทบทวนคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลทุกประเภทในระบบสารสนเทศ

๓.๒) กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ระบบสารสนเทศ โดยใช้หลักการเครื่องหมายระดับน้ำสูงสุด หรือ High Water Mark ตามแต่ละวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (การรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน) ซึ่งหลังจากพิจารณาระดับผลกระทบสำหรับข้อมูลทุกประเภทในระบบสารสนเทศนั้น และใช้ระดับผลกระทบสูงสุด ตามแต่ละวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

(๑) หากทุกปัจจัยอยู่ในระดับต่ำ ระบบจะถูกจัดให้อยู่ในระดับต่ำ

(๒) หากมีอย่างน้อย ๑ ปัจจัย ในระดับกลาง และไม่มีระดับสูง ระบบจะถูกจัดให้อยู่ในระดับกลาง

(๓) หากมีอย่างน้อย ๑ ปัจจัย ในระดับสูง ระบบจะถูกจัดให้อยู่ในระดับสูง

๓.๓) บันทึกการกำหนด และเหตุผลการตัดสินใจในการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางทั้งหมด

๓.๔) กำหนดให้ผู้ให้บริการขนส่งทางรางดำเนินการพิจารณาทบทวนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศทุก ๓ ปี หรือดำเนินการทบทวนเมื่อข้อมูลหรือระบบสารสนเทศ หรือหน้าที่ของผู้ให้บริการขนส่งทางรางมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ พร้อมทั้งบันทึกผลการพิจารณาทบทวน และเหตุผลในการคงไว้ หรือแก้ไขเปลี่ยนแปลงระดับผลกระทบที่อาจเกิดขึ้นของวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วย ด้านความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability)

ตารางที่ ๒ ตัวอย่างของขั้นตอนการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

ระบบสารสนเทศ	ประเภทข้อมูลที่อยู่ในระบบ	ระดับผลกระทบที่อาจเกิดขึ้น		
		ด้านการรักษาความลับ	ด้านการรักษาความถูกต้องครบถ้วน	ด้านการรักษาสภาพพร้อมใช้งาน
ระบบซื้อตั๋วออนไลน์	ข้อมูลผู้โดยสาร	สูง	กลาง	สูง
	ข้อมูลการชำระเงิน	สูง	สูง	กลาง
	ข้อมูลโปรโมชั่นและส่วนลด	ต่ำ	กลาง	สูง
	สรุประดับผลกระทบ (High watermark)	**สูง**	**สูง**	**สูง**
	ระดับผลกระทบต่อระบบสารสนเทศโดยรวม : สูง			
ระบบควบคุมการเดินรถ	ข้อมูลตารางเวลาเดินรถ	กลาง	กลาง	กลาง
	ข้อมูลตำแหน่งรถไฟแบบเรียลไทม์	ต่ำ	กลาง	กลาง
	ข้อมูลเซ็นเซอร์ตรวจจับสิ่งกีดขวาง	ต่ำ	กลาง	กลาง
	สรุประดับผลกระทบ (High watermark)	**กลาง**	**กลาง**	**กลาง**
	ระดับผลกระทบต่อระบบสารสนเทศโดยรวม : กลาง			
ระบบจัดการข้อมูลลูกค้า	ข้อมูลติดต่อผู้โดยสาร	ต่ำ	ต่ำ	ต่ำ
	สรุประดับผลกระทบ (High watermark)	**ต่ำ**	**ต่ำ**	**ต่ำ**
	ระดับผลกระทบต่อระบบสารสนเทศโดยรวม : ต่ำ			

ตารางที่ ๓ เกณฑ์การประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objective)	ผลกระทบที่อาจเกิดขึ้น (Potential impact)		
	ระดับต่ำ (Low)	ระดับกลาง (Medium)	ระดับสูง (High)
ด้านการรักษาความลับ (Confidentiality)	๑. ***ไม่มีผลกระทบหรือผลกระทบต่ำมาก*** เนื่องจากระบบ และ/หรือ ข้อมูล และ/หรือ บริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางรางสามารถถูกเปิดเผยและเข้าถึงได้จากสาธารณะ	๑. หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาตจะส่งผลให้เกิดความเสียหายกับงานบริการที่สำคัญ หรือระบบงานที่สำคัญขององค์กร ***แต่ยังสามารถให้บริการได้ หรือการให้บริการช้าลง*** หรือ ๒. ทำให้ข้อมูล***ระดับชั้น “ลับ” หรือ “ใช้ภายในเท่านั้น”*** ขององค์กรถูกเปิดเผย	๑. หากสามารถเข้าถึงหรือใช้งานโดยไม่ได้รับอนุญาต จะส่งผลให้เกิดความเสียหายกับบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***ทำให้ไม่สามารถให้บริการได้*** หรือ ๒. ทำให้ข้อมูล***ระดับชั้น “ลับที่สุด” “ลับมาก”*** ขององค์กรถูกเปิดเผย
ด้านความถูกต้องครบถ้วน (Integrity)	ระบบทำงานหรือประมวลผลข้อมูลผิดพลาด หรือเป็นข้อมูลที่ไม่ถูกต้อง ***แต่ไม่ส่งผลกระทบต่อการให้บริการ***	ระบบทำงานหรือประมวลผลข้อมูลผิดพลาดหรือเป็นข้อมูลที่ไม่ถูกต้องจะส่งผลกระทบกับบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***แต่ยังสามารถให้บริการได้ หรือการให้บริการช้าลง หรือสามารถให้บริการในรูปแบบอื่นทดแทนได้***	ทรัพย์สินนั้นทำงานหรือประมวลผลข้อมูลผิดพลาด หรือเป็นข้อมูลที่ไม่ถูกต้องจะส่งผลกระทบต่อบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***ทำให้ไม่สามารถดำเนินการได้อย่างถูกต้องครบถ้วน***
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	๑. ระบบ และ/หรือ ข้อมูลไม่พร้อมใช้งาน ส่งผลกระทบต่อการบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***ทำให้การให้บริการล่าช้า และกระทบต่อผู้ใช้งานไม่เกินหนึ่งหมื่นคน*** หรือ ๒. ทำให้องค์กรต้อง***สูญเสียเงินหรือรายได้จำนวนไม่เกิน หนึ่งล้านบาท***	๑. ระบบ และ/หรือ ข้อมูลไม่พร้อมใช้งานจะส่งผลกระทบต่อบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***ทำให้การให้บริการล่าช้า และกระทบต่อผู้ใช้งานเกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน*** หรือ ๒. ทำให้องค์กรต้อง***สูญเสียเงินหรือรายได้จำนวนไม่เกิน หนึ่งร้อยล้านบาท***	๑. ระบบ และ/หรือ ข้อมูลไม่พร้อมใช้งานจะส่งผลกระทบต่อบริการที่สำคัญ หรือระบบงานที่สำคัญของผู้ให้บริการขนส่งทางราง ***ทำให้ไม่สามารถให้บริการได้ และกระทบต่อการใช้ชีวิตประจำวันของผู้ใช้บริการเกินกว่าหนึ่งแสนคน หรือเป็นอันตรายต่อชีวิตตั้งแต่หนึ่งคนขึ้นไป*** หรือ ๒. ทำให้องค์กรต้อง***สูญเสียเงินหรือรายได้จำนวน เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป***

๓.๒ แนวทางการกำหนดมาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์

หลังจากหน่วยงานผู้ให้บริการขนส่งทางรางได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ ซึ่งพิจารณาจากวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ในเรื่องการรักษาความลับ การรักษาความถูกต้องครบถ้วน และการรักษาสภาพพร้อมใช้งาน และได้ระดับผลกระทบที่อาจเกิดขึ้นตามวัตถุประสงค์แต่ละเรื่องเป็นระดับต่ำ ระดับกลาง หรือระดับสูง ตามแนวทางการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศแล้ว ให้หน่วยงานผู้ให้บริการขนส่งทางรางกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศในแต่ละระดับ ***ตามประกาศกรอบมาตรฐาน และประมวลแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสำหรับผู้ให้บริการขนส่งทางราง*** โดยพิจารณาจากคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ดังต่อไปนี้

(๑) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **“ระดับต่ำ”** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อต่อไปนี้

(A) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)

(B) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

(C) การจัดการทรัพย์สิน (Asset Management)

(D) การควบคุมการเข้าถึง (Access Control)

(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

(๒) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **“ระดับกลาง”** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศให้ดำเนินการตาม (๑) ตั้งแต่ข้อ (A) ถึง (I) และกำหนดมาตรการเพิ่มเติม ดังนี้

(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)

(K) การเชื่อมต่อระยะไกล (Remote Connection)

(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

(๓) ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **“ระดับสูง”** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศให้ดำเนินการตาม (๑) และ (๒) ตั้งแต่ข้อ (A) ถึง (L) รวมถึงกำหนดมาตรการเพิ่มเติม ดังนี้

(M) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

(N) การจัดการผู้ให้บริการภายนอก (Third Party Management)

(O) การแบ่งปันข้อมูล (Information Sharing)

(P) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๓.๓ การจำแนกหมวดหมู่ภัยคุกคามทางไซเบอร์

หลังจากหน่วยงานผู้ให้บริการขนส่งทางรางได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล หรือระบบสารสนเทศ รวมถึงได้กำหนดมาตรการขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศที่มีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในแต่ละระดับแล้วนั้น หากเกิดภัยคุกคามทางไซเบอร์ขึ้น ผู้ให้บริการขนส่งทางรางต้องดำเนินการ ดังนี้

๑) ดำเนินการจำแนกหมวดหมู่ภัยคุกคามทางไซเบอร์ ตามตาราง ดังนี้

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๙	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

๒) กำหนดลักษณะของภัยคุกคามทางไซเบอร์ โดยแบ่งออกเป็น ๓ ระดับ ได้แก่

(๑) ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง หมายถึง ภัยคุกคามทางไซเบอร์ที่มีความเสี่ยงอย่างมีนัยสำคัญถึงระดับที่ทำให้ระบบคอมพิวเตอร์ของหน่วยงานผู้ให้บริการขนส่งทางรางมีประสิทธิภาพลดลง

(๒) ภัยคุกคามทางไซเบอร์ในระดับร้ายแรง หมายถึง ภัยคุกคามที่มีลักษณะการเพิ่มขึ้นอย่างมีนัยสำคัญของการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ หรือข้อมูลคอมพิวเตอร์ โดยมุ่งหมายเพื่อโจมตีการให้บริการของผู้ให้บริการขนส่งทางราง และการโจมตีนั้น มีผลทำให้ระบบคอมพิวเตอร์ หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับการให้บริการของผู้ให้บริการขนส่งทางรางไม่สามารถทำงาน หรือให้บริการได้

(๓) ภัยคุกคามทางไซเบอร์ในระดับวิกฤต หมายถึง ภัยคุกคามทางไซเบอร์ที่มีลักษณะดังต่อไปนี้

(ก) เป็นภัยคุกคามทางไซเบอร์ที่เกิดจากการโจมตีระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ในระดับที่สูงขึ้นกว่าภัยคุกคามทางไซเบอร์ในระดับร้ายแรง โดยส่งผลกระทบรุนแรงต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการขนส่งทางราง ในลักษณะที่เป็นวงกว้าง จนทำให้การทำงานของผู้ให้บริการขนส่งทางรางที่ให้กับประชาชนล้มเหลวทั้งระบบ จนไม่สามารถควบคุมการทำงานส่วนกลางของระบบคอมพิวเตอร์ได้ หรือการใช้มาตรการเยียวยาตามปกติในการแก้ไขปัญหาภัยคุกคามไม่สามารถแก้ไขปัญหาได้ และมีความเสี่ยงที่จะลุกลามไปยังโครงสร้างพื้นฐานสำคัญอื่น ๆ ของประเทศ ซึ่งอาจมีผลทำให้บุคคลจำนวนมากเสียชีวิตหรือระบบคอมพิวเตอร์ คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์จำนวนมากถูกทำลายเป็นวงกว้างในระดับประเทศ

(ข) เป็นภัยคุกคามทางไซเบอร์อันกระทบ หรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศ หรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขันหรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบ หรือการสงคราม ซึ่งจำเป็นต้องมีมาตรการเร่งด่วน เพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุขตามรัฐธรรมนูญแห่งราชอาณาจักรไทย เอกราชและบูรณภาพแห่งอาณาเขต ผลประโยชน์ของชาติ การปฏิบัติตามกฎหมาย ความปลอดภัยของประชาชน การดำรงชีวิตโดยปกติสุข ของประชาชน การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย หรือประโยชน์ส่วนรวม หรือการป้องปัด หรือแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

๓) รายงานภัยคุกคามทางไซเบอร์ไปยังหน่วยงานกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยดำเนินการ ดังนี้

(๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของผู้ให้บริการขนส่งทางรางให้ดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้องของข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ รวมถึงพฤติการณ์แวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือไม่ และเป็นภัยคุกคามระดับใด หากตรวจพบต้องดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตามแนวปฏิบัติแผนการรับมือภัยคุกคามทางไซเบอร์ และดำเนินการรายงานไปยังกรมการขนส่งทางราง โดยใช้เอกสาร ก๑ ข้อมูลที่ต้องแจ้งโดยอ้างอิงระยะเวลาการแจ้งและรายงานตามข้อ (๓)

(๒) ในกรณีที่มีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของผู้ให้บริการขนส่งทางรางให้จัดทำและส่งรายงานเหตุภัยคุกคามทางไซเบอร์ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และกรมการขนส่งทางราง โดยอ้างอิงระยะเวลาการแจ้งและรายงานตามข้อ (๓) หลังจากการตรวจพบ หรือเกิดภัยคุกคามทางไซเบอร์ โดยใช้เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

(๓) ดำเนินการแจ้ง หรือรายงานภัยคุกคามทางไซเบอร์ ตามระยะเวลา ดังนี้

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้กรมการขนส่งทางราง (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๒	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๓	ทุกเหตุการณ์	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๔	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๘ ชั่วโมง
๕	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๖	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๒๐ นาที	๑ ชั่วโมง	๒ ชั่วโมง
	ไม่ร้ายแรง	๓๐ นาที	๒ ชั่วโมง	๔ ชั่วโมง
๗	วิกฤต	๑๐ นาที	๓๐ นาที	๑ ชั่วโมง
	ร้ายแรง	๑๐ นาที	๑ ชั่วโมง	๑ ชั่วโมง

หมวดหมู่ภัยคุกคามทางไซเบอร์	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้กรมการขนส่งทางราง (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
	ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๘ ชั่วโมง**
๘	-	**๒๐ นาที**	**หลังจากสืบสวนเสร็จภายใน ๒ ชม.**	**หลังจากสืบสวนเสร็จภายใน ๔ ชม.**
๙	-	-	**๔ ชั่วโมง**	**๑๒ ชั่วโมง**

(๔) จัดทำรายงานประจำปี และส่งรายงานให้สำนักงาน และกรมการขนส่งทางราง ภายในวันที่ ๓๑ มกราคม ของปีถัดไป โดยรายงานต้องมีรายละเอียดดังต่อไปนี้

(ก) ระบุจำนวนและลักษณะของเหตุการณ์ภัยคุกคามทางไซเบอร์ของหน่วยงานผู้ให้บริการขนส่งทางราง ตามเอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบ (๑) ปี

(ข) วิเคราะห์สาเหตุ หรือผลกระทบที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(ค) ปัญหา และอุปสรรคในการดำเนินงาน

(ง) ข้อเสนอแนะต่าง ๆ ซึ่งรวมถึงข้อเสนอแนะเชิงนโยบาย

บทที่ ๔
การกำกับดูแลการรักษาความมั่นคงปลอดภัยไซเบอร์ (Good Governance in Cybersecurity)

๑. ผู้ให้บริการขนส่งทางราง ควรพิจารณาจัดโครงสร้างองค์กรให้มีการถ่วงดุล โดยกำหนดอำนาจ บทบาทหน้าที่ และความรับผิดชอบ (Authorities, Roles and Responsibilities) ที่ชัดเจนเกี่ยวกับการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ ให้มีการถ่วงดุลตามหลักการควบคุม กำกับ และตรวจสอบ (Three Lines of Defense) โดยจัดให้มีผู้ที่ทำหน้าที่ควบคุม กำกับ และตรวจสอบที่เป็นอิสระและสามารถทำหน้าที่ได้อย่างมีประสิทธิผล ซึ่งควรประกอบด้วย

๑) ผู้ก่อให้เกิดความเสี่ยงและควบคุมความเสี่ยงในชั้นแรก (Business Unit หรือ First Line of Defense) มีหน้าที่ดูแลและปฏิบัติงานให้เป็นไปตามกฎเกณฑ์ที่กำหนดไว้ มีการควบคุมภายใน และมีการจัดการความเสี่ยงอย่างเหมาะสม

๒) หน่วยงานหรือผู้กำกับภายใน (Second Line of Defense) เช่น หน่วยงานบริหารความเสี่ยง (Risk Management) หน่วยงานกำกับการปฏิบัติตามกฎเกณฑ์ (Compliance)

๓) หน่วยงานหรือผู้ตรวจสอบภายใน (Internal Audit หรือ Third Line of Defense) เพื่อส่งเสริมให้มีกลไกการตรวจสอบและถ่วงดุลที่เหมาะสม

๒. หน่วยงานผู้ให้บริการขนส่งทางรางต้องกำหนดให้มีผู้รับผิดชอบบริหารจัดการความมั่นคงปลอดภัยสารสนเทศ โดยจัดให้มีผู้บริหารที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) หรือเทียบเท่า โดยบุคคลดังกล่าวต้องเป็นผู้ที่มีความรู้ หรือประสบการณ์ด้านเทคโนโลยีสารสนเทศ การบริหารความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือกับภัยคุกคามทางไซเบอร์

ทั้งนี้ ผู้บริหารที่ทำหน้าที่ดังกล่าว ควรมีความเป็นอิสระจากงานด้านการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) รวมทั้งควรมีบทบาทหน้าที่ และความรับผิดชอบให้หน่วยงานดำเนินการ เพื่อความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศอย่างน้อย ดังนี้

๑) กำหนดให้มีนโยบาย มาตรฐาน และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งดูแลให้มีการปฏิบัติตามนโยบาย มาตรฐาน และแนวทางที่กำหนด

๒) มีข้อกำหนดด้านความมั่นคงปลอดภัย (Security Specification) และสถาปัตยกรรมด้านความมั่นคงปลอดภัย (IT Security Architecture)

๓) บริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ให้สอดคล้องกับความเสี่ยงที่องค์กรมี และรายงานนำเสนอความเสี่ยงต่อคณะกรรมการหน่วยงานหรือคณะกรรมการบริหารจัดการความเสี่ยงขององค์กรอย่างสม่ำเสมอเป็นวาระประจำ

๔) ดูแลและดำเนินการให้หน่วยงานมีความพร้อมในการรับมือภัยคุกคามทางไซเบอร์

๕) ดูแลและดำเนินการให้บุคลากรในองค์กรมีความรู้และความตระหนักรู้ เรื่องความเสี่ยง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศด้านภัยคุกคามทางไซเบอร์

๓. หน่วยงานผู้ให้บริการขนส่งทางรางต้องจัดให้มีผู้บริหารระดับสูง ที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงานผู้ให้บริการขนส่งทางราง

ทั้งนี้ ผู้บริหารระดับสูงที่ทำหน้าที่ที่ปฏิบัติหน้าที่ดังกล่าวควรเป็นอิสระจากงานด้านการปฏิบัติงานเทคโนโลยีสารสนเทศ (IT operation) และงานด้านพัฒนาระบบเทคโนโลยีสารสนเทศ (IT development) และมีอำนาจหน้าที่ (Authority) เพียงพอในการปฏิบัติงานในหน้าที่ CISO ได้อย่างมีประสิทธิภาพและประสิทธิผล โดยสามารถดำเนินการอย่างน้อย ดังนี้

๑) ดำเนินการรายงานปัญหา หรือเหตุการณ์ที่มีนัยสำคัญด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ต่อผู้บริหารในตำแหน่งสูงสุด คณะกรรมการของหน่วยงานผู้ให้บริการขนส่งทางราง และคณะกรรมการที่เกี่ยวข้องโดยตรง

๒) ดำเนินการให้ความเห็นด้านภัยคุกคามทางไซเบอร์ และการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัย ด้านเทคโนโลยีสารสนเทศต่อคณะกรรมการของหน่วยงานผู้ให้บริการขนส่งทางราง คณะกรรมการที่เกี่ยวข้องกับการบริหารจัดการ และกำกับดูแลการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ เช่น IT steering committee หรือ IT risk committee และร่วมตัดสินใจดำเนินการในเรื่องความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และด้านภัยคุกคามทางไซเบอร์ที่กระทบต่อหน่วยงานผู้ให้บริการขนส่งทางรางอย่างมีนัยสำคัญ

๔. หน่วยงานผู้ให้บริการขนส่งทางรางต้องแจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการพร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาสามสิบ (๓๐) นาที เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน และกรมการขนส่งทางราง

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานและกรมการขนส่งทางรางทราบภายในระยะเวลาสิบห้า (๑๕) วัน นับแต่วันที่มีการเปลี่ยนแปลง

๕. หน่วยงานผู้ให้บริการขนส่งทางรางต้องแจ้งรายชื่อหน่วยงานภายใน หรือบุคคลที่เป็นเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ พร้อมด้วยข้อมูลการติดต่อที่สามารถติดต่อได้ในกรณีมีเหตุฉุกเฉินภายในระยะเวลาสามสิบ (๓๐) นาที ไปยังสำนักงาน กรมการขนส่งทางราง และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยบุคคลดังกล่าวต้องเป็นบุคคลผู้ซึ่งรับผิดชอบในการบริหารงานของหน่วยงานผู้ให้บริการขนส่งทางราง

ทั้งนี้ ในกรณีที่มีการเปลี่ยนแปลงข้อมูล ให้แจ้งรายชื่อหรือข้อมูลการติดต่อที่เปลี่ยนแปลงให้สำนักงานกรมการขนส่งทางราง และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ก่อนการเปลี่ยนแปลงล่วงหน้าไม่น้อยกว่า ๗ วัน เว้นแต่มีเหตุจำเป็นอันไม่อาจล่วงรู้ได้ให้แจ้งภายในระยะเวลาสิบห้า (๑๕) วัน นับแต่วันที่มีการเปลี่ยนแปลง

การเปลี่ยนแปลงข้อมูลให้รวมถึงการดำเนินการที่มีผลเป็นการเปลี่ยนแปลงเจ้าของกรรมสิทธิ์ ผู้ครอบครองคอมพิวเตอร์ และผู้ดูแลระบบคอมพิวเตอร์ของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การเปลี่ยนแปลงหน่วยงานต้นสังกัดของหน่วยงานผู้ให้บริการขนส่งทางราง การยุบ หรือควบรวมกิจการ การเพิ่มหน่วยงานย่อยภายในหน่วยงานผู้ให้บริการขนส่งทางราง

บทที่ ๕
ประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง

ผู้ให้บริการขนส่งทางราง ดำเนินการจัดทำประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของตน พร้อมทั้งจัดให้มีการทบทวน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ โดยพิจารณารายละเอียดประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับผู้ให้บริการขนส่งทางราง อย่างน้อยดังนี้

๕.๑ มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ มีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับต่ำ

ในกรณีที่ข้อมูลหรือระบบสารสนเทศของผู้ให้บริการขนส่งทางรางมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **“ระดับต่ำ”** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ ตามหัวข้อต่อไปนี้

(A) แนวทางการประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

เพื่อให้ผู้ให้บริการขนส่งทางรางสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง กรมการขนส่งทางราง จึงกำหนดกรอบแนวปฏิบัติการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อเป็นกรอบในการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และเพื่อให้การดำเนินการเป็นไปตามหลักการ โดยครอบคลุมกระบวนการอย่างน้อยในเรื่องดังต่อไปนี้

๑. กำหนดบริบทของความเสี่ยง (Establish Risk Context) ประกอบด้วย

๑) กำหนดคำนิยามความเสี่ยง (Define Risk) โดยพิจารณาดังนี้

- เหตุการณ์ภัยคุกคาม (Threat Event) หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ภัยคุกคาม (Threat Vector) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตรายในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures: TTP) ที่ใช้โดยผู้คุกคาม
- ผู้คุกคาม หมายถึง บุคคลหรือหน่วยงานที่รับผิดชอบต่อเหตุการณ์ที่อาจก่อให้เกิดอันตราย
- เวกเตอร์ภัยคุกคาม หมายถึง เส้นทางที่ผู้คุกคามใช้เพื่อโจมตีเป้าหมาย โดยระบุจุดทั้งหมด ที่สามารถเข้าถึงระบบคอมพิวเตอร์ หรือเครือข่าย
- ช่องโหว่ (Vulnerability) หมายถึง จุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สิน หรือการควบคุมภายในของกระบวนการ
- ผลกระทบที่อาจเกิดขึ้น (Impact) หรือความรุนแรง (Severity) หมายถึง ขนาด หรือระดับของความอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ หรือชุดของช่องโหว่ ความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคลที่เกี่ยวข้องกับหน่วยงานผู้ให้บริการขนส่งทางรางทั้งภายในและภายนอก

- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) คือ ความไม่แน่นอน โดยรวมที่หน่วยงานผู้ให้บริการขนส่งทางรางยอมรับได้ โดยการดำเนินการตามภาระหน้าที่ความรับผิดชอบยังคงดำเนินการได้บรรลุตามเป้าหมาย
- ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) หมายถึง ขอบเขตของความเบี่ยงเบนที่ยอมรับได้จากเป้าหมายที่ตั้งไว้ หรือจากระดับความเสี่ยงที่กำหนดตาม Risk Appetite
- แนวโน้มหรือโอกาส (Likelihood) หมายถึง แนวโน้มหรือโอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ โดยใช้ประโยชน์จากช่องโหว่ที่มีอยู่ หรือชุดของช่องโหว่ ซึ่งความน่าจะเป็นนี้สามารถประมาณการได้จากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

๒) กำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Determine Risk Appetite) ควรกำหนดให้มีความชัดเจน ดังนี้

- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) เป็นการกำหนดระดับความเสี่ยงที่หน่วยงานผู้ให้บริการขนส่งทางรางยอมรับในการดำเนินงาน ซึ่งอาจพิจารณาจาก วัตถุประสงค์ พันธกิจ หรือวัฒนธรรมความเสี่ยง (Risk Culture) ของหน่วยงานผู้ให้บริการขนส่งทางราง
- ขีดแบ่งความเสี่ยงที่ไม่สามารถยอมรับได้ (Risk Threshold) เป็นการกำหนดเกณฑ์ที่เป็นเส้นแบ่งของความเสี่ยงที่ยอมรับได้ และยอมรับไม่ได้สำหรับความเสี่ยงด้านต่าง ๆ เกณฑ์เหล่านี้กำหนดจุดที่ความเสี่ยงไม่สามารถยอมรับได้ และต้องมีการดำเนินการเพื่อจัดการความเสี่ยงที่เกิดขึ้น
- คำชี้แจงความเสี่ยงด้านความมั่นคงปลอดภัยที่ยอมรับได้ (Risk Appetite Statement) เป็นการจัดทำข้อความที่ชัดเจนและรัดกุมซึ่งแสดงถึงความมุ่งมั่นของหน่วยงานผู้ให้บริการขนส่งทางรางที่จะยอมรับความเสี่ยงในด้านต่าง ๆ เช่น ความมั่นคงปลอดภัยทางไซเบอร์ การปกป้องข้อมูล หรือความมั่นคงปลอดภัยทางกายภาพ

ตัวอย่าง กำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Determine Risk Appetite) ของหน่วยงานผู้ให้บริการขนส่งทางราง

- คำชี้แจงความเสี่ยงด้านความมั่นคงปลอดภัย “ในฐานะที่ผู้ให้บริการขนส่งทางรางมีหน้าที่ให้บริการระบบขนส่งทางรางของประเทศไทย” จึงมีความเข้าใจและมุ่งมั่นถึงความสำคัญของข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชนผู้ใช้บริการระบบขนส่งทางราง จึงมีการกำหนดระดับความเสี่ยงที่ยอมรับได้ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยที่อาจส่งผลต่อความมั่นคงปลอดภัยของข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชนผู้ใช้บริการระบบขนส่งทางรางในระดับต่ำ”
- ระดับความเสี่ยงที่ยอมรับได้ของผู้ให้บริการขนส่งทางรางซึ่งกำหนดระดับความเสี่ยงที่ยอมรับได้เป็น “ระดับต่ำ” ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยต่อข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชนผู้ใช้บริการระบบขนส่งทางราง
- ระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) ของผู้ให้บริการขนส่งทางราง ซึ่งกำหนดระดับความเสี่ยงที่ยอมให้เบี่ยงเบนได้ (Risk Tolerance) เป็น “ระดับปานกลาง” ต่อเหตุการณ์ด้านความมั่นคงปลอดภัยต่อข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชนผู้ใช้บริการระบบขนส่งทางราง และต้องการดำเนินการกำหนดมาตรการในการควบคุมความเสี่ยงไม่ให้มีระดับที่สูงขึ้น

- การกำหนดเกณฑ์ขีดแบ่งความเสี่ยง ที่ไม่สามารถยอมรับได้สำหรับเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ดังนี้

- การละเมิดการรักษาความมั่นคงปลอดภัยของผู้ให้บริการขนส่งทางรางที่อาจนำไปสู่การเข้าถึงพื้นที่รักษาความมั่นคงปลอดภัยโดยไม่ได้รับอนุญาต ถือว่าไม่สามารถยอมรับได้

- การโจมตีทางไซเบอร์ใด ๆ ที่ส่งผลกระทบต่อข้อมูลที่เกี่ยวข้องกับการให้บริการประชาชนผู้ใช้บริการระบบขนส่งทางรางทำให้ข้อมูลรั่วไหล หรือถูกเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ถือว่าไม่สามารถยอมรับได้

- การดำเนินการลดความเสี่ยง ใช้การควบคุมการเข้าถึงที่เข้มงวดขั้นตอนการคัดกรองความมั่นคงปลอดภัยมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ รวมถึงข้อกำหนดเรื่องการตอบสนองเหตุฉุกเฉิน สำหรับระบบที่เกี่ยวข้องกับการให้บริการ ๔ บริการที่สำคัญ ดังนี้

๑. บริการขายตั๋วและสำรองที่นั่ง (ระบบขายตั๋วและจองตั๋ว)

๒. บริการที่เกี่ยวข้องกับการส่งสัญญาณ การสื่อสาร และการส่งข้อมูล (เกี่ยวกับระบบ signaling ในการเดินรถ)

๓. บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง (ระบบที่ใช้ควบคุมการเดินรถจากส่วนกลางของโอเปอเรเตอร์แต่ละราย (OCC หรือ CTC))

๔. บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแลและเก็บข้อมูล (ระบบ SCADA และ OT ที่เป็นระบบที่ควบคุมตัวสถานีทั้งหมด เช่น แอร์ บันไดเลื่อน กล้องวงจรปิด ระบบป้ายต่าง ๆ ที่เป็นดิจิทัลควบคุมด้วยคอมพิวเตอร์)

๓) กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

ดำเนินการกำหนดบทบาทและความรับผิดชอบของผู้ที่เกี่ยวข้องในการประเมินความเสี่ยงให้ชัดเจน เพื่อให้ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องตระหนักถึงบทบาทหน้าที่ที่ได้รับ ซึ่งควรพิจารณาอย่างน้อยดังนี้

- หัวหน้าหน่วยงาน (Head of Organization) มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้

- เจ้าของกระบวนการธุรกิจ (Business Owner) มีหน้าที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากิจกรรมตามภาระหน้าที่บรรลุเป้าหมาย รวมถึงระบุข้อกังวลเกี่ยวกับผลกระทบที่มีต่อการดำเนินการตามภารกิจหน้าที่ในกรณีที่ระบบมีการหยุดชะงัก

- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการเกี่ยวกับการบริหารความเสี่ยง (Risk Management Function) มีหน้าที่รับผิดชอบในการบริหารความเสี่ยงทั้งหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงทำหน้าที่เป็นหน่วยงานเชื่อมระหว่างฝ่ายงานอื่น ๆ ของหน่วยงานผู้ให้บริการขนส่งทางรางในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการด้านเทคโนโลยีและด้านการปฏิบัติ (Technology and Operations Function) มีหน้าที่รับผิดชอบในการบำรุงรักษาและปฏิบัติการเกี่ยวกับ

โครงสร้างพื้นฐาน ทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชันที่สนับสนุนการทำงานของระบบหรือกิจกรรมตามภารกิจของหน่วยงานผู้ให้บริการขนส่งทางราง

- ผู้รับผิดชอบ หรือผู้ที่ได้รับมอบหมายดำเนินการด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function) มีหน้าที่รับผิดชอบในการดำเนินการเกี่ยวกับการบำรุงรักษา และควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง และทำหน้าที่ระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ รวมถึงพิจารณาสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสม เพื่อจัดการกับภัยคุกคามหรือการโจมตี

๒. ดำเนินการประเมินความเสี่ยง (Conduct Risk Assessment)

๑) การประเมินความเสี่ยง (Risk assessment)

(๑) การระบุความเสี่ยง (Risk identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าว อาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก โดยสามารถพิจารณาระบุความเสี่ยง (Risk Identification) ดังนี้

๑) ระบุทรัพย์สิน (Identify Asset) ดำเนินการระบุและสร้างทะเบียนทรัพย์สินทั้งหมดที่เป็นส่วนประกอบของระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง โดยต้องมีการบันทึกรายการทรัพย์สิน ดังนี้

- ทรัพย์สินสำคัญ ซึ่งเป็นทรัพย์สินที่มีความสำคัญต่อการบรรลุวัตถุประสงค์หลักในการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง
- ทรัพย์สินที่เกี่ยวข้อง เป็นทรัพย์สินที่ผู้โจมตีต้องการควบคุม และใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ เช่น ในระบบวินโดวส์เครื่องแม่ข่ายที่เป็นระบบบริหารจัดการจากศูนย์กลาง (Active Directory: AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลการรับรองการเข้าสู่ระบบของผู้ใช้งาน
- ดำเนินการสร้างแผนผังสถาปัตยกรรมเครือข่ายที่แสดงให้เห็นถึงภาพของเส้นทางการเชื่อมต่อและการสื่อสารระหว่างทรัพย์สินสำคัญ และทรัพย์สินที่เกี่ยวข้อง และระบุช่องทางการเข้าถึง (Entry Point) ทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์ หรือเครือข่ายของทรัพย์สินสำคัญ และทรัพย์สินที่เกี่ยวข้อง

๒) สร้างแบบจำลองภัยคุกคามทางไซเบอร์ (Threat Modeling)

ดำเนินการระบุเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นจากการที่ผู้ไม่ประสงค์ดีสามารถใช้ประโยชน์จากช่องโหว่ของทรัพย์สินแต่ละรายการ เพื่อทำการวิเคราะห์เชิงลึกทางเทคนิค โดยการสร้างแบบจำลองภัยคุกคามทางไซเบอร์มีขั้นตอนต่อไปนี้

- การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition)
- การระบุภัยคุกคามทางไซเบอร์ (Threat Identification) เป็นการระบุเหตุการณ์ที่เป็นไปได้ ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

- การสร้างแบบจำลองการโจมตี (Attack Modelling) โดยระบุเหตุการณ์ภัยคุกคามทางไซเบอร์ หรือแนวทางการบุกรุกของผู้โจมตีที่เป็นไปได้ให้กับทรัพย์สินแต่ละรายการแล้ว

๓) สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

เป็นการพิจารณาถึงสถานการณ์ที่อาจมีสิ่งผิดปกติเกิดขึ้น การสมมติสถานการณ์เหล่านี้ควรจะใกล้เคียงความเป็นจริง และเหมาะสมกับบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง สภาพแวดล้อมของระบบ และภัยคุกคามทางไซเบอร์ที่เกี่ยวข้อง โดยการสร้างสถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้

- ทรัพย์สิน (Asset) คือ ทรัพย์สินที่ได้รับการระบุใน ๑) ระบุทรัพย์สิน (Identify Asset)
- เหตุการณ์ภัยคุกคามทางไซเบอร์ (Threat Event) คือ เหตุการณ์การโจมตีที่ระบุใน ๒) สร้างแบบจำลองภัยคุกคามทางไซเบอร์ (Threat Modeling)
- ช่องโหว่ (Vulnerability) คือ จุดอ่อนในทรัพย์สิน หรือกระบวนการสนับสนุนการทำงานที่ผู้ไม่ประสงค์ดีสามารถใช้ช่องโหว่เหล่านั้นในการโจมตีหรือเข้าถึงทรัพย์สินได้ ซึ่งช่องโหว่นี้อาจทราบได้จากการตรวจสอบ (Audit) และหรือการทดสอบการเจาะระบบ หรือจากสภาพแวดล้อมของการใช้งานเทคโนโลยีหรือกระบวนการปฏิบัติงาน
- ผลที่ตามมา (Consequence) คือ ผลลัพธ์โดยตรงที่เกิดจากเหตุภัยคุกคามทางไซเบอร์

ตัวอย่าง เหตุการณ์ความเสี่ยง (Risk Scenario) ของการโจมตีแบบฟิชชิ่ง

- ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้ที่ไม่สังเกต ซึ่งเมื่อผู้ใช้คลิกอีเมล แล้วทำให้บัญชีผู้ใช้ดำเนินการตรวจสอบสิทธิ์ SMB กับเครื่องแม่ข่ายที่เป็นอันตรายและเปิดเผยข้อมูลสิ่งที่ใช้รับรองตัวตน

ตัวอย่าง เหตุการณ์ความเสี่ยง (Risk Scenario) ของการโจมตีแบบ SQL

- ผู้โจมตีทำการแทรก SQL บนเว็บแอปพลิเคชันเก่าที่ไม่ได้แพตช์ เพื่อสร้างโหลดเกินความจำเป็นให้กับฐานข้อมูล ทำให้ฐานข้อมูลและเว็บแอปพลิเคชันทำงานช้าลง หรือหยุดการให้บริการโดยสิ้นเชิง

(๒) การวิเคราะห์ความเสี่ยง (Risk analysis)

ดำเนินการวิเคราะห์ความเสี่ยงโดยวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์ เพื่อดำเนินการ

๑) กำหนดแนวโน้ม หรือโอกาสของสถานการณ์ความเสี่ยง (Determine Likelihood) โดยประเมินความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรพิจารณาจากในแง่ของภัยคุกคามและช่องโหว่ โดยพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- ความสามารถในการค้นพบ (Discoverability) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตี จะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ซึ่งความสามารถในการค้นพบมักขึ้นอยู่กับการเปิดเผยหรือมีข้อมูล เผยแพร่เกี่ยวกับช่องโหว่และทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตีจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ทั้งนี้ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคในการโจมตี
- ความสามารถในการทำซ้ำ (Reproducibility) เป็นปัจจัยที่ใช้พิจารณาว่าผู้โจมตีจะสามารถ ทำการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด ซึ่งขึ้นอยู่กับความซับซ้อนของการปรับแต่งวิธีการใช้ประโยชน์ จากช่องโหว่และสภาพแวดล้อมในการดำเนินการโจมตี

ตัวอย่างดังตาราง

ระดับ โอกาสที่จะเกิด	ไม่มีนัยสำคัญ หรือ ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก (๕)
(๑) เปอร์เซ็นต์โอกาสที่อาจจะเกิดเหตุการณ์ความเสี่ยง	เกิดขึ้นได้ยากมาก (น้อยกว่า ๑๐%)	มีโอกาสเกิดขึ้นน้อย (๑๑% - ๒๕%)	มีโอกาสเกิดขึ้นได้ในบางครั้ง (๒๖% - ๕๐%)	มีโอกาสเกิดขึ้นค่อนข้างสูง (๕๑% - ๗๕%)	มีโอกาสเกิดขึ้นสูง (มากกว่า ๗๕%)
(๒) โอกาสที่อาจจะเกิดเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ	เหตุการณ์ผิดปกตินี้ไม่เคยเกิดขึ้นเลย หรือคาดว่ามากกว่า ๓ ปี จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือ คาดว่าภายใน ๓ ปี จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือคาดว่าภายใน ๑ ปี จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือคาดว่าภายใน ๑ เดือน จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง	เคยเกิดเหตุการณ์ผิดปกติขึ้นแล้ว หรือคาดว่าภายใน ๑ สัปดาห์ จะมีโอกาสเกิดขึ้น >= ๑ ครั้ง
(๓) โอกาสที่จะเกิดเหตุการณ์ความเสี่ยงจากการถูกโจมตีทางไซเบอร์					
๓.๑ Discoverability จุดอ่อนของทรัพย์สิน พิจารณาจาก ผู้ไม่หวังดีสามารถค้นพบจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน	• สามารถค้นพบได้โดยการอ่าน Source Code หรือ blueprint ของระบบ/โปรแกรม **หรือ** • สามารถค้นพบและโจมตีได้จากการเข้าถึงด้านกายภาพ	• สามารถค้นพบได้โดยการใช้งานจากการติดตั้งจริง หรือการติดตั้งที่คล้ายกันของเป้าหมาย **หรือ** • สามารถค้นพบและโจมตีได้จากการเข้าถึงระบบ แบบ Local	• สามารถค้นพบได้จากโดยตรวจสอบการตอบสนองพฤติกรรม และการสื่อสารของเป้าหมาย (network sniffing) **หรือ** • สามารถค้นพบและโจมตีได้จากภายในเครือข่ายย่อยหรือเครือข่ายเดียวกัน	• สามารถค้นพบได้จากการสแกน Port **หรือ** • สามารถค้นพบและโจมตีจากเครือข่ายที่อยู่ใกล้เคียง หรือติดกัน (adjacent subnets or network segments)	• สามารถค้นพบได้จากการสแกน Public Domain **หรือ** • สามารถค้นพบและโจมตีจากเครือข่ายภายนอกได้ (Public Network)
๓.๒ Exploitability การโจมตี พิจารณาจากผู้ไม่หวังดีสามารถใช้ประโยชน์จากจุดอ่อนของทรัพย์สินได้ง่ายแค่ไหน	• สามารถโจมตีได้โดยใช้สิทธิพิเศษ (admin/ system/root) ที่ต้องมีการใช้ Multi Factor Authentication ในการเข้าถึง **หรือ** • สามารถทำได้ด้วยเครื่องมือเฉพาะที่ต้องใช้ความรู้ด้านเทคนิคจากผู้เชี่ยวชาญ **หรือ**	• สามารถโจมตีได้โดยใช้สิทธิพิเศษ (admin/ system/ root) ในการเข้าถึง **หรือ** • สามารถโจมตีได้โดยใช้เครื่องมือที่เฉพาะทางที่เผยแพร่เป็นสาธารณะ แต่ต้องใช้ความรู้เทคนิคระดับสูง **หรือ**	• สามารถโจมตีได้โดยใช้สิทธิการเข้าถึงของเป้าหมายที่มีสิทธิพิเศษ (admin/system/root) **หรือ** • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้เทคนิคระดับปานกลาง	• สามารถโจมตีได้โดยใช้สิทธิการเข้าถึงของเป้าหมาย (เช่น User) **หรือ** • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยมีความรู้ขั้นพื้นฐาน	• สามารถโจมตีได้โดยไม่มีสิทธิการเข้าถึงของเป้าหมาย **หรือ** • สามารถโจมตีได้โดยใช้เครื่องมือที่เผยแพร่เป็นสาธารณะ โดยไม่มีต้องมีความรู้ด้านเทคนิค

ระดับ โอกาสที่จะเกิด	ไม่มีนัยสำคัญ หรือ ต่ำมาก (๑)	ต่ำ (๒)	ปานกลาง (๓)	สูง (๔)	สูงมาก (๕)
	• ต้องการการเชื่อมต่อช่องโหว่หลายอันเพื่อให้สามารถโจมตีได้	• อาจจะต้องทำการเชื่อมต่อช่องโหว่หลายอันเพื่อให้สามารถโจมตีได้			
๓.๓ Reproducibility การโจมตี พิจารณาจากผู้ไม่หวังดีสามารถโจมตีซ้ำทรัพย์สินได้ง่ายแค่ไหน	• ไม่สามารถทำซ้ำได้บนเป้า**หมาย หรือ** • สามารถทำซ้ำได้โดยใช้ช่องโหว่ที่ไม่ได้เผยแพร่เฉพาะเป้าหมาย	• สามารถทำซ้ำได้โดยมีเงื่อนไขเหตุการณ์จากการสุ่ม **หรือ** • สามารถทำซ้ำได้จากทฤษฎี หรือช่องโหว่ที่มีการพิสูจน์และเผยแพร่สู่สาธารณะ	• สามารถโจมตีซ้ำได้โดยมีเงื่อนไขเหตุการณ์ที่คาดการณ์ได้ **หรือ** • สามารถโจมตีซ้ำได้ด้วยการปรับแต่งช่องโหว่เฉพาะสำหรับเป้าหมาย	• สามารถโจมตีซ้ำได้หลายครั้งโดยมีการกำหนดค่าบางอย่างในเป้าหมาย **หรือ** • สามารถโจมตีซ้ำได้ด้วยการปรับแต่งช่องโหว่ที่เผยเล็กน้อย เช่น การเปลี่ยนพารามิเตอร์	• สามารถโจมตีซ้ำได้ตามต้องการโดยไม่จำเป็นต้องมีการกำหนดค่า หรือเงื่อนไขเหตุการณ์ใดๆ **หรือ** • สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งเครื่องมือโจมตีที่เผยแพร่ไว้

๒) กำหนดผลกระทบที่อาจเกิดขึ้น (Determine Impact) สถานการณ์ที่มีความเสี่ยงอาจเป็นอันตรายต่อการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของทรัพย์สิน เช่น ข้อมูล อุปกรณ์ต่าง ๆ และการโจมตีใด ๆ ต่อทรัพย์สินอาจส่งผลกระทบใน ๓ ระดับต่อไปนี้

- ระดับชาติ (National) ซึ่งเป็นผลกระทบที่ถูกมองว่าเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ
- หน่วยงาน (Organizational) ซึ่งเป็นผลกระทบที่ถูกมองว่าเป็นการหยุดชะงักในการดำเนินตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางรางซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน
- บุคคล (Individual) ซึ่งเป็นผลกระทบที่สามารถมองได้ว่าเป็นการสูญเสียชีวิตและหรือการได้รับบาดเจ็บ

๓) การประเมินค่าความเสี่ยง (Risk evaluation)

ดำเนินการประเมินค่าความเสี่ยง ประกอบด้วยการดำเนินการ ดังนี้

(๑) กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritize Risk) โดยดำเนินการเปรียบเทียบสถานการณ์ความเสี่ยงกับระดับการยอมรับความเสี่ยงที่กำหนด ซึ่งสถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการตอบสนองต่อความเสี่ยงจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ และในการจัดลำดับความสำคัญของความเสี่ยงในการตอบสนองต่อความเสี่ยง ต้องกำหนดระยะเวลาที่คาดหวังในการดำเนินการลดความเสี่ยงให้ชัดเจน

(๒) ดำเนินการจัดทำทะเบียนความเสี่ยง (Document Risk) โดยผลลัพธ์จากการประเมินความเสี่ยงจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยง เพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และการจัดทำทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด ซึ่งทะเบียนความเสี่ยงเป็นเอกสารที่ต้องได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (Update) เป็นประจำอย่างน้อยปีละ ๑ ครั้ง ซึ่งทะเบียนความเสี่ยงควรมีข้อมูลอย่างน้อยดังต่อไปนี้

- วันที่ระบุสถานการณ์ความเสี่ยง (Identification Date)
- หมวดหมู่ทรัพย์สินที่เกี่ยวข้อง (Asset Group) ตามทะเบียนทรัพย์สิน (Inventory) ที่ได้จัดทำขึ้น
- คำอธิบายของความเสี่ยง (Description of the Risk หรือ Risk Scenario) โดยระบุรายละเอียดของสถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน
- มาตรการปัจจุบัน (Existing Measures) ที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง
- โอกาสที่จะเกิดความเสี่ยง (Likelihood of Occurrence)
- ความรุนแรงของเหตุการณ์ หรือระดับผลกระทบ (Severity of the Occurrence)

- ความเสี่ยงในปัจจุบัน (Current Risk) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่
- เจ้าของความเสี่ยง (Risk Owner) ที่รับผิดชอบในการดูแลความเสี่ยงที่เหลืออยู่ให้อยู่ในระดับที่ยอมรับได้
- ตัวเลือกการจัดการความเสี่ยง (Risk Treatment Option) เช่น ลดความเสี่ยง (Mitigate) โอนย้าย (Transfer) หลีกเลี่ยง (Avoid) ยอมรับความเสี่ยง (Accept)
- แผนจัดการความเสี่ยง (Risk Treatment Plan: RTP) ในกรณีที่การจัดการความเสี่ยงไม่ได้อยู่ในระดับที่ยอมรับได้ ต้องจัดทำ RTP โดยกำหนดกิจกรรมที่จะวางแผนดำเนินการ เช่น การใช้มาตรการควบคุมเพิ่มเติม และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้
- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) หลังจากดำเนินการตามแผนจัดการความเสี่ยง
- สถานะความคืบหน้า (Progress Status) สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

๒. การจัดการความเสี่ยง (Risk Treatment/Respond)

๑) มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

๒) แนวทางการตอบสนองความเสี่ยง (Risk Respond) ควรมีการกำหนดอย่างน้อย ๔ แนวทาง ดังนี้

(๑) การควบคุม/ลดความเสี่ยง (Treat/Reduce)

(๒) การหาผู้ร่วมรับความเสี่ยง (Transfer/Share)

(๓) การหลีกเลี่ยงความเสี่ยง (Avoid/Terminate)

(๔) การยอมรับ (Accept/Take)

นอกจากนี้ ต้องกำหนดดัชนีชี้วัดความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่สำคัญ (Key Risk Indicators) ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๓. การติดตามและทบทวนความเสี่ยง (Risk monitoring and review)

กำหนดกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๔. การรายงานความเสี่ยง (Risk reporting)

กำหนดรอบในการรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของผู้ให้บริการขนส่งทางรางที่ได้รับมอบหมายเป็นประจำอย่างน้อยปีละ ๑ ครั้ง และจัดทำผลสรุปรายงานการดำเนินการ โดยแยกจากรายงานการประเมินความเสี่ยงของหน่วยงานผู้ให้บริการขนส่งทางราง พร้อมทั้งส่งสรุปรายงานไปยังสำนักงาน และส่งสำเนาไปยังกรมการขนส่งทางราง ภายใน ๓๐ วัน นับตั้งแต่วันที่ดำเนินการแล้วเสร็จ แต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป

โดยการจัดทำรายงานผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรประกอบไปด้วย

๑) บทนำ (Introduction)

- วัตถุประสงค์ของรายงาน
- ขอบเขตของรายงาน
- มาตรฐานที่ใช้ (Risk Management Frameworks)

๒) ภาพรวมและบริบทองค์กร

- นโยบายและกรอบการบริหารความเสี่ยงขององค์กร
- ระดับความเสี่ยงที่ยอมรับได้ (Risk Appetite) และเกณฑ์ความเสี่ยง (Risk Criteria)
- ปัจจัยภายนอกและภายในที่ส่งผลต่อระดับความเสี่ยง เช่น
  - ปัจจัยภายนอก เช่น สภาพเศรษฐกิจ การเปลี่ยนแปลงทางกฎหมาย การแข่งขันในอุตสาหกรรม
  - ปัจจัยภายใน เช่น โครงสร้างองค์กร การเปลี่ยนแปลงเทคโนโลยี การดำเนินงาน
- การเปลี่ยนแปลงสำคัญในสภาพแวดล้อมการดำเนินธุรกิจ (ถ้ามี)
- ตัวชี้วัดความเสี่ยง (Risk Indicators)

๓) กระบวนการบริหารความเสี่ยง (Risk Management Process)

- วิธีการระบุความเสี่ยง (Risk Identification)
  - ทะเบียนความเสี่ยงองค์กร (Risk Register) ที่ระบุเหตุการณ์ความเสี่ยงที่เกิดขึ้นจริงและผลกระทบแยกตามประเภทความเสี่ยง
- การวิเคราะห์และประเมินความเสี่ยง (Risk Assessment)
  - วิธีการและเกณฑ์การประเมินความเสี่ยง เช่น ผลกระทบ (Impact) โอกาสเกิดขึ้น (Likelihood) ผลการประเมินโอกาสและผลกระทบของความเสี่ยงแต่ละรายการ
  - การเปรียบเทียบระดับความเสี่ยงกับเกณฑ์ความเสี่ยงที่กำหนด
  - ความเสี่ยงที่เกินระดับที่ยอมรับได้
- การจัดการและบรรเทาความเสี่ยง (Risk Mitigation Strategies)
  - กลยุทธ์การจัดการความเสี่ยงแต่ละรายการ เช่น
    - การหลีกเลี่ยงความเสี่ยง (Risk Avoidance)
    - การลดความเสี่ยง (Risk Reduction)
    - การถ่ายโอนความเสี่ยง (Risk Transfer) เช่น การทำประกันภัย
    - การยอมรับความเสี่ยง (Risk Acceptance) เมื่อผลกระทบอยู่ในระดับที่ยอมรับได้
  - ระบุความเสี่ยงที่ต้องได้รับการจัดการเร่งด่วน
  - มาตรการควบคุมที่มีอยู่เดิมและประสิทธิผลของการควบคุม

- แผนปฏิบัติการจัดการความเสี่ยง
- ผู้รับผิดชอบและกรอบเวลาในการดำเนินการ
- ความเสี่ยงคงเหลือหลังการควบคุม (Residual Risk)

๔) การติดตามและรายงานผล (Monitoring & Reporting)

- ผลการติดตามตัวชี้วัดความเสี่ยงและแนวโน้ม
- สถานะการดำเนินการตามแผนจัดการความเสี่ยง
- ความคืบหน้าในการดำเนินการตามแผนจัดการความเสี่ยง
- ปัญหาและอุปสรรคในการดำเนินการ

๕) ข้อเสนอแนะ (ถ้ามี)

๕. ทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กำหนดให้มีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ กรณีที่มีการเปลี่ยนแปลงกระบวนการที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

(B) แนวทางการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องระบุรายละเอียดอย่างน้อย ดังนี้

๑) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคน และรายละเอียดการติดต่อ

๒) โครงสร้างการรายงานเหตุการณ์ซึ่งกำหนดว่าผู้ให้บริการขนส่งทางรางจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และกฎหมายลำดับรองใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้อง

๓) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

๔) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๑) การเรียกใช้งานกระบวนการกู้คืน

(๒) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๓) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึง แต่ไม่จำกัดเพียงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๔) ระเบียบวิธีการมีส่วนร่วม (Engagement protocols) กับบุคคลภายนอกรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์ / การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๕) กระบวนการทบทวนหลังการดำเนินการ (After-action review process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๒. กำหนดให้มีการจัดทำ และสื่อสารแผนการรับมือภัยคุกคามทางไซเบอร์ ให้ผู้เกี่ยวข้องทราบและมีการตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญขององค์กร

๓. ดำเนินการการทบทวน และปรับปรุงแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง นับแต่วันที่แผนได้รับการอนุมัติ โดยเริ่มทบทวนตั้งแต่การจัดทำแผนฯ เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล หรือดำเนินการทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น การเปลี่ยนแปลงกลยุทธ์และข้อกำหนดของหน่วยงานผู้ให้บริการขนส่งทางราง ระเบียบข้อบังคับ และกฎหมายที่เกี่ยวข้อง ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ภัยคุกคามทางไซเบอร์ และสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของการให้บริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง และควรดำเนินการทบทวนเพิ่มเติมเมื่อมีเหตุการณ์ ดังนี้

(ก) บทเรียนจากการปฏิบัติการตอบสนองต่อเหตุการณ์ภัยคุกคามที่เกิดขึ้นจริงในแต่ละวัน

(ข) สิ่งที่ได้จากการฝึกหัด/การอบรม

(ค) ผลที่ได้จากการฝึกซ้อมและข้อเสนอแนะหลังจากการฝึกซ้อมตามแผนการรับมือภัยคุกคามทางไซเบอร์ดังกล่าว

(ง) กลยุทธ์และข้อกำหนดของหน่วยงานที่อาจมีการเปลี่ยนแปลง

(จ) สภาพแวดล้อมของการปฏิบัติการทางไซเบอร์ของการให้บริการในหน่วยงานที่สำคัญที่อาจมีการเปลี่ยนแปลง

(ฉ) ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และภูมิทัศน์ภัยคุกคามทางไซเบอร์ (Threat Landscape) ที่มีการเปลี่ยนแปลง

(ช) ระเบียบ ข้อบังคับ และกฎหมายใหม่

(ซ) เทคโนโลยีใหม่

(ฌ) การเปลี่ยนแปลงยุทธศาสตร์ระดับชาติที่เกี่ยวข้องกับลำดับความสำคัญของระบบสารสนเทศหรือของการดำเนินงานตามภารกิจของหน่วยงาน

(ญ) ข้อมูลที่ได้จากระบบข่าวกรองภัยคุกคามทางไซเบอร์ (Cyber Threat Intelligence: CTI)

๔. ดำเนินการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดขึ้น อย่างน้อยปีละ ๑ ครั้ง พร้อมทั้งทบทวนปัญหา และอุปสรรคที่เกิดขึ้นระหว่างการฝึกซ้อมแผนการรับมือภัยคุกคามทางไซเบอร์

(C) การจัดการทรัพย์สิน (Asset Management)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ผู้ให้บริการขนส่งทางรางต้องดำเนินการบริหารจัดการทรัพย์สิน โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้มีการจัดทำบัญชีทรัพย์สิน (Asset Inventory) หรือนำระบบการบริหารจัดการทรัพย์สินมาช่วยในการบริหารจัดการทรัพย์สิน ที่ระบุทรัพย์สินของบริการที่สำคัญ และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยการจัดทำบัญชีทรัพย์สินครอบคลุมทั้ง ข้อมูลและสารสนเทศ (Information) ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) เครือข่าย (Network) บุคลากร (Personnel) สถานที่ (Site) Cloud Assets เป็นต้น ซึ่งทะเบียนทรัพย์สินต้องมีข้อมูลอย่างน้อย ดังนี้

(๑) ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น ชื่อและคำอธิบายข้อมูลกำหนด คุณลักษณะของฮาร์ดแวร์ เครื่องเสมือน ซอฟต์แวร์ อุปกรณ์เครือข่าย

(๒) หมวดหมู่ทรัพย์สิน (Asset Group) โดยหน่วยงานอาจจัดให้ทรัพย์สินที่เกี่ยวข้องกันอยู่ในหมวดหมู่เดียวกัน (เช่น กลุ่มของฮาร์ดแวร์และซอฟต์แวร์ที่ใช้สำหรับการให้บริการแต่ละบริการ) หรือจัดหมวดหมู่ทรัพย์สินตามประเภททรัพย์สินย่อย (Asset Subtype)

(๓) ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางโดยหากเกิดการแก้ไข เสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจของหน่วยงานผู้ให้บริการขนส่งทางราง

(๔) การระบุและการจัดลำดับความสำคัญของของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

(๕) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

(๖) ตำแหน่งทางกายภาพของทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง แต่ละรายการ

(๗) การขึ้นต่อกันของทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางในระบบ/เครือข่ายภายใน และ/หรือภายนอก เช่น เครื่องแม่ข่ายให้บริการเบิกสวัสดิการผู้ปฏิบัติงานต้องดึงข้อมูลจากเครื่องแม่ข่ายที่ให้บริการฐานข้อมูลผู้ปฏิบัติงาน และต้องส่งข้อมูลผ่านสวิตช์หลัก

๒) ระบุขอบเขตเครือข่ายของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface) เช่น โซน Demilitarized (DMZ) สำหรับให้ผู้ใช้ภายนอกสามารถเข้าถึงได้ และโซนที่อยู่ภายในที่ป้องกันไม่ให้ผู้ใช้ภายนอกเข้าถึง โดยการพิจารณาระบุขอบเขตของเครือข่ายของบริการที่สำคัญ ควรพิจารณาดำเนินการดังนี้

- พิจารณาทุกทรัพย์สินของทุกบริการที่สำคัญ เพื่อระบุจุดที่ข้อมูลไหลเข้า และออกจากเครือข่าย (Entry and Exit Point) เช่น จุดที่มีการเชื่อมต่ออินเทอร์เน็ต จุดที่ยอมให้มีการเข้าถึงจากระยะไกล (Remote Access) และจุดที่มีการเชื่อมต่อกับหน่วยงานอื่นที่เป็นหน่วยงานพันธมิตร (Partner)
- พิจารณาเทียบกับแผนภาพเครือข่าย (Network Diagram) ที่มีอยู่ เพื่อนำมาสร้างแผนภาพขอบเขตของเครือข่ายของบริการที่สำคัญ ซึ่งแสดงถึงอุปกรณ์เครือข่าย ไฟร์วอลล์ ระบบตรวจจับการบุกรุก ระบบป้องกันการบุกรุก และเครือข่ายเสมือน รวมถึงการเชื่อมต่อของแต่ละทรัพย์สินที่เกี่ยวข้องกับบริการที่สำคัญ ทั้งการเชื่อมต่อทางกายภาพ และการเชื่อมต่อเชิงตรรกะ (Physical and Logical Connection)

๓) ดำเนินการตรวจสอบ และทบทวนขอบเขตของเครือข่าย รวมถึงปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง โดยพิจารณาหัวข้อในการตรวจสอบ และทบทวน ดังนี้

(๑) ตรวจสอบความถูกต้องของข้อมูลในทะเบียน โดยตรวจสอบและทบทวน ชื่อ คำอธิบาย หมวดหมู่ ทรัพย์สิน ลำดับความสำคัญ เจ้าของ ตำแหน่ง และการขึ้นต่อกันของทรัพย์สิน เช่น การปรับปรุงเวอร์ชันของซอฟต์แวร์ การปรับระดับความสำคัญของระบบสารสนเทศให้สูงขึ้นในกรณีที่กฎหมายใหม่มีผลบังคับใช้ หรือการเชื่อมต่ออุปกรณ์ใหม่เข้ากับทรัพย์สินในทะเบียน

(๒) จำนวนของทรัพย์สิน (Inventory Status) เช่น การตรวจนับจำนวนทรัพย์สิน

(๓) สถานะเชิงคุณภาพของทรัพย์สิน เช่น การตรวจสอบทรัพย์สินที่ชำรุด เสื่อมสภาพ สูญไป หรือทรัพย์สินที่ไม่จำเป็นต้องใช้ ในกรณีที่ทรัพย์สินอยู่ในสถานะชำรุด เสื่อมสภาพ หรือสูญไป ต้องดำเนินการสอบหาสาเหตุ พร้อมทั้งระบุผู้ที่เข้าข่ายต้องรับผิดชอบต่อความเสียหาย

(๔) ข้อกำหนดด้านความมั่นคงปลอดภัยของทรัพย์สิน (Security Requirement) เช่น กฎหมาย หรือมาตรฐานที่เปลี่ยนแปลงไปหรือที่ถูกกำหนดขึ้นใหม่ การเปลี่ยนแปลงของระยะเวลาการกู้ข้อมูลที่ยอมรับได้ ระยะเวลาสูงสุดที่ยอมให้การดำเนินการตามภารกิจหน้าที่หยุดชะงัก (Maximum Tolerable Downtime) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective)

(๕) กลยุทธ์และมาตรการควบคุม เพื่อการป้องกันทรัพย์สินและบริการ เช่น การกำหนดให้ใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-factor Authentication) สำหรับการเข้าถึงระบบสารสนเทศที่มีความเสี่ยงต่อการถูกโจมตีมากขึ้น การกำหนดวิธีการเข้ารหัสข้อมูลที่มีความอ่อนไหวให้มีความปลอดภัยมากขึ้น โดยการเพิ่มจำนวนบิตที่ใช้การเข้ารหัส การใช้เทคโนโลยีใหม่ที่สามารถกู้ข้อมูลได้เร็วขึ้น

(๖) กลยุทธ์และแผนความต่อเนื่องให้กับทรัพย์สินและบริการ เช่น การทบทวนแผนความต่อเนื่อง (Continuity Plan) และแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan)

ทั้งนี้ การตรวจสอบ และทบทวนทรัพย์สินต้องกำหนดให้มีการนำเสนอสถานะปัจจุบันของทรัพย์สินต่อผู้บริหารระดับสูงอย่างสม่ำเสมอตามรอบที่กำหนด

๔) กำหนดให้มีการบริหารจัดการทรัพย์สิน (Asset Management) ตั้งแต่เริ่มจัดทำรายการทรัพย์สินจนถึงการบำรุงรักษา (Maintaining) รายการทรัพย์สินให้ถูกต้องครบถ้วน ซึ่งข้อมูลที่นำมาจัดทำ

รายการทรัพย์สินสามารถข้อมูลนำมาจากฐานข้อมูลการจัดการทรัพย์สินของหน่วยงานผู้ให้บริการขนส่งทางราง หรือดำเนินการสำรวจข้อมูลที่กับหน่วยงานภายในที่เกี่ยวข้องกับบริการที่สำคัญ หรือระบบงานที่สำคัญ หรือจากรายการทรัพย์สินของผู้ให้บริการภายนอกในกรณีที่มีการใช้บริการผู้ให้บริการภายนอกจัดหา ทั้งนี้ต้องจัดให้มีการบริหารจัดการทรัพย์สินด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ควรมีการพิจารณาดำเนินการ ดังนี้

(๑) ดำเนินการบริหารความเสี่ยง (Risk Management) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ โดยการทำความเข้าใจ และดำเนินการจัดการความเสี่ยงทางไซเบอร์ที่เกี่ยวข้องอยู่กับทรัพย์สินที่ระบุไว้ในทะเบียนทรัพย์สินของบริการที่สำคัญหรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางตามลำดับความสำคัญของความเสี่ยง รวมถึงติดตาม ทบทวนความเสี่ยงอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๒) การบริหารจัดการทรัพย์สินล้าสมัย (Managing Legacy) หากซอฟต์แวร์และฮาร์ดแวร์ล้าสมัยการใช้ทรัพย์สินหรือผลิตภัณฑ์นั้นอาจก่อให้เกิดความเสี่ยง หรือต้นทุนสำหรับการลดความเสี่ยงเพิ่มขึ้น จึงควรมีการดำเนินการจัดการทรัพย์สินติดตามการสนับสนุนทรัพย์สินหรือผลิตภัณฑ์เป็นระยะ เพื่อติดตามการประกาศการให้การสนับสนุนได้สิ้นสุดลง (End of Support) ของผู้ผลิตและดำเนินการวางแผนปรับปรุงเปลี่ยนแปลงล่วงหน้า

(๓) กำหนดให้มีการจัดการข้อมูลประจำตัวและการเข้าถึง (Identity and Access Management) ทรัพย์สินนั้น ๆ โดยให้มีการระบุผู้ใช้และอุปกรณ์ที่ใช้งาน เพื่อควบคุมการเข้าถึง (Access Control) ทรัพย์สิน และทรัพยากรของหน่วยงานผู้ให้บริการขนส่งทางราง

(๔) กำหนดให้มีการดำเนินการประเมินช่องโหว่และการจัดการแพตช์ (Vulnerability and Patch Management) อย่างสม่ำเสมอ

(๕) กำหนดให้มีการเฝ้าระวังการใช้งานทรัพย์สิน (Monitoring) โดยการตรวจจับ (Detect) และสืบสวน (Investigate) การบุกรุกที่อาจเกิดขึ้นก่อนดำเนินการลดภัยคุกคาม

(๖) การจัดการเหตุภัยคุกคามทางไซเบอร์การตอบสนองและการฟื้นฟู (Incident Management, Response and Recovery) โดยดำเนินการวางแผน ตอบสนอง และกู้คืนจากเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้น เพื่อลดการหยุดชะงักการให้บริการ (Minimize Disruption)

๕) ในกรณีที่มีการพิจารณานำระบบการจัดการทรัพย์สินมาใช้บริหารจัดการ ควรมีการพิจารณาการออกแบบระบบให้สามารถดำเนินการได้ ดังนี้

- การค้นหาทรัพย์สิน (Asset Discovery) เพื่อสแกนสภาพแวดล้อมของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อหาทรัพย์สินใหม่หรือลบรายการทรัพย์สินเก่าออกอย่างสม่ำเสมอและต่อเนื่อง
- เก็บข้อมูลจากแหล่งข้อมูลที่เชื่อถือ และข้อมูลที่ถูกต้อง (Authoritative Source of Information & Accurate Source of Information) โดยการกำหนดมาตรฐานสำหรับทะเบียนทรัพย์สินเพื่อหลีกเลี่ยงการบันทึกข้อมูลที่ซ้ำซ้อน และออกแบบระบบให้ผู้ใช้สามารถเข้าถึงข้อมูลได้ง่ายขึ้น รวมถึงข้อมูล

ทรัพย์สินควรถูกรวบรวมและอัปเดตอย่างสม่ำเสมอ และควรดำเนินการจัดทำรายการความถี่ในการอัปเดตข้อมูลตามความเหมาะสม หรือระดับการเปลี่ยนแปลงของประเภททรัพย์สิน เช่น

(ก) เครื่องแม่ข่าย (Server) ดำเนินการอัปเดตข้อมูลเป็นรายเดือนหรือรายไตรมาส เนื่องจากมีการเปลี่ยนแปลงไม่บ่อย

(ข) เครื่องเดสก์ท็อป (Desktop) ดำเนินการอัปเดตข้อมูลเป็นรายสัปดาห์ หรือรายเดือน เพื่อรองรับการจัดการค่ากำหนด (Configuration) และการจัดการช่องโหว่ (Vulnerability Management) การกำหนดรอบการอัปเดตตามระดับความสำคัญของระบบ

- ความพร้อมใช้งานของข้อมูลทรัพย์สิน (Availability of Asset Information) โดยจัดให้มีการบริหารจัดการกำหนดค่าฐานข้อมูล (Configuration Management Database: CMDB) รวมถึงกำหนดให้มีการตรวจสอบ และปรับปรุงค่าที่กำหนดอย่างสม่ำเสมอ
- พิจารณาการนำไปใช้งานของผู้ใช้งาน (Human Factors) เช่น ความสะดวกในการใช้งาน (Usability) และความสะดวกในการเข้าถึง (Accessibility) รวมถึงนำแนวทางที่เน้นปฏิบัติงานที่ใช้ได้จริง (Pragmatic Approach) มาเป็นหลักการในการพัฒนาหรือจัดหาระบบ
- พิจารณาใช้ระบบอัตโนมัติ (Automation) เป็นกลไกในการปรับปรุงรายการทรัพย์สินที่ถูกใช้งานได้จริงให้เป็นปัจจุบัน
- การทำงานของระบบครอบคลุม (Comprehensive Visibility) ตามจุดประสงค์ และวิธีการใช้ข้อมูลทรัพย์สินที่หน่วยงานผู้ให้บริการขนส่งทางรางกำหนดขึ้น และมีข้อมูลที่ละเอียดเพียงพอตามวัตถุประสงค์ของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การระบุเวอร์ชันของซอฟต์แวร์ทั้งหมดที่ติดตั้งในเครื่องคอมพิวเตอร์ของหน่วยงานผู้ให้บริการขนส่งทางราง
- สามารถตรวจจับการเปลี่ยนแปลง (Change Detection) ข้อมูลทรัพย์สินได้รับการบันทึก และใช้แหล่งข้อมูลหลายแหล่งเพื่อระบุความไม่สอดคล้องกัน (Identify Inconsistencies) เช่น พบอุปกรณ์ใหม่บนเครือข่ายและยังไม่ได้ถูกลงทะเบียน
- การรักษาความลับ (Confidentiality) โดยพิจารณาให้สามารถกำหนดให้มีการเข้าถึงได้ตามสิทธิ์การเข้าถึงตามหน้าที่ความรับผิดชอบ เพื่อดำเนินการการป้องกันและการจำกัดการเข้าถึงที่เหมาะสมกับระดับความอ่อนไหว รวมถึงกำหนดให้มีการเฝ้าระวังการเข้าถึงข้อมูลทรัพย์สิน เช่น ตรวจสอบ log เข้าถึงอย่างสม่ำเสมอ หรือเมื่อมีเหตุผิดปกติ
- สามารถจัดประเภททรัพย์สิน (Asset Classification) โดยกำหนดประเภททรัพย์สินและจำแนกทรัพย์สินให้สอดคล้องกับแนวทางการบริหารความเสี่ยงของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การจัดประเภทตามความอ่อนไหวของข้อมูลที่ประมวลผล หรือความสำคัญของระบบต่อภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑) กำหนดภาระหน้าที่ความรับผิดชอบบริหารจัดการต่อทรัพย์สินอย่างชัดเจน และกำหนดให้มีการลงนามยอมรับข้อตกลงการใช้งานทรัพย์สิน เช่น คอมพิวเตอร์แบบพกพา (Notebook) พร้อมทั้งกำหนดให้มีการอบรมแนวทางการใช้และดูแลรักษาทรัพย์สินก่อนการใช้งาน

๒) กำหนดให้มีผู้รับผิดชอบถือครองทรัพย์สินที่ชัดเจน เพื่อรับผิดชอบในการดูแลติดตามและรายงานการสูญหายหรือชำรุด

๓) กำหนดให้มีการใช้ทรัพย์สินอย่างเหมาะสม โดยการพิจารณาให้มีมาตราการควบคุมอย่างน้อย ดังนี้

(๑) ใช้ทรัพย์สินตามวัตถุประสงค์ทางราชการ หรือขององค์กร ภายใต้หน้าที่ความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

(๒) ห้ามติดตั้งซอฟต์แวร์หรือเชื่อมต่อกับอุปกรณ์ส่วนตัว โดยไม่ได้รับอนุญาต

(๓) กำหนดให้มีแนวปฏิบัติการใช้งานเทคโนโลยีสารสนเทศ (Acceptable Use Policy) และกฎระเบียบด้านความมั่นคงปลอดภัยสารสนเทศ และไซเบอร์

๔) กำหนดให้มีการควบคุมการคืนทรัพย์สิน โดยพิจารณาอย่างน้อย ดังนี้

(๑) เมื่อผู้ใช้งานลาออก เปลี่ยนตำแหน่ง หรือพ้นจากหน้าที่ความรับผิดชอบ ต้องดำเนินการคืนทรัพย์สินให้กับองค์กรตามกระบวนการ หรือขั้นตอนการคืนทรัพย์สินขององค์กร พร้อมทั้งกำหนดให้มีการจัดเก็บหลักฐานการคืนทรัพย์สิน และการตรวจสอบทรัพย์สินก่อนรับทรัพย์สินคืน

(๒) หากทรัพย์สินนั้นมีข้อมูลสำคัญ ต้องมีการดำเนินการกำหนดให้มีการลบข้อมูล (Sanitization) ก่อนส่งต่อหรือก่อนนำไปทำลาย

๕) กำหนดให้มีการบริหารจัดการนำทรัพย์สินขององค์กรออกนอกสถานที่ (Off-site Asset Control and Security Management) ต้องดำเนินการขออนุมัติจากผู้มีอำนาจก่อนนำทรัพย์สินออกนอกสถานที่ และกำหนดให้มีหลักฐานการขอนำทรัพย์สินออกนอกสถานที่ (Asset Movement Request Form) รวมถึงระบุรายละเอียด อย่างน้อย ดังนี้ ประเภทอุปกรณ์, หมายเลขทรัพย์สิน, ผู้ใช้งาน, จุดประสงค์, ระยะเวลาใช้งาน และสถานที่ปลายทาง เป็นต้น รวมถึงบันทึกทะเบียนการนำทรัพย์สินออกนอกสถานที่

๖) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของอุปกรณ์ โดยพิจารณาอย่างน้อยดังนี้

(๑) พิจารณาติดตั้งระบบรักษาความปลอดภัยพื้นฐาน เช่น Antivirus, Firewall, Full-disk Encryption เป็นต้น

(๒) อุปกรณ์ต้องมีรหัสผ่าน หรือวิธีการพิสูจน์ตัวตนตามระดับความเสี่ยงของการนำไปใช้งาน เช่น MFA เป็นต้น

(๓) ห้ามเก็บข้อมูลสำคัญในอุปกรณ์ โดยไม่มีการเข้ารหัส

(๔) ห้ามใช้อุปกรณ์ขององค์กรร่วมกับเครือข่ายที่ไม่ปลอดภัย โดยไม่มี VPN หรือระบบรักษาความปลอดภัย

๗) กำหนดให้มีการควบคุมอุปกรณ์ในระหว่างใช้งาน โดยพิจารณาอย่างน้อยดังนี้

(๑) ผู้ใช้งานต้องไม่ปล่อยให้อุปกรณ์ถูกทิ้งไว้ โดยไม่มีการดูแลหรือใช้งานในพื้นที่สาธารณะที่มีความเสี่ยงต่ออุปกรณ์

(๒) หากเกิดการสูญหาย หรือถูกขโมย ต้องดำเนินการรายงานต่อฝ่ายเทคโนโลยีสารสนเทศหรือฝ่ายที่ได้รับมอบหมาย ภายใน ๒๔ ชั่วโมง

(๓) ห้ามติดตั้งซอฟต์แวร์ใด ๆ เพิ่มเติม หรือเปลี่ยนแปลงการตั้งค่า โดยไม่ได้รับอนุญาต

๘) กำหนดให้มีการส่งคืนและตรวจสอบทรัพย์สิน โดยพิจารณาอย่างน้อยดังนี้

(๑) หลังสิ้นสุดการใช้งานนอกสถานที่ ต้องส่งคืนทรัพย์สินให้ฝ่ายเทคโนโลยีสารสนเทศหรือฝ่ายที่ได้รับมอบหมายภายในเวลาที่กำหนด

(๒) ดำเนินการตรวจสอบความสมบูรณ์ของอุปกรณ์ และล้างข้อมูลที่ไม่จำเป็นออกจากอุปกรณ์

(๓) อัปเดตสถานะในทะเบียนสินทรัพย์ เพื่อบันทึกการคืนและความสมบูรณ์ของทรัพย์สิน

๙) กำหนดให้มีการกำจัดหรือทำลายอุปกรณ์ที่หมดอายุการใช้งาน โดยพิจารณาอย่างน้อยดังนี้

(๑) ดำเนินการตรวจสอบ และบันทึกข้อมูลในทะเบียนสินทรัพย์ก่อนทำลายหรือถ่ายโอน

(๒) ดำเนินการล้างข้อมูลอย่างปลอดภัย (Data Sanitization) ด้วยวิธีการที่รับรองได้ เช่น

(๒.๑) การเขียนทับหลายรอบ (Overwrite)

(๒.๒) การล้างด้วยซอฟต์แวร์มาตรฐาน (Wipe tools)

(๒.๓) การทำลายทางกายภาพ เช่น การบด การเผา หรือการเจาะ

(๓) จัดให้มีหลักฐานการทำลาย เช่น แบบฟอร์มยืนยัน ภาพถ่าย รายงานการทำลายจากผู้รับจ้าง เป็นต้น

(๔) ดำเนินการล้าง หรือทำลายอุปกรณ์โดยบุคลากรที่ได้รับอนุญาต หรือผู้ให้บริการที่มีข้อตกลงความมั่นคงปลอดภัยที่ชัดเจน เช่น NDA, SLA เป็นต้น

๑๐) กำหนดให้มีการควบคุมการนำอุปกรณ์ไปใช้งานซ้ำ (Reuse/Repurpose) โดยพิจารณาอย่างน้อยดังนี้

(๑) ดำเนินการตรวจสอบให้แน่ใจว่าได้ล้างข้อมูลจากอุปกรณ์อย่างครบถ้วนก่อนการนำอุปกรณ์ไปใช้งาน

(๒) อัปเดตทะเบียนสินทรัพย์ และระบุการเปลี่ยนแปลงผู้ใช้งาน หรือหน่วยงานที่ได้รับอุปกรณ์ไปใช้งาน

(๓) กำหนดให้มีการตั้งค่าความมั่นคงปลอดภัยพื้นฐาน (Baseline Configuration) ก่อนการแจกจ่ายให้กับหน่วยงานภายในของผู้ให้บริการขนส่งทางราง รวมถึงปรับระดับสิทธิ และการเข้าถึงให้เหมาะสมกับผู้ใช้งานใหม่

๑๑) กำหนดให้มีการจัดการอุปกรณ์ที่ถูกปล่อยทิ้ง (Unattended Equipment) โดยพิจารณาอย่างน้อยดังนี้

(๑) อุปกรณ์ที่พบนอกพื้นที่ควบคุม หรือถูกทิ้งไว้โดยไม่มีเจ้าของชัดเจน ต้องถูกนำมาจัดเก็บในพื้นที่ปิด และมีการควบคุม

(๒) ผู้ที่พบเห็น หรือผู้ดูแลพื้นที่ต้องรายงานต่อฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายทันที

(๓) ดำเนินการตรวจสอบความเสี่ยง เช่น การเชื่อมต่อเครือข่าย หรือข้อมูลในเครื่อง เป็นต้น

(๔) จัดเก็บอุปกรณ์ในที่ปลอดภัย และเก็บบันทึกการตรวจพบและการดำเนินการไว้สำหรับตรวจสอบย้อนหลัง

๑๒) กำหนดให้มีการกำหนดระดับชั้นความลับของทรัพย์สินสารสนเทศ โดยพิจารณา อย่างน้อยดังนี้

(๑) พิจารณากำหนดระดับชั้นความลับของข้อมูล โดยกำหนดให้มีระดับชั้นความลับอย่างต่ำ ๓ - ๔ ระดับชั้น เช่น ลับที่สุด ลับมาก ลับ และสาธารณะ พร้อมทั้งคำอธิบายในการเข้าถึงแต่ละระดับชั้นความลับ

(๒) กำหนดให้มีการบ่งชี้ระดับชั้นความลับของสารสนเทศ (Labeling & Marking) โดยการพิจารณาอย่างน้อย ดังนี้

(๒.๑) ข้อมูลที่ถูกจัดระดับชั้นความลับต้องมีสัญลักษณ์ระบุระดับชั้นความลับ (Label) เช่น บนหัวกระดาษ ชื่อไฟล์ Metadata หรือ Watermark เป็นต้น และในกรณีที่เป็นเอกสารหรือข้อมูลในรูปแบบอิเล็กทรอนิกส์ไฟล์ให้พิจารณากำหนดให้มีข้อความระบุระดับความลับที่ชัดเจนทุกหน้า

(๒.๒) พิจารณาใช้ระบบช่วยในการชี้บ่งระดับชั้นความลับ (Tag) อัตโนมัติ เช่น DLP, Microsoft Purview, Data Classification Tool เป็นต้น

(๒.๓) พิจารณากำหนดการจัดการทรัพย์สินตามชั้นความลับ เช่น ข้อมูลที่เป็น "ลับมากที่สุด" ต้องจัดให้มีการเข้ารหัสระหว่างจัดเก็บและส่งต่อ (Encryption at rest/in transit) กำหนดให้มีการจัดเก็บในระบบที่มีการควบคุมการเข้าถึง ห้ามนำข้อมูลลับใส่ USB โดยไม่ได้รับอนุญาต เป็นต้น รวมถึงการทำลายข้อมูลต้องกำหนดวิธีที่เหมาะสมตามระดับชั้นความลับ เช่น Overwrite, Degauss, Physical Destruction เป็นต้น

๑๓) กำหนดให้มีการบริหารจัดการเข้ารหัสข้อมูลตามระดับชั้นความลับ โดยพิจารณาใช้อัลกอริทึมที่สอดคล้องกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการเกี่ยวกับการเข้ารหัสข้อมูลเป็นไปในทิศทางเดียวกัน

๑๔) จัดให้มีและปฏิบัติตามขั้นตอนปฏิบัติการบริหารจัดการกุญแจเข้ารหัสข้อมูล เพื่อให้มีกระบวนการที่รัดกุมตลอดช่วงเวลาการใช้งาน (Key management whole life cycle) โดยมีการคัดเลือกวิธีการเข้ารหัส การกำหนดความยาวของกุญแจเพื่อเข้ารหัส การจัดเก็บ การใช้งาน และการยกเลิกการใช้งานกุญแจรหัส

๑๕) มีการอนุญาตการเข้าถึงรหัสลับเฉพาะผู้ที่รับผิดชอบเท่านั้น เพื่อป้องกันการถูกแก้ไข หรือเปิดเผยรวมทั้งติดตามให้มีการปฏิบัติให้เป็นไปตามขั้นตอนปฏิบัติดังกล่าวอย่างเคร่งครัด

๑๖) กำหนดให้มีการบริหารจัดการความเป็นส่วนตัว และการปกป้องข้อมูลส่วนบุคคล โดยระบุข้อมูลส่วนบุคคลและการทำบันทึกรายการประมวลผล (ROPA) ที่เกี่ยวข้องกับข้อมูลส่วนบุคคล

๑๗) กำหนดให้มีหลักการประมวลผลข้อมูลส่วนบุคคล โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดวัตถุประสงค์ในการประมวลผลข้อมูลส่วนบุคคลที่ชัดเจน และใช้ข้อมูลเท่าที่จำเป็น (Data Minimization)

(๒) ใช้ฐานทางกฎหมายในการประมวลผลข้อมูลส่วนบุคคลที่เหมาะสม เช่น ความยินยอม (Consent) สัญญา หรือภาระหน้าที่ทางกฎหมาย เป็นต้น

(๓) กำหนดให้มีการแจ้งวัตถุประสงค์ต่อเจ้าของข้อมูล (Privacy Notice) ก่อนดำเนินการจัดเก็บ หรือใช้ข้อมูลส่วนบุคคลตามวัตถุประสงค์

(๔) กำหนดให้มีการจัดเก็บข้อมูลให้นานเท่าที่จำเป็น และระบุระยะเวลาที่สามารถระบุได้ รวมถึงทำลายข้อมูลอย่างเหมาะสมตามระดับชั้นความลับของข้อมูลเมื่อหมดวัตถุประสงค์

๑๘) กำหนดให้มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดให้มีการเข้ารหัสข้อมูล (Encryption) และควบคุมสิทธิการเข้าถึงข้อมูลเท่าที่จำเป็นตามหน้าที่ความรับผิดชอบ (Role-Based Access Control: RBAC) รวมถึงมาตรการควบคุมที่เหมาะสม เช่น การพิสูจน์ตัวตนก่อนเข้าถึงข้อมูล เป็นต้น

(๒) กำหนดให้มีแผนสำรองและกู้คืนข้อมูลในกรณีเกิดเหตุฉุกเฉินด้านความมั่นคงปลอดภัย (Backup & Recovery)

๑๙) กำหนดให้มีสิทธิของเจ้าของข้อมูล (Data Subject Rights) ตาม พ.ร.บ. คุ้มครองข้อมูลส่วนบุคคลกำหนด เช่น สิทธิการเข้าถึง สิทธิขอลบข้อมูล เป็นต้น รวบถึงกำหนดกระบวนการบริหารจัดการสิทธิของเจ้าของข้อมูลส่วนบุคคล

๒๐) กำหนดให้มีการจัดการเหตุละเมิดข้อมูลส่วนบุคคล (Data Breach Management) โดยกำหนดให้การจัดทำแผนการตอบสนองต่อเหตุการณ์ข้อมูลรั่วไหล รวมถึงกำหนดให้มีการแจ้งฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย ในกรณีที่พบเหตุการรั่วไหลของข้อมูลส่วนบุคคล ทันที หรือภายใน ๒๔ ชั่วโมง เมื่อทราบเหตุ

๒๑) กำหนดให้มีการบริหารจัดการถ่ายโอนสารสนเทศ โดยจัดทำข้อตกลงการถ่ายโอน โดยพิจารณาอย่างน้อยดังนี้

(๑) กำหนดข้อตกลงการถ่ายโอนข้อมูลโดยพิจารณาจากวัตถุประสงค์การถ่ายโอน ประเภทของข้อมูล ความสำคัญของข้อมูล และระดับความลับของข้อมูล

(๒) จัดให้มีข้อตกลงในการถ่ายโอนข้อมูล (Information Sharing Agreement / Data Transfer Agreement) กรณีที่ต้องดำเนินการส่งข้อมูลให้บุคคลภายนอก

(๓) ระบุสิทธิ์และบทบาทของผู้ส่งและผู้รับในการรักษาข้อมูล เช่น ห้ามส่งต่อ ห้ามใช้ซ้ำโดยไม่ได้รับอนุญาต เป็นต้น

(๔) กำหนดช่องทางในการถ่ายโอนข้อมูลที่ชัดเจน เช่น ผ่านช่องทางอีเมลที่กำหนดโดยเฉพาะหรือระบบคลาวด์ที่มีการเข้ารหัสข้อมูลและกำหนดสิทธิในการเข้าถึงเฉพาะผู้ที่มีสิทธิเข้าถึงเท่านั้น รวมถึงจัดให้มีการเก็บรักษาหลักฐานการถ่ายโอนข้อมูล (Transfer Log)

(๕) ตรวจสอบความสมบูรณ์ของข้อมูลหลังการรับ - ส่ง หากพบการเปลี่ยนแปลง หรือสูญหาย ต้องแจ้งฝ่ายเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายทันที

(๖) ไม่อนุญาตให้มีการถ่ายโอนข้อมูลผ่านอุปกรณ์พกพาส่วนตัว โดยไม่มีการขออนุมัติและมาตรการควบคุม

(๗) จัดให้มีช่องทางในการรายงานเหตุการณ์ผิดปกติจากการถ่ายโอน เช่น ข้อมูลหลุด ข้อมูลสูญหาย เป็นต้น รวมถึงวิเคราะห์เหตุการณ์และทบทวนมาตรการ เพื่อป้องกันไม่ให้เกิดเหตุการณ์ผิดปกติซ้ำ

๒๒) กำหนดให้มีมาตรการเพิ่มเติมสำหรับการถ่ายโอนข้อมูลส่วนบุคคล โดยพิจารณาอย่างน้อยดังนี้

(๑) ดำเนินการประเมินผลกระทบด้านข้อมูลส่วนบุคคล (DPIA) หากมีการส่งข้อมูลส่วนบุคคลจำนวนมาก หรือข้อมูลส่วนบุคคลละเอียดอ่อน

(๒) พิจารณาใช้ระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention – DLP) เพื่อควบคุมการส่งข้อมูลส่วนบุคคลไปยังภายนอก

(๓) พิจารณาใช้เทคนิค Masking หรือ Anonymization ในกรณีที่จำเป็นต้องถ่ายโอนข้อมูลส่วนบุคคลไปยังภายนอก

๒๓) จัดให้มีการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ โดยพิจารณาอย่างน้อย ดังนี้

(๑) จัดทำทะเบียนซอฟต์แวร์ (Software Inventory) ที่มีการบันทึกรายละเอียด เช่น ชื่อซอฟต์แวร์, เวอร์ชัน, หมายเลขลิขสิทธิ์ (License Key), วันที่หมดอายุ และสถานะการใช้งาน และทบทวนปรับปรุงอย่างสม่ำเสมอ

(๒) กำหนดให้มีการจัดซื้อและติดตั้งซอฟต์แวร์ผ่านช่องทางที่ได้รับการรับรอง หรือผู้จำหน่ายที่ได้รับอนุญาตเท่านั้น และห้ามติดตั้งซอฟต์แวร์ที่ไม่ได้รับอนุญาตโดยเด็ดขาด

(๓) กำหนดให้มีการตรวจสอบการใช้งานซอฟต์แวร์ในระบบอย่างสม่ำเสมอ เช่น ทุก ๖ เดือน หรือปีละ ๑ ครั้ง

(๔) กำหนดให้มีการควบคุมสิทธิ์การติดตั้งซอฟต์แวร์ โดยอนุญาตเฉพาะผู้มีอำนาจ เช่น ผู้ดูแลระบบ (System Administrator) เป็นต้น

(๕) กำหนดให้มีนโยบายการใช้งานซอฟต์แวร์ (Software Usage Policy) และเผยแพร่ให้บุคลากรที่เกี่ยวข้องรับทราบ

๒๔) กำหนดให้มีการบริหารจัดการสิทธิในทรัพย์สินทางปัญญา (Intellectual Property Rights Management) ซึ่งต้องจัดทำบัญชีทะเบียนทรัพย์สินทางปัญญา (IP Inventory) โดยระบุประเภทเจ้าของสิทธิ ข้อกำหนดการใช้งาน และสถานะสิทธิ์ รวมถึงทบทวนปรับปรุงรายการทรัพย์สินทางปัญญาอย่างสม่ำเสมอ เช่น ทุก ๖ เดือน เป็นต้น

๒๕) กำหนดให้มีการควบคุมการเข้าถึงและการใช้งาน โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

(๑) กำหนดสิทธิการเข้าถึงทรัพย์สินทางปัญญาตามหลักการสิทธิน้อยที่สุด (Least Privilege) และหลักรับรู้เท่าที่จำเป็น (Need to Know)

(๒) ควบคุมการคัดลอก การแจกจ่าย หรือการเผยแพร่ทรัพย์สินทางปัญญา ทั้งภายในและภายนอกองค์กร

(๓) พิจารณาให้มีการใช้มาตรการด้านเทคโนโลยีในการควบคุม เช่น การเข้ารหัสไฟล์ การใช้งานระบบ Digital Rights Management (DRM) และระบบ Watermarking สำหรับงานสำคัญ เป็นต้น

(๔) ไม่อนุญาตให้ติดตั้งหรือใช้งานซอฟต์แวร์ละเมิดลิขสิทธิ์ (Pirated Software)

(๕) กำหนดให้มีการตรวจสอบ เพื่อให้แน่ใจว่าซอฟต์แวร์ที่ใช้ในองค์กรมีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๖) พิจารณาจัดให้มีสัญญาข้อตกลงไม่เปิดเผยข้อมูล (Non-Disclosure Agreement (NDA)) สำหรับผู้ปฏิบัติงาน หรือบุคคลภายนอกที่เข้าถึงข้อมูลทรัพย์สินทางปัญญา

๒๖) จัดให้มีการบริหารจัดการป้องกันโปรแกรมไม่ประสงค์ดี (Malware Protection) โดยพิจารณาอย่างน้อย ดังนี้

(๑) จัดให้มีการติดตั้ง และอัปเดตโปรแกรมป้องกันไวรัส/มัลแวร์ (Antivirus/Antimalware Software) อย่างสม่ำเสมอ

(๒) กำหนดให้มีการใช้งานระบบป้องกันแบบแสดงผลทันที (Real-time) และกำหนดให้มีการสแกนอัตโนมัติอย่างน้อยวันละครั้ง

(๓) กำหนดมาตรการควบคุมการนำเข้าข้อมูลผ่านสื่อบันทึกข้อมูลภายนอก (เช่น USB, External HDD)

(๔) กำหนดให้มีการตั้งค่าให้ระบบปฏิบัติการ และซอฟต์แวร์ที่ใช้งานทำการอัปเดตแพตช์ (Security Patches) โดยอัตโนมัติหรือภายในระยะเวลาที่กำหนด

(๕) จำกัดสิทธิ์การใช้งานระบบ (Privilege Management) เพื่อลดความเสี่ยงจากการติดตั้งโปรแกรมไม่ประสงค์ดี

(D) การควบคุมการเข้าถึง (Access Control)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้การควบคุมการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางถูกจำกัดไว้ที่

๑) บุคลากร/เจ้าหน้าที่ ที่ปฏิบัติงานให้หน่วยงานผู้ให้บริการขนส่งทางรางและกิจกรรมที่ได้รับอนุญาตจากหน่วยงานผู้ให้บริการขนส่งทางราง

๒) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตจากหน่วยงานผู้ให้บริการขนส่งทางราง

๒. กำหนดให้แต่ละบุคลากร/เจ้าหน้าที่ กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญหรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางต้องมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

๓. กำหนดให้มีการจัดเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง และตรวจสอบบันทึกเหล่านี้ เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ ความสม่ำเสมอในการตรวจสอบบันทึกการเข้าถึงควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงบริการที่สำคัญหรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

๔. กำหนดให้ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญหรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น USB, พอร์ตอนุกรม ซึ่งเป็นจุดที่ผู้ใช้หรืออุปกรณ์ภายนอกสามารถเชื่อมต่อเข้ากับระบบ โดยต้องควบคุมการเข้าถึงอย่างเข้มงวด เช่น การกำหนดให้มีการอนุญาตเฉพาะบุคลากรของหน่วยงานผู้ให้บริการขนส่งทางรางที่มีสิทธิ์ในการเข้าถึงเท่านั้น หรือการใช้มาตรการที่ช่วยป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การใช้ ระบบการยืนยันตัวตนก่อนการเข้าถึง

๕. กำหนดให้ตรวจสอบการเข้าถึงทางลอจิคอล (Logical) ให้อยู่ภายใต้การดูแลของหน่วยงานผู้ให้บริการขนส่งทางรางเท่านั้น โดยการควบคุมการเข้าถึงระบบและข้อมูลที่อยู่ในระบบคอมพิวเตอร์ เช่น การเข้าสู่ระบบปฏิบัติการหรือแอปพลิเคชัน และจัดให้มีการกำหนดบทบาทและสิทธิ์การเข้าถึง (Role-based Access Control) เพื่อให้แน่ใจว่าบุคคลมีสิทธิ์เข้าถึงข้อมูล หรือระบบตามที่จำเป็นเท่านั้น และกำหนดบุคลากรที่รับผิดชอบดูแลการเข้าถึงอินเทอร์เฟซ และระบบในช่วงที่ผู้ให้บริการภายนอกมาปฏิบัติงาน เช่น หากมีการเชื่อมต่ออุปกรณ์ภายนอก (USB) ต้องจัดให้มีการตรวจสอบ และควบคุมโดยบุคลากรภายในหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงควรพิจารณาให้ดำเนินการในสถานที่ของหน่วยงานผู้ให้บริการขนส่งทางราง (หากเป็นไปได้) และพิจารณาติดตามและเฝ้าระวังการเข้าถึงด้วยเครื่องมือที่สามารถตรวจสอบและแจ้งเตือนอัตโนมัติเมื่อมีเหตุการณ์ที่ผิดปกติ เช่น Security Event Manager หรือ USB Defender

๖. กำหนดให้มีการดำเนินการจัดการดูแลระบบให้มีความมั่นคงปลอดภัย (Principles of Secure System Administration) โดยพิจารณาดำเนินการตามหลักการ ๕ หลักการ ดังนี้

(๑) ดำเนินการตรวจสอบและป้องกันไม่ให้อุปกรณ์ที่ใช้ในการดูแลระบบ (Gain Trust in your Management Devices) เช่น อุปกรณ์จัดการเซิร์ฟเวอร์ระบบควบคุมการเข้าถึง หรืออุปกรณ์เครือข่ายถูกโจมตีหรือถูกใช้ในทางที่ผิด โดยการรักษาความมั่นคงปลอดภัยของอุปกรณ์ สามารถพิจารณาได้ ดังนี้

- ดำเนินการตั้งค่ารหัสผ่านอุปกรณ์การจัดการทั้งหมด และใช้รหัสผ่านที่มีความยาวและซับซ้อน เช่น การใช้ตัวเลข ตัวอักษร และอักขระพิเศษ รวมทั้งการเปลี่ยนรหัสผ่านเป็นระยะ ตัวอย่างเช่น ตั้งรหัสผ่านที่ยาวกว่า ๑๒ ตัวอักษร และหลีกเลี่ยงการใช้รหัสผ่านที่เดาง่าย เช่น “๑๒๓๔๕๖” หรือ “password” เป็นต้น

- พิจารณาใช้การยืนยันตัวตนด้วยหลายปัจจัย (Multi-Factor Authentication - MFA) เช่น การยืนยันตัวตนผ่านรหัสผ่านและรหัส OTP (One-Time Password) ที่ส่งไปยังมือถือ เช่น ใช้ระบบที่มีการส่งรหัส OTP ผ่านแอปพลิเคชัน (เช่น Google Authenticator) หรือ SMS เพื่อยืนยันตัวตน

- พิจารณาการควบคุมการเข้าถึง (Access Control) อุปกรณ์โดยจำกัดเฉพาะผู้ที่ได้รับอนุญาต เช่น ผู้ดูแลระบบ หรือบุคลากรที่จำเป็นต้องทำงานกับอุปกรณ์เท่านั้น เช่น ใช้การตั้งค่า Role-based Access Control (RBAC) เพื่อให้ผู้ที่มีบทบาทเฉพาะสามารถเข้าถึงอุปกรณ์ที่เกี่ยวข้องเท่านั้น

- พิจารณาเข้ารหัสข้อมูล (Encryption) ที่ถูกส่งหรือเก็บในอุปกรณ์การจัดการควรถูกเข้ารหัส เพื่อป้องกันการดักจับ หรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต เช่น ใช้การเข้ารหัสไฟล์ข้อมูลด้วย AES-๒๕๖ หรือการเชื่อมต่อแบบ SSL/TLS สำหรับ การส่งข้อมูลผ่านเครือข่าย

- พิจารณาบันทึกและเฝ้าระวังการเข้าถึง (Logging and Monitoring) โดยติดตั้งระบบการบันทึกและเฝ้าระวังการเข้าถึงอุปกรณ์การจัดการ เพื่อสามารถตรวจสอบการเข้าถึงที่ผิดปกติหรือไม่สามารถตรวจสอบได้ เช่น ใช้ระบบ Security Information and Event Management (SIEM)

- พิจารณาอัปเดตซอฟต์แวร์และแพตช์ (Software Updates and Patching) อุปกรณ์การจัดการอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ที่อาจเกิดขึ้นจากซอฟต์แวร์ที่ล้าสมัย เช่น ตั้งค่าให้อุปกรณ์จัดการอัปเดตแพตช์อัตโนมัติ เพื่อป้องกันช่องโหว่ที่อาจถูกใช้ ในการโจมตี

- พิจารณาจำกัดการใช้งานในช่วงเวลาที่จำเป็น โดยจำกัดการเข้าถึงอุปกรณ์การจัดการเฉพาะในเวลาที่จำเป็น เช่น เมื่อมีการตรวจสอบหรือบำรุงรักษาเท่านั้น และทำการล็อกการเข้าถึงในเวลาที่ไม่ได้ใช้งาน เช่น ใช้การกำหนดเวลาเข้าถึงระบบให้สามารถเข้าถึงเครื่องแม่ข่ายการจัดการได้เฉพาะในช่วงเวลาทำการเท่านั้น

- ดำเนินการตรวจสอบสิทธิ์การเข้าถึง (Access Review) อุปกรณ์การจัดการอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เช่น ทบทวนสิทธิ์การเข้าถึงของผู้ใช้ในทุก ๆ ไตรมาส รวมถึงใช้มาตรการอื่นที่เข้มงวดร่วมกัน เช่น การใช้รหัสผ่านที่แข็งแรง การยืนยันตัวตนด้วยหลายปัจจัย การควบคุมการเข้าถึงที่จำกัด และการตรวจสอบการเข้าถึงอย่างสม่ำเสมอ

- ในกรณีที่มีการพิจารณาใช้ระบบ Cloud ต้องพิจารณาดำเนินการเลือกผู้ให้บริการ Cloud ที่มีการรับรองมาตรฐานความปลอดภัย เช่น ISO/IEC ๒๗๐๐๑, SOC๒ เป็นต้น และพิจารณาให้มีการควบคุมความมั่นคงปลอดภัยภายในบริการ Cloud ดังนี้

- มีการใช้การเข้ารหัส (Encryption) ข้อมูลทั้งในขณะที่เก็บ (Data at Rest) และขณะส่งข้อมูล (Data in Transit) แม้ว่าอุปกรณ์จะเชื่อมต่อผ่านอินเทอร์เน็ต เช่น บริการ Cloud ที่ใช้การเข้ารหัส AES-๒๕๖ เพื่อปกป้องข้อมูลที่จัดเก็บบนคลาวด์ และการเข้ารหัส SSL/TLS ในการส่งข้อมูล
- มีการควบคุมการเข้าถึง (Access Control) โดยตั้งค่าการควบคุมการเข้าถึงบริการ Cloud โดยใช้เทคนิค Multi-Factor Authentication (MFA) และ Role-based Access Control (RBAC) เช่น การตั้งค่าให้เฉพาะผู้ที่ผ่านการยืนยันตัวตนหลายขั้นตอน เช่น รหัสผ่านและ OTP ถึงจะสามารถเข้าถึงระบบได้
- มีการตรวจสอบและบันทึกข้อมูล (Logging and Monitoring) โดยใช้ระบบตรวจสอบและบันทึกกิจกรรมในระบบ Cloud เพื่อให้สามารถติดตามและตรวจสอบเหตุการณ์ที่เกิดขึ้น เช่น การตรวจสอบกิจกรรมที่ผิดปกติ หรือการเข้าถึงที่ไม่เหมาะสม เช่น การใช้เครื่องมือ Security Information and Event Management (SIEM) เพื่อตรวจจับการพยายามเข้าถึงโดยไม่ได้รับอนุญาต หรือการเปลี่ยนแปลงที่ผิดปกติในระบบ Cloud
- มีการแยกข้อมูลและการควบคุมภายในระบบ (Segmentation and Internal Controls) Cloud โดยแยกข้อมูล (data segmentation) และจัดแบ่งข้อมูลในพื้นที่ที่มีการควบคุมที่แตกต่างกัน เช่น การจัดเก็บข้อมูลที่สำคัญในสภาพแวดล้อมที่แยกออกจากข้อมูลที่ไม่สำคัญ เช่น บริการ Cloud ที่ให้จัดการกับ Virtual Private Cloud (VPC) เพื่อให้ระบบต่าง ๆ ที่เชื่อมต่อกันในพื้นที่แยกต่างหากและมีการควบคุมที่ดีขึ้น
- มีการจัดการช่องโหว่ (Vulnerability Management) โดยการตรวจสอบ และป้องกันช่องโหว่ในระบบ Cloud ด้วยการอัปเดตแพตช์ซอฟต์แวร์และการใช้เครื่องมือในการทดสอบเจาะระบบ (Penetration Testing) เช่น การใช้เครื่องมือ Qualys หรือ Tenable ในการตรวจสอบความเสี่ยงและช่องโหว่ในระบบ Cloud

(๒) ออกแบบระบบให้มีการป้องกันช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ (Protect your Administration Interfaces) โดยให้สิทธิ์การดำเนินงานพิเศษแก่ผู้ใช้ที่เข้าถึงระบบผ่านช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบและบริการของหน่วยงานผู้ให้บริการขนส่งทางรางเท่านั้น (Administration Interfaces) และอนุญาตให้เฉพาะผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่จะเข้าถึงช่องทางหรือระบบที่กำหนด เช่น

- การใช้รหัสผ่านที่เข้มงวดและการยืนยันตัวตนหลายขั้นตอน (Multi-Factor Authentication: MFA) ใช้ระบบที่ต้องการทั้งรหัสผ่านและรหัส OTP (One-Time Password) เพื่อเพิ่มความมั่นคงปลอดภัย เมื่อเข้าถึงช่องทางการเชื่อมต่อสำหรับการจัดการ เช่น เมื่อผู้ดูแลระบบต้องการเข้าถึงเครื่องแม่ข่ายเซิร์ฟเวอร์ หรือระบบสำคัญ ผู้ดูแลต้องใช้รหัสผ่านร่วมกับรหัส OTP ที่ส่งไปยังมือถือ เพื่อยืนยันตัวตนก่อนการเข้าถึง

- การตั้งค่าการเข้าถึงที่จำกัด (Access Control) กำหนดให้การเข้าถึงเครื่องมือการจัดการดูแลระบบสามารถทำได้เฉพาะผู้ที่ได้รับอนุญาต เช่น ผู้ดูแลระบบเท่านั้น เช่น จำกัดการเข้าถึง SSH (Secure Shell) หรือ Remote Desktop (RDP) โดยผู้ที่มีบทบาทในการดูแลระบบหรือผู้มีสิทธิ์พิเศษเท่านั้น
- การใช้ช่องทางการเชื่อมต่อที่มีความมั่นคงปลอดภัยสูง เช่น การเข้ารหัสการเชื่อมต่อ (SSL/TLS) สำหรับการเข้าถึงระบบจากภายนอก โดยการใช้ Virtual Private Network (VPN) หรือ SSH ในการเข้าถึงเครื่องแม่ข่าย หรือฐานข้อมูลภายใน เพื่อป้องกันการดักจับข้อมูลระหว่างทาง

ตัวอย่างการใช้โค้ดและการตั้งค่าในการจัดการระบบ

- การใช้โค้ดสำหรับการติดตั้ง และอัปเดตซอฟต์แวร์ หน่วยงานอาจใช้ Automated Scripts หรือ Configuration Management Tools เช่น Ansible, Puppet, หรือ Chef เพื่อจัดการติดตั้งและอัปเดตซอฟต์แวร์โดยอัตโนมัติ โดยไม่ต้องเข้าถึงระบบด้วยการเชื่อมต่อแบบตรง ตัวอย่างเช่น ใช้โค้ดหรือสคริปต์ในการติดตั้งแอปพลิเคชันบนเซิร์ฟเวอร์หลายเครื่องในคราวเดียว โดยไม่ต้องใช้การเข้าถึงทางกายภาพ หรือการเชื่อมต่อจากระยะไกล
- การจัดการการตั้งค่าผ่านไฟล์คอนฟิก โดยใช้ Configuration Files เช่น JSON หรือ YAML ในการกำหนดค่าของระบบต่าง ๆ การกำหนดสิทธิการเข้าถึงระบบผ่านไฟล์คอนฟิกที่ได้รับการตรวจสอบและบันทึกไว้ เช่น การตั้งค่าผู้ใช้ การตั้งค่าความมั่นคงปลอดภัย หรือการตั้งค่าฐานข้อมูล
- การใช้โค้ดในการควบคุมการเข้าถึง เช่น เซิร์ฟเวอร์, เครือข่าย, ฐานข้อมูล, Storage, Load Balancer, Firewall, และการตั้งค่าต่าง ๆ ด้วยการเขียนโค้ด (Code) โดยใช้แนวคิด และวิธีการจัดการโครงสร้างพื้นฐานด้านไอที (Infrastructure as Code (IaC)) เช่น
  - Terraform ซึ่งใช้ในการจัดเตรียมและจัดการทรัพยากรบน Cloud Provider ต่าง ๆ เช่น AWS, Azure, GCP และ On-Premises
  - Ansible ซึ่งเน้นการจัดการ Configuration Management เช่น ติดตั้งซอฟต์แวร์, ตั้งค่าเซิร์ฟเวอร์ และ Automation
  - Puppet, Chef, Salt Stack เป็นเครื่องมือเน้น Configuration Management คล้าย Ansible
  - AWS CloudFormation เป็นเครื่องมือ IaC เฉพาะสำหรับ Amazon Web Services (AWS)
  - Azure Resource Manager (ARM) Templates เป็นเครื่องมือ IaC เฉพาะสำหรับ Microsoft Azure
  - Google Cloud Deployment Manager เป็นเครื่องมือ IaC เฉพาะสำหรับ Google Cloud Platform (GCP)

(๓) จัดการดูแลและการบริหารความเสี่ยงโดยใช้ระดับชั้น (Risk Manage Administration Using Tiers) โดยประยุกต์การบริหารความเสี่ยงที่ใช้ในทางปฏิบัติกับการจัดการดูแลระบบของหน่วยงานผู้ให้บริการขนส่งทางรางให้สอดคล้องกับระดับชั้น (Tiered Administration) โดยพิจารณาดำเนินการ ดังนี้

๑) ดำเนินการระบุและประเมินความเสี่ยงของช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ (Identify and Assess the Risks your Administration Interfaces) ในแต่ละระดับชั้น (Tier) โดยช่องทางการเชื่อมต่อแบ่งเป็น ๓ ส่วนหลัก ๆ ดังนี้

(๑) การเชื่อมต่อผ่านเครือข่าย (Network-based Connection) ได้แก่

- Secure Shell (SSH) ซึ่งเป็นโปรโตคอลที่ใช้ในการเข้าถึง และจัดการเซิร์ฟเวอร์หรืออุปกรณ์เครือข่ายระยะไกลได้อย่างปลอดภัย โดยมีการเข้ารหัสข้อมูลเหมาะสำหรับการบริหารจัดการ Linux/Unix server และอุปกรณ์ network เช่น Router, Switch
- Remote Desktop Protocol (RDP) ใช้สำหรับเข้าถึงและควบคุมเครื่องคอมพิวเตอร์ Windows ระยะไกลแบบกราฟิก (GUI) ทำให้ผู้ดูแลระบบสามารถทำงานบนเครื่องนั้นได้เหมือนนั่งอยู่หน้าจอ
- Virtual Network Computing (VNC) มีลักษณะคล้ายกับ RDP แต่สามารถใช้งานได้หลากหลายแพลตฟอร์ม (Windows, Linux, macOS) เพื่อเข้าถึงและควบคุมเดสก์ท็อประยะไกล
- Web-based Interface (Console/Management Portal) เป็นอุปกรณ์เครือข่ายและซอฟต์แวร์หลายตัวมีหน้าเว็บสำหรับจัดการทำให้ผู้ดูแลระบบสามารถเข้าถึงและกำหนดค่าผ่านเว็บเบราว์เซอร์ได้จากทุกที่ที่มีอินเทอร์เน็ต เช่น เราเตอร์, สวิตช์, ไฟร์วอลล์, หรือแพลตฟอร์มคลาวด์
- SNMP (Simple Network Management Protocol) เป็นโปรโตคอลที่ใช้ในการตรวจสอบและจัดการอุปกรณ์เครือข่ายผู้ดูแลระบบสามารถใช้เครื่องมือ SNMP เพื่อรวบรวมข้อมูลสถานะของอุปกรณ์, ตั้งค่าการแจ้งเตือน, และควบคุมการทำงานบางอย่างได้
- APIs (Application Programming Interfaces) ใช้สำหรับระบบที่มีความซับซ้อนและต้องการการจัดการแบบอัตโนมัติ (Automation) ผู้ดูแลระบบสามารถใช้ API เพื่อเขียนสคริปต์หรือโปรแกรมในการสั่งการและรวบรวมข้อมูลจากระบบได้โดยตรง

(๒) การเชื่อมต่อแบบกายภาพ (Physical Connection) ได้แก่

- Console Port/Serial Port เป็นอุปกรณ์เครือข่ายหลายตัว เช่น Router, Switch มีพอร์ต Console ที่ใช้สายเคเบิล Serial เช่น RJ๔๕ to DB๙ สำหรับการเชื่อมต่อโดยตรงจากคอมพิวเตอร์เพื่อเข้าถึง Command Line Interface (CLI) ในการกำหนดค่าเริ่มต้นหรือแก้ไขปัญหาเมื่อการเชื่อมต่อเครือข่ายยังไม่พร้อมใช้งาน
- Keyboard, Video, Mouse (KVM) Switch ใช้สำหรับควบคุมเซิร์ฟเวอร์หลายเครื่องจากชุดคีย์บอร์ด, จอภาพ, และเมาส์ชุดเดียว เหมาะสำหรับศูนย์ข้อมูลหรือห้องเซิร์ฟเวอร์ที่มีอุปกรณ์จำนวนมาก
- Out-of-Band Management (OOB) เป็นช่องทางการจัดการที่แยกออกจากเครือข่ายหลัก มักใช้ในกรณีที่เครือข่ายหลักมีปัญหา เช่น IPMI (Intelligent Platform Management Interface) บนเซิร์ฟเวอร์ที่ช่วยให้สามารถควบคุมเปิด - ปิด, รีบูต, หรือเข้าถึงคอนโซลของเซิร์ฟเวอร์ได้แม้จะไม่มีระบบปฏิบัติการทำงานอยู่

(๓) เครื่องมือและแพลตฟอร์มเฉพาะ ได้แก่

- Google Admin, Family Link เป็นแพลตฟอร์มสำหรับการจัดการบัญชีและอุปกรณ์ของผู้ใช้ในบริบทเฉพาะ เช่น Google Workspace, บัญชีครอบครัว
- Managed Network Services เช่น จาก UIH เป็นบริการจากผู้ให้บริการภายนอกที่ดูแลจัดการระบบเครือข่ายทั้งหมดให้องค์กร โดยผู้ดูแลระบบขององค์กรจะเชื่อมต่อกับแพลตฟอร์มหรือทีมงานของผู้ให้บริการเพื่อจัดการ

๒) ดำเนินการระบุระดับชั้นการจัดการดูแลระบบ (Identify your Administration Tiers) ซึ่งควรใช้ผลจากการประเมินความเสี่ยง เพื่อกำหนดระดับชั้นของช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบ เช่น

- ระดับชั้น ๐ (Tier ๐) เป็นระดับชั้นที่เป็นรากฐานในการดำเนินการจัดการดูแลอื่น ๆ ดังนั้น หากผู้โจมตีสามารถโจมตีรากฐานได้ผู้โจมตีสามารถเข้าถึงส่วนประกอบในระดับชั้นอื่น ๆ เช่น
  - ผู้ดูแลระบบที่มีสิทธิสูงสุดในการเข้าถึง และจัดการทรัพยากรทั้งหมดในโดเมน (Root Domain Administrators) รวมถึงสามารถสร้างบัญชีที่มีสิทธิพิเศษ (Highly Privilege Accounts) เพิ่มเติมได้
  - บัญชีรูท (Root Account) ในบริการคลาวด์ที่จัดการสิทธิของบัญชีอื่น ๆ ทั้งหมด (Manages the Privileges of all Other Accounts)
  - โครงสร้างพื้นฐานแบบออฟไลน์ (Offline Infrastructure) เพื่อสร้างเอกสาร อุปกรณ์หรือ เครื่องมือใด ๆ ที่มีข้อมูลเกี่ยวกับการเข้ารหัส และมีความสำคัญต่อการเข้ารหัส ถอดรหัส หรือการยืนยันตัวตน ของการสื่อสารทางไกลการเข้ารหัส (Cryptographic Material)
- ระดับชั้น ๑ (Tier ๑) เป็นระดับชั้นของโครงสร้างพื้นฐานที่ช่วยให้สามารถดำเนินการที่ต้องใช้สิทธิพิเศษ (Highly Privileged Functions) ต่อระบบที่สำคัญได้ ซึ่งการโจมตีโครงสร้างพื้นฐานในระดับชั้น ๑ อาจก่อให้เกิดการหยุดชะงักในวงกว้าง เช่น
  - ผู้ดูแลระบบของฐานข้อมูลที่สำคัญ เนื่องจากจัดเก็บข้อมูลที่อ่อนไหวจำนวนมาก ซึ่งระบบอื่น จำเป็นต้องใช้ฐานข้อมูลนี้ในการดำเนินงานด้วย
  - ความสามารถในการควบคุมและจัดการบริการที่สำคัญจำนวนมากในสภาพแวดล้อมแบบคลาวด์
  - โครงสร้างพื้นฐานที่ใช้ในการกำหนดค่าขีดแบ่งให้แก่ระบบควบคุมที่สำคัญ (Set Operational Thresholds on Critical Control Systems)
- ระดับชั้น ๒ (Tier ๒) เป็นระดับชั้นของโครงสร้างพื้นฐานที่ช่วยให้ดำเนินการที่ต้องใช้สิทธิพิเศษ (Privileged Functions) ได้ และเป็นการดำเนินการต่อส่วนประกอบจำนวนน้อย “ส่วนประกอบ” ซึ่งหมายถึง ฟังก์ชันหรือบริการที่เกี่ยวข้องกับการเข้าถึงและการดำเนินการของผู้ดูแลระบบ เช่น การเข้าถึงแอปพลิเคชันสำคัญ การจัดการเครื่องแม่ข่าย หรือการปรับค่าระบบในลักษณะที่มีผลกระทบต่อการทำงานของระบบ แต่ไม่ได้ส่งผลกระทบสูงต่อการดำเนินงานตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น

- การเข้าถึงแอปพลิเคชันสนับสนุนธุรกิจที่สำคัญ (Important Business Support Application) ของผู้ดูแลระบบ
- การเข้าถึงระดับรูทบนเว็บเครื่องแม่ข่ายเว็บส่วนหน้า (Front End Web Server) ซึ่งเป็นส่วนหนึ่ง ของสถาปัตยกรรมระบบคลาวด์ที่เป็นระบบใหญ่
- การจัดการดูแลแผงควบคุม (Dashboard) ที่หน่วยงานใช้เฝ้าระวังระบบควบคุมอุตสาหกรรม (Monitoring an Industrial Control System)

● ระดับชั้น ๓ (Tier ๓) เป็นระดับชั้นของโครงสร้างพื้นฐานที่อนุญาตให้ดำเนินการได้อย่างจำกัด (A Constrained Set of Functions) และเป็นการดำเนินการต่อส่วนประกอบเดียว หรือจำนวนน้อย ซึ่งผลกระทบของการโจมตีโครงสร้างพื้นฐานในระดับนี้เป็นสิ่งที่ไม่ต้องการให้เกิด เนื่องจากอาจส่งผลถึงชื่อเสียงของหน่วยงานผู้ให้บริการขนส่งทางราง แต่ไม่ส่งผลเสียหายต่อการดำเนินการมากนัก เช่น

- บุคลากรฝ่ายสนับสนุนด่านหน้า (First Line Support staff) ใช้คำสั่งรีเซ็ตรหัสผ่าน
- ความสามารถในการทริกเกอร์หรือกระตุ้น (Trigger) การกระทำที่กำหนดไว้ล่วงหน้า (Predefined Action) ในสภาพแวดล้อมระบบคลาวด์ เช่น การใช้ฟีเจอร์โค้ดใหม่ในสภาพแวดล้อมที่ใช้งานจริง
- การปรับเปลี่ยนค่าในระบบควบคุมอุตสาหกรรมที่ถูกจำกัดขอบเขตไว้ด้วยส่วนประกอบ หรือด้วยผู้ดูแลระบบในระดับที่ต่ำกว่า

๓) กำหนดกลยุทธ์การจัดการดูแลระบบ (Define an Administration Strategy) เมื่อระบบมีผู้ใช้งานมากขึ้น และผลกระทบจากการโจมตีมีความสำคัญมากขึ้น โดยทบทวนกลยุทธ์การจัดการดูแลระบบในแต่ละระดับชั้น (Tier) ให้เหมาะสมกับความเสี่ยงที่เพิ่มขึ้น โดยให้ความสำคัญกับการจัดการสิทธิพิเศษในระดับชั้น ๐ (Tier ๐) และลดความเสี่ยงในระดับชั้นที่ต่ำกว่า

๔) ดำเนินการตามกลยุทธ์การจัดการดูแล (Implement your Administration Strategy) โดยกำหนดมาตรการควบคุมทางเทคนิคที่เหมาะสมสำหรับแต่ละระดับชั้น เช่น การใช้การพิสูจน์ตัวตนหลายปัจจัย (MFA) ในระดับชั้น ๐ (Tier ๐) และการใช้การควบคุมสิทธิพิเศษ (Privileged Access Management) โดยควรคำนึงถึงการให้สิทธิน้อยที่สุด (Least Privilege) และการรักษาความสมดุลระหว่างความเสี่ยงและความคล่องตัวในการจัดการ

๕) ปรับแต่งกลยุทธ์ (Evolve and Refine your Strategy) โดยใช้ข้อมูลจากการบันทึก (Logging Data) และการทำงานร่วมกับผู้ดูแลระบบในแต่ละระดับชั้น เพื่อปรับปรุงและพัฒนากลยุทธ์การจัดการดูแลระบบอย่างต่อเนื่อง โดยปรับให้เหมาะสมกับความเสี่ยงที่เพิ่มขึ้นในแต่ละระดับ

๖) สนับสนุนผู้ดูแลระบบ (Support your Administrators) โดยส่งเสริมให้มีการดำเนินการทำงานร่วมกับผู้ดูแลระบบในแต่ละระดับชั้น เพื่อกำหนดนโยบายและการดำเนินการที่โปร่งใส และช่วยสนับสนุนการดำเนินการให้ผู้ดูแลระบบสามารถทำงานได้อย่างมีประสิทธิภาพ โดยให้การควบคุมที่เหมาะสมตามระดับความสำคัญของแต่ละชั้น

(๔) จัดการการเข้าถึงด้วยสิทธิพิเศษ (Use Privileged Access Management) โดยการอนุญาตให้บุคคลเข้าถึงระบบหนึ่ง ๆ เป็นการอนุญาตให้เข้าถึง ณ เวลาใด ด้วยเหตุผลและวิธีการใด รวมถึงให้สิทธิน้อยที่สุด (Least Privilege) แก่ผู้ดูแลระบบ (Privileged User) และยกเลิกสิทธิ เมื่อผู้ดูแลระบบไม่จำเป็นต้องใช้สิทธินั้น โดยพิจารณาดำเนินการ ดังนี้

- ยอมให้เข้าถึงจากอุปกรณ์ที่ได้รับอนุญาตเท่านั้น (Only Allow Permitted Devices) โดยกำหนดมาตรการควบคุมทางสถาปัตยกรรม และยอมให้อุปกรณ์ได้รับอนุญาตสามารถเข้าถึง (Privileged Access Management: PAM) และช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบได้เท่านั้น
- ยอมให้เฉพาะผู้ใช้ที่ได้รับอนุญาตสามารถร้องขอข้อมูลประจำตัว (Only Allow Permitted Users) โดยกำหนดให้มีการพิสูจน์ตัวตนที่รัดกุม (Strong Authentication) และยอมให้เฉพาะผู้ดูแลระบบที่ได้รับอนุญาตเท่านั้นเข้าสู่ระบบ เพื่อขอข้อมูลประจำตัวชั่วคราวสำหรับการจัดการดูแลระบบ
- แจ้งเหตุผลอันสมควรในการจัดการดูแล (Justify Administration Intent) กำหนดให้ผู้ดูแลระบบต้องแสดงเหตุผลในการจัดการดูแลระบบ เพื่อเป็นข้อมูลของกระบวนการร้องขอในการพิจารณาอนุมัติ หรือยับยั้งบุคคลภายในที่เป็นอันตรายที่จะเข้าถึงระบบ
- กำหนดให้มีการอนุมัติที่เหมาะสม (Use Appropriate Approvals) โดยพิจารณาคำร้องขอและกฎสำหรับการอนุมัติการเข้าถึงช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบอย่างรอบคอบ โดยพิจารณาจากระดับความเสี่ยงของระบบ รวมถึงผลกระทบจากเหตุการณ์ที่ผู้โจมตีสามารถเข้าถึงช่องทางการเชื่อมต่อ
- กำหนดให้รับรองตัวตนที่มีความมั่นคงปลอดภัยและรัดกุม (Use Secure and Strong Credentials) โดยเข้ารหัสระหว่างการส่งข้อมูลประจำตัว และเข้ารหัสข้อมูลประจำตัวที่ยากต่อการปลอมแปลงและถอดรหัส
- จำกัดระยะเวลาการใช้งานสิ่งที่ใช้รับรองตัวตน (Constrain Credential Validity Period) โดยจัดให้มีการดำเนินการกำหนดกรอบเวลาการใช้งานข้อมูลประจำตัวของผู้ดูแลระบบของแต่ละระบบตามความต้องการในการใช้งานข้อมูลประจำตัว
- ให้สิทธิน้อยที่สุดแก่ผู้ที่มีบทบาทในการจัดการดูแลระบบ (Use Least Privilege on Administration Roles) ให้กับผู้ดูแลระบบ เพื่อทำงานที่จำเป็นสำเร็จเท่านั้น
- ในกรณีที่มีการพิจารณาใช้ระบบ PAM (Protect the PAM System) ต้องดำเนินการพิจารณามาตรการปกป้องระบบ PAM (Protect the PAM System) ใช้มาตรการควบคุมทางสถาปัตยกรรม เช่น การป้องกันหลายชั้น (Defense in Depth) หลักการให้สิทธิ์น้อยที่สุด (Principle of Least Privilege) การแบ่งแยกหน้าที่ (Separation of Duties) เป็นต้น รวมถึงติดตั้งหรืออัปเดตแพตช์เป็นประจำ และกำหนดให้ระบบ PAM อยู่ในกลยุทธ์การเฝ้าระวังความมั่นคงปลอดภัย (Security Monitoring Strategy)
- พิจารณาความพร้อมใช้งานของ PAM (Consider PAM Availability) ให้มีสภาพพร้อมใช้งานสูง (High Availability) และกำหนดกระบวนการสำรองฉุกเฉิน (Emergency Backup Process) สำหรับการเข้าถึงระบบต่าง ๆ

(๕) บันทึกและตรวจสอบกิจกรรมการจัดการดูแลระบบ (Log and Audit Administration Activities) ที่เกี่ยวข้องกับการจัดการดูแลระบบ และตรวจสอบบันทึกอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าผู้ดูแลระบบได้ดำเนินการตามขั้นตอนที่ได้รับอนุมัติและไม่เกิดการกระทำที่ผิดพลาดหรือไม่เหมาะสม โดยพิจารณาดำเนินการ ดังนี้

- ดำเนินการเฝ้าระวังโดยพิจารณาผลประเมินความเสี่ยง และภัยคุกคามที่อาจเกิดขึ้น เพื่อระบุช่องทางการเชื่อมต่อสำหรับการจัดการดูแลระบบที่อาจตกเป็นเป้าหมายการโจมตี ทั้งนี้สามารถนำข้อมูลผลประเมินความเสี่ยง และภัยคุกคามที่อาจเกิดขึ้น มากำหนดกลยุทธ์การรวบรวมบันทึกและการเฝ้าระวังความมั่นคงปลอดภัย
- ดำเนินการรวบรวมข้อมูลที่ถูกต้อง (Collect the Right Data) โดยพิจารณาข้อมูลที่จำเป็นต้องใช้ เพื่อสนับสนุนการตรวจสอบและการเฝ้าระวัง และดำเนินการรวบรวมข้อมูลนั้น
- กำหนดนิยามสถานะปกติ (Define Normal) เพื่อใช้เป็นข้อมูลพื้นฐานสำหรับการเฝ้าระวังความมั่นคงปลอดภัย
- ทำงานร่วมกับนักวิเคราะห์ความมั่นคงปลอดภัย (Work with Security Analysis) เพื่อให้เข้าใจการทำงานของระบบ และสถานะปกติของระบบ เพื่อให้นักวิเคราะห์สามารถระบุพฤติกรรมที่น่าสงสัยได้ถูกต้อง
- ทดสอบการเฝ้าระวัง (Test your Monitoring) โดยการตรวจสอบประสิทธิภาพการทำงานของช่องทางการเชื่อมต่อ สำหรับการจัดการดูแลระบบ โดยฝึกซ้อมการโจมตีร่วมกับฝึกการป้องกัน (Run Red and Blue Team Exercises) ที่ช่องทางการเชื่อมต่อ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการควบคุมสิทธิการเข้าถึงเครือข่ายและบริการเครือข่าย โดยพิจารณาอย่างน้อย ดังนี้

๑) จัดกลุ่มผู้ใช้งานและอุปกรณ์เครือข่ายตามบทบาทหน้าที่ และกำหนดสิทธิการเข้าถึงเครือข่ายแยกตาม VLAN หรือ Segment รวมถึงกำหนดให้มีการบังคับใช้นโยบายการเข้าถึงเท่าที่จำเป็น (Least Privilege)

๒) พิจารณาใช้ระบบควบคุมการเข้าถึงเครือข่าย (NAC – Network Access Control) เพื่อตรวจสอบสถานะของอุปกรณ์ก่อนเชื่อมต่อ

๓) กำหนดให้ผู้ใช้งานต้องยืนยันตัวตนด้วยรหัสผ่านที่รัดกุม หรือ Multi-Factor Authentication (MFA)

๔) กำหนดให้มีการใช้งาน VPN พร้อมทั้งกำหนดให้มีการตรวจสอบสิทธิ์ ในกรณีที่มีผู้ใช้งานภายนอกต้องการเข้าถึงระบบ เช่น พาร์ตเนอร์ หรือผู้รับจ้าง เป็นต้น

๕) กำหนดให้มีการจำกัดเวลาการเชื่อมต่อและ Session Timeout สำหรับการเข้าถึงจากภายนอก

๖) กำหนดให้มีการแยกเครือข่ายที่สำคัญไว้ใน Zone ที่มีมาตรการควบคุมเคร่งครัด เช่น DMZ เป็นต้น

๗) กำหนดให้มีการเปิดใช้งานเฉพาะพอร์ต หรือโปรโตคอลที่จำเป็น (Port Management) และปิดพอร์ตที่ไม่ได้ใช้งาน

๘) กำหนดให้มีการบันทึก Log การเข้าถึงเครือข่ายทุกประเภท เช่น การพิสูจน์ตัวตน การเชื่อมต่อและการปฏิเสธการเข้าถึง

๙) กำหนดให้มีการตรวจสอบและวิเคราะห์ Log อย่างสม่ำเสมอ เพื่อค้นหาพฤติกรรมผิดปกติ

๑๐) พิจารณาติดตั้งระบบ IDS/IPS หรือ Firewall ที่มีความสามารถในการตรวจจับการรุกล้ำ

๒. กำหนดให้มีการบริหารจัดการอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคล (BYOD) โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการขออนุมัติ พร้อมทั้งลงทะเบียนอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคลในกรณีที่มีการนำอุปกรณ์ส่วนบุคคลมาใช้งาน

๒) จำกัดการเข้าถึงของอุปกรณ์พกพาและอุปกรณ์ส่วนบุคคล เฉพาะเครือข่าย Guest หรือ VLAN ที่แยกจากเครือข่ายหลัก

๓) ห้ามเชื่อมต่ออุปกรณ์ IoT ที่ไม่ได้รับอนุญาตเข้ากับเครือข่ายหลัก

๓. กำหนดให้มีการบริหารจัดการลงทะเบียนการเข้าถึงระบบของผู้ใช้งาน ก่อนที่จะได้รับอนุญาตให้เข้าใช้งานระบบ ตามสิทธิหน้าที่ความรับผิดชอบของผู้ใช้งาน หากในกรณีที่มีสิทธิพิเศษที่นอกเหนือหน้าที่ความรับผิดชอบ ต้องได้รับอนุญาตจากเจ้าของระบบ หรือผู้มีอำนาจก่อนได้รับสิทธิ

๔. ห้ามใช้งานบัญชีร่วมกัน ยกเว้นกรณีจำเป็น และต้องกำหนดมาตรการควบคุมการเข้าถึงให้สามารถชี้บ่งถึงตัวบุคคลที่เข้าถึงระบบในแต่ละช่วงเวลา

๕. กำหนดให้มีการบริหารจัดการถอดถอนสิทธิการเข้าถึงทันที หรือกำหนดระยะเวลาภายใน ๒๔ ชั่วโมง หลังได้รับแจ้ง ในกรณีที่ผู้ปฏิบัติงานลาออก, พ้นจากอำนาจหน้าที่, โยกย้ายตำแหน่ง, หรือครบกำหนดตามสัญญา เป็นต้น

๖. ในกรณีที่บัญชีมีความจำเป็นต้องเก็บไว้ เพื่อการสอบสวน หรือตรวจสอบ ต้องมีมาตรการควบคุมพิเศษให้ผู้ใช้งานไม่สามารถเข้าถึงได้ พร้อมทั้งระบุเหตุผลให้ชัดเจน

๗. กำหนดให้มีการบันทึก Log การเข้าถึงระบบอย่างน้อย ๙๐ วัน รวมถึงกำหนดให้มีการตรวจสอบ log อย่างน้อยปีละ ๑ ครั้งในระบบงานที่สำคัญ หรือบริการที่สำคัญ

๘. กำหนดให้มีการบริหารจัดการบัญชีผู้ใช้งานชั่วคราว (Temporary Access) โดยกำหนดอายุบัญชีผู้ใช้งานชั่วคราว (Account Expiry) ให้ชัดเจน และเมื่อครบกำหนดต้องมีการลบบัญชีหรือยกเลิกสิทธิอัตโนมัติ รวมถึงห้ามแปลงบัญชีชั่วคราวเป็นบัญชีถาวรโดยไม่มีการอนุมัติใหม่

๙. กำหนดให้มีการบันทึก Log การเปิด หรือปิดบัญชีผู้ใช้งานชั่วคราว และกำหนดให้มีการทบทวนหรือตรวจสอบบัญชีผู้ใช้งานชั่วคราวที่ไม่มีการใช้งานเป็นระยะเวลานาน เช่น เกินกว่า ๔๕ วัน หรือ ๙๐ วัน เพื่อตัดสิทธิ์หรือปิดบัญชีผู้ใช้งานชั่วคราว

๑๐. กำหนดให้มีการบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน โดยพิจารณาอย่างน้อยดังนี้

๑) พิจารณาให้มีการพิสูจน์ตัวตนโดยใช้รูปแบบ Multi-Factor Authentication (MFA) สำหรับระบบงานที่สำคัญ หรือบริการที่สำคัญ

๒) กำหนดให้มีการตั้งรหัสผ่านตามแนวทางการบริหารจัดการรหัสผ่าน และห้ามนำรหัสผ่านที่เหมือนกันไปใช้งานซ้ำในหลายระบบ

๓) การจัดเก็บข้อมูลความลับสำหรับการพิสูจน์ตัวตน ต้องพิจารณาให้มีมาตรการควบคุมอย่างน้อย ดังนี้

(๑) ต้องเข้ารหัสด้วยอัลกอริทึมที่เหมาะสม เช่น PBKDF๒, bcrypt, Argon๒ เป็นต้น

(๒) ห้ามแชร์ข้อมูลลับผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมล หรือ Line เป็นต้น

๔) กำหนดให้มีการเปลี่ยนรหัสผ่าน เมื่อมีเหตุบ่งชี้ว่ารหัสถูกเปิดเผย หรือถูกใช้ผิดปกติ รวมถึงห้ามใช้รหัสเดียวกันตลอดไป

๕) กำหนดให้มีการตรวจสอบบัญชีที่มีความพยายามเข้าสู่ระบบผิดซ้ำ ๆ หรือเข้าสู่ระบบผิดเวลาปกติ

๑๑. กำหนดให้มีการบริหารจัดการทบทวนสิทธิการเข้าถึงของผู้ใช้งาน โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดรอบการทบทวนสิทธิการเข้าถึงของผู้ใช้งานทุกคน อย่างน้อยปีละ ๑ ครั้ง

๒) กำหนดให้มีการทบทวนสิทธิสำหรับบัญชีที่มีสิทธิพิเศษ เช่น Admin, Root, Cloud Admin อย่างน้อย ทุก ๖ เดือน

๓) ในกรณีที่มีการเปลี่ยนแปลงผู้ใช้งาน เช่น เปลี่ยนตำแหน่ง, ย้ายหน่วยงาน, ลาออก ต้องทบทวนสิทธิทันทีหลังจากได้รับแจ้ง

๔) จัดให้มีหลักฐานในการทบทวนสิทธิตามรอบที่กำหนด เช่น จัดทำรายงานการทบทวนสิทธิ

๑๒. กำหนดให้มีการกำหนดหน้าที่และความรับผิดชอบของผู้ใช้งาน โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดบทบาทหน้าที่ความรับผิดชอบ โดยจัดหมวดหมู่ผู้ใช้งานให้ชัดเจน เช่น ผู้ใช้งานทั่วไป (End User) เจ้าของระบบ (Data Owner) ผู้ดูแลระบบ (Admin) เป็นต้น

๒) พิจารณาจัดทำ Role Responsibility Matrix (RACI) หรือ user Matrix ให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานในแต่ละหมวดหมู่ และสิทธิ์ในการเข้าถึงระบบ

๓) กำหนดให้มีการทบทวน Role Responsibility Matrix (RACI) หรือ User Matrix อย่างสม่ำเสมอ

๑๓. กำหนดให้มีการพิสูจน์ตัวตนที่ปลอดภัย (Authentication Control) โดยพิจารณากำหนดให้มีการบังคับใช้รหัสผ่านที่ปลอดภัยตามแนวทางการบริหารจัดการรหัสผ่าน

๑๔. กำหนดให้มีการควบคุมพฤติกรรมการเข้าสู่ระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการจำกัดจำนวนครั้งของการพยายามเข้าสู่ระบบ หากเกินจำนวนครั้งที่กำหนดให้ระบบทำการล็อคบัญชีไว้ชั่วคราว

๒) กำหนดให้มีการตั้งค่า Session Timeout เมื่อไม่มีการใช้งานระบบ

๓) กำหนดเงื่อนไข Context-based เช่น ไม่อนุญาต Login ข้ามประเทศ หรือข้ามเวลาทำการในระบบงานที่สำคัญ

๑๕. กำหนดให้มีมาตรการควบคุมการเข้าสู่ระบบแบบปลอดภัยสำหรับผู้ดูแลระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการแยกบัญชีผู้ใช้งานออกจากบัญชีผู้ดูแลระบบ (Admin) อย่างชัดเจน

๒) กำหนดให้มีการบันทึกกิจกรรมการเข้าระบบ (Log) ของผู้ดูแลระบบทุกครั้งที่มีการเข้าสู่ระบบ

๑๖. กำหนดให้มีมาตรการควบคุมการบันทึกและตรวจสอบการเข้าสู่ระบบ โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการบันทึกกิจกรรมการเข้าถึงระบบ (Log) เช่น วันเวลา, ชื่อผู้ใช้, IP, สถานะ (สำเร็จ/ล้มเหลว) การเข้าถึงระบบ

๒) กำหนดให้มีการจัดเก็บบันทึกกิจกรรมการเข้าถึงระบบ (Log) อย่างน้อย ๙๐ วัน หรือมากกว่าสำหรับระบบงานที่สำคัญ หรือบริการที่สำคัญ

๓) กำหนดให้มีการตรวจสอบบันทึกกิจกรรมการเข้าถึงระบบ (Log) เป็นประจำ เพื่อตรวจหาเหตุผิดปกติ เช่น Brute - Force หรือการเข้าระบบ (Login) จากตำแหน่งผิดปกติ เป็นต้น

๑๗. กำหนดให้มีการบริหารจัดการจำกัดการเข้าถึงข้อมูล โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้มีการจำแนกระดับข้อมูล เพื่อกำหนดการเข้าถึงข้อมูลตามระดับความสำคัญของข้อมูล

๒) จัดให้มีการระบุเจ้าของข้อมูล (Data Owner) เพื่อควบคุมการเข้าถึง และการปรับปรุงสิทธิ์

๓) ดำเนินการควบคุมสิทธิ์การเข้าถึง โดยพิจารณาหลักการ ดังนี้

(๑) กำหนดให้มีการใช้หลัก Least Privilege โดยให้ผู้ใช้งานเข้าถึงเฉพาะข้อมูลที่เกี่ยวข้องกับภาระหน้าที่งานเท่านั้น

(๒) ควบคุมการเข้าถึงโดยใช้หลัก Role-Based Access Control (RBAC) หรือ Attribute-Based Access Control (ABAC)

(๓) กำหนดให้ระบบต้องสามารถกำหนดสิทธิ์การเข้าถึง โดยแยกตามโฟลเดอร์ ไฟล์ หรือฐานข้อมูล เป็นต้น

(๔) กำหนดให้การขอเข้าถึงข้อมูลนอกเหนือจากอำนาจหน้าที่ต้องได้รับอนุมัติจากเจ้าของข้อมูล หรือผู้ที่ได้รับมอบอำนาจก่อนการเข้าถึง

(๕) กำหนดให้มีการทบทวนสิทธิ์การเข้าถึงข้อมูลอย่างน้อยปีละ ๑ ครั้ง

(๖) กำหนดให้มีการบันทึกกิจกรรมการเข้าถึงข้อมูล (Log) เช่น ชื่อผู้ใช้งาน เวลาที่เข้าใช้งาน และกิจกรรมที่ผู้ใช้งานดำเนินการกับระบบ เป็นต้น

(๗) พิจารณานำระบบ DLP (Data Loss Prevention) หรือ SIEM ตรวจจับพฤติกรรมเสี่ยงในการเข้าถึงข้อมูล

๑๘. กำหนดให้มีการบริหารจัดการรหัสผ่าน โดยพิจารณาตามแนวทางมาตรฐานสากล เช่น NIST SP ๘๐๐-๖๓B หรือ ISO๒๗๐๐๑ โดยกำหนดมาตรการ อย่างน้อยดังนี้

๑) รหัสผ่านต้องมีความยาวอย่างน้อย ๘ ตัวอักษร และสามารถใช้ได้สูงสุดถึง ๖๔ ตัวอักษร

๒) เน้นรหัสผ่านที่จำง่าย แต่ยากต่อการคาดเดา เช่น วลี หรือประโยคสั้น ๆ ที่มีความหมายเฉพาะตัว ตัวอย่าง: “chanrakmaw ๓ tuamakmak” “ฉันชอบกินข้าวผัดกะเพราไข่ดาว”

๓) เปลี่ยนรหัสผ่านเมื่อมีเหตุผล เช่น เมื่อสงสัยว่ารหัสผ่านอาจรั่วไหล หรือเมื่อมีการเปลี่ยนแปลงบทบาทในองค์กร

๔) หลีกเลี่ยงการใช้รหัสผ่านที่เป็น Common password หรือ Default password หรือรหัสผ่านที่รั่วไหลจากฐานข้อมูลที่ถูกแฮก หรือสิ่งที่สามารถคาดเดาได้ง่าย หรือข้อมูลส่วนตัวที่สามารถหาได้จากโซเชียลมีเดีย ตัวอย่าง: "password๑๒๓", "admin๑๒๓๔“ “วันเกิด” “หมายเลขโทรศัพท์”

๕) ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้ เช่น ใช้รหัส OTP ที่ส่งมาทาง SMS หรือแอปพลิเคชัน Authenticator หรือการยืนยันตัวตนทางชีวมิติ (Biometric Authentication) เช่น ลายนิ้วมือ หรือใบหน้า เป็นต้น

๖) ไม่ควรใช้รหัสผ่านซ้ำกันในแต่ละระบบ และไม่ควรบอกรหัสผ่านแก่ผู้อื่น

๑๙. กำหนดให้มีการบริหารจัดการใช้โปรแกรมอรรถประโยชน์ โดยพิจารณามาตรการควบคุมอย่างน้อยดังนี้

๑) จัดทำ Whitelist ของ โปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานในองค์กร

๒) ห้ามติดตั้งหรือใช้งานโปรแกรมอรรถประโยชน์ที่ไม่ได้รับอนุญาต โดยเฉพาะจากแหล่งที่ไม่น่าเชื่อถือ

๓) จำกัดสิทธิ์ในการใช้งานโปรแกรมตามหลัก Least Privilege

๔) บันทึก Log การเปิดใช้งานและคำสั่งที่รันจากโปรแกรมอรรถประโยชน์ โดยเฉพาะโปรแกรมที่มีผลต่อระบบหรือข้อมูล

๕) พิจารณาใช้ระบบ SIEM หรือ Endpoint Detection & Response (EDR) ตรวจจับพฤติกรรมเสี่ยงหรือพฤติกรรมผิดปกติ เช่น การรัน PowerShell ผิดปกติ

๖) ตรวจสอบ Log อย่างสม่ำเสมอ และพิจารณาเปิดการแจ้งเตือนเมื่อมีการใช้งานโปรแกรมต้องสงสัย

๗) ห้ามผู้ใช้งานทั่วไปติดตั้งโปรแกรมอรรถประโยชน์ด้วยตนเอง

๘) โปรแกรมที่ไม่ใช้งานอีกต่อไปต้องถูกถอนการติดตั้งหรือล็อกการใช้งาน

๙) กำหนดให้มีการทบทวนรายชื่อผู้ใช้งานและสิทธิ์การใช้โปรแกรมอรรถประโยชน์อย่างน้อยปีละ ๑ ครั้ง

๑๐) ดำเนินการถอนโปรแกรมอรรถประโยชน์ทันที เมื่อพนักงานพ้นหน้าที่ หรือไม่มีความจำเป็นในการใช้งาน

(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการจัดทำขั้นตอนของการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัย ประกอบด้วย ๔ ขั้นตอนหลัก ดังนี้

(๑) การวางแผน (Planning) โดยจัดให้มีการวางแผน และพัฒนานโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management : SecCM) รวมถึงการนำนโยบายและกระบวนการที่กำหนดนำผนวกเข้ากับแผนเทคโนโลยีสารสนเทศ และความมั่นคงปลอดภัยที่มีอยู่ รวมถึงระบุขอบเขตหรือการบังคับใช้กระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management : SecCM) และดำเนินการเผยแพร่นโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management : SecCM) ซึ่งนโยบายที่จัดทำขึ้นควรพิจารณาเนื้อหาครอบคลุมอย่างน้อย ดังนี้ การนำแผนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management : SecCM) ไปใช้รวมเข้ากับแผนความมั่นคงปลอดภัยที่มีอยู่ คณะกรรมการควบคุมการกำหนดค่า (CCB) กระบวนการควบคุมการเปลี่ยนแปลงการกำหนดค่า เครื่องมือและเทคโนโลยี การใช้การกำหนดค่าความมั่นคงปลอดภัยทั่วไป และการกำหนดค่าขั้นต่ำ การเฝ้าระวัง และชี้วัดสำหรับการปฏิบัติตามข้อกำหนด

(๒) จัดให้มีการระบุและใช้งานการกำหนดค่า (Identifying and Implementing Configuration) หลังจากกิจกรรมการวางแผนและการจัดเตรียมเสร็จสิ้น โดยดำเนินการพัฒนา สอบทาน อนุมัติ และนำการกำหนดค่าขั้นต่ำที่มั่นคงปลอดภัยสำหรับระบบไปใช้การกำหนดค่าขั้นต่ำที่ได้รับอนุมัติสำหรับระบบและส่วนประกอบที่เกี่ยวข้อง (Associated Component) ซึ่งต้องสอดคล้องกับข้อกำหนดและข้อจำกัดในการปฏิบัติงาน รวมถึงระบุการกำหนดค่าขั้นต่ำที่มั่นคงปลอดภัย (Secure Baseline) สำหรับระบบทั่วไป ควรพิจารณากำหนดให้มีการตั้งค่าคอนฟิกูเรชัน (Configuration Setting) การโหลดซอฟต์แวร์ (Software Load) ระดับแพตช์ (Patch Level) วิธีการจัดระบบข้อมูลทางกายภาพหรือทางตรรกะ วิธีการควบคุมความมั่นคงปลอดภัยต่าง ๆ ที่ถูกนำมาใช้รวมถึงคู่มือหรือเอกสารประกอบ

ทั้งนี้ อาจใช้ระบบอัตโนมัติโดยตั้งค่าให้เครื่องมือสามารถทำงานร่วมกัน (Interoperability) และกำหนดค่าขั้นต่ำของระบบต่าง ๆ ในรูปแบบเดียวกัน (Uniformity)

(๓) กำหนดให้มีการบริหารจัดการควบคุมการเปลี่ยนแปลงการกำหนดค่าที่มั่นคงปลอดภัย (Controlling Configuration Change) เมื่อมีการเปลี่ยนแปลงที่สำคัญที่เกิดขึ้น เพื่อรักษาระดับพื้นฐานที่มั่นคงปลอดภัย โดยต้องดำเนินการอย่างน้อย ดังนี้ ระบุถึงการเปลี่ยนแปลงค่าที่ปลอดภัย นำเสนอ สอบทานและวิเคราะห์ผลกระทบด้านความมั่นคงปลอดภัย รวมถึงดำเนินการทดสอบ และขออนุมัติอย่างเป็นทางการก่อนนำไปใช้งาน

(๔) การเฝ้าระวัง (Monitoring) เป็นกิจกรรมการตรวจสอบ และติดตามการปฏิบัติตามนโยบายและกระบวนการจัดการกำหนดค่าที่เน้นความมั่นคงปลอดภัยของระบบ (Security-Focused Configuration Management : SecCM) โดยการสุ่มตรวจสอบการตั้งค่าของระบบต่าง ๆ ที่มีความสำคัญเทียบกับเอกสารการกำหนดการตั้งค่าระบบ (System Configuration Management) รวมถึงกำหนดให้รายงานสถานะความมั่นคงปลอดภัยของการจัดการกำหนดค่าแต่ละรายการที่ดำเนินการตรวจสอบ และนำข้อมูล

การไม่ดำเนินการตามนโยบายและกระบวนการที่กำหนดเป็นข้อมูลตั้งต้นในการดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยต่อไป

๒. การจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) โดยอ้างอิงข้อกำหนดการตั้งค่าระบบจากแหล่งที่น่าเชื่อถือ เช่น ISO/IEC ๒๗๐๐๒, Center for Internet Security (CIS), Security Technical Implementation Guides (STIG), NIST, ENISA หรือตามคำแนะนำของเจ้าของผลิตภัณฑ์ และจัดทำเป็นเอกสารอย่างเป็นลายลักษณ์อักษร โดยมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) แบ่งแยกหน้าที่ (Separation of Duties)

๓) บังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) ลบบัญชีที่ไม่ได้ใช้

๕) ลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น ลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)

๖) ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันท่วงทีและเหมาะสม

๙) ปิดการใช้งานอัลกอริทึมที่ไม่มีความปลอดภัย เช่น ๓DES, RC๔, SSLv๒, SSlv๓

ตัวอย่างการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด	N/A	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติและทบทวนการแบ่งแยกหน้าที่ (Separation of Duties) อย่างน้อยปีละ ๑ ครั้ง	สิทธิพิเศษในการเข้าถึงน้อยที่สุดต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติโดยมีการกำหนดสิทธิจากส่วนกลาง และทบทวนการแบ่งแยกหน้าที่ (Separation of Duties) อย่างน้อยปีละ ๑ ครั้ง
๒) แบ่งแยกหน้าที่	N/A	การแบ่งแยกหน้าที่ต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติ และทบทวนการแบ่งแยกหน้าที่อย่างน้อยปีละ ๑ ครั้ง	การแบ่งแยกหน้าที่ต้องมีการได้รับอนุมัติเป็นลายลักษณ์อักษร และนำมาปฏิบัติโดยมีการกำหนดสิทธิจากส่วนกลาง และทบทวนการแบ่งแยกหน้าที่อย่างน้อยปีละ ๑ ครั้ง

มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
๓) บังคับใช้นโยบายความซับซ้อนของรหัสผ่าน	รหัสผ่านต้องยาวกว่า ๘ ตัวอักษร	รหัสผ่านต้องยาวกว่า ๑๐ ตัวอักษรและควรมีการใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication)	รหัสผ่านต้องยาวกว่า ๑๒ ตัวอักษรและต้องมีการใช้การยืนยันตัวตนโดยใช้หลายปัจจัย (Multi-Factor Authentication)
๔) ลบบัญชีที่ไม่ได้ใช้	ลบบัญชีที่ไม่ได้ใช้หรือปิดการใช้งานไว้ (Disable) ภายใน ๗๒ ชั่วโมง เมื่อสิ้นสุดกิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือปิดการใช้งานไว้ (Disable) ภายใน ๔๘ ชั่วโมง เมื่อสิ้นสุดกิจกรรม	ลบบัญชีที่ไม่ได้ใช้หรือหรือปิดการใช้งานไว้ (Disable) ทันที เมื่อสิ้นสุดกิจกรรม
๕) ลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น ลบคอมไพเลอร์และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก	ตรวจสอบการลบบริการ และแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอกก่อนนำมาใช้งาน และตรวจสอบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอกก่อนนำมาใช้งาน และตรวจสอบอย่างน้อย ไตรมาสละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ	ตรวจสอบการลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอกก่อนนำมาใช้งาน และตรวจสอบอย่างน้อยเดือนละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ
๖) ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน และมีการป้องกันการเข้าถึงพอร์ตทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน มีการป้องกันการเข้าถึงพอร์ตทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุม การเข้าถึงทางกายภาพ	ปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งานโดยควบคุมจากส่วนกลาง เช่น ระบบบริหารจัดการจากศูนย์กลาง (Active Directory: AD) เป็นต้น มีการป้องกัน การเข้าถึงพอร์ตทางกายภาพ เช่น มีกรงกั้น มีรั้ว และการควบคุม การเข้าถึงทางกายภาพ
๗) การป้องกันมัลแวร์ (Malware)	อัปเดตฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอ	อัปเดตฐานข้อมูลสำหรับการตรวจสอบรูปแบบมัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์สำหรับการป้องกันมัลแวร์อยู่อย่างสม่ำเสมอ พร้อมทั้งมีการจัดเก็บบันทึกกิจกรรม (Log)	อัปเดตฐานข้อมูลสำหรับการตรวจสอบรูปแบบ มัลแวร์ (Signature) และเวอร์ชันของซอฟต์แวร์ สำหรับการป้องกันมัลแวร์ พร้อมทั้งมีการจัดเก็บบันทึกกิจกรรม (Log) อย่างสม่ำเสมอ และมีการส่งบันทึก (Log) ไปยังระบบส่วนกลางเพื่อตรวจจับและวิเคราะห์ความผิดปกติ รวมถึงมีเทคโนโลยีขั้นสูงอื่น ๆ เช่น IDS, IPS, EDR เป็นต้น
๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน ๗ วัน เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน ๗๒ ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต	ปรับปรุงซอฟต์แวร์ และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบภายใน ๔๘ ชั่วโมง เมื่อมีแพตช์ระดับวิกฤต

๓. กำหนดให้มีการตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญ ตามตัวอย่างดังตาราง

ทรัพย์สิน	รายการที่ต้องดำเนินการ	การตั้งค่าตามมาตรฐานการกำหนดค่าขั้นต่ำ	สถานะการตรวจสอบ
เครื่องแม่ข่ายที่จะเชื่อมต่อกับบริการที่สำคัญ	ตั้งรหัสผ่าน BIOS/เฟิร์มแวร์	รหัสผ่านต้องยาวมากกว่า ๑๒ ตัวอักษร	Yes / No
	ตั้งรหัสผ่านบูตโหลดเดอร์ (Boot Loader)	รหัสผ่านต้องยาวมากกว่า ๑๒ ตัวอักษร	Yes / No
	กำหนดค่าสำหรับการพิสูจน์ตัวตนเพื่อเข้าถึงระบบปฏิบัติการ (Configure OS User Authentication)	- รหัสผ่านของบัญชีผู้ใช้ต้องยาวมากกว่า ๑๒ ตัวอักษร - สร้างบัญชีผู้ใช้ตามที่ได้รับอนุญาตเท่านั้น หรือต้องดำเนินการด้วยระบบ LDAP หรือ RADIUS ของหน่วยงานเท่านั้น - ห้ามการเข้าถึงจากระยะไกลด้วยบัญชี Root	Yes / No
	กำหนดเทคโนโลยีการพิสูจน์ตัวตน และเทคโนโลยีการเข้ารหัส	- กำหนดการเข้าถึงโปรแกรมประยุกต์ที่สำคัญต้องทำผ่านการยืนยันตัวตนด้วยสองปัจจัยเป็นอย่างน้อย (๒-FA) - เปิดใช้งานการเข้ารหัส TLS ๑.๓ ขึ้นไปสำหรับ Web services และโปรแกรมประยุกต์	Yes / No

๔. กำหนดให้มีการตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๕. กำหนดให้มีการบริหารจัดการการเปลี่ยนแปลง โดยจัดทำเป็นเอกสาร ซึ่งควรประกอบด้วยขั้นตอน ดังนี้ การร้องขอการเปลี่ยนแปลง โดยใช้แบบฟอร์มการร้องขอการเปลี่ยนแปลง (Change Request) เพื่อประเมินผลกระทบการเปลี่ยนแปลงก่อนดำเนินการเปลี่ยนแปลง โดยระบุข้อมูลอย่างน้อย ดังนี้ วัตถุประสงค์, ขอบเขต, รายละเอียดการเปลี่ยนแปลง, ความเสี่ยง, แผนการดำเนินงาน, ผู้รับผิดชอบ, แผนทดแทน และแผนย้อนกลับ (Rollback Plan) และขออนุมัติก่อนดำเนินการเปลี่ยนแปลง

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการประเมินผลกระทบและความเสี่ยง โดยวิเคราะห์ผลกระทบต่อระบบสารสนเทศความต่อเนื่องในการให้บริการ และความมั่นคงปลอดภัยของข้อมูล

๒. กำหนดให้มีการอนุมัติการเปลี่ยนแปลง โดยพิจารณาให้มีการประชุม เพื่อพิจารณาอนุมัติหรือปฏิเสธการเปลี่ยนแปลงที่สำคัญ

๓. กำหนดให้ต้องมีการจัดแผน Rollback ที่สามารถดำเนินการได้ทันทีหากเกิดปัญหาในการเปลี่ยนแปลง

๔. กำหนดให้มีการติดตามผลและการปิดการเปลี่ยนแปลง พร้อมทั้งจัดทำรายงาน Post-Implementation Review (PIR) หรือ Lessons Learned และบันทึกข้อมูลการเปลี่ยนแปลงอย่างเป็นระบบ

๕. กำหนดให้มีการบริหารจัดการพัฒนาซอฟต์แวร์ โดยจัดให้มีการกำหนดความต้องการด้านความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) จัดให้มีการเก็บข้อมูลความต้องการด้านความมั่นคงปลอดภัย เช่น การพิสูจน์ตัวตน, การเข้ารหัส, การควบคุมสิทธิ์ เป็นต้น

๒) ดำเนินการวิเคราะห์ภัยคุกคาม (Threat Modeling) และความเสี่ยงของระบบก่อนเริ่มพัฒนาซอฟต์แวร์

๓) จัดให้มีรายการตรวจสอบข้อกำหนดด้านความมั่นคงปลอดภัย (Security Requirement Checklist) และจัดเก็บเอกสารไว้เป็นหลักฐานการตรวจสอบ

๖. กำหนดให้มีการบริหารจัดการวงจรชีวิตของระบบ (System Lifecycle Security Management) โดยวางแผน วิเคราะห์และออกแบบ รวมถึงความต้องการด้านความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ดำเนินการประเมินความเสี่ยงเบื้องต้นของระบบ พร้อมทั้งระบุระดับความสำคัญของข้อมูลและระดับผลกระทบ (Impact Level) เพื่อกำหนดมาตรการควบคุมที่เหมาะสม

๒) นำหลักการ "Security by Design" และ "Privacy by Design" ผนวกเข้ากับการออกแบบระบบ โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดมาตรการควบคุมด้านการพิสูจน์ตัวตน การเข้ารหัสข้อมูล และการตรวจสอบการเข้าถึง

(๒) ดำเนินการวิเคราะห์ผลกระทบด้านข้อมูลส่วนบุคคล (Data Protection Impact Assessment: DPIA) ในกรณีที่ระบบมีการจัดเก็บข้อมูลส่วนบุคคล

๗. กำหนดให้มีการพัฒนาและทดสอบความปลอดภัยของระบบ โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ปฏิบัติตามแนวทางการพัฒนาซอฟต์แวร์อย่างปลอดภัย (Secure Software Development Lifecycle - SSDLC) โดยจัดให้มีการดำเนินการทดสอบความมั่นคงปลอดภัยของระบบ เช่น Penetration Test, Vulnerability Scan พร้อมทั้งจัดทำเอกสารด้านความมั่นคงปลอดภัย เช่น Secure Configuration Guidelines เป็นต้น

๘. กำหนดให้มีการบริหารจัดการติดตั้งระบบ โดยดำเนินการติดตั้งระบบตามมาตรฐานความปลอดภัยที่กำหนด (Security Baseline) ขององค์กร และกำหนดให้มีการดำเนินการตรวจสอบความมั่นคงปลอดภัยก่อนนำระบบขึ้นใช้งานจริง (Go-live Security Assessment) รวมถึงจัดทำแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) และแผนบริหารความต่อเนื่อง (BCP/DRP)

๙. กำหนดให้มีการบริหารจัดการบำรุงรักษาและติดตาม โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการตรวจสอบและติดตามการใช้งานระบบอย่างสม่ำเสมอ (Monitoring and Logging)

๒) กำหนดให้มีการจัดการอัปเดตซอฟต์แวร์ แพตช์ รวมถึงกำหนดให้มีการเปลี่ยนแปลงระบบอย่างปลอดภัย (Patch and Change Management)

๓) กำหนดให้มีการประเมินและทบทวนความเสี่ยงอย่างต่อเนื่องตลอดอายุการใช้งานของระบบ

๑๐. กำหนดให้มีการบริหารจัดการควบคุมความเสี่ยงในกรณีที่มีการยกเลิกใช้งานระบบ (Disposal Phase) โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการวางแผนการยกเลิกใช้งานระบบอย่างปลอดภัย (Secure Decommissioning Plan)

๒) ดำเนินการวางแผนลบข้อมูลหรือทำลายข้อมูลอย่างปลอดภัย (Secure Data Erasure) ตามมาตรฐาน เช่น NIST SP ๘๐๐-๘๘ เป็นต้น

๓) ดำเนินการถอดถอนระบบงานออกจากการใช้งาน และอัปเดตบัญชีสินทรัพย์ไอที (IT Asset Inventory)

๑๑. กำหนดให้มีการออกแบบและพัฒนาอย่างปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการจัดการช่องโหว่ในไลบรารีและส่วนประกอบซอฟต์แวร์ โดยจัดให้มีกระบวนการตรวจหาไลบรารีภายนอก เช่น frameworks, packages, modules เป็นต้น ที่นำมาใช้ในซอฟต์แวร์ เพื่อตรวจสอบช่องโหว่ด้านความมั่นคงปลอดภัย (Vulnerabilities) พร้อมทั้งอัปเดตให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ

๒) กำหนดให้มีการตรวจสอบความมั่นคงปลอดภัยของโค้ด (Security Code Review) ก่อนนำระบบขึ้นใช้งานจริง (Production)

๑๒. กำหนดให้มีการดำเนินการทดสอบความมั่นคงปลอดภัย เช่น Static Application Security Testing (SAST) Dynamic Application Security Testing (DAST) หรือ Penetration Testing เป็นต้น พร้อมทั้งจัดทำบันทึกผลการทดสอบ และแก้ไขช่องโหว่ก่อนขึ้นใช้งานจริง

๑๓. กำหนดให้มีการควบคุมเวอร์ชันและการเปลี่ยนแปลง โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) จัดเก็บซอร์สโค้ดและเวอร์ชันใน Git หรือระบบควบคุมเวอร์ชันที่ปลอดภัย

๒) บังคับใช้แนวปฏิบัติการควบคุมการเปลี่ยนแปลง ในกรณีที่ระบบมีการเปลี่ยนแปลง พร้อมทั้งบันทึกการเปลี่ยนแปลงโค้ด และเหตุผลในการเปลี่ยนแปลงรวมถึงผู้รับผิดชอบ (Change Log)

๑๔. กำหนดให้มีการควบคุมในกรณีที่มีการจ้างหน่วยงานภายนอกพัฒนา โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ระบุข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญาให้ชัดเจน (Security Clause in Contract)

๒) กำหนดให้มีการตรวจสอบผลทดสอบช่องโหว่ก่อนรับมอบงาน

๓) ห้ามผู้พัฒนาภายนอกเข้าถึงระบบงาน (Production) โดยตรง ในกรณีที่ความจำเป็นต้องเข้าถึงระบบงาน (Production) ต้องมีกระบวนการอนุมัติ และกำหนดสิทธิการเข้าถึงให้ชัดเจน รวมถึงระยะเวลาในการเข้าถึง

๑๕. กำหนดให้มีการควบคุมข้อมูลในสภาพแวดล้อมพัฒนา โดยพิจารณาให้มีการดำเนินการอย่างน้อยดังนี้

๑) ห้ามใช้ข้อมูลจริงในการพัฒนาระบบ รวมถึงการทดสอบระบบ โดยไม่มีการปกปิดข้อมูล (Masking/Anonymization)

๒) กำหนดให้มีการควบคุมการนำข้อมูลออกนอกระบบพัฒนา เช่น ผ่าน USB, Cloud Drive, หรือ Email ส่วนตัว เป็นต้น

๓) กำหนดให้มีการบันทึกกิจกรรม (Log) รวมถึงการติดตามบันทึกกิจกรรม (Log) การเข้าถึงและการทำงานในระหว่างการพัฒนาระบบอย่างต่อเนื่อง

๑๖. กำหนดให้มีการบริหารจัดการข้อจำกัดการติดตั้งซอฟต์แวร์ โดยกำหนดสิทธิ์ในการติดตั้งซอฟต์แวร์ โดยพิจารณาอย่างน้อยดังนี้

๑) อนุญาตให้ติดตั้งซอฟต์แวร์เฉพาะผู้ปฏิบัติงานฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ปฏิบัติที่ได้รับมอบหมายตามหน้าที่ความรับผิดชอบ

๒) ไม่อนุญาตให้ผู้ใช้งานทั่วไปมีสิทธิ์ในการติดตั้งซอฟต์แวร์บนอุปกรณ์

๓) ซอฟต์แวร์ที่อนุญาตให้ติดตั้ง หรือใช้งานต้องผ่านการประเมินความมั่นคงปลอดภัยความเข้ากันได้กับระบบ และการตรวจสอบลิขสิทธิ์

๔) กำหนดให้มีการจัดทำ “บัญชีซอฟต์แวร์ที่ได้รับอนุญาต” (Approved Software List) เพื่อใช้ในการควบคุมการติดตั้งซอฟต์แวร์

๕) กำหนดให้มีรายการตรวจสอบการติดตั้งซอฟต์แวร์ พร้อมทั้งจัดทำบันทึกการติดตั้งเป็นหลักฐาน

๖) พิจารณาใช้ระบบตรวจจับและป้องกันการใช้งานซอฟต์แวร์ต้องห้าม เช่น Application Whitelisting หรือ Endpoint Detection and Response (EDR) เป็นต้น พร้อมทั้งตั้งค่าระบบให้แจ้งเตือนเมื่อมีการพยายามติดตั้งโปรแกรมจากแหล่งที่ไม่ได้รับอนุญาต

๗) กำหนดให้มีการตรวจสอบรายงานการใช้งานซอฟต์แวร์อย่างน้อยปีละ ๑ ครั้ง และดำเนินการลบหรือล็อกการใช้งาน ในกรณีที่พบสิ่งผิดปกติ

๘) จัดให้มีการเก็บบันทึก (Logs) การติดตั้งและถอนการติดตั้งซอฟต์แวร์ เพื่อใช้ในการตรวจสอบย้อนหลัง

๙) กำหนดให้มีการถอนการติดตั้งและจัดการซอฟต์แวร์ เมื่อเลิกใช้งานหรือหมดอายุการใช้งาน โดยต้องถอนการติดตั้งซอฟต์แวร์ทันที และในกรณีที่ซอฟต์แวร์ที่ไม่มีการอัปเดตจากผู้ผลิต หรือไม่มีความจำเป็นต้องใช้งาน ต้องพิจารณาเลิกใช้งาน เพื่อบริหารจัดการความเสี่ยงจากช่องโหว่ของซอฟต์แวร์

๑๗. กำหนดให้มีการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย โดยการออกแบบโครงสร้างเครือข่ายที่ปลอดภัย โดยคำนึงถึงการพิจารณา อย่างน้อย ดังนี้

๑) จัดแบ่งเครือข่ายออกเป็นโซนตามระดับความสำคัญและความอ่อนไหวของข้อมูล เช่น โซนอินเทอร์เน็ต โซนเครือข่ายภายใน โซนเซิร์ฟเวอร์ และโซนข้อมูลสำคัญ

๒) จัดให้มีการป้องกันหลายชั้น โดยไม่พึ่งพาเพียงกลไกป้องกันเดียว (Defense-in-Depth)

๓) กำหนดโซน DMZ สำหรับเซิร์ฟเวอร์ที่ต้องเชื่อมต่อกับเครือข่ายภายนอก

๑๘. กำหนดให้มีการติดตั้งและการกำหนดค่าอุปกรณ์เครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) ปิดพอร์ตและบริการที่ไม่จำเป็นต่อการทำงาน

๒) อัปเดตเฟิร์มแวร์ของอุปกรณ์เครือข่ายให้เป็นเวอร์ชันล่าสุดอย่างสม่ำเสมอ

๓) กำหนดให้ใช้การพิสูจน์ตัวตนหลายปัจจัยสำหรับการเข้าถึงอุปกรณ์สำคัญ

๔) กำหนดมาตรฐานการตั้งค่าความปลอดภัยสำหรับอุปกรณ์แต่ละประเภท

๕) สำรองและจัดเก็บการกำหนดค่าของอุปกรณ์อย่างปลอดภัย

๑๙. กำหนดให้มีการเข้ารหัสข้อมูลในการส่งผ่านเครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้ใช้ TLS/SSL สำหรับการสื่อสารผ่านเว็บ

๒) กำหนดนโยบายการใช้ VPN สำหรับการเข้าถึงจากระยะไกล

๓) กำหนดให้ใช้การพิสูจน์ตัวตนหลายปัจจัยสำหรับการเชื่อมต่อ VPN

๒๐. กำหนดให้มีการตรวจสอบและการตรวจจับภัยคุกคาม โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดนโยบายบันทึกเหตุการณ์จากอุปกรณ์เครือข่าย

๒) ใช้ระบบรวมศูนย์การเก็บบันทึกเหตุการณ์ เช่น SIEM (Security Information and Event Management)

๓) ดำเนินการสแกนช่องโหว่ของระบบเครือข่ายอย่างสม่ำเสมอ

๔) จัดให้มีการทดสอบเจาะระบบเครือข่าย โดยผู้เชี่ยวชาญอย่างน้อยปีละ ๑ ครั้ง

๒๑. กำหนดให้มีการควบคุมการเข้าถึงเครือข่าย โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จำกัดสิทธิ์การเข้าถึงเครือข่ายตามหน้าที่และความรับผิดชอบ

๒) ทบทวนสิทธิ์การเข้าถึงเครือข่ายเป็นประจำ

๒๒. กำหนดให้มีการบริหารจัดการรักษาความปลอดภัยฐานข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีการจัดทำแนวปฏิบัติการบริหารจัดการฐานข้อมูลที่ครอบคลุมการควบคุมการเข้าถึง การปกป้องข้อมูล และการติดตามตรวจสอบ

๒) กำหนดให้มีการจัดทำแนวปฏิบัติการจัดการบัญชีผู้ใช้ และสิทธิ์การเข้าถึงฐานข้อมูล (Database Access Control Policy)

๓) กำหนดให้มีการจัดทำแนวปฏิบัติการสำรองและกู้คืนข้อมูลฐานข้อมูล (Database Backup and Recovery Policy)

๔) การบริหารจัดการควบคุมการเข้าถึงฐานข้อมูล ต้องประกอบไปด้วย

(๑) จำกัดการเข้าถึงเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องตามหลัก Least Privilege

(๒) กำหนดให้มีการแยกหน้าที่ความรับผิดชอบระหว่างผู้ดูแลระบบและผู้พัฒนาระบบ (Segregation of Duties) อย่างชัดเจน

(๓) กำหนดให้ใช้การพิสูจน์ตัวตนแบบเข้มงวด เช่น การใช้รหัสผ่านที่ซับซ้อน, Multi-Factor Authentication (MFA) เป็นต้น

(๔) กำหนดระยะเวลา Session Timeout สำหรับการเชื่อมต่อฐานข้อมูล

๒๓. การบริหารจัดการปกป้องข้อมูลในฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการเข้ารหัสข้อมูลที่สำคัญทั้งขณะจัดเก็บ (Encryption at Rest) และขณะส่งข้อมูล (Encryption in Transit)

๒) กำหนดให้ใช้เทคนิคการ Masking หรือ Anonymization กับข้อมูลที่ใช้ในระบบทดสอบ (Test Data Protection)

๓) กำหนดให้ใช้มาตรการควบคุมความสมบูรณ์ของข้อมูล เช่น ตรวจสอบค่า Hash หรือใช้การทำ Data Integrity Verification

๔) กำหนดนโยบายการจัดการข้อมูลที่หมดอายุหรือไม่จำเป็น เช่น การลบหรือทำลายข้อมูลอย่างปลอดภัย (Secure Deletion)

๒๔. การบริหารจัดการติดตามและตรวจสอบการใช้งานฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการเปิดใช้งานระบบบันทึกการทำงาน (Database Auditing) เพื่อบันทึกกิจกรรมที่สำคัญ เช่น การเข้าใช้ การอ่าน การแก้ไข และการลบข้อมูล

๒) พิจารณาใช้เครื่องมือวิเคราะห์และตรวจจับพฤติกรรมผิดปกติ (Database Activity Monitoring : DAM)

๓) กำหนดการทบทวน Log การใช้งานฐานข้อมูลอย่างสม่ำเสมอ และแจ้งเตือนเมื่อพบกิจกรรมต้องสงสัย

๔) พิจารณาตั้งค่าระบบแจ้งเตือน (Alert System) สำหรับเหตุการณ์ผิดปกติที่มีความเสี่ยงสูง

๒๕. การบริหารจัดการสำรองและการกู้คืนฐานข้อมูล ต้องประกอบไปด้วย

๑) กำหนดให้มีการสำรองฐานข้อมูลอย่างสม่ำเสมอ และกำหนดระยะเวลาการสำรองข้อมูลให้เป็นไปตามระดับความสำคัญของข้อมูล

๒) กำหนดให้มีกระบวนการกู้คืนข้อมูล (Recovery Test) อย่างสม่ำเสมอ เช่น ไตรมาสละ ๑ ครั้ง เป็นต้น

๓) กำหนดให้มีการจัดเก็บข้อมูลสำรองแยกจากระบบปฏิบัติการหลัก และปกป้องข้อมูลสำรองด้วยการเข้ารหัสและควบคุมการเข้าถึง

๒๖. กำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยด้านกายภาพและสภาพแวดล้อม โดยกำหนดมาตรการควบคุมการเข้า - ออก เพื่อดูแลรักษาความปลอดภัย โดยบุคคลที่ต้องการสิทธิในการเข้า - ออก ต้องขออนุญาตเป็นลายลักษณ์อักษร

๒๗. ต้องทำการยืนยันตัวตนก่อนเข้าพื้นที่ทุกครั้ง เพื่อป้องกันการเข้า - ออกโดยไม่ได้รับอนุญาต

๒๘. ควบคุมการลงชื่อ บันทึกวัน เวลา และวัตถุประสงค์การเข้า - ออก ของผู้ใช้งาน และบุคคลภายนอก (Visitors) ทุกครั้ง

๒๙. ตรวจสอบการเข้าถึงอาคารต่าง ๆ ที่มีระบบสารสนเทศที่สำคัญอย่างต่อเนื่อง รวมถึงการจัดให้มีอุปกรณ์หรือเครื่องมือแจ้งเตือน เพื่อตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต หรือพฤติกรรมที่น่าสงสัย

๓๐. ดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอก (Visitors) ในขณะที่ปฏิบัติงาน จนกระทั่งเสร็จสิ้นภารกิจและออกจากศูนย์คอมพิวเตอร์ เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพ โดยไม่ได้รับอนุญาต

๓๑. กำหนดให้มีการบริหารจัดการระบบ และอุปกรณ์สนับสนุนการทำงาน ต้องดำเนินการวางแผนและติดตั้งอุปกรณ์ โดยพิจารณาอย่างน้อยดังนี้

๑) ต้องติดตั้งอุปกรณ์สนับสนุนในพื้นที่ควบคุมที่มีการออกแบบตามมาตรฐานความปลอดภัย เช่น TIA-๙๔๒ หรือ Uptime Tier เป็นต้น

๒) ดำเนินการตรวจสอบให้มั่นใจว่าอุปกรณ์ที่ติดตั้งมีคุณสมบัติรองรับภาระงานของระบบและมีระบบสำรองหากเกิดความล้มเหลว รวมถึงควบคุมการเข้าถึงพื้นที่ที่มีอุปกรณ์สำคัญ

๓๒. กำหนดให้มีการบำรุงรักษาและตรวจสอบสภาพการทำงาน โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำ แผนบำรุงรักษาเชิงป้องกัน (Preventive Maintenance Plan) สำหรับอุปกรณ์ทั้งหมด โดยกำหนดความถี่ที่เหมาะสม เช่น รายเดือน รายไตรมาส เป็นต้น

๒) พิจารณาให้มีการตรวจสอบสถานะการทำงานของอุปกรณ์แบบเรียลไทม์ด้วยระบบ Monitoring พร้อมแจ้งเตือนเมื่อเกิดเหตุผิดปกติ รวมถึงบันทึกผลการบำรุงรักษาและเหตุขัดข้องในระบบ Log สำหรับการตรวจสอบย้อนหลัง

๓) ติดตั้งระบบสำรองไฟ เช่น UPS Generator เป็นต้น และทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ

๔) ตรวจสอบระบบดับเพลิงอัตโนมัติ เช่น FM-๒๐๐ CO_2 หรือระบบ Clean Agent เป็นต้น พร้อมทั้งตรวจสอบระบบดับเพลิงตามรอบระยะเวลา เช่น ทุก ๓ เดือน หรือ ๖ เดือน เป็นต้น

๕) กำหนดให้มีการใช้เซ็นเซอร์ตรวจจับความชื้น น้ำรั่ว และอุณหภูมิภายในห้องเซิร์ฟเวอร์ พร้อมตั้งค่าการแจ้งเตือน และกำหนดให้มีการตรวจสอบอย่างสม่ำเสมอ

๖) กำหนดให้มีการสำรองอุปกรณ์ หรือจัดทำแผนรองรับฉุกเฉิน ในกรณีที่อุปกรณ์สำคัญล้มเหลว

๗) จำกัดการเข้าถึงห้องระบบเฉพาะผู้มีหน้าที่รับผิดชอบ หรือผู้ที่ได้รับมอบหมาย โดยใช้ระบบควบคุมการเข้าออก เช่น การใช้บัตรผ่านเข้า - ออก หรือใช้ข้อมูลการยืนยันตัวตนทางชีวมิติ (Biometric Authentication) สำหรับการควบคุมการเข้า - ออก เป็นต้น และเก็บข้อมูลการเข้า - ออก อย่างน้อย ๙๐ วัน

๘) ในกรณีที่มีการเข้าถึงจากผู้ให้บริการภายนอก บุคคลภายนอก หรือผู้ที่ไม่มีสิทธิการเข้าถึงตามหน้าที่ความรับผิดชอบต้องจัดให้มีการลงทะเบียนเข้า - ออก และปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร

๓๓. กำหนดให้มีการบริหารความมั่นคงปลอดภัยของการเดินสายสัญญาณ และสายสื่อสาร โดยการออกแบบ และติดตั้งสายสัญญาณและสายสื่อสาร ควรพิจารณาอย่างน้อย ดังนี้

๑) การเดินสายสัญญาณและสายสื่อสารต้องวางแผนตามมาตรฐานอุตสาหกรรม เช่น TIA/EIA-๕๖๘, ISO/IEC ๑๑๘๐๑ เป็นต้น

๒) แยกสายสัญญาณข้อมูลออกจากสายไฟฟ้าแรงสูง เพื่อป้องกันการรบกวนทางแม่เหล็กไฟฟ้า (EMI) และพิจารณาใช้สายที่มีฉนวนหุ้มป้องกันการดักฟัง (Shielded Cable / Armored Fiber) ในพื้นที่สำคัญ

๓) กำหนดให้มีการใช้ท่อหรือรางสาย (Cable Conduit/Duct) ที่สามารถป้องกันการเข้าถึงสายสัญญาณ และสายสื่อสารจากภายนอก

๔) ต้องมีการควบคุมการเข้า - ออก ในพื้นที่ที่ติดตั้งสาย เช่น ห้อง Data Center เป็นต้น รวมถึงจัดให้มีการเก็บบันทึกการเข้าออก

๕) กำหนดสิทธิเฉพาะผู้ที่ได้รับมอบหมาย หรือมีหน้าที่ความรับผิดชอบที่ชัดเจนในการปรับเปลี่ยน ดัดแปลง หรือซ่อมบำรุงรักษา

๖) จัดทำแผนผังการเดินสาย (Cabling Layout) และอัปเดตเมื่อมีการเปลี่ยนแปลง

๗) กำหนดรอบการตรวจสอบความสมบูรณ์ และการทำงานของสาย เช่น ทุก ๖ เดือน หรือ ๑๒ เดือน เป็นต้น และแยกการทดสอบสายสื่อสารในระบบสำคัญออกจากระบบที่ใช้งานทั่วไป รวมถึงจัดให้มีบันทึกการตรวจสอบ และบำรุงรักษา

๓๔. กำหนดให้มีการบริหารจัดการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ (Equipment Maintenance and Repair Security Management) โดยการวางแผนและบันทึกประวัติการบำรุงรักษา ควรพิจารณาอย่างน้อย ดังนี้

๑) จัดทำแผนบำรุงรักษาเชิงป้องกัน (Preventive Maintenance Plan) รายปี โดยระบุอุปกรณ์ ช่วงเวลา และผู้รับผิดชอบ เป็นต้น

๒) บันทึกการดำเนินการทุกครั้งที่มีการเปลี่ยนแปลง เช่น รายการอุปกรณ์ที่บำรุงรักษา วันเวลา รายชื่อผู้ดำเนินการ และผลการตรวจสอบ เป็นต้น

๓) ดำเนินการแยกบันทึกสำหรับอุปกรณ์สำคัญ (Critical Assets) และกำหนดระดับความเร่งด่วนหากพบข้อบกพร่อง

๓๕. กำหนดให้มีการควบคุมการเข้าถึงในระหว่างการซ่อมบำรุง โดยพิจารณาอย่างน้อยดังนี้

๑) อนุญาตให้เฉพาะบุคลากรที่มีสิทธิ หรือผู้ให้บริการที่ผ่านการตรวจสอบเข้าไปยังพื้นที่อุปกรณ์

๒) ผู้ให้บริการภายนอกต้องลงทะเบียนเวลาเข้า - ออก และต้องมีเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายควบคุมดูแลขณะดำเนินการ

๓) ห้ามคัดลอกข้อมูล หรือถ่ายภาพหน้าจอ หรือการตั้งค่าระบบ โดยไม่ได้รับอนุญาต

๓๖. กำหนดให้มีมาตรการด้านข้อมูลระหว่างการซ่อมบำรุง โดยพิจารณาอย่างน้อยดังนี้

๑) กรณีต้องส่งอุปกรณ์ซ่อมภายนอกต้องดำเนินการล้างข้อมูล หรือเข้ารหัสข้อมูลก่อนส่งอุปกรณ์เข้าซ่อม

๒) หากจำเป็นต้องเปิดระบบให้เข้าถึงข้อมูล ควรใช้บัญชีควบคุมพิเศษ และปิดใช้งานทันทีหลังดำเนินการ

๓) ห้ามนำอุปกรณ์ทดแทนที่ไม่ผ่านการรับรองเข้าระบบ โดยไม่มีการตรวจสอบด้านความปลอดภัยล่วงหน้า

๓๗. กำหนดให้มีมาตรการตรวจสอบหลังการซ่อม โดยพิจารณาอย่างน้อยดังนี้

๑) ตรวจสอบความสมบูรณ์ของระบบหลังจากการบำรุงรักษา เช่น การทำงานของระบบปฏิบัติการ ความสมบูรณ์ของไฟล์ Log และการเชื่อมต่อเครือข่าย เป็นต้น

๒) กรณีที่ต้องดำเนินการเปลี่ยนอะไหล่ หรืออุปกรณ์ต้องบันทึกหมายเลขซีเรียลใหม่และอัปเดตทะเบียนสินทรัพย์

๓) หากพบสิ่งผิดปกติต้องรายงานต่อฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายเพื่อพิจารณาดำเนินการเพิ่มเติม

๓๘. กำหนดให้มีการบริหารการติดตั้งและป้องกันอุปกรณ์ (Installation and Protection of Equipment Management) โดยการวางแผนและการติดตั้งอุปกรณ์ ควรพิจารณาอย่างน้อยดังนี้

๑) การติดตั้งอุปกรณ์ต้องอยู่ภายใต้การอนุมัติ และดำเนินการตามแบบแปลนที่ได้รับอนุมัติ

๒) ตำแหน่งติดตั้งต้องคำนึงถึงความปลอดภัยทางกายภาพ ความร้อน ความชื้น และความเสี่ยงต่อไฟฟ้าลัดวงจร

๓) อุปกรณ์ที่มีความสำคัญควรติดตั้งในห้องควบคุมพิเศษ เช่น Server Room, Data Center เป็นต้น และต้องมีการดำเนินการควบคุมการเข้า - ออกอย่างเคร่งครัด เช่น บัตรพนักงาน หรือระบบสแกนชีวมิติ เป็นต้น รวมถึงจัดเก็บ log การเข้าถึง

๔) การเชื่อมต่อสายสัญญาณ และพลังงานต้องพิจารณาให้เป็นไปตามมาตรฐานด้านความปลอดภัยไฟฟ้าและสื่อสาร

๕) จัดให้มีแผนบำรุงรักษาอุปกรณ์ตามระยะเวลา (Preventive Maintenance Schedule) เช่น ทุก ๖ เดือน หรือ ๑ ปี เป็นต้น

๖) พิจารณาติดตั้งระบบตรวจสอบสถานะการทำงานของอุปกรณ์ (Monitoring Tools) และแจ้งเตือนเมื่อเกิดเหตุผิดปกติ รวมถึงเก็บประวัติการติดตั้ง ซ่อมบำรุง และเปลี่ยนอุปกรณ์ในระบบทะเบียนสินทรัพย์ (Asset Register)

๓๙. กำหนดให้มีการบริหารจัดการเมื่อถอดถอน หรือย้ายอุปกรณ์ โดยพิจารณาอย่างน้อยดังนี้

๑) กำหนดให้การย้ายอุปกรณ์ต้องมีบันทึกการเคลื่อนย้าย พร้อมทั้งได้รับอนุมัติก่อนการเคลื่อนย้าย

๒) ต้องจัดให้มีการดำเนินการ Backup ข้อมูลก่อนถอดถอน และล้างข้อมูล (Data Sanitization) ในกรณีที่ต้องดำเนินการส่งคืน หรือจำหน่าย

๓) ดำเนินการปรับปรุงทะเบียนสินทรัพย์ให้เป็นปัจจุบัน

(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๑. จัดให้มีการกำหนดนโยบายการสร้างความตระหนัก โดยพิจารณาอย่างน้อย ดังนี้

๑) กำหนดให้มีแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอกบุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(๑) มีกิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่ พนักงานใหม่ (New Employees) ผู้ใช้และระดับบริหาร (Users and Management) เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ผู้ขาย ผู้รับเหมาและผู้ให้บริการ (Vendors, Contractors and Service Providers)

(๒) เผยแพร่ความรับผิดชอบของกลุ่ม และบุคคลตามลำดับสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

(๓) ให้ความรู้ด้านกฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๔) การสื่อสารอย่างสม่ำเสมอ และทันท่วงทีครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ ผลกระทบและการบรรเทาผลกระทบ

(๕) กำหนดให้การสร้างความตระหนักเป็นกิจกรรมที่ดำเนินการต่อเนื่องเป็นประจำทุกปี

(๖) การสร้างความตระหนักต้องผนวกรวมเข้าเป็นส่วนหนึ่งของวัฒนธรรมองค์กรและกระบวนการบริหารจัดการความเสี่ยง

(๗) ดำเนินการทบทวนแผนงาน/กิจกรรมในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบัน และมีรายละเอียดที่เกี่ยวข้องเหมาะสม

๒. จัดให้มีแนวทางในการยกระดับทักษะความรู้และความเชี่ยวชาญในด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ หรือมาตรการในการพัฒนาศักยภาพบุคลากรของหน่วยงานผู้ให้บริการขนส่งทางรางในด้านทักษะของบุคลากร โดยให้มีการส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง รวมถึงจัดให้มีโครงการพัฒนาศักยภาพผู้ปฏิบัติงานของหน่วยงานผู้ให้บริการขนส่งทางราง และหลักสูตรหรือโครงการสร้างความตระหนักรู้และการฝึกอบรม และแผนงานที่เกี่ยวข้อง โดยต้องดำเนินการจัดประเภทของผู้ปฏิบัติงาน โครงการ หลักสูตร และกำหนดแผนงานให้เหมาะสมกับผู้ปฏิบัติงานแต่ละประเภท เพื่อเป็นการยกระดับทักษะความรู้ และความเชี่ยวชาญของบุคลากรของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งประกอบไปด้วย

๑) ขอบเขตการพัฒนาผู้ปฏิบัติงาน ประกอบด้วย

(๑) ทักษะของบุคลากร (Skillsets) เพื่อกำหนดแนวทางการพัฒนาผู้ปฏิบัติงานของหน่วยงานผู้ให้บริการขนส่งทางราง หรือบุคลากรอื่นที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ ให้มีทักษะที่จำเป็นเหมาะสมในการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมถึงต้องประเมินและวางแผนการพัฒนาอย่างต่อเนื่อง

(๒) สภาพแวดล้อม และระบบการทำงานที่ส่งเสริมและสนับสนุนการเรียนรู้ และการพัฒนาบุคลากรอย่างต่อเนื่อง เพื่อส่งเสริมและเอื้อต่อการเรียนรู้ และการพัฒนากรอบความคิด และกรอบทักษะสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์อย่างต่อเนื่อง

๒) การพัฒนาทักษะของบุคลากร โดยกำหนดแนวทางการสร้างความตระหนักรู้และการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วยแนวทางการส่งเสริมการเรียนรู้ ดังนี้

(๑) การสร้างความตระหนักรู้ (Awareness)

(๒) การฝึกอบรม (Training)

(๓) การศึกษา (Education)

ซึ่งควรนำทั้ง ๓ แนวทางการส่งเสริมการเรียนรู้มากำหนดให้มีความต่อเนื่องในการดำเนินการพัฒนาทักษะของบุคลากร โดยเริ่มจากการสร้างความตระหนักรู้ สร้างการฝึกอบรม และพัฒนาไปสู่การศึกษา

๓) บุคคลที่เกี่ยวข้องกับการพัฒนาทักษะของผู้ปฏิบัติงานของหน่วยงานผู้ให้บริการขนส่งทางราง ประกอบด้วย

(๑) หัวหน้าหน่วยงาน

(๒) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

(๓) หัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์ หรือผู้บริหารระดับสูงที่มีหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) ที่ได้รับการแต่งตั้งให้ดำเนินการเป็นหัวหน้าแผนงานหรือโครงการด้านความมั่นคงปลอดภัยไซเบอร์

(๔) หัวหน้าส่วนงาน

(๕) ผู้ใช้งาน ประกอบด้วย บุคคลภายในหน่วยงานผู้ให้บริการขนส่งทางราง และบุคคลภายนอกหน่วยงานผู้ให้บริการขนส่งทางราง

๔) ขั้นตอนการพัฒนาทักษะของผู้ปฏิบัติงานของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งประกอบด้วย

(๑) ขั้นตอนที่ ๑ การออกแบบแผนงาน หรือโครงการสร้างความตระหนักรู้และการฝึกอบรม

(๒) ขั้นตอนที่ ๒ การพัฒนาเอกสาร สื่อ เนื้อหาสำหรับแผนงาน หรือโครงการสร้างความตระหนักรู้ และการฝึกอบรม

(๓) ขั้นตอนที่ ๓ การดำเนินการแผนงาน หรือโครงการ

(๔) ขั้นตอนที่ ๔ หลังดำเนินการแผนงาน หรือโครงการ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. จัดให้มีการกำหนดกิจกรรมส่งเสริมความตระหนัก โดยพิจารณาอย่างน้อย ดังนี้

๑) จัดอบรมและสัมมนาเชิงปฏิบัติการเกี่ยวกับภัยคุกคามทางไซเบอร์ และวิธีการป้องกันอย่างน้อยปีละ ๑ ครั้ง

๒) จัดทำสื่อประชาสัมพันธ์ เช่น Infographic, Video Clip, E-Newsletter ที่เกี่ยวกับการรักษาความปลอดภัยของข้อมูล เป็นต้น

๓) จัดกิจกรรม Cybersecurity Awareness Campaign เช่น การจัดกิจกรรมรายสัปดาห์แห่งความมั่นคงปลอดภัยไซเบอร์ เป็นต้น

๔) จัดทำหลักสูตร e-Learning และแบบทดสอบออนไลน์ เพื่อวัดระดับความเข้าใจของบุคลากร

๕) จัดให้มีกิจกรรมตอบคำถามหรือแข่งขันด้านความรู้ความปลอดภัยไซเบอร์ เพื่อกระตุ้นการมีส่วนร่วม

๖) กำหนดให้มีการแจ้งเตือนภัยคุกคามใหม่ ๆ ผ่านช่องทางภายใน เช่น Intranet, Email Notification เป็นต้น

๒. จัดให้มีการกำหนดเนื้อหาหลักในการสร้างความตระหนักรู้ โดยพิจารณาอย่างน้อย ดังนี้

๑) ความสำคัญของการรักษาความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล (CIA Triad)

๒) วิธีป้องกันภัยฟิชชิง (Phishing), มัลแวร์ (Malware) และการโจมตีทางไซเบอร์รูปแบบต่าง ๆ

๓) แนวทางการใช้รหัสผ่านอย่างปลอดภัย และการจัดการบัญชีผู้ใช้ (Password and Account Management)

๔) การรักษาความปลอดภัยของอุปกรณ์พกพา และการทำงานจากระยะไกล (Mobile and Remote Working Security)

๕) นโยบายการใช้งานอินเทอร์เน็ต อีเมล และอุปกรณ์เทคโนโลยีสารสนเทศภายในองค์กร

๖) กระบวนการรายงานเหตุการณ์ผิดปกติ หรือเหตุการณ์ด้านความมั่นคงปลอดภัย (Incident Reporting)

๓. จัดให้มีการประเมินผลและปรับปรุง โดยพิจารณาอย่างน้อย ดังนี้

๑) ประเมินผลการสร้างความตระหนักรู้ผ่านการสอบหลังการอบรม การสัมภาษณ์ หรือแบบสอบถาม

๒) กำหนดให้มีการติดตามผล และวิเคราะห์พฤติกรรมการใช้งานระบบของบุคลากรอย่างต่อเนื่อง

๓) นำผลการประเมินไปปรับปรุงกิจกรรม และเนื้อหาให้เหมาะสมกับภัยคุกคาม และบริบทขององค์กรที่เปลี่ยนแปลง

๔. กำหนดให้มีการบริหารจัดการควบคุมการส่งข้อความอิเล็กทรอนิกส์ โดยพิจารณาให้มีการควบคุมอย่างน้อย ดังนี้

๑) กำหนดให้มีการควบคุมและเข้ารหัสข้อมูลสำคัญหรือข้อมูลส่วนบุคคลที่ส่งผ่านข้อความอิเล็กทรอนิกส์ และจำกัดสิทธิ์การแนบไฟล์ หรือส่งลิงก์ไปยังผู้ใช้งานภายนอก

๒) พิจารณาติดตั้งระบบ Email Security Gateway เพื่อคัดกรอง Spam และ Phishing

๓) กำหนดให้มีการควบคุมและจำกัดสิทธิ์การส่งข้อความอิเล็กทรอนิกส์ โดยการห้ามใช้ Email ส่วนตัว ในการส่งข้อมูลขององค์กร เว้นแต่ได้รับอนุญาต

๔) กำหนดให้มีการบันทึกและตรวจสอบการรับ - ส่งข้อความอิเล็กทรอนิกส์ โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดให้มีการบันทึกกิจกรรมระบบ (Log) การรับ - ส่งข้อความอิเล็กทรอนิกส์ เช่น ผู้ส่ง, ผู้รับ, เวลา, ขนาดไฟล์แนบ เป็นต้น และจัดเก็บไว้อย่างน้อย ๙๐ วัน

(๒) กำหนดให้มีการตรวจสอบพฤติกรรมผิดปกติ เช่น ส่งข้อมูลจำนวนมากผิดเวลา, แนบไฟล์น่าสงสัย เป็นต้น

๕) กำหนดให้มีการอบรมผู้ใช้งานข้อความอิเล็กทรอนิกส์ โดยให้ความรู้เกี่ยวกับความเสี่ยงจากการใช้ข้อความอิเล็กทรอนิกส์ เช่น Social Engineering, Business Email Compromise (BEC) เป็นต้น พร้อมทั้งกำหนดช่องทางแจ้งเตือนหรือรายงานอีเมลต้องสงสัย

(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๑. กำหนดให้มีการสร้าง การทบทวน หรือปรับปรุงมาตรการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และขีดความสามารถในการจัดเก็บข้อมูลจราจร (Implementing a Cybersecurity Monitoring and Logging Capability) โดยพิจารณากำหนดกระบวนการ ๗ ขั้นตอน ดังนี้

๑) กำหนดให้มีการพัฒนาแผนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจร (Develop a Cybersecurity Monitoring and Logging) โดยพิจารณาสำรวจสมรรถนะในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และความต้องการในการเก็บข้อมูลจราจรของผู้ให้บริการขนส่งทางราง รวมถึงส่วนประกอบอื่นที่เกี่ยวข้อง เช่น งบประมาณ ทรัพยากร และวิธีดำเนินการเก็บข้อมูลจราจรที่ต้องการหรือคาดหวังและนำขออนุมัติจากผู้บริหารระดับสูง หรือคณะกรรมการที่ได้รับมอบหมาย ทั้งนี้ การพิจารณาแนวทางที่ดีสำหรับการวางแผนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจร สามารถพิจารณาออกเป็น ๔ ประเภทหลัก ดังนี้

(๑) วัตถุประสงค์ที่ชัดเจน (Clear Purpose) เช่น ตั้งเป้าหมายที่ชัดเจน ระบุประโยชน์ของการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร สำรวจบริบทของผู้ให้บริการขนส่งทางราง เพื่อกำหนดวัตถุประสงค์ ของผู้ให้บริการขนส่งทางราง

(๒) การดำเนินการตามกระบวนการที่ขับเคลื่อนด้วยความเสี่ยง (Risk-driven, Process-based Approach) เช่น ใช้แนวทางการประเมินความเสี่ยงในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจร สามารถเชื่อมโยงข้อมูลข่าวกรองความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นจริงกับการประเมินความเสี่ยง เป็นต้น

(๓) ให้ความสำคัญกับการวิเคราะห์ภัยคุกคามมากขึ้น (More Focused Threat Analysis) เช่น นำเครื่องมือในการจัดการกับข้อมูลจราจรมาใช้อย่างเหมาะสมกับภัยคุกคามและความเสี่ยงของผู้ให้บริการขนส่งทางราง ศึกษาพฤติกรรมปกติ และความผิดปกติของระบบหรือเครือข่าย รวมถึงกำหนดกระบวนการที่สามารถเข้าถึงข้อมูลแหล่งที่มาของภัยคุกคามได้ทันเวลา บูรณาการ และใช้งานข้อมูลข่าวและข่าวกรองภัยคุกคามได้

(๔) การจัดสรรทรัพยากรที่ดีขึ้น (Better Resourcing) เช่น ลงทุนในการสร้างทักษะให้แก่บุคลากร ดำเนินการจัดสรรเวลา หรือทรัพยากรอย่างต่อเนื่อง และสร้างความร่วมมือกับผู้ให้บริการด้านการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และบริการเก็บข้อมูลจราจร

๒) กำหนดข้อกำหนดเบื้องต้น สำหรับการเฝ้าระวัง และการเก็บข้อมูลจราจรความมั่นคงปลอดภัยไซเบอร์ (Carry out Prerequisites for Cybersecurity Monitoring and Logging) และการดำเนินการซึ่งข้อกำหนดควรพิจารณาประกอบด้วย

- วัตถุประสงค์และขอบเขตและสินทรัพย์ที่ต้องตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Agreeing Objectives and Scope) การเฝ้าระวังและการเก็บข้อมูลจราจรความมั่นคงปลอดภัยไซเบอร์ เช่น บริการที่สำคัญ หรือระบบงานที่สำคัญ ระบบเครือข่าย (Network Infrastructure) เป็นต้น
- กำหนดทรัพย์สินหลัก หรือทรัพย์สินที่สำคัญ และกำหนดตำแหน่งที่อยู่ของทรัพย์สินนั้น
- ระบุจุดเชื่อมต่อไปยังภายนอก เช่น อินเทอร์เน็ต
- พิจารณาลักษณะการโจมตีการรักษาความมั่นคงปลอดภัยไซเบอร์ในทรัพย์สินที่สำคัญ

- พิจารณาหามาตรการ เพื่อลดเส้นทางการโจมตีไปยังทรัพย์สิน และกำหนดมาตรการควบคุมทางเทคนิคที่สำคัญและลดขอบเขตการโจมตี
- ทบทวนและปรับปรุงมาตรการควบคุมความมั่นคงปลอดภัยทางไซเบอร์ (Reviewing and Revising Cybersecurity Controls) และอื่น ๆ ให้เหมาะสมกับเป้าหมายของผู้ให้บริการขนส่งทางราง

๓) ระบุแหล่งที่มาของสัญญาณเตือนเหตุภัยคุกคามทางไซเบอร์ (Signs of Cybersecurity Incidents) รวมถึงการกำหนดให้มีการแยก “สัญญาณเตือน” (Signal) ที่แท้จริงออกจาก “สัญญาณรบกวน” (Noise) แหล่งข้อมูลต่าง ๆ ที่เกี่ยวข้องกับการวิเคราะห์ตัวบ่งชี้ถึงการบุกรุก (IOC) เช่น

- พิจารณาใช้บริการโดยผู้ให้บริการภายนอกที่ให้บริการซอฟต์แวร์รักษาความมั่นคงปลอดภัย เช่น IDS, IPS, DLP, SIEM, ซอฟต์แวร์ป้องกันไวรัสและสแปม, ซอฟต์แวร์ตรวจสอบความสมบูรณ์ของไฟล์และบริการเฝ้าระวัง (Monitoring Services)
- พิจารณาใช้เครื่องมือที่สามารถแยกมัลแวร์ และเทคนิคการสืบสวนสอบสวน (Malware Isolation and Investigation Techniques) เช่น การทำแซนด์บ็อกซ์ (Sandboxing) หรือเอ็นจิ้นการดำเนินการเสมือน (Virtual Execution Engines)
- พิจารณาให้มีข้อมูลบันทึกการใช้งาน เช่น ข้อมูลการจราจรระบบปฏิบัติการ บันทึกบริการและแอปพลิเคชัน บันทึกอุปกรณ์เครือข่าย และการไหลของข้อมูลในเครือข่าย
- พิจารณาแยกข้อมูลที่เปิดเผยต่อสาธารณะ เช่น ข้อมูลเกี่ยวกับการแสวงหาประโยชน์ใหม่ ๆ (Information on New Exploits) ที่ต้องเปิดเผยต่อบุคคลหรือหน่วยงานที่สาม

๔) ดำเนินการออกแบบความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจร (Design Your Cybersecurity Monitoring and Logging Capability) เมื่อข้อกำหนดต่าง ๆ เสร็จสมบูรณ์ และได้ระบุแหล่งที่มาของสัญญาณเตือนเหตุภัยคุกคามทางไซเบอร์ (Signs of Cybersecurity Incidents) แล้วเสร็จ โดยดำเนินการพิจารณาออกแบบการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์โดยรวมและความสามารถในการเก็บข้อมูลจราจร โดยพิจารณาด้านต่าง ๆ ดังนี้

- บุคลากร (People) ที่ต้องรับผิดชอบในการวิเคราะห์ข้อมูล ซึ่งต้องมีทักษะเฉพาะ
- กระบวนการ (Process) เช่น กำหนดกระบวนการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์และกระบวนการตอบสนองต่อเหตุการณ์ กระบวนการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ ซึ่งประกอบด้วย ๔ ขั้นตอนหลัก ดังนี้ ๑. รวบรวมข้อมูลเหตุการณ์ที่เกี่ยวข้อง ๒. รวมข้อมูลเข้าด้วยกัน ๓. พิจารณาวิเคราะห์เหตุการณ์ที่ผิดปกติ ๔. ดำเนินการจัดการเหตุการณ์ที่ผิดปกติ
- เทคโนโลยี (Technology) โดยพิจารณาใช้เครื่องมือ SIEM และเครื่องมือในการจัดการเก็บข้อมูลจราจร และการวิเคราะห์เหตุการณ์ที่หลากหลายร่วมกัน
- ข้อมูล (Information) โดยพิจารณาข่าวกรองความมั่นคงปลอดภัยไซเบอร์ที่เชื่อถือได้ (Reliable) และเป็นปัจจุบัน

๕) พิจารณาสร้างหรือซื้อบริการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Build or Buy Cybersecurity Monitoring and Logging Services) โดยพิจารณาวิธีการใช้งานอย่างมีประสิทธิภาพ และมีค่าใช้จ่ายที่สมเหตุสมผลกับผู้ให้บริการขนส่งทางรางซึ่งควรมีการพิจารณา ดังนี้

- การดำเนินการภายในหน่วยงาน (In-sourced Service)
- การใช้ระบบคลาวด์ และอุปกรณ์ หรือซอฟต์แวร์ในฐานะผู้ให้บริการ (Cloud & Appliance Based/ Software as a Service Provider)
- การใช้บริการจากผู้ให้บริการเครือข่าย หรือผู้ให้บริการด้านเทคโนโลยีสารสนเทศหรือผู้ให้บริการจัดการการรักษาความมั่นคงปลอดภัย (Managed Security Services Provider: MSSP)
- การใช้โมเดลแบบผสม (Hybrid Model)

ทั้งนี้ ในกรณีที่เลือกใช้บริการจากผู้ให้บริการภายนอก ควรมีการพิจารณาข้อกำหนด ดังนี้

(๑) เข้าใจถึงประโยชน์ของการใช้บริการผู้ให้บริการภายนอก

(๒) พิจารณาว่าควรจ้างกิจกรรมใดบ้าง จากผู้ให้บริการภายนอก

(๓) กำหนดเกณฑ์การคัดเลือกผู้ให้บริการภายนอก

(๔) แต่งตั้ง และกำหนดหน้าที่ความรับผิดชอบของผู้ให้บริการภายนอกที่ได้รับการคัดเลือก

๖) บูรณาการความสามารถในการเฝ้าระวังและการเก็บข้อมูลจราจรเข้ากับกรอบความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Integrate the Capability into Your Cybersecurity Framework) โดยนำระบบต่าง ๆ ที่เกี่ยวข้องมารวมกัน จัดเก็บข้อมูล และวิเคราะห์ข้อมูล เช่น ระบบที่จัดเก็บข้อมูลจราจร และระบบ SIEM เพื่อจัดเก็บ และวิเคราะห์ข้อมูลจราจร

๗) ดำเนินการรักษาระดับความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจร (Maintain the Cybersecurity Monitoring and Logging Capability) อย่างต่อเนื่อง โดยดำเนินการรักษาความสามารถในการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจรของผู้ให้บริการขนส่งทางราง และติดตาม รวมถึงพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์สม่ำเสมออย่างน้อยปีละ ๑ ครั้ง รวมถึงกำหนดให้มีการศึกษาแนวโน้มเทคโนโลยี หรือการดำเนินการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์ และการเก็บข้อมูลจราจรตามความต้องการ และหรือตามเป้าหมายของผู้ให้บริการขนส่งทางรางในอนาคต ซึ่งการเฝ้าระวังความมั่นคงปลอดภัยไซเบอร์และการเก็บข้อมูลจราจรควรพิจารณาให้ความสำคัญ ๓ ส่วนหลัก ดังนี้

(๑) การบริหารจัดการข้อมูลจราจร (Log Management)

(๒) การตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident Response)

(๓) การบริหารจัดการข่าวกรองความมั่นคงปลอดภัยไซเบอร์ และการรับรู้สถานการณ์ (Cybersecurity Intelligence and Situational Awareness)

๒. กำหนดให้มีกลไกและกระบวนการ เพื่อตรวจจับ จัดประเภท และวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ พร้อมทั้งจัดให้มีการวิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง โดยพิจารณาดำเนินการ ดังนี้

๑) จัดหาเทคโนโลยีสำหรับการรวบรวมข้อมูล (Technologies for Data Gathering) โดยใช้เครื่องมือที่มีความสามารถในการสังเกต ตรวจจับ ป้องกัน หรือบันทึกภัยคุกคามทางไซเบอร์ และช่องโหว่ที่รู้จัก และหรือแก้ไขหรือจัดการด้านต่าง ๆ ของการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่นำมาใช้

เพื่อจัดการภัยคุกคามและช่องโหว่ และพิจารณาจากวัตถุประสงค์ในการเฝ้าติดตาม และความสามารถของสถาปัตยกรรมของหน่วยงานผู้ให้บริการขนส่งทางราง และมาตรการการเฝ้าติดตามอย่างต่อเนื่อง ดังนี้

- การจัดการช่องโหว่ (Vulnerability Management)
- การจัดการแพตช์ (Patch Management)
- การจัดการเหตุการณ์ (Event Management)
- การจัดการเหตุภัยคุกคามทางไซเบอร์ (Incident Management)
- การตรวจจับมัลแวร์ (Malware Detection)
- การจัดการทรัพย์สิน (Asset Management)
- การจัดการกำหนดค่า (Configuration Management)
- การจัดการเครือข่าย (Network Management)
- การจัดการไลเซนส์ (License Management)
- การจัดการสารสนเทศ (Information Management)
- การรับประกันซอฟต์แวร์ (Software Assurance)

๒) พิจารณาเทคโนโลยีสำหรับการรวบรวม และการวิเคราะห์ (Technologies for Aggregation and Analysis) โดยนำเทคโนโลยีที่มีความสามารถในการรวบรวมข้อมูลดิบที่ได้จากการควบคุมความมั่นคงปลอดภัยอย่างน้อยหนึ่งรายการ หรือจากเทคโนโลยีการรวบรวมข้อมูลโดยตรงอื่น ๆ มาทำการเชื่อมโยง วิเคราะห์ และแสดงข้อมูลดิบในลักษณะที่ให้มุมมองที่มีความหมายมากขึ้นเกี่ยวกับประสิทธิภาพของการรักษาความมั่นคงปลอดภัย เช่น การจัดการเหตุการณ์และสารสนเทศความมั่นคงปลอดภัย (Security Information and Event Management : SIEM) รวมถึงจัดให้มีแดชบอร์ดการจัดการความมั่นคงปลอดภัย หรือข้อมูลสรุปการควบคุมการจัดการสารสนเทศความมั่นคงปลอดภัย โดยรวบรวมและสื่อสารข้อมูลที่เกี่ยวข้องกับสถานะความมั่นคงปลอดภัยของหน่วยงานแบบเรียลไทม์ และรายงานไปยังผู้เกี่ยวข้องในการจัดการความมั่นคงปลอดภัย เช่น ผู้ดูแลระบบทางเทคนิค CISO ผู้บริหารความเสี่ยง เป็นต้น และแสดงให้เห็นถึงการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในกฎหมาย ข้อบังคับ และนโยบายในกรณีที่ไม่มีวิธีการทำงานที่เป็นมาตรฐาน และเป็นไปโดยอัตโนมัติ

ทั้งนี้ ควรพิจารณาใช้เครื่องมือที่สามารถทำงานโดยอัตโนมัติ เพื่อให้สามารถรักษาความมั่นคงปลอดภัยไซเบอร์ ดังนี้

- สแกนหาช่องโหว่และใช้แพตช์ที่เหมาะสมโดยอัตโนมัติ
- เปิดใช้งานการกำหนดค่าความมั่นคงปลอดภัยโดยอัตโนมัติ ตามรายการตรวจสอบการตั้งค่าความมั่นคงปลอดภัย (Checklist of Security Settings)
- สแกนหาความสอดคล้องกับรายการตรวจสอบการตั้งค่าความมั่นคงปลอดภัยที่กำหนดไว้ล่วงหน้า
- รวบรวมตัวชี้วัดความมั่นคงปลอดภัยจากเครื่องมือ และรายงานไปยังแผงควบคุมสำหรับการจัดการ (Management Console) ในรูปแบบมาตรฐาน

๓) จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบเมื่อได้รับการแจ้งเตือนการเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์จากกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยวิเคราะห์และคัดแยกเหตุภัยคุกคามทางไซเบอร์ (Incident Triage) กำหนดประเภทและขอบเขตของเหตุการณ์กับความสัมพันธ์กับเหตุการณ์อื่น ๆ และเรียงลำดับเหตุการณ์ เพื่อดำเนินการแก้ไขตามลำดับความร้ายแรงของผลกระทบ ซึ่งควรพิจารณากำหนดกระบวนการคัดแยกเหตุการณ์ (Triage Process) อย่างชัดเจน ซึ่งควรประกอบด้วยกระบวนการหลัก ดังนี้

(๑) ดำเนินการระบุเหตุการณ์ (Event Identification) โดยทีมรักษาความมั่นคงปลอดภัยที่ได้รับมอบหมายดำเนินการระบุเหตุการณ์ที่มีการแจ้งเตือนเหตุการณ์

(๒) ดำเนินการประเมินเบื้องต้น (Initial Assessment) เพื่อพิจารณาการแจ้งเตือนเป็นเท็จ (False Positive) หรือเป็นภัยคุกคามทางไซเบอร์ที่แท้จริง ทั้งที่จะเกิดขึ้น ในอนาคต หรือกำลังเกิดขึ้นในขณะนี้ โดยการตรวจสอบข้อมูลจราจร ตรวจสอบการรับส่งข้อมูลเครือข่าย หรือดำเนินการประเมินช่องโหว่ เป็นต้น

(๓) ดำเนินการจัดประเภท (Classification) โดยจำแนกประเภทของเหตุการณ์ และวิเคราะห์เหตุภัยคุกคามทางไซเบอร์นั้นเป็นภัยคุกคามอย่างไร ตามที่กำหนดในประกาศความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

(๔) ดำเนินการจัดลำดับความสำคัญ (Prioritization) โดยอิงกับผลการประเมินเบื้องต้นและผลการจัดประเภท เพื่อทราบถึงความเร่งด่วน และวางแผนการดำเนินการ

(๕) ดำเนินการระงับ (Containment) เพื่อจำกัดขอบเขต และระงับภัยคุกคามทางไซเบอร์

(๖) ดำเนินการทางนิติเวช และการสืบสวน (Forensics and Investigation) โดยละเอียดเพื่อหาหลักฐาน ระบุที่มาของการจู่โจม ประเมินข้อมูลที่ได้รับผลกระทบ และการสูญเสียข้อมูลที่อาจเกิดขึ้น

(๗) ดำเนินการสื่อสาร (Communication) กับบุคลากรที่ได้รับผลกระทบ เช่น เจ้าหน้าที่เทคโนโลยีสารสนเทศ ฝ่ายบริหาร เพื่อแจ้งให้ทราบเกี่ยวกับเหตุการณ์ และให้คำแนะนำในการรักษาความมั่นคงปลอดภัย

(๘) ดำเนินการแก้ไข (Resolution) ตามมาตการเพื่อแก้ไขปัญหาที่อาจเกิดขึ้นอีก

(๙) จัดทำเอกสารประกอบ (Documentation) และเก็บรักษาเอกสารอย่างละเอียดตลอดกระบวนการตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการและการสำรวจ

(๑๐) ดำเนินการทบทวน และนำมาเป็นบทเรียน (Review and Lessons Learned) เพื่อนำมาประเมินปัญหา และอุปสรรคที่เกิดขึ้น พร้อมทั้งปรับปรุงแก้ไข

ตัวอย่างของการดำเนินการตามกระบวนการคัดแยกระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และเหตุภัยคุกคามทางไซเบอร์ (Security Event and an Incident)

เหตุการณ์ที่ ๑ ตัวอย่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๑.๑ คำอธิบายเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์กิจกรรมที่ผิดปกติบนเครื่องแม่ข่าย (Unusual Activity on a Server)

- ระบบตรวจสอบความมั่นคงปลอดภัยของหน่วยงาน จะสร้างการแจ้งเตือนเกี่ยวกับกิจกรรมที่ผิดปกติบนเครื่องแม่ข่ายให้บริการเว็บไซต์ของบริษัทหนึ่ง
- การแจ้งเตือนบ่งชี้ว่ามีการรับส่งข้อมูลเครือข่ายเพิ่มขึ้นอย่างมาก และการพยายามเข้าสู่ระบบล้มเหลวหลายครั้งภายในกรอบเวลาอันสั้น
- ไม่พบหลักฐานโดยตรงของการเข้าถึง โดยไม่ได้รับอนุญาต หรือการละเมิดข้อมูล

๑.๒ ตัวอย่างกระบวนการคัดแยก (Triage Process)

๑. การระบุเหตุการณ์ (Event Identification) ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์ เมื่อระบบตรวจสอบสร้างการแจ้งเตือน

๒. การประเมินเบื้องต้น (Initial Assessment) ทีมรักษาความมั่นคงปลอดภัยจะเริ่มการประเมินเหตุการณ์เบื้องต้น และตรวจสอบการแจ้งเตือน และรวบรวมข้อมูลเกี่ยวกับเครื่องแม่ข่ายลักษณะของกิจกรรม และตัวบ่งชี้ที่เป็นไปได้ของการโจมตี

๓. การจัดประเภท (Classification) จากการประเมินเบื้องต้นทีมปฏิบัติงานจัดประเภทเหตุการณ์นี้เป็นเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แทนที่จะเป็นเหตุภัยคุกคามทางไซเบอร์ เนื่องจากยังไม่มีหลักฐานที่เป็นรูปธรรมของการละเมิดความมั่นคงปลอดภัย จึงถือเป็นงานรักษาความมั่นคงปลอดภัยเนื่องจากมีกิจกรรมที่ผิดปกติ

๔. การจัดลำดับความสำคัญ (Prioritization) เหตุการณ์นี้จัดอยู่ในลำดับความสำคัญต่ำถึงปานกลาง เนื่องจากไม่มีข้อบ่งชี้ถึงการละเมิดในทันที มีการติดตามอย่างใกล้ชิดแต่ไม่ต้องการการตอบสนองอย่างเร่งด่วน

๕. เอกสารประกอบ (Documentation) รายละเอียดของเหตุการณ์ รวมถึงการแจ้งเตือน การประเมินเบื้องต้น และการจัดหมวดหมู่ ได้รับการบันทึกไว้ เพื่อใช้อ้างอิงและการวิเคราะห์ในอนาคต

เหตุการณ์ที่ ๒ ตัวอย่างเหตุภัยคุกคามทางไซเบอร์ (Incident)

๒.๑ คำอธิบายเหตุภัยคุกคามทางไซเบอร์การละเมิดข้อมูล (Data Breach)

- หลายวันต่อมา ทีมรักษาความมั่นคงปลอดภัยตรวจพบการถ่ายโอนข้อมูลที่น่าสงสัยจากเครื่องแม่ข่ายที่ถูกบุกรุกไปยังที่อยู่ IP ภายนอก
- การตรวจสอบเพิ่มเติมเผยให้เห็นการเข้าถึงข้อมูลลูกค้าที่ละเอียดอ่อนโดยไม่ได้รับอนุญาต
- มีการยืนยันการมีอยู่ของมัลแวร์บนเครื่องแม่ข่ายที่ถูกบุกรุก

๒.๒ กระบวนการคัดแยก

๑. การระบุเหตุภัยคุกคามทางไซเบอร์ (Incident Identification) ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์เมื่อยืนยันการเข้าถึง โดยไม่ได้รับอนุญาตและการขโมยข้อมูล

๒. การประเมินเบื้องต้น (Initial Assessment) การประเมินอย่างละเอียดจะดำเนินการเพื่อทำความเข้าใจขอบเขตและผลกระทบของเหตุการณ์ รวบรวมหลักฐาน และระบุว่าการละเมิดเกิดขึ้นได้อย่างไร

๓. การจำแนกประเภท (Classification) ขณะนี้เหตุการณ์นี้ถูกจัดว่าเป็นเหตุภัยคุกคามทางไซเบอร์ (Incident) เนื่องจากการเข้าถึงที่ไม่ได้รับอนุญาต และการละเมิดข้อมูลได้รับการยืนยัน

๔. การจัดลำดับความสำคัญ (Prioritization) เหตุการณ์นี้จัดอยู่ในประเภทวิกฤติ โดยต้องมีการดำเนินการทันที เพื่อหยุดการละเมิดแยกระบบที่ได้รับผลกระทบ และเริ่มการสืบสวนสอบสวนโดยละเอียด

๕. การระงับ (Containment) ทีมรักษาความมั่นคงปลอดภัยจะดำเนินการทันที เพื่อควบคุมเหตุการณ์ เช่น การแยกเครื่องแม่ข่ายที่ถูกบุกรุกออกจากเครือข่าย และการปิดกั้นการขโมยข้อมูลเพิ่มเติม

๖. นิติเวชและการสืบสวน (Forensics and Investigation) มีการดำเนินการสืบสวนสอบสวนโดยละเอียด เพื่อระบุสาเหตุที่แท้จริง วิเคราะห์มัลแวร์ และกำหนดขอบเขตของการละเมิดข้อมูล

๗. การสื่อสาร (Communication) ผู้มีส่วนได้ส่วนเสีย รวมถึงผู้บริหารระดับสูง ทีมกฎหมาย และลูกค้าที่ได้รับผลกระทบ จะได้รับแจ้งเกี่ยวกับเหตุการณ์ดังกล่าวตามแผนการตอบสนองต่อเหตุการณ์ของหน่วยงาน

๘. การแก้ไข (Resolution) ทีมรักษาความมั่นคงปลอดภัยทำงานเพื่อแก้ไขปัญหา ลบมัลแวร์ แก้ไขช่องโหว่ และใช้มาตรการรักษาความมั่นคงปลอดภัยไซเบอร์เพิ่มเติม เพื่อป้องกันการละเมิดในอนาคต

๙. เอกสารประกอบ (Documentation) มีการเก็บรักษาเอกสารตลอดกระบวนการตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการ การสำรวจ และบทเรียนที่ได้รับ

๑๐. การทบทวนและบทเรียนที่ได้รับ (Review and Lessons Learned) หลังจากแก้ไขเหตุการณ์แล้ว การทบทวนหลังเหตุการณ์จะดำเนินการ เพื่อประเมินการตอบสนองของหน่วยงาน ระบุพื้นที่สำหรับการปรับปรุง และปรับปรุงขั้นตอนการตอบสนองต่อเหตุการณ์ให้สอดคล้องกัน ตัวอย่างนี้ แสดงให้เห็นถึงความแตกต่างระหว่างเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และเหตุภัยคุกคามทางไซเบอร์ และวิธีที่กระบวนการคัดแยกแตกต่างกันตามลักษณะของสถานการณ์ รวมถึงความเป็นไปได้ที่เหตุการณ์อาจหรือไม่อาจบานปลายไปสู่เหตุการณ์ต่าง ๆ ในกรณีที่เหตุการณ์ได้รับการยืนยันว่ามีการละเมิดความมั่นคงปลอดภัยไซเบอร์ หน่วยงานต้องใช้ความพยายามตอบสนองในทันที

เหตุการณ์ที่ ๓ การจราจรขาออกที่ผิดปกติพุ่งสูงขึ้น

๓.๑ คำอธิบายเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- บันทึกไฟร์วอลล์ของหน่วยงานแสดงให้เห็นว่า การรับส่งข้อมูลขาออกจากเวิร์กสเตชันแห่งใดแห่งหนึ่ง พุ่งสูงขึ้นอย่างกะทันหัน
- จากการสืบสวนสอบสวน พบว่าพนักงานกำลังดาวน์โหลดการอัปเดตซอฟต์แวร์ขนาดใหญ่ ส่งผลให้มีการรับส่งข้อมูลเพิ่มขึ้น

๓.๒ กระบวนการคัดแยก

๑. การระบุเหตุการณ์ ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์ เมื่อสังเกตเห็นปริมาณการรับส่งข้อมูลที่เพิ่มขึ้นอย่างรวดเร็วในบันทึกไฟร์วอลล์

๒. การประเมินเบื้องต้น จะดำเนินการเพื่อทำความเข้าใจสาเหตุของการจราจรที่เพิ่มขึ้นอย่างรวดเร็ว จากการตรวจสอบพบว่าไม่เป็นอันตราย และเกี่ยวข้องกับการอัปเดตซอฟต์แวร์ที่ถูกต้องตามกฎหมาย

๓. การจัดประเภทเหตุการณ์ดังกล่าว จัดเป็นเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ แต่ไม่ใช่เหตุภัยคุกคามทางไซเบอร์ เนื่องจากไม่มีข้อบ่งชี้ถึงการเข้าถึง โดยไม่ได้รับอนุญาตหรือกิจกรรมที่เป็นอันตราย

๔. การจัดลำดับความสำคัญ เนื่องจากไม่ใช่เหตุภัยคุกคามทางไซเบอร์ จึงได้รับมอบหมายลำดับความสำคัญต่ำและไม่ต้องการการตอบสนองอย่างเร่งด่วน

๕. เอกสารประกอบรายละเอียดของเหตุการณ์ รวมถึงผลการสืบสวนสอบสวนได้รับการบันทึกไว้เพื่อใช้อ้างอิง

เหตุการณ์ที่ ๔ การโจมตีแบบฟิชชิ่ง

๔.๑ คำอธิบายเหตุภัยคุกคามทางไซเบอร์

- พนักงานหลายคนรายงานว่าได้รับอีเมลที่น่าสงสัยพร้อมไฟล์แนบ
- การสืบสวนสอบสวนพบว่าอีเมลเหล่านี้ เป็นส่วนหนึ่งของแคมเปญฟิชชิ่งที่พยายามขโมยข้อมูล รับรองการเข้าสู่ระบบ

๔.๒ กระบวนการคัดแยก

๑. การระบุเหตุการณ์ ทีมรักษาความมั่นคงปลอดภัยจะระบุเหตุการณ์ เมื่อพนักงานหลายคนรายงานอีเมลที่น่าสงสัย

๒. การประเมินเบื้องต้น การประเมินเบื้องต้นจะดำเนินการ เพื่อประเมินอีเมลระบุเจตนาร้ายและประเมินผลกระทบที่อาจเกิดขึ้น

๓. การจัดประเภท เหตุการณ์นี้จัดเป็นเหตุภัยคุกคามทางไซเบอร์ (Incident) เนื่องจากเกี่ยวข้องกับการโจมตีแบบฟิชชิ่งที่ได้รับการยืนยันแล้ว ซึ่งอาจมีผลกระทบด้านความมั่นคงปลอดภัยไซเบอร์

๔. การจัดลำดับความสำคัญ เหตุการณ์นี้จัดอยู่ในลำดับความสำคัญปานกลาง แม้ว่าจะไม่เร่งด่วนเท่ากับเหตุการณ์ร้ายแรง แต่ก็จำเป็นต้องดำเนินการทันที เพื่อลดภัยคุกคามทางไซเบอร์

๕. การระงับผู้ใช้ที่ได้รับผลกระทบจะได้รับคำสั่งไม่ให้เปิดไฟล์แนบที่น่าสงสัย และตัวกรองอีเมล จะได้รับการอัปเดต เพื่อปิดกั้นอีเมลฟิชชิ่งที่คล้ายกัน

๖. นิติเวชและการสืบสวนสอบสวน มีการดำเนินการสืบสวนสอบสวนโดยละเอียดเพื่อระบุแหล่งที่มาของอีเมลฟิชชิ่ง ประเมินว่าข้อมูลประจำตัวใด ๆ ถูกบุกรุกหรือไม่ และระบุการสูญเสียข้อมูลที่อาจเกิดขึ้น

๗. การสื่อสาร ทีมตอบสนองต่อเหตุการณ์จะสื่อสารกับพนักงานที่ได้รับผลกระทบ เจ้าหน้าที่เทคโนโลยีสารสนเทศ และฝ่ายบริหาร เพื่อแจ้งให้ทราบเกี่ยวกับเหตุการณ์ดังกล่าวและให้คำแนะนำในการรักษาความมั่นคงปลอดภัยไซเบอร์

๘. การแก้ไขมีการใช้มาตรการ เพื่อลบเนื้อหาที่เป็นอันตราย อัปเดตการกำหนดค่าความมั่นคงปลอดภัยของอีเมล และให้ความรู้แก่พนักงานเกี่ยวกับภัยคุกคามทางไซเบอร์ กรณีฟิชชิ่ง

๙. เอกสารประกอบ มีการเก็บรักษาเอกสารตลอดกระบวนการตอบสนองต่อเหตุการณ์ รวมถึงการดำเนินการและการสำรวจ

๑๐. การทบทวนและบทเรียนที่ได้รับ หลังจากแก้ไขเหตุการณ์แล้ว จะมีการดำเนินการทบทวนหลังเหตุการณ์ เพื่อประเมินการตอบสนองของหน่วยงาน ระบุพื้นที่สำหรับการปรับปรุง และปรับปรุงมาตรการต่อต้านการฟิชชิ่ง ตัวอย่างเหล่านี้ แสดงให้เห็นถึงความแตกต่างระหว่างเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์และเหตุภัยคุกคามทางไซเบอร์ โดยอิงตามลักษณะของกิจกรรมที่สังเกตได้ วิธีที่กระบวนการคัดแยกจะแตกต่างกันไป หน่วยงานต้องสอบสวนเหตุการณ์ แม้ว่าเหตุการณ์อาจไม่เกี่ยวข้องกับการโจมตีทางไซเบอร์ ในกรณีที่ได้รับการยืนยันว่าเป็นเหตุภัยคุกคามทางไซเบอร์หรือกิจกรรมที่เป็นอันตราย หน่วยงานต้องตอบสนองอย่างเร่งด่วน

๔) ดำเนินการระบุถึงเหตุภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญ โดยดำเนินการวิเคราะห์ข้อมูล ดังนี้

- จำนวนผู้ได้รับผลกระทบ
- ผลกระทบที่เกิดขึ้น
- ระยะเวลาที่คาดว่าจะใช้ดำเนินการแก้ไขเหตุภัยคุกคามทางไซเบอร์
- บริการที่ได้รับผลกระทบเป็นบริการที่สำคัญหรือไม่ หากใช่ให้พิจารณาว่าเป็นเหตุการณ์ที่ต้องแจ้งไปยังหน่วยงานกำกับดูแล และสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๕) ดำเนินการทบทวนกลไกและกระบวนการตรวจจับเหตุภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง เพื่อปรับเปลี่ยนกฎ (Rules) ของระบบที่มีการทำงานอิงตามกฎ (Rule-based) ให้มีความเหมาะสมและตรงกับนโยบายความมั่นคงปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง หรือในกรณีที่การทำงานของระบบอิงกับพฤติกรรมของการจู่โจม (Behavior-based) อาจปรับเปลี่ยนค่า Baseline เพื่อให้มีความเหมาะสมกับพฤติกรรมการใช้งานที่แท้จริง รวมถึงการปรับปรุงความถี่ในการตรวจสอบ ปรับปรุงรายการการตรวจสอบ (Checklist) ในการวิเคราะห์ และปรับกระบวนการต่าง ๆ เป็นต้น

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการเก็บบันทึก และวิเคราะห์เหตุการณ์ (Log Management and Analysis) โดยจัดเก็บ Log จากระบบต่าง ๆ เช่น firewall, IDS/IPS, endpoint, server และกำหนดให้มีการจัดเก็บ log อย่างน้อย ๙๐ วัน หรือพิจารณาระยะเวลาจัดเก็บตามระดับความเสี่ยงของบริการที่สำคัญ หรือระบบงานที่สำคัญ

๒. พิจารณาใช้เครื่องมือ SIEM (Security Information and Event Management) เพื่อวิเคราะห์และแจ้งเตือนภัยคุกคามทางไซเบอร์

๓. กำหนดให้มีการประเมินความเสี่ยงจากภัยคุกคามใหม่ที่เกิดขึ้นอย่างสม่ำเสมอ รวมถึงทบทวนรายการภัยคุกคาม และแนวโน้มใหม่ที่เกิดขึ้นอย่างน้อยทุกไตรมาส

๔. จัดให้มีการอบรมให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง โดยมีเนื้อหาที่เกี่ยวข้องกับภัยคุกคามใหม่ ๆ

๕. กำหนดให้มีการบริหารจัดการข้อมูลจราจรคอมพิวเตอร์ (Log) โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จัดให้มีการกำหนดประเภทของข้อมูลจราจรที่ต้องจัดเก็บ ประกอบด้วยข้อมูลอย่างน้อย ดังนี้

(๑) ข้อมูลการพิสูจน์ตัวตน (Authentication Logs) เช่น การเข้าใช้งานระบบ (Login) และการออกจากระบบ (Logout) เป็นต้น

(๒) ข้อมูลการรับส่งข้อมูล (Access Logs, Traffic Logs) เช่น URL ที่เข้าใช้งาน ปริมาณการรับส่งข้อมูล เป็นต้น

(๓) ข้อมูลการเปลี่ยนแปลงระบบ (System Change Logs) เช่น การติดตั้ง/ถอนการติดตั้งโปรแกรม การแก้ไขสิทธิ์ผู้ใช้งาน เป็นต้น

(๔) ข้อมูลการใช้งานทรัพยากร (Resource Usage Logs) เช่น การใช้ CPU, Memory, Storage เป็นต้น

(๕) ข้อมูลเหตุการณ์ผิดปกติด้านความปลอดภัย (Security Event Logs) เช่น การถูกโจมตี การตรวจจับมัลแวร์ เป็นต้น

๒) จัดให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) กำหนดให้มีการจัดเก็บข้อมูลจราจรคอมพิวเตอร์อย่างน้อย ๙๐ วัน ตามกฎหมายกำหนด

(๒) ระบบที่มีข้อมูลสำคัญ หรือระบบที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ให้พิจารณาเก็บไม่น้อยกว่า ๑๘๐ วัน ถึง ๑ ปี ตามระดับความเสี่ยง

(๓) ใช้ระบบกลางในการรวบรวมข้อมูล (เช่น Centralized Log Server, SIEM) เพื่อให้การจัดเก็บ วิเคราะห์ และสำรองข้อมูลเป็นไปอย่างมีประสิทธิภาพ

(๔) ข้อมูล Log ต้องมีการประทับเวลาที่ถูกต้อง (Time Synchronization) กับแหล่งเวลาอ้างอิงที่น่าเชื่อถือ (เช่น NTP Server)

๓) จัดให้มีแนวทางการรักษาความปลอดภัยของข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) จำกัดสิทธิ์การเข้าถึงข้อมูลจราจรเฉพาะผู้ที่มีหน้าที่รับผิดชอบ (Role-Based Access Control)

(๒) เข้ารหัสข้อมูลระหว่างการรับส่งและขณะจัดเก็บ (Encryption In Transit and At Rest)

(๓) กำหนดมาตรการป้องกันการแก้ไข ลบ หรือเข้าถึงข้อมูล Log โดยมิชอบ

(๔) ดำเนินการสำรองข้อมูลจราจร (Log Backup) อย่างสม่ำเสมอ และเก็บรักษาในสถานที่ปลอดภัย

๔) กำหนดให้มีการตรวจสอบและการใช้ประโยชน์จากข้อมูลจราจรคอมพิวเตอร์ โดยพิจารณาอย่างน้อยดังนี้

(๑) จัดให้มีการตรวจสอบข้อมูลจราจรอย่างสม่ำเสมอ เพื่อค้นหาความผิดปกติ เช่น รายสัปดาห์ รายเดือน หรือรายไตรมาส เป็นต้น

(๒) กำหนดกระบวนการให้ข้อมูลจราจรแก่หน่วยงานภายนอกตามกฎหมาย พร้อมการอนุมัติจากผู้มีอำนาจ

๖. กำหนดให้มีการบริหารจัดการตั้งนาฬิการะบบให้ถูกต้อง โดยพิจารณาอย่างน้อยดังนี้

๑) จัดให้มีการกำหนดแหล่งเวลาสำหรับเวลาที่ใช้ในการอ้างอิงการตั้งเวลาระบบให้ชัดเจน เช่น กรมอุทกศาสตร์ กองทัพเรือ

๒) จัดให้มีการจัดการสำหรับระบบที่แยกขาด หรือมีความปลอดภัยสูง โดยดำเนินการใช้ NTP Server ภายในที่อ้างอิงกับ GPS หรือ Atomic Clock หรือกำหนดให้มีการตรวจสอบความถูกต้องของเวลาของระบบความปลอดภัยสูงทุกวัน

๗. กำหนดให้มีการบริหารจัดการขีดความสามารถของระบบ (System Capacity Management) โดยวางแผนขีดความสามารถของระบบ และดำเนินการประเมินความต้องการของระบบในระยะสั้น กลาง และยาว และทบทวนอย่างสม่ำเสมอ โดยพิจารณาปัจจัยสำคัญ เช่น จำนวนผู้ใช้งานพร้อมกัน ปริมาณข้อมูลที่จัดเก็บ ปริมาณการร้องขอบริการต่อวินาที

๘. กำหนดให้มีการตรวจสอบ ติดตาม และประเมินความมั่นคงปลอดภัย โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) ติดตามสถานะการใช้งาน CPU, RAM, Storage, Bandwidth อย่างสม่ำเสมอ

๒) กำหนดให้มีการตั้งค่าการแจ้งเตือน (Alert) หากการใช้ทรัพยากรเข้าใกล้ หรือเกินกว่าค่ากำหนด (Threshold)

๓) ทบทวนขีดจำกัดของอุปกรณ์รักษาความปลอดภัย เช่น Firewall, SIEM หรือ Antivirus Server อย่างสม่ำเสมอ

๙. กำหนดให้มีการบริหารจัดการทดสอบซอฟต์แวร์ ซึ่งต้องดำเนินการวางแผนการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำแผนการทดสอบ (Test Plan) โดยรวมถึงการทดสอบความมั่นคงปลอดภัย เช่น การทดสอบ input validation, access control, error handling เป็นต้น

๒) กำหนดให้มีการแยกสภาพแวดล้อมการทดสอบออกจากระบบงานจริง

๓) กำหนดบทบาทหน้าที่ และสิทธิของผู้ทดสอบ, ผู้พัฒนา และผู้ดูแลระบบ ออกจากกันอย่างชัดเจน

๔) กำหนดให้มีการควบคุมการใช้ข้อมูลในการทดสอบ โดยห้ามใช้ข้อมูลจริง (Production Data) ในการทดสอบระบบทดสอบ หากจำเป็นต้องใช้ข้อมูลจริงต้องดำเนินการกำหนดมาตรการควบคุม เช่น Approval, NDA และมาตรการป้องกันข้อมูลส่วนบุคคล เป็นต้น

๑๐. กำหนดให้มีการทดสอบความมั่นคงปลอดภัยของซอฟต์แวร์ เช่น

๑) การทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันโดยการวิเคราะห์ซอร์สโค้ด หรือไบนารีแบบไม่ต้องรันโปรแกรม เพื่อค้นหาช่องโหว่ด้านความปลอดภัยตั้งแต่ระยะเริ่มต้นของการพัฒนา (Static Application Security Testing (SAST))

๒) การทดสอบความมั่นคงปลอดภัยของแอปพลิเคชันขณะกำลังทำงานจริง โดยจำลองการโจมตีจากภายนอก เพื่อค้นหาช่องโหว่ด้านความปลอดภัยจากพฤติกรรมของระบบ (Dynamic Application Security Testing (DAST))

๓) การวิเคราะห์ส่วนประกอบของซอฟต์แวร์ เช่น ไลบรารีโอเพ่นซอร์ส เพื่อระบุช่องโหว่ที่รู้จักและความเสี่ยงด้านลิขสิทธิ์ที่อาจส่งผลต่อความมั่นคงปลอดภัยของระบบ (Software Composition Analysis (SCA))

๔) การทดสอบระบบแบบองค์รวมเพื่อยืนยันว่าระบบทำงานสอดคล้องตามข้อกำหนดทางธุรกิจและความต้องการของผู้ใช้งาน ก่อนการนำระบบไปใช้งานจริง (System acceptance testing)

๕) การประเมินความมั่นคงปลอดภัยของระบบโดยรวม เพื่อตรวจสอบมาตรการควบคุมด้านความปลอดภัย เช่น การตรวจสอบสิทธิ์ การเข้ารหัส และการป้องกันการบุกรุก ว่ามีประสิทธิภาพและเหมาะสมกับความเสี่ยงที่คาดการณ์ไว้ (System security testing)

๑๑. กำหนดให้มีการควบคุมสภาพแวดล้อมการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จำกัดการเข้าถึงระบบทดสอบ โดยให้เข้าถึงเฉพาะผู้มีสิทธิ์ รวมถึงพิจารณาใช้การยืนยันตัวตนที่มั่นคงปลอดภัย เช่น MFA, Role-based Access เป็นต้น

๒) กำหนดให้มีการบันทึก Log การเข้าถึงและการเปลี่ยนแปลงระบบในช่วงทดสอบ

๓) ตรวจสอบให้แน่ใจว่าไม่มีข้อมูลหรือรหัสสำคัญค้างอยู่ในระบบหลังดำเนินการทดสอบแล้วเสร็จ

๑๒. กำหนดให้มีการประเมินผลและจัดการช่องโหว่ก่อนนำระบบไปใช้งานจริง และหากพบข้อบกพร่อง หรือช่องโหว่ในการทดสอบ ต้องดำเนินการประเมินความเสี่ยง และกำหนดระดับความรุนแรง พร้อมทั้งแก้ไขและทำการทดสอบซ้ำ (Retesting) ก่อนส่งมอบระบบ

๑๓. จัดทำรายงานการทดสอบ (Test Report) และรายการข้อบกพร่อง (Defect List) เพื่อใช้ในการตรวจสอบภายหลัง

๑๔. กำหนดให้มีการบริหารจัดการพิสูจน์การทดสอบและการตรวจรับงาน โดยกำหนดให้วางแผนการทดสอบ โดยพิจารณาอย่างน้อยดังนี้

๑) จัดทำแผนการทดสอบ (Test Plan) โดยกำหนดให้มีการทดสอบ อย่างน้อย ดังนี้

(๑) การทดสอบส่วนย่อยที่สุดของโปรแกรม เช่น ฟังก์ชันหรือเมธอด เพื่อให้มั่นใจว่าทำงานได้ถูกต้องตามที่ออกแบบไว้ โดยไม่ขึ้นกับส่วนอื่นของระบบ (Unit Test)

(๒) การทดสอบการทำงานร่วมกันของหน่วยโปรแกรมต่าง ๆ หรือระบบย่อยหลายระบบ เพื่อให้แน่ใจว่ามีการสื่อสาร และทำงานร่วมกันได้ถูกต้อง (Integration Test)

(๓) การทดสอบโดยผู้ใช้งานหรือผู้แทนของธุรกิจ เพื่อประเมินว่าระบบตอบสนองต่อความต้องการ และสามารถใช้งานได้จริงตามวัตถุประสงค์ก่อนนำไปใช้งานจริง (UAT)

(๔) การทดสอบเพื่อประเมินความมั่นคงปลอดภัยของระบบ โดยมุ่งตรวจสอบช่องโหว่ความเสี่ยง และความสามารถของระบบในการป้องกันภัยคุกคามทางไซเบอร์ (Security Testing) เช่น SAST, DAST, Vulnerability Scan, Penetration Test เป็นต้น

๒) กำหนดผู้รับผิดชอบ ช่วงเวลา เครื่องมือ และเกณฑ์การผ่าน (Acceptance Criteria)

๓) กำหนดให้มีหลักฐานการทดสอบที่ชัดเจน เช่น รายการทดสอบ พร้อมผลการทดสอบ เป็นต้น

๑๕. กำหนดให้มีการทดสอบด้านความมั่นคงปลอดภัย โดยประกอบด้วย อย่างน้อยดังนี้

๑) ทำการทดสอบความปลอดภัยในขั้นตอน UAT หรือก่อนขึ้นระบบ (Go-live)

๒) เครื่องมือ หรือบริการที่ใช้ในการทดสอบต้องผ่านการรับรอง เช่น OWASP ZAP, Burp Suite, Nessus เป็นต้น

๓) หากพบความเสี่ยงระดับสูงหรือช่องโหว่สำคัญ ต้องดำเนินการแก้ไขให้แล้วเสร็จก่อนที่จะดำเนินการขึ้นระบบ (Go-live)

๑๖. กำหนดให้มีการบันทึกผลและจัดทำรายงานผลการทดสอบไว้เป็นหลักฐานการทดสอบ

๑๗. กำหนดให้มีการทบทวนภายหลังการขึ้นระบบงาน (Post-Acceptance Review) โดยดำเนินการอย่างน้อย ดังนี้

๑) ตรวจสอบความเสถียร และความมั่นคงปลอดภัยหลังจากที่มีการใช้งานระบบ ๓๐ วัน นับจากที่มีการขึ้นระบบ ในกรณีที่พบปัญหาต้องดำเนินการบันทึกปัญหา การแก้ไข และแจ้งกลับผู้พัฒนาระบบ เพื่อนำไปปรับปรุงระบบ

๒) ดำเนินการสรุปปัญหา ผลการวิเคราะห์ และวิธีการแก้ไข เพื่อนำไปเป็นบทเรียน (Lessons Learned) สำหรับใช้ปรับปรุงในอนาคต

๑๘. กำหนดให้มีการจำกัดการปรับแต่งซอฟต์แวร์สำเร็จรูป โดยพิจารณาให้มีการดำเนินการประเมินก่อนปรับแต่งซอฟต์แวร์สำเร็จรูป โดยดำเนินการอย่างน้อย ดังนี้

๑) วิเคราะห์ความจำเป็นในการปรับแต่ง เทียบกับความสามารถมาตรฐานของซอฟต์แวร์ (Out-of-the-box)

๒) ประเมินผลกระทบด้านความมั่นคงปลอดภัย ความเข้ากันได้กับแพตช์ และ SLA การบำรุงรักษาของซอฟต์แวร์

๓) พิจารณาทางเลือกอื่น เช่น การปรับกระบวนการองค์กรให้สอดคล้องกับระบบแทนที่จะปรับระบบให้สอดคล้องกับองค์กร

๑๙. กำหนดให้มีการควบคุมขอบเขตการปรับแต่งซอฟต์แวร์สำเร็จรูป โดยพิจารณาให้มีการควบคุมอย่างน้อย ดังนี้

๑) จำกัดการปรับแต่งเฉพาะฟังก์ชันที่ปลอดภัย และสามารถแยกออกจากซอฟต์แวร์หลัก เช่น ผ่าน API, Extension Framework เป็นต้น

๒) ห้ามแก้ไขซอร์สโค้ดของระบบหลักโดยตรง เว้นแต่ได้รับอนุญาตจากผู้ผลิต และไม่กระทบกับการดำเนินการด้านความมั่นคงปลอดภัยของระบบหลัก

๓) ในกรณีที่มีการเปลี่ยนแปลงต้องดำเนินการจัดเก็บ Script, Code และ Log การเปลี่ยนแปลงทั้งหมด พร้อมทั้ง Version Control และจัดทำ Change Log เป็นลายลักษณ์อักษร

๔) กำหนดให้มีการขออนุมัติการปรับแต่งซอฟต์แวร์สำเร็จรูปจากเจ้าของระบบและฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมาย

๕) กำหนดสิทธิการเข้าถึงเฉพาะผู้ที่ได้รับอนุมัติ หรืออนุญาตให้มีสิทธิปรับแต่งซอฟต์แวร์สำเร็จรูปเท่านั้น พร้อมทั้งจัดทำบันทึกประวัติการเข้าถึง หรือบันทึกกิจกรรมการเข้าถึง (Log)

๖) กำหนดให้มีกระบวนการทดสอบในระบบ UAT/Sandbox แยกจาก Production พร้อมทั้งต้องมีแผน Rollback ที่สามารถใช้คืนระบบสู่สภาพเดิมได้หากเกิดข้อผิดพลาด

๗) ในกรณีที่มีการอัปเดตแพตช์จากผู้ผลิต ต้องมีการดำเนินการตรวจสอบผลกระทบของการปรับแต่งก่อนดำเนินการ

๘) ในกรณีที่มีการปรับปรุงเวอร์ชันใหม่ของซอฟต์แวร์ ผู้ดูแลระบบและผู้ที่ได้รับมอบหมายให้ดำเนินการปรับแต่งซอฟต์แวร์ต้องร่วมกันประเมินผลกระทบต่อประสิทธิภาพของการใช้งาน

๒๐. กำหนดให้มีการจัดการทบทวนทางเทคนิคของแอปพลิเคชันหลังจากเปลี่ยนแปลงโครงสร้างพื้นฐานของระบบ โดยพิจารณาให้มีการดำเนินการอย่างน้อย ดังนี้

๑) กำหนดให้มีการลงทะเบียนการเปลี่ยนแปลงตามกระบวนการเปลี่ยนแปลงขององค์กร พร้อมทั้งระบุรายละเอียดการเปลี่ยนแปลง เช่น ประเภทของการเปลี่ยนแปลง ช่วงเวลา ระบบที่เกี่ยวข้อง และแอปพลิเคชันที่คาดว่าจะได้รับผลกระทบจากการเปลี่ยนแปลง เป็นต้น

๒) กำหนดให้มีการประเมินผลกระทบเชิงเทคนิค เช่น การเชื่อมต่อระบบภายนอก/ภายใน (IP, Port, Firewall) การเรียกใช้งาน API, Library, หรือบริการ (Service) ที่ได้รับผลกระทบ และตรวจสอบความเข้ากันได้ของเวอร์ชันใหม่กับซอฟต์แวร์ หรือเฟรมเวิร์กของแอปพลิเคชัน เป็นต้น

๓) กำหนดให้มีการทดสอบก่อนและหลังการนำไปใช้งาน โดยจัดให้มีการทดสอบฟังก์ชันที่สำคัญในแอปพลิเคชันในสภาพแวดล้อมสำหรับการทดสอบ เช่น Sandbox, UAT เป็นต้น รวมถึงทดสอบการเชื่อมต่อ ความเร็ว การพิสูจน์ตัวตน และการเข้าถึงข้อมูลหลังจากการเปลี่ยนแปลง

๔) กำหนดให้มีการตรวจประเมินความมั่นคงปลอดภัยหลังจากที่มีการเปลี่ยนแปลงโครงสร้างพื้นฐาน เช่น สแกนช่องโหว่ (Vulnerability Scanning) ทดสอบสิทธิและการควบคุมการเข้าถึง ประเมินผลกระทบต่อมาตรการรักษาความมั่นคงปลอดภัยข้อมูลส่วนบุคคล (PDPA) หรือการรักษาความมั่นคงปลอดภัยสารสนเทศ (ISO/IEC ๒๗๐๐๑)

๕) จัดให้มีรายงาน Application Review Result ที่แสดงผลการตรวจสอบและทดสอบ รวมถึงผลการติดตามการแก้ไขในกรณีที่พบข้อบกพร่อง พร้อมทั้งจัดเก็บไว้เป็นหลักฐาน

(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

กำหนดให้มีการจัดทำแผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan) โดยดำเนินการอย่างน้อย ดังนี้

๑) มีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดวัตถุประสงค์ของแผนการสื่อสารในภาวะวิกฤต และครอบคลุมการสื่อสารภายในและการสื่อสารไปยังภายนอกให้ครบถ้วน รวมถึงมีการระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้ และแผนการดำเนินการที่เกี่ยวข้อง

๒) กำหนดและวิเคราะห์กลุ่มผู้มีส่วนได้ส่วนเสีย (Stakeholder) ทั้งภายใน และภายนอก รวมทั้งระบุกลุ่มเป้าหมายที่ต้องสื่อสารเมื่อเกิดเหตุการณ์วิกฤต โดยพิจารณาจากสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๓) จัดโครงสร้างของทีมสื่อสารในภาวะวิกฤตพร้อมทั้งหน้าที่ความรับผิดชอบ ให้สอดคล้องกับบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง โดยทีมสื่อสารในภาวะวิกฤตอาจประกอบด้วย ผู้บริหาร เจ้าหน้าที่ ฝ่ายประชาสัมพันธ์ เจ้าหน้าที่ฝ่ายทรัพยากรมนุษย์ เจ้าหน้าที่ฝ่ายกฎหมาย เป็นต้น

๔) จัดเตรียมร่างข้อความที่ใช้สื่อสารเมื่อเกิดภาวะวิกฤต และกำหนดโฆษกหลัก และผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กร เมื่อมีการกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิม และโซเชียลมีเดีย สำหรับการเผยแพร่ข้อมูล

๖) ตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบ เพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๗) ดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงที และมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้หน่วยงานผู้ให้บริการขนส่งทางรางจัดเตรียมบุคลากรสำหรับฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) โดยดำเนินการอย่างน้อย ดังนี้

๑) สนับสนุนบุคลากรและเจ้าหน้าที่ ให้เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำโดยคณะกรรมการ การฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าวอาจดำเนินการได้ ทั้งในระดับชาติหรือระดับภาคส่วน โดยบุคลากรและเจ้าหน้าที่ที่อยู่ในแผนการรับมือภัยคุกคามทางไซเบอร์มีส่วนร่วมในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว

๒) เข้าร่วมฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ตามที่คณะกรรมการกำหนด อย่างน้อยปีละ ๑ ครั้ง

๓) ปฏิบัติตามคำขอของคณะกรรมการ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญเพื่อวัตถุประสงค์ในการวางแผน และดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้ รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์ และแผนการสื่อสารในภาวะวิกฤตที่กำหนดขึ้น

๔) จัดทำตารางรายการตรวจสอบ (Checklist) โดยรวบรวมรายชื่อผู้ที่อยู่ในแผนการรับมือภัยคุกคามทางไซเบอร์ และดำเนินการตรวจสอบว่าบุคคลดังกล่าวตามรายชื่อมีการเข้าร่วมฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์หรือไม่ รวมถึงจัดให้มีการรายงานให้ผู้บริหารรับทราบ

๒. กำหนดให้มีการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise) โดยดำเนินการอย่างน้อย ดังนี้

๑) กำหนดนโยบายในการฝึกซ้อม ประกอบด้วยเป้าหมาย ขอบเขตของการใช้งาน การบังคับใช้ผู้ที่เกี่ยวข้องในการฝึกซ้อมแผน เป็นต้น

๒) กำหนดบทบาทหน้าที่และความรับผิดชอบ (Identify Roles and Responsibilities) ในการดูแลโปรแกรมการฝึกซ้อม ซึ่งพิจารณากำหนดเป็นบุคคล หรือทีมที่รับผิดชอบในการวางแผนการฝึกซ้อม รวมถึงทำหน้าที่ในการประสานงานกิจกรรมต่าง ๆ และดูแลบำรุงรักษาแผนการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์

๓) กำหนดตารางการฝึกซ้อม โดยพิจารณาข้อกำหนด หรือกฎหมายที่เกี่ยวข้องในการระบุความถี่ในการทบทวนหรือทดสอบแผน รวมทั้งความถี่ในการฝึกซ้อม พร้อมทั้งดำเนินการภายในระยะเวลาที่กำหนด

๔) กำหนดให้มีการจัดทำเอกสารที่เกี่ยวข้องกับการวางแผนการฝึกซ้อม ประกอบด้วย

(๑) การกำหนดหัวข้อ และขอบเขตของกิจกรรม ระบุวัตถุประสงค์พื้นฐานตามหัวข้อและขอบเขตที่จะทำการฝึกซ้อม และกำหนดบุคลากรที่ควรเข้าร่วมกิจกรรม รวมถึงกำหนดให้ผู้ดูแลโปรแกรมการฝึกซ้อม ดำเนินการพิมพ์เอกสาร การเตรียมห้องฝึกซ้อม อาหาร และอุปกรณ์เครื่องเสียงหรือวิดีโอ

(๒) การจัดทำเอกสารในการดำเนินกิจกรรม เช่น คู่มือสำหรับผู้เข้าร่วมฝึก แผนการทดสอบ สคริปต์ เกณฑ์การประเมิน เป็นต้น

(๓) จัดทำรายงานผลของการฝึกอบรมหรือทดสอบตามกิจกรรมที่ได้ออกแบบ

(๔) ดำเนินการประเมินกิจกรรมที่จัดขึ้น หรืออุปสรรคที่เกิดขึ้นระหว่างการดำเนินการ รวมถึงรับฟังความคิดเห็นของผู้เข้าร่วมกิจกรรมที่จัดขึ้น เพื่อใช้ในการปรับปรุงแผนและปรับปรุงการดำเนินงาน

๕.๒ มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับกลาง

ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **"ระดับกลาง"** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศให้ดำเนินการตามข้อ ๕.๑ ตั้งแต่ข้อ (A) ถึง (I) และกำหนดมาตรการเพิ่มเติม ดังนี้

(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)

๑. กำหนดให้ผู้ตรวจสอบต้องได้รับการอนุมัติ หรือแต่งตั้งโดยผู้บริหารสูงสุด หรือผู้ที่ได้รับมอบอำนาจของหน่วยงานผู้ให้บริการขนส่งทางราง ก่อนดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

๒. กำหนดให้มีการพิจารณผู้ตรวจสอบตามเกณฑ์การพิจารณาข้างต้นอย่างน้อยดังนี้ ความเป็นอิสระและความสามารถของผู้ตรวจสอบ

๓. กำหนดให้ทีมตรวจสอบและผู้ตรวจสอบที่ได้รับการแต่งตั้ง ควรมีคุณลักษณะดังนี้

ก. ไม่อยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of Interest) โดยผลประโยชน์ทับซ้อนหมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจก่อให้เกิดการแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบจนทำให้การดำเนินการตรวจสอบไม่เป็นอิสระ หรือไม่มีตรงกับหลักฐานที่ปรากฏ

ข. มีความสามารถทางเทคนิคที่จำเป็นต่อการดำเนินการตรวจสอบ เช่น มีคุณวุฒิวิชาชีพใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง

๔. ในกรณีที่ไม่มีบุคคลที่มีคุณสมบัติตรงตามเกณฑ์ที่กำหนด สำหรับการเป็นผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ สามารถพิจารณาดำเนินการได้ ดังนี้

(๑) พิจารณาพัฒนาและอบรมบุคลากรภายใน (Internal Development) โดยพิจารณา ดังนี้

- จัดอบรมและพัฒนาทักษะบุคลากรภายในให้มีคุณสมบัติที่เหมาะสม เช่น การฝึกอบรมหลักสูตรเกี่ยวกับการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือการสอบใบรับรองวิชาชีพที่เกี่ยวข้อง เช่น CISA, ISO ๒๗๐๐๑ Lead Auditor, CISSP
- จัดทำแผนพัฒนาบุคลากรโดยให้พนักงานเข้ารับการฝึกอบรมเป็นระยะ หรือส่งพนักงานเข้าร่วมโครงการพี่เลี้ยง (Mentorship) จากผู้เชี่ยวชาญ

(๒) พิจารณาว่าจ้างผู้ตรวจสอบภายนอก (External Hiring) โดยพิจารณา ดังนี้

- ว่าจ้างผู้ตรวจสอบภายนอก (Third-Party Auditor) หรือสำนักงานตรวจสอบที่ได้รับการรับรอง ซึ่งมีคุณสมบัติตรงตามที่กำหนด
- ใช้บริการที่ปรึกษาด้านความมั่นคงปลอดภัยไซเบอร์ที่มีประสบการณ์ในการตรวจสอบ

(๓) พิจารณาใช้ทีมตรวจสอบภายในจากหน่วยงานอื่น (Internal Rotation or Collaboration) โดยพิจารณา ดังนี้

- หากหน่วยงานมีหลายแผนกอาจพิจารณาส่งบุคลากรจากแผนกอื่นที่ไม่มีผลประโยชน์ทับซ้อนมาทำหน้าที่ตรวจสอบ
- ขอความร่วมมือจากพันธมิตรที่สามารถส่งบุคลากรที่มีคุณสมบัติเข้ามาตรวจสอบได้

(๔) พิจารณากำหนดข้อยกเว้น และแผนระยะยาว (Exception Handling & Long-Term Plan) โดยพิจารณา ดังนี้

- ในกรณีที่ไม่สามารถหาได้จริงอาจดำเนินการกำหนดข้อยกเว้นชั่วคราว เช่น ใช้บุคลากรที่มีความรู้พื้นฐาน และให้มีการตรวจสอบเพิ่มเติมโดยผู้เชี่ยวชาญภายนอก

- จัดทำแผนระยะยาวในการพัฒนาทีมตรวจสอบภายใน เพื่อให้มีบุคลากรที่เพียงพอในอนาคต

๕. กำหนดให้มีการดำเนินการจัดทำขั้นตอนการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ หรือประยุกต์ใช้ขั้นตอนการตรวจสอบเดิมของหน่วยงานผู้ให้บริการขนส่งทางราง และเพิ่มเติมขั้นตอนที่เกี่ยวข้องสอดคล้องกับข้อกำหนดกฎหมายด้านความมั่นคงปลอดภัยไซเบอร์ โดยต้องมีขั้นตอนตั้งแต่การวางแผนการตรวจสอบ จัดเตรียมผู้ตรวจสอบ ประชุมเปิดตรวจสอบ ดำเนินการตรวจสอบ สรุปการตรวจสอบ ประชุมปิดการตรวจสอบ จัดทำรายงานและนำเสนอคณะกรรมการ หรือผู้บริหารที่เกี่ยวของหน่วยงานผู้ให้บริการขนส่งทางราง

๖. กำหนดขอบเขตการตรวจสอบ (Audit Scope) ต้องครอบคลุมรายละเอียดอย่างน้อยดังนี้

รายการ	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบ
กระบวนการหรือบริการที่ถูกตรวจสอบ (System or Service Audit)	(๑) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) (๒) บริการที่สำคัญของหน่วยงานตามผลการวิเคราะห์ในข้อ (๑) (๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใดๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงานและที่คณะกรรมการประกาศกำหนดกระบวนการหรือบริการที่ถูกตรวจสอบต้องครอบคลุมกระบวนการหรือบริการทั้งหมดที่ใช้ข้อมูลหรือระบบสารสนเทศที่มีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ในระดับกลางหรือระดับสูง ในกรณีที่หน่วยงานเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ตรวจสอบดำเนินการตรวจสอบบริการที่สำคัญตามมาตรา ๔๙ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ รวมถึงตรวจสอบกระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ อันเป็นการดำเนินการของหน่วยงานเพื่อให้ได้มาซึ่งบริการที่สำคัญดังกล่าวเพิ่มเติม
ระยะเวลาการตรวจสอบ (Audit Period)	อย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการดำเนินการตามข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายลำดับรอง นโยบายหรือคำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง (Compliance) เช่น - นโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบกับประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. ๒๕๖๕ – ๒๕๗๐)

รายการ	คำอธิบาย (Description)
	● ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะหน้าที่และความรับผิดชอบของศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศและภารกิจหรือให้บริการที่เกี่ยวข้อง พ.ศ. ๒๕๖๔ ● ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ ● ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๗. กำหนดให้มีการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานผู้ให้บริการขนส่งทางราง โดยดำเนินการ ดังนี้

๑) กำหนดให้มีการจัดทำแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และดำเนินการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ซึ่งอาจเป็นผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตของการตรวจสอบ อย่างน้อยประกอบด้วย

(๑) การวิเคราะห์ผลกระทบการดำเนินการตามภารกิจหน้าที่ (Business Impact Analysis: BIA) ประกอบด้วยข้อมูล ดังนี้

- ผลกระทบการดำเนินการตามภารกิจหน้าที่ (Business Impact Analysis: BIA) ที่ผู้มีส่วนได้ส่วนเสียพิจารณาร่วมกัน และได้รับอนุมัติ จากผู้บริหารสูงสุดของหน่วยงานผู้ให้บริการขนส่งทางราง หรือบุคคลหรือคณะกรรมการที่ได้รับมอบหมาย
- รายการกระบวนการทางธุรกิจ พร้อมระบุระดับผลกระทบ ระยะเวลาสูงสุดที่ยอมให้การดำเนินการตามหน้าที่ความรับผิดชอบหยุดชะงัก ระยะเวลาในการกู้คืนระบบ ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย และคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของระบบสารสนเทศที่เกี่ยวข้อง
- ทรัพยากรที่ต้องใช้ดำเนินการแก้ปัญหาการหยุดชะงัก
- บริการที่สำคัญที่ได้รับผลกระทบจากการดำเนินการตามภารกิจหน้าที่ (Business Impact Analysis: BIA) โดยบริการที่สำคัญต้องมีความเชื่อมโยงกับวัตถุประสงค์ และพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางราง

(๒) บริการที่สำคัญที่หน่วยงานผู้ให้บริการขนส่งทางราง เป็นเจ้าของและใช้บริการตามผลกระทบทางการดำเนินการตามภารกิจหน้าที่ (Business Impact Analysis: BIA) ซึ่งต้องมีการตรวจสอบตามนโยบาย การกำหนดหน้าที่รับผิดชอบ ฮาร์ดแวร์และซอฟต์แวร์ที่เกี่ยวข้อง แผนและผลของการปรับปรุงการดำเนินการตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ซึ่งประกอบด้วยรายการอย่างน้อย ดังนี้

- การจัดทำทะเบียนทรัพย์สิน และการจัดทำขอบเขตเครือข่ายของบริการที่สำคัญ
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ครอบคลุมบริการที่สำคัญ
- การประเมินช่องโหว่ และแผนการจัดการช่องโหว่ที่ครอบคลุมบริการที่สำคัญ
- การจัดการผู้ให้บริการภายนอกที่เกี่ยวข้องกับบริการที่สำคัญ

- การควบคุมการเข้าถึงบริการที่สำคัญ
- การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ที่ครอบคลุมถึงบริการที่สำคัญ
- การควบคุมเชื่อมต่อระยะไกล (Remote Connection) ที่เชื่อมต่อมายังบริการที่สำคัญ
- การควบคุมสื่อเก็บข้อมูลแบบถอดได้ (Removable Media) ที่เชื่อมต่อกับบริการที่สำคัญ
- การเผยแพร่ความรับผิดชอบของกลุ่มและบุคคลที่เกี่ยวข้องกับบริการที่สำคัญ
- การตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) ให้กับบริการที่สำคัญ
- การจัดแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan)

(๓) การปฏิบัติตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ และประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์นี้ และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มาตรฐานการปฏิบัติงาน และทิศทางที่คณะกรรมการประกาศกำหนด

ทั้งนี้ ผู้ตรวจสอบสามารถพิจารณาตรวจสอบตามความเสี่ยงได้จากการพิจารณาผลการตรวจสอบครั้งที่ผ่านมา การเกิดเหตุภัยคุกคามทางไซเบอร์ครั้งล่าสุดที่ส่งผลกระทบต่อหน่วยงานผู้ให้บริการขนส่งทางรางและข้อร้องเรียนของผู้ใช้บริการ ผลการประเมินช่องโหว่ หรือผลการทดสอบเจาะระบบ (Vulnerability Assessment or Penetration Testing Report) เหตุละเมิดข้อมูลส่วนบุคคลที่ผ่านมาการไม่ปฏิบัติการตามกฎหมายกฎระเบียบ (Noncompliance) ผลการประเมินความเสี่ยง

๒) กำหนดระดับผลการตรวจสอบ โดยแบ่งหมวดหมู่ของความสอดคล้องอย่างน้อยเป็น ๓ ระดับ ดังนี้

- ความไม่สอดคล้องที่สำคัญ (Major Non-Conformity: Major NC) หมายถึง การไม่ปฏิบัติตามข้อกำหนดกฎหมายข้อใดข้อหนึ่งหรือทั้งหมด และทำให้ระบบการจัดการล้มเหลว หรือมีความเสี่ยงสูง หรือมีเหตุนำมาซึ่งความเสียหายอย่างร้ายแรงต่อระบบ หรือผู้ตรวจสอบพบความไม่สอดคล้องย่อย (Minor Non-Conformity) หลาย ๆ จุดในข้อกำหนดเดียว ซึ่งเมื่อพิจารณาแล้วมีผลกระทบต่อระบบการจัดการโดยรวม
- ความไม่สอดคล้องย่อย (Minor Non-Conformity: Minor NC) หมายถึง การไม่ปฏิบัติตามข้อกำหนดกฎหมายบางส่วน มีการละเลยการดำเนินการเพียงบางส่วน หรือปฏิบัติไม่ครอบคลุม ซึ่งจะไม่ทำให้ระบบการจัดการล้มเหลว หรือไม่ได้เป็นเหตุที่จะนำมาซึ่งความเสียหายอย่างร้ายแรงต่อระบบ
- การดำเนินการสอดคล้อง (Conformity: C) หมายถึง หน่วยงานดำเนินการตามที่ประกาศกำหนดทั้งหมด

๓) ในกรณีที่ผู้ตรวจสอบพบข้อสังเกต (Observation: OBS) ที่อาจมีผลกระทบ โดยไม่ถือเป็นความไม่สอดคล้องย่อย แต่หากหน่วยงานปล่อยทิ้งไว้ หรือละเลยอาจนำไปสู่ความไม่สอดคล้องได้ (Potential Non-Conformity) จึงควรปรับปรุงตามข้อสังเกต เพื่อป้องกันความไม่สอดคล้องมิให้เกิดขึ้น หรือในกรณีที่ผู้ตรวจสอบอาจพบโอกาสในการปรับปรุง (Opportunity for Improvement: OFI) ซึ่งหมายความว่าข้อเสนอแนะ หรือโอกาสเพื่อการปรับปรุงในการปฏิบัติให้ดียิ่งขึ้น หรือเพื่อป้องกันความไม่สอดคล้อง

๔) กำหนดให้มีการดำเนินการสรุปผลการตรวจสอบ (Audit Conclusion) โดยผู้ตรวจสอบต้องให้ความเห็นและข้อสรุป โดยมีประเด็นอย่างน้อย ดังนี้

ก. ความเหมาะสมของการตอบสนองต่อผลการตรวจสอบจากฝ่ายบริหาร

ข. ประสิทธิผลและความเหมาะสมของมาตรการควบคุมของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และโอกาสในการปรับปรุง เพื่อรักษาความมั่นคงปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง

๕) การแก้ไขความไม่สอดคล้องที่ตรวจพบ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ให้หน่วยงานผู้ให้บริการขนส่งทางรางที่มีฐานะเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขในกรณีที่พบความไม่สอดคล้องที่สำคัญ (Major Non-Conformity) ไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ ขร. ภายในกำหนด ๓๐ (สามสิบ) วันนับจากวันที่การจัดทำรายงานการตรวจสอบเสร็จสิ้น โดยใช้แบบฟอร์มการร้องขอให้แก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR) ตามตัวอย่างในภาคผนวก และระบุรายละเอียดของแผนการดำเนินการแก้ไขอย่างน้อยดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานผู้ให้บริการขนส่งทางรางจะดำเนินการเพื่อจัดการกับความไม่สอดคล้องที่ตรวจพบ และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ (ก)

๖) ผู้ให้บริการขนส่งทางรางที่มีฐานะเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศต้องจัดส่งผลสรุปรายงานการตรวจสอบ ด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงาน ภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จ แต่ไม่เกินวันที่ ๓๑ มกราคมของปีถัดไป พร้อมทั้งส่งสำเนาให้กรมการขนส่งทางราง ซึ่งรูปแบบและรายละเอียดผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ ควรประกอบไปด้วยข้อมูลอย่างน้อย ดังนี้

- บทสรุปผู้บริหาร (Executive Summary)
- วัตถุประสงค์ (Purpose)
- เกณฑ์ในการตรวจสอบ (Audit Criteria)
- ขอบเขตการตรวจสอบ (Audit Scope)
- วันเวลาที่ตรวจสอบ
- ผู้ตรวจสอบ
- ผู้มีส่วนได้ส่วนเสีย (Stakeholders)
- วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)
- สิ่งที่พบจากการตรวจสอบ (Audit Finding)
- สรุปการตรวจสอบ (Audit Conclusion)

๗) การจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๕๔ วรรค ๒ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ของหน่วยงานผู้ให้บริการขนส่งทางรางจะต้องจัดส่งผลสรุปรายงานการดำเนินการ ประกอบด้วย การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ ขร. ภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ ซึ่งวันที่ดำเนินการแล้วเสร็จหมายถึง วันที่ผู้บริหารสูงสุดของหน่วยงานผู้ให้บริการขนส่งทางรางได้รับทราบรายงานการประเมินความเสี่ยง และรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเป็นลายลักษณ์อักษร นอกจากนี้ หน่วยงานผู้ให้บริการขนส่งทางรางอาจจัดให้มีการตรวจสอบตามปีงบประมาณ หรือตามปีปฏิทิน โดยให้จัดส่งผลสรุปรายงานการดำเนินการต่อสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และ ขร. ภายในสามสิบวันนับ

แต่วันที่ดำเนินการแล้วเสร็จ ทั้งนี้ ไม่เกินวันที่ ๓๐ มกราคม ของปีถัดไป ทั้งนี้ รายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต้องมีเนื้อหาครอบคลุมตามหัวข้อ ๖) ข้างต้น

๘) ในกรณีที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไขให้หน่วยงานผู้ให้บริการขนส่งทางราง ดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) กำหนดโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานผู้ให้บริการขนส่งทางรางที่มีฐานะเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ (ก)

๙) ในกรณีที่ กกม. หรือ ขร. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานผู้ให้บริการขนส่งทางรางที่มีฐานะเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงาน และ ขร. ภายในระยะเวลาที่กำหนด และเมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจากคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.) หรือ ขร. ผู้ให้บริการขนส่งทางรางที่มีฐานะเป็นหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้เสร็จสิ้น ภายในระยะเวลาตามที่ระบุไว้ในแผนดังกล่าว

(K) การเชื่อมต่อระยะไกล (Remote Connection)

๑. กำหนดให้มีการพิจารณาด้านความมั่นคงปลอดภัยของกลไกหรือเครื่องมือสำหรับการทำงานจากระยะไกลและการเข้าถึงจากระยะไกล (Security Considerations for the Telework and Remote Access Life Cycle) โดยแบ่งออกเป็น ๕ ขั้นตอน ดังนี้

๑) ขั้นตอนเริ่มต้น (Initiation)

กำหนดนโยบายความมั่นคงปลอดภัยของการทำงานจากระยะไกล (Telework Security Policy) เป็นส่วนหนึ่งในแผนการรักษาความมั่นคงปลอดภัยของระบบ (System Security Plan) รวมถึงควรครอบคลุมข้อกำหนด ดังนี้

๑.๑) กำหนดประเภทของกลไก หรือเครื่องมือสำหรับการเข้าถึงจากระยะไกลที่อนุญาตให้เข้าถึงได้จากระยะไกล เช่น การติดตั้งซอฟต์แวร์สำหรับการทำงานจากระยะไกล (Software Already Installed on Telework Device) ที่สามารถใช้สำหรับการเข้าถึงจากระยะไกล รวมถึงไม่ควรอนุญาตให้ใช้ประเภทการเข้าถึงจากระยะไกลที่ไม่สอดคล้องกับนโยบาย

๑.๒) ข้อจำกัดเกี่ยวกับอุปกรณ์ หรือโปรแกรมสำหรับการขอใช้บริการสำหรับการทำงานจากระยะไกลและระดับการเข้าถึงจากระยะไกล (Restrictions on Telework Client Devices and Remote Access Levels) โดยกำหนดประเภทของไคลเอนต์และระดับชั้นการเข้าถึงที่อนุญาตให้เข้าถึง โดยอิงตามระดับความเสี่ยงของทรัพยากรที่เกี่ยวข้อง ดังนี้

(๑) การกำหนดข้อจำกัดทั่วไปด้านความมั่นคงปลอดภัยในการทำงานจากระยะไกลที่มีควรพิจารณา ดังนี้

- การเข้าถึงข้อมูล หรือทรัพยากรที่มีความอ่อนไหวต้องมีการข้อกำหนดที่เข้มงวดมากขึ้น (Restrictive Requirement) เช่น การอนุญาตให้ใช้เฉพาะอุปกรณ์การทำงานจากระยะไกลที่ควบคุมโดยหน่วยงานผู้ให้บริการขนส่งทางรางเท่านั้น เข้าถึงข้อมูลที่มีความอ่อนไหว
- กำหนดค่าของอุปกรณ์สำหรับการทำงานจากระยะไกล เพื่อให้มั่นใจในความมั่นคงปลอดภัยในระดับต้น ในกรณีที่อุปกรณ์ที่ไม่ได้ควบคุมโดยหน่วยงานผู้ให้บริการขนส่งทางราง (Non-Organization-Controlled Device) สามารถใช้เครื่องแม่ข่ายสำหรับการเข้าถึงจากระยะไกล (Remote Access Server) เพื่อตรวจสอบอุปกรณ์ที่ร้องขอใช้บริการให้เป็นตามข้อกำหนดของหน่วยงานผู้ให้บริการขนส่งทางรางได้ รวมถึงสร้างความตระหนักถึงความรับผิดชอบของผู้ร้องขอเข้าถึงจากระยะไกลให้มีความระมัดระวัง และคำนึงถึงการรักษาความมั่นคงปลอดภัยของอุปกรณ์ตลอดเวลา

ทั้งนี้ อุปกรณ์ที่ควบคุมโดยบุคคล หรือผู้ให้บริการภายนอก ต้องมีข้อกำหนดบังคับให้บุคคล หรือผู้ให้บริการภายนอกปฏิบัติตามนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง ผ่านข้อกำหนดในสัญญา

- ข้อจำกัดทางเทคนิค (Technical Limitation) ในการทำงานจากระยะไกลอาจจำเป็นต้องใช้อุปกรณ์เฉพาะเครื่องแม่ข่ายที่ให้บริการการเข้าถึงจากระยะไกลบางประเภท ซึ่งสามารถรองรับการเชื่อมต่อผ่านโปรแกรมไคลเอนต์เฉพาะ (Custom Client) เท่านั้น

- การกำหนดให้ต้องปฏิบัติตามข้อกำหนดเกี่ยวกับการทำงานจากระยะไกล ให้เป็นไปตามนโยบายการเข้าถึงข้อมูลจากระยะไกล และนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง

(๒) การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในการทำงานจากระยะไกลที่มีความเสี่ยงสูงเป็นพิเศษ ควรพิจารณา ดังนี้

- อนุญาตการทำงานจากระยะไกลที่มีความเสี่ยงสูงจากอุปกรณ์ระยะไกลที่หน่วยงานผู้ให้บริการขนส่งทางราง จัดหาให้เป็นการเฉพาะเท่านั้นและมีมาตรการความมั่นคงปลอดภัย (Organization-Issued and Secured Telework Device)
- พิจารณาให้ใช้การยืนยันตัวตนด้วยหลายปัจจัย (Multi-factor Authentication) สำหรับการเข้าถึงอุปกรณ์การทำงานจากระยะไกล และการเข้าถึงจากระยะไกล
- กำหนดให้มีการเข้ารหัสที่เก็บข้อมูล (Use Storage Encryption) บนอุปกรณ์การทำงานจากระยะไกล เพื่อปกป้องข้อมูลที่มีความอ่อนไหวทั้งหมด เช่น กำหนดให้เข้ารหัสดิสก์เต็มรูปแบบ เพื่อลดความเสี่ยงจากผู้โจมตีที่ได้รับสิทธิเข้าถึงทางกายภาพ รวมกับการเข้ารหัสดิสก์เสมือน (Virtual Disk) หรือการเข้ารหัสไฟล์/โฟลเดอร์ และกำหนดให้มีการเข้ารหัสข้อมูลที่เกิดจากการทำงานจากระยะไกล (Telework Data) ที่อยู่ในสื่อเก็บข้อมูลแบบถอดได้ (Removable Media)
- โอนย้ายทรัพยากรที่มีความเสี่ยงสูงไปยังเครื่องแม่ข่ายที่มีความสามารถในการปกป้องทรัพยากรดังกล่าว (Migrate High-Risk Resources to Servers that Assume Responsibility for Protecting Them) เช่น กำหนดให้ผู้ปฏิบัติงานจากระยะไกลต้องเชื่อมต่อกับเครื่องแม่ข่ายเทอร์มินัลที่เก็บข้อมูลสำคัญที่ผู้ปฏิบัติงานจากระยะไกลจำเป็นต้องใช้
- จัดเก็บและอนุญาตเข้าถึงข้อมูลที่จำเป็นเท่านั้น (Store and Access Only the Minimum Data Necessary) ในกรณีที่ให้บุคลากรยืมอุปกรณ์ ต้องดำเนินการล้าง (Wipe) ข้อมูลทั้งหมดก่อนและหลังการทำงานจากระยะไกลที่มีความเสี่ยงสูง เช่น บุคลากรทำงานขณะการเดินทางไปต่างจังหวัด หรือต่างประเทศ และใส่เฉพาะข้อมูลและแอปพลิเคชันที่ได้รับอนุญาต และจำเป็นสำหรับการทำงานจากระยะไกลเท่านั้นในอุปกรณ์ และไม่อนุญาตให้เชื่อมต่อกับเครือข่ายภายในของหน่วยงานผู้ให้บริการขนส่งทางราง
- ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (System Command) เช่น คำสั่ง Start, Stop, Restart/Reboot, Shutdown, Disable/Enable, Rollback, Upgrade, Reset, Factory Reset ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างชัดเจน เนื่องจากมีความจำเป็นต่อการดำเนินงานภารกิจ และหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง
- จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ เช่น การเปิดบริการ หรือฟังก์ชันบนเครื่องแม่ข่ายให้แก่การทำงานจากระยะไกลเฉพาะบริการ หรือฟังก์ชันที่จำเป็นเท่านั้น รวมถึงการกำหนดสิทธิการเข้าถึงข้อมูล เช่น ไม่ให้ส่งไฟล์ไปยังเครื่องแม่ข่าย ไม่ให้เข้าถึงข้อมูล อ่านข้อมูลได้อย่างเดียว หรืออ่านและเขียนได้ รวมถึงตั้งค่า Firewall เพื่ออนุญาตการเชื่อมต่อกับบริการหรือฟังก์ชันบนเครื่องแม่ข่ายในกรณีที่จำเป็นเท่านั้น

ทั้งนี้ ในกรณีที่อยู่ในสถานการณ์ที่มีความเสี่ยงสูงของหน่วยงานผู้ให้บริการขนส่งทางราง อาจพิจารณาห้ามการทำงานจากระยะไกล และห้ามการเข้าถึงจากระยะไกล โดยเฉพาะที่ต้องเข้าถึงข้อมูลบางประเภท เช่น ข้อมูลที่ระบุตัวตนได้ และมีความอ่อนไหว เป็นต้น

(๓) การกำหนดแนวทางการกำหนดระดับการเข้าถึง (Access Tier) จากระยะไกลให้แก่อุปกรณ์ไคลเอนต์ สามารถพิจารณาแบ่งได้เป็น ๗ ประเภท ดังนี้

- อุปกรณ์ที่หน่วยงานผู้ให้บริการขนส่งทางรางจัดหา (Furnished Equipment: FE) และอยู่ในสำนักงาน
- อุปกรณ์ที่หน่วยงานผู้ให้บริการขนส่งทางราง จัดหาสำหรับการทำงานจากระยะไกล (FE in Telework)
- อุปกรณ์ส่วนตัว BYOD ที่ผู้ใช้นำมาใช้งานในสำนักงานของหน่วยงานผู้ให้บริการขนส่งทางราง (BYOD in office)
- อุปกรณ์ส่วนตัว BYOD ที่ผู้ใช้นำมาใช้ทำงานจากระยะไกล (BYOD in Telework)
- อุปกรณ์ของผู้ให้บริการภายนอก, พันธมิตรทางธุรกิจ (Contractor, Partner, Vendor in Office)
- อุปกรณ์ของผู้ให้บริการภายนอก, พันธมิตรทางธุรกิจ ที่นำมาใช้เข้าถึงข้อมูลหรือบริการของหน่วยงานจากระยะไกล (Contractor, Partner, Vendor in Telework)
- อุปกรณ์อื่น ๆ ของบุคคลที่สาม เช่น อุปกรณ์ของอินเทอร์เน็ตคาเฟ่ หรือโรงแรม

ทั้งนี้ ต้องกำหนดให้มีการเฝ้าระวังความมั่นคงปลอดภัยของเครือข่ายส่วนบุคคลไร้สาย (Wireless Personal Area Networks: WPAN) ซึ่งเป็นอุปกรณ์เครือข่ายไร้สายขนาดเล็กที่ไม่ใช่โครงสร้างพื้นฐานสำหรับการทำงาน เช่น การใช้แป้นพิมพ์ หรือเมาส์ไร้สายกับคอมพิวเตอร์ การพิมพ์แบบไร้สาย การเชื่อมต่อสมาร์โฟนกับคอมพิวเตอร์ และการเชื่อมต่อชุดหูฟัง หรือหูฟังไร้สายกับสมาร์ทโฟน โดยต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลควรปิดใช้งานเทคโนโลยี WPAN เมื่อไม่ได้ใช้งาน เพื่อป้องกันการใช้งานในทางที่ผิด โดยไม่ได้รับอนุญาต

๒) ขั้นตอนการพัฒนา (Development)

การพัฒนากลไกหรือเครื่องมือ เพื่อรองรับการทำงานจากระยะไกลควรมีการพิจารณาด้านความมั่นคงปลอดภัยทางเทคนิคที่สำคัญ อย่างน้อยดังนี้

๒.๑) สถาปัตยกรรม (Architecture) ดำเนินการพิจารณาการออกแบบสถาปัตยกรรม รวมถึงการจัดวางเครื่องแม่ข่ายการเข้าถึงจากระยะไกล (Placement of the Remote Access Server) การเลือกซอฟต์แวร์ไคลเอนต์การเข้าถึงจากระยะไกล (Remote Access Client Software) และการออกแบบเซ็กเมนต์เครือข่ายของหน่วยงานผู้ให้บริการขนส่งทางราง (Organization Network Segment) เฉพาะสำหรับการเชื่อมต่อกับอุปกรณ์ไคลเอนต์ที่ไม่ได้ควบคุมโดยหน่วยงานผู้ให้บริการขนส่งทางราง (Non-Organization-Controlled Client Device) ซึ่งอาจพิจารณาออกแบบให้มีเซ็กเมนต์เพียงเซ็กเมนต์เดียว หรือหลายเซ็กเมนต์ตามความเหมาะสม และวัตถุประสงค์ของหน่วยงานผู้ให้บริการขนส่งทางราง

๒.๒) การพิสูจน์ตัวตน (Authentication) ดำเนินการคัดเลือกเทคโนโลยีหรือวิธีการพิสูจน์ตัวตนการเข้าถึงจากระยะไกล และกำหนดวิธีการใช้ส่วนประกอบของเทคโนโลยี การใช้งานไคลเอนต์ และการใช้งานเครื่องแม่ข่าย รวมถึงขั้นตอนสำหรับการเริ่มใช้งานและการรีเซ็ตค่าการใช้งานของเทคโนโลยี (Issuing and Resetting Authenticator) และขั้นตอนการจัดเตรียมเทคโนโลยีให้กับผู้ใช้และอุปกรณ์ของผู้ใช้งาน

๒.๓) พิจารณาการเข้ารหัสลับ (Cryptography) รวมถึงการเลือกอัลกอริทึมสำหรับการเข้ารหัส (Encryption) การป้องกันความถูกต้องครบถ้วน (Integrity Protection) ของการสื่อสารการเข้าถึงจากระยะไกล และการตั้งค่าความแข็งแกร่งของคีย์สำหรับอัลกอริทึมที่รองรับความยาวของคีย์หลายรายการ (Support Multiple Key Length)

๒.๔) กำหนดให้มีการควบคุมการเข้าถึง (Access Control) โดยการกำหนดว่าการเข้าถึงจากระยะไกลประเภทไหนที่อนุญาตให้เข้าถึง หรือปฏิเสธการเข้าถึง

๒.๕) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของอุปกรณ์ปลายทาง (Endpoint Security) สำหรับการทำงานจากระยะไกล และอุปกรณ์ไคลเอนต์ รวมถึงพิจารณาถึงการจัดการหรือการตอบสนองเหตุภัยคุกคามทางไซเบอร์ (Incident) ที่เกี่ยวข้องกับการทำงานจากระยะไกลและการเข้าถึงจากระยะไกล และระบุไว้ในแผนความมั่นคงปลอดภัยของระบบให้ชัดเจน

๓) ขั้นตอนการนำไปใช้งาน (Implementation)

๓.๑) การเชื่อมต่อ (Connectivity) โดยจัดให้มีการตรวจสอบให้มั่นใจว่าผู้ทำงานจากระยะไกลสามารถเชื่อมต่อกับทรัพยากรทั้งหมดที่ได้รับอนุญาต และไม่สามารถเชื่อมต่อกับทรัพยากรอื่นได้และเข้าถึงข้อมูล และระบบตามสิทธิ์ที่ได้รับ

๓.๒) การป้องกัน (Protection) โดยจัดให้มีการตรวจสอบให้มั่นใจว่าข้อมูลที่ถูกส่งในเครือข่ายจะได้รับการป้องกันสอดคล้องกับข้อกำหนดของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งรวมถึงข้อมูลที่ถูกส่งระหว่างอุปกรณ์ไคลเอนต์ สำหรับการทำงานจากระยะไกล (Telework Client Device) และเครื่องแม่ข่ายการเข้าถึงจากระยะไกล และข้อมูลที่ถูกส่งระหว่างเครื่องแม่ข่าย และทรัพยากรภายในหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การเฝ้าติดตามการรับส่งข้อมูลเครือข่าย (Monitoring Network Traffic) หรือการตรวจสอบข้อมูลจราจรการรับส่งข้อมูล (Checking Traffic Log)

๓.๓) การพิสูจน์ตัวตน (Authentication) โดยกำหนดให้มีการบังคับใช้นโยบายการพิสูจน์ตัวตนทุกครั้งที่มีการเชื่อมต่อ และจัดให้มีการตรวจสอบให้มั่นใจว่าการพิสูจน์ตัวตนสามารถป้องกันการถูกโจมตีหรือถูกละเมิด เพื่อลดความเสี่ยงการเข้าถึงทรัพยากรภายในของหน่วยงานผู้ให้บริการขนส่งทางราง

๓.๔) แอปพลิเคชัน (Application) สำหรับการทำงานจากระยะไกลที่นำมาใช้งานต้องไม่ขัดขวางการทำงานของอุปกรณ์ไคลเอนต์สำหรับการทำงานจากระยะไกล เช่น ไคลเอนต์ VPN ที่ต้องทำงานร่วมกับไฟร์วอลล์บนโฮสต์ (Host-Based Firewall)

๓.๕) การจัดการ (Management) กำหนดให้ผู้ดูแลระบบต้องกำหนดค่าความมั่นคงปลอดภัย และการทำงานของแอปพลิเคชัน (Application) สำหรับการทำงานจากระยะไกลให้มีประสิทธิภาพ รวมถึงส่วนประกอบอื่น ๆ เช่น เครื่องแม่ข่ายการเข้าถึงจากระยะไกล การพิสูจน์ตัวตน (Authentication

Services) และซอฟต์แวร์ไคลเอนต์ การปรับใช้และการกำหนดค่า เช่น สามารถกำหนดค่าไคลเอนต์อัตโนมัติเต็มรูปแบบ (Fully Automated Client Configuration) ได้แทนการกำหนดค่าไคลเอนต์แต่ละเครื่องด้วยตัวผู้ดูแลระบบเอง

๓.๖) การเก็บข้อมูลจราจร (Logging) จัดให้มีการเก็บข้อมูลจราจรเหตุการณ์ด้านความมั่นคงปลอดภัย (Security Event) ตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงพิจารณาให้มีการจัดเก็บข้อมูลอื่น ๆ เช่น การบันทึกการใช้งานแอปพลิเคชันแต่ละแอปพลิเคชัน

๓.๗) การตรวจสอบประสิทธิภาพ (Performance) โดยจัดให้มีการตรวจสอบประสิทธิภาพและความเพียงพอสำหรับปริมาณการใช้งานปกติ และสำหรับปริมาณการใช้งานสูงสุด รวมถึงพิจารณาถึงประสิทธิภาพของอุปกรณ์ที่เป็นตัวกลาง เช่น เราเตอร์และไฟร์วอลล์ และส่วนประกอบต่าง ๆ โดยเฉพาะในช่วงการอัปเดตซอฟต์แวร์ขนาดใหญ่ ผ่านการทำงานและการเข้าถึงจากระยะไกล ซึ่งการดำเนินการทดสอบประสิทธิภาพ ควรพิจารณาทดสอบโดยการใช้ปริมาณงานที่สร้างขึ้นไว้เป็นต้นแบบ (Load of a Prototype) โดยใช้ตัวสร้างข้อมูลในเครือข่าย (Traffic) จำลองบนเครือข่ายทดสอบ (Live Test Network) เพื่อเลียนแบบลักษณะที่แท้จริงของทราฟฟิกที่คาดหวัง และใกล้เคียงการใช้งานจริงที่สุด ซึ่งการทดสอบนี้ ต้องรวมปริมาณงานของแอปพลิเคชันต่าง ๆ ที่จะถูกใช้ร่วมกับการทำงานและการเข้าถึงจากระยะไกล

๓.๘) ความมั่นคงปลอดภัยของการดำเนินการ (Security of the Implementation) ต้องจัดให้มีการอัปเดตด้วยแพตช์ล่าสุด และกำหนดค่าตามแนวทางปฏิบัติด้านความมั่นคงปลอดภัย รวมถึงการตรวจสอบค่าเริ่มต้น (Default Setting) อย่างละเอียดสำหรับการตั้งค่าการเข้าถึงจากระยะไกลแต่ละรายการ และแก้ไขการตั้งค่าตามความจำเป็น เพื่อรองรับข้อกำหนดด้านความมั่นคงปลอดภัย และจัดให้มีการประเมินช่องโหว่ของส่วนประกอบของระบบสำหรับการเข้าถึงจากระยะไกล

๔) ขั้นตอนการดำเนินงานและการบำรุงรักษา (Operation and Maintenance) เป็นกระบวนการดำเนินงาน (Operational Processes) เกี่ยวกับการดูแลระบบการทำงานหรือการเข้าถึงจากระยะไกลให้มีความมั่นคงปลอดภัย ๆ อย่างน้อยทุก ๖ เดือน หรือทุก ๑ ปี ตามระดับความเสี่ยงของการอนุญาตให้มีการทำงานระยะไกล โดยดำเนินการ ดังนี้

๔.๑) ดำเนินการตรวจสอบเจ้าของผลิตภัณฑ์เกี่ยวกับการอัปเดตโปรแกรม ในกรณีที่มีการประกาศการอัปเดตโปรแกรมรุ่นล่าสุดแล้วให้หน่วยงานผู้ให้บริการขนส่งทางราง หรือผู้ดูแลผลิตภัณฑ์ดำเนินการจัดหา (Acquiring) ทดสอบ (Testing) และใช้งานโปรแกรมรุ่นล่าสุด (Deploying)

๔.๒) ตรวจสอบให้แน่ใจว่าองค์ประกอบโครงสร้างพื้นฐานการเข้าถึงจากระยะไกลแต่ละรายการ เช่น เครื่องแม่ข่าย เกตเวย์ เครื่องแม่ข่ายการพิสูจน์ตัวตน ฯลฯ มีการตั้งเวลาที่ถูกต้องเพื่อให้การประทับเวลา (Timestamp) ตรงกับระบบตั้งค่าเวลา

๔.๓) ดำเนินการตรวจสอบ และปรับเปลี่ยนการตั้งค่าการควบคุมการเข้าถึง (Access Control Setting) ตามความจำเป็นตามเหตุการณ์ต่าง ๆ เช่น มีการเปลี่ยนแปลงนโยบาย มีการเปลี่ยนแปลงเทคโนโลยี มีข้อแนะนำหรือการสำรวจช่องโหว่ (Gap) จากการตรวจสอบ (Audit Findings) หรือมีความต้องการด้านความมั่นคงปลอดภัยใหม่

๔.๔) ตรวจจับและบันทึกความผิดปกติที่ตรวจพบภายในโครงสร้างพื้นฐานสำหรับการทำงาน หรือเข้าถึงจากระยะไกล ในกรณีที่พบความผิดปกติต้องนำรายงานไปยังผู้ดูแลระบบ และผู้ดูแลระบบอื่นที่เกี่ยวข้อง และดำเนินการประเมินการดำเนินงานเป็นระยะ ๆ อย่างน้อยทุก ๖ เดือน หรือทุก ๑ ปี ตามระดับความเสี่ยงของการอนุญาตให้มีการทำงานระยะไกล เช่น การประเมินอาจเป็นแบบแพสซิฟ (Passive) เช่น การตรวจสอบบันทึก หรือการประเมินแบบแอ็กทิฟ (Active) เช่น การสแกนช่องโหว่และการทดสอบเจาะระบบ เป็นต้น

๕) ขั้นตอนการกำจัด (Disposal) กำหนดให้มีการลบข้อมูลที่มีความอ่อนไหวออกจากอุปกรณ์ไคลเอนต์หรือเครื่องแม่ข่ายสำหรับการเข้าถึงจากระยะไกลก่อนที่จะดำเนินการกำจัดหรือเลิกใช้อุปกรณ์ เช่น สัญญาเช่าเครื่องแม่ข่ายหมดอายุ หรือเมื่อเครื่องคอมพิวเตอร์ที่ล้าสมัยกำลังถูกรีไซเคิล เป็นต้น รวมถึงกำหนดให้มีการล้าง (Wipe) ข้อมูลออกจากอุปกรณ์ที่ถูกยืมโดยผู้ปฏิบัติงานจากระยะไกล โดยเฉพาะอย่างยิ่งเป็นการยืมสำหรับการเดินทาง และตรวจสอบให้แน่ใจว่าการล้างข้อมูลได้ดำเนินการล้างข้อมูลทุกจุดที่สามารถจัดเก็บข้อมูลได้ เช่น ซอฟต์แวร์ที่ทำงานภายใต้ Microsoft Windows มักจะเก็บข้อมูลที่อาจมีความสำคัญไว้ในรีจิสทรีของ Windows ในกรณีที่มีการจัดจ้างให้ผู้ให้บริการภายนอกดำเนินการล้างข้อมูลต้องกำหนดให้มีการตรวจสอบการดำเนินการของผู้ให้บริการภายนอกหลังดำเนินการแล้วเสร็จ และจัดทำเอกสารการตรวจสอบไว้เป็นหลักฐาน

(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการบริหารจัดการสื่อบันทึกข้อมูลที่ถอดแยกได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แล็ปท็อป กับบริการที่สำคัญ หรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง โดยใช้มาตรการอย่างน้อย ดังนี้

๑) สื่อบันทึกข้อมูลทุกประเภท และทุกชนิด ต้องได้รับอนุญาตก่อนนำมาเชื่อมต่อทั้งหมด และห้ามนำสื่อบันทึกข้อมูลส่วนตัวมาเชื่อมต่อกับอุปกรณ์องค์กรโดยไม่ได้รับอนุญาต

๒) กำหนดให้มีการลงทะเบียนสื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media Register) ก่อนนำไปใช้งาน รวมถึงกำหนดให้มีการบำรุงรักษา และการตรวจสอบการลงทะเบียนของสื่อเก็บข้อมูล แบบถอดได้เป็นประจำ อย่างน้อยทุก ๓ เดือน หรือ ๖ เดือนตามระดับความเสี่ยงที่นำไปใช้งานกับระบบหรือข้อมูล พร้อมทั้งจัดทำบันทึกการติดตาม และตรวจสอบปรับปรุงทะเบียนทรัพย์สินสำหรับสื่อเก็บข้อมูลแบบถอดได้ที่ได้รับอนุญาต

๓) ดำเนินการติดฉลากให้แก่สื่อเก็บข้อมูลแบบถอดได้ ยกเว้นสื่อเก็บข้อมูลแบบถอดได้ที่ติดตั้งถาวรภายในอุปกรณ์ ICT เพื่อให้ทราบถึงระดับความอ่อนไหว หรือชั้นความลับของข้อมูล รวมถึงช่วยให้มั่นใจว่ามีการใช้มาตรการที่เหมาะสมในการจัดเก็บ การจัดการ และการนำไปใช้งาน โดยอาจจะดำเนินการติดป้ายสีเพื่อระบุความสำคัญแทนการติดเป็นข้อความ รวมถึงจัดการฝึกอบรมการใช้งานให้แก่บุคลากรอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔) กำหนดให้มีการใช้สื่อเก็บข้อมูลแบบถอดได้เฉพาะกับระบบที่ได้รับอนุญาตให้ประมวลผล จัดเก็บหรือส่งข้อมูล โดยใช้สื่อเก็บข้อมูลแบบถอดได้เท่านั้น

๕) กำหนดให้มีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลแบบถอดได้ รวมถึงหากเป็นในระดับชั้นความลับ ลับมากที่สุด ลับมาก ต้องพิจารณาดำเนินการอย่างน้อยดังนี้ เข้ารหัส (Encryption) ระบุผู้รับผิดชอบ (ผู้ถือครอง) และบันทึก ในทะเบียนสื่อบันทึกข้อมูล รวมถึงกำหนดให้มีการทบทวนการกำหนดระดับชั้นความลับให้กับสื่อเก็บข้อมูลแบบถอดได้อย่างสม่ำเสมอ

๒. กำหนดให้มีมาตรการในการปกป้องข้อมูล และความเป็นส่วนตัวให้กับข้อมูลที่จัดเก็บบนสื่อบันทึกข้อมูลที่ถอดได้ ดังนี้

๑) ติดตั้งโปรแกรมป้องกันไวรัสที่สามารถสแกนหาไวรัสและลบไวรัสออกจากสื่อเก็บข้อมูลแบบถอดได้ หากมีการใช้สื่อใหม่ เช่น แฟลชไดรฟ์ USB หรือการ์ดหน่วยความจำ รวมถึงกำหนดให้ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมด ไม่มีมัลแวร์ (Malware) ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญหรือระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

๒) ปิดการใช้งานคุณสมบัติการเล่นอัตโนมัติและการเปิดใช้งานอัตโนมัติของคอมพิวเตอร์ (Disable Computer's Autoplay and Auto-Run Features) ก่อนที่จะเชื่อมต่อสื่อแบบถอดได้เข้ากับคอมพิวเตอร์ เพื่อป้องกันคอมพิวเตอร์จากการเปิดโฟลเดอร์ที่มีไวรัส โดยอัตโนมัติ

๓) จัดให้มีการใส่รหัสผ่านป้องกันอุปกรณ์สื่อเก็บข้อมูลแบบถอดได้ (Password Protect Removable Storage Media Devices) เพื่อควบคุมการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต รวมถึงตรวจสอบให้แน่ใจว่าการใช้รหัสผ่านมีความรัดกุม และป้องกันรหัสผ่านไม่ให้รั่วไหล

๔) ไม่ทิ้งสื่อบันทึกข้อมูลไว้โดยไม่มีบุคคลดูแล หรือถูกเก็บในที่ที่อาจถูกขโมยได้ง่าย เช่น โต๊ะทำงาน รวมถึงทำให้มั่นใจว่าการเข้าถึงสื่อบันทึกข้อมูลต้องใช้รหัสผ่านเสมอ

๕) กำหนดให้มีการเข้ารหัสข้อมูล หากมีข้อมูลที่อ่อนไหวหรือความลับในสื่อเก็บข้อมูลแบบถอดได้ เช่น ข้อมูลที่มีชั้นความลับในระดับลับมากหรือระดับลับที่สุดของหน่วยงานผู้ให้บริการขนส่งทางราง หรือข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ เช่น ข้อมูลการตั้งค่าระบบ เป็นต้น

๖) กำหนดเจ้าของสื่อเก็บข้อมูลแบบถอดได้ให้ชัดเจน เช่น ชื่อบุคคลที่รับผิดชอบ ชื่อหน่วยงานที่รับผิดชอบ และห้ามบุคลากรที่ไม่เกี่ยวข้องใช้สื่อเก็บข้อมูลแบบถอดได้ และหากสื่อเก็บข้อมูลไม่สามารถระบุเจ้าของหรือบุคลากรที่รับผิดชอบได้ ไม่อนุญาตให้ใช้งานสื่อบันทึกนั้น

๗) ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๘) กำหนดให้มีการทำลายสื่อบันทึกข้อมูล โดยพิจารณาดำเนินการดังนี้

(๑) ดำเนินการประเมินระดับชั้นความลับของข้อมูลก่อนทำลาย

(๒) กำหนดวิธีการทำลายข้อมูลให้สอดคล้องกับระดับชั้นความลับของข้อมูลในแต่ละลำดับชั้น พร้อมทั้งจัดให้มีหลักฐานการทำลายข้อมูล พร้อมทั้งกำหนดให้มีการลงนามโดยผู้มีอำนาจอนุมัติทำลายข้อมูล

(๓) ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกทำลายสื่อบันทึก ควรพิจารณาจัดจ้างผู้ให้บริการที่ได้รับการรับรอง พร้อมทั้งกำหนดให้มีการกำหนดรูปแบบการทำลาย พร้อมวิธีการทำลายให้ฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายก่อนดำเนินการทำลาย

๙) กำหนดให้ใช้สื่อเก็บข้อมูลแบบถอดได้แบบเขียนครั้งเดียว (Write-once Media) ในการถ่ายโอนข้อมูลระหว่างระบบที่อยู่บนโดเมนความปลอดภัยที่แตกต่างกัน และกำหนดมาตรการป้องกันข้อมูลรั่วไหล หรือเข้าถึงโดยไม่ได้รับอนุญาตอย่างเหมาะสม เช่น การใช้คอมแพคดิสก์ที่ไม่สามารถเขียนซ้ำได้ (Non-Rewritable Compact Discs) เป็นต้น ในกรณีที่ไม่สามารถใช้สื่อเก็บข้อมูลแบบถอดได้บันทึกแบบครั้งเดียวในการถ่ายโอนข้อมูลระหว่างระบบ ควรตรวจสอบให้แน่ใจว่าระบบปลายทางมีกลไกการเข้าถึงแบบอ่านอย่างเดียวได้ (Read-only Access) เช่น ผ่านอุปกรณ์แบบอ่านอย่างเดียวหรือตัวบล็อกการเขียนด้วยฮาร์ดแวร์ (Read-only Device or Hardware Write-blocker) และควรกำหนดให้มีการลบ (Sanitize) ข้อมูลทั้งหมดจากสื่อบันทึกข้อมูลหลังการถ่ายโอนข้อมูลแต่ละครั้ง

๑๐) กำหนดบุคลากรที่มีหน้าที่ตรวจสอบการเชื่อมต่อให้ชัดเจน โดยมีหน้าที่ อย่างน้อยดังนี้

(๑) ทบทวนและตอบสนองต่อข้อมูลที่แจ้งเกี่ยวกับการเชื่อมต่อที่ผิดปกติ เช่น ข้อมูลการแจ้งเตือนจากระบบปฏิบัติการ จาก Endpoint Detection and Response (EDR) หรือจาก Security Information and Event Management (SIEM) ภายในระยะเวลาที่เหมาะสม

(๒) ดำเนินการปรับปรุง (Update) ซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ตามนโยบายความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานผู้ให้บริการขนส่งทางราง

(๓) จัดทำรายงานการตรวจสอบการเชื่อมต่อสื่อบันทึกข้อมูล เพื่อให้ผู้บังคับบัญชาทบทวนหลังจากที่การดำเนินการตรวจสอบแล้วเสร็จภายใน ๑ สัปดาห์

๑๑) กำหนดให้มีการตรวจสอบการควบคุมการเชื่อมต่อของสื่อบันทึกข้อมูลแบบถอดได้กับบริการที่สำคัญ เพื่อให้แน่ใจว่ามีการดำเนินการอย่างน้อย ดังนี้

ก) ในกรณีที่สามารถปิดใช้งานได้ ให้ปิดใช้งานพอร์ตสำหรับการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และเปิดใช้งานก็ต่อเมื่อจำเป็นเท่านั้น

(ข) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตและกำหนดไว้ในนโยบาย หรือแนวปฏิบัติของหน่วยงานเท่านั้น

(ค) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ทั้งหมดไม่มีไวรัส หรือมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(ง) กำหนดให้ผู้ปฏิบัติงานทำการตรวจสอบ โดยเปรียบเทียบการตั้งค่าการใช้งานพอร์ตและการอนุญาตให้ใช้สื่อบันทึกข้อมูลตามมาตรการข้อ (ก) และ (ค)

(จ) มีซอฟต์แวร์ป้องกันไวรัสและมัลแวร์ พร้อมตั้งค่าให้ทำงานทุกครั้งที่มีการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ กับบริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. ในกรณีที่มีการขนย้ายสื่อบันทึกข้อมูล ควรพิจารณาดำเนินการดังนี้

(๑) จัดให้มีบรรจุภัณฑ์ที่มั่นคงและปิดผนึก

(๒) กำหนดให้ใช้วิธีการเคลื่อนย้ายที่สามารถตรวจสอบได้ เช่น มีหลักฐานการรับและหลักฐานการส่งสื่อบันทึกข้อมูลโดยการลงนามรับและส่ง เป็นต้น

(๓) ข้อมูลที่อยู่ในระดับชั้นความลับในชั้น “ลับมากที่สุด” “ลับมาก” ควรดำเนินการขนย้ายโดยผู้ปฏิบัติงานที่ได้รับมอบหมายโดยเฉพาะ พร้อมทั้งบันทึกเส้นทางการเคลื่อนย้าย

(๔) ห้ามทิ้งสื่อบันทึกข้อมูลไว้ โดยไม่มีผู้ดูแลในพื้นที่สาธารณะหรือยานพาหนะ

๕.๓ มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง

ในกรณีที่ข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ใน **"ระดับสูง"** ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศให้ดำเนินการตามข้อ ๕.๑ และ ข้อ ๕.๒ ตั้งแต่ข้อ (A) ถึง (L) รวมถึงกำหนดมาตรการเพิ่มเติม ดังนี้

(M) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการจัดทำขั้นตอนการประเมินช่องโหว่ของระบบ ประกอบด้วยอย่างน้อย ๖ ขั้นตอน ดังนี้

(๑) การกำหนดขอบเขต (Scoping) โดยขอบเขตการประเมินต้องได้รับความเห็นชอบจากผู้ดำเนินการประเมินและผู้รับการประเมิน โดยจะต้องระบุรายละเอียดเกี่ยวกับทรัพย์สินที่จะตรวจสอบกฎของการประเมิน และความต้องการของผู้รับการประเมิน ซึ่งขอบเขตของการประเมินควรครอบคลุมดังนี้

- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) เพื่อให้แน่ใจว่าสอดคล้องกับการดำเนินงานของหน่วยงานผู้ให้บริการขนส่งทางรางต้องรวมถึงสถาปัตยกรรมของระบบสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ เช่น เครื่องคอมพิวเตอร์แม่ข่าย (Server), เครื่องคอมพิวเตอร์ลูกข่าย (Client), ระบบเครือข่าย และการแบ่งแยกเครือข่าย (Network Segmentation)
- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) ที่เกี่ยวข้องกับบริการสำคัญ
- การประเมินความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ (Host Security Assessment) แม่ข่ายที่มีความสำคัญและเป็นเป้าหมายของการโจมตี

(๒) ขั้นตอนการสแกน (Scanning) เป็นการตรวจสอบทรัพย์สิน เพื่อหาช่องโหว่หรือส่วนที่ไม่ปฏิบัติตามข้อกำหนด และอาจเป็นอันตรายต่อความมั่นคงปลอดภัยของสารสนเทศ ซึ่งการทดสอบความมั่นคงปลอดภัยของคอมพิวเตอร์ ระบบเครือข่าย ซอฟต์แวร์ หรือระบบอื่น ๆ สามารถทำได้ทั้งด้วยเครื่องมือสแกนอัตโนมัติ หรือการประเมินด้วยตนเอง โดยสามารถพิจารณาดำเนินการดังนี้

(๒.๑) การพิจารณาดำเนินการตรวจสอบช่องโหว่สำหรับระบบ IT

- การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) สามารถดำเนินการได้ ดังนี้

- ตรวจสอบผังกระบวนการ หรือไดอะแกรมที่แสดงการเข้าถึงบริการสำคัญและการเชื่อมโยงไปยังระบบต่าง ๆ
- พิจารณาสถาปัตยกรรมของระบบสารสนเทศที่เกี่ยวข้องกับบริการสำคัญ เช่น ระบบเครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และอุปกรณ์ต่าง ๆ
- ใช้มาตรการป้องกันหลายชั้น ตามหลักการป้องกันเชิงลึก (Defense in Depth) เพื่อลดความเสี่ยง

- พิจารณาการแบ่งแยกเครือข่าย (Network Segmentation) เพื่อให้เครือข่ายของบริการสำคัญมีอุปกรณ์ที่เกี่ยวข้อง และมีความปลอดภัยเข้ามาในเครือข่ายเท่านั้น

- พิจารณาออกแบบระบบให้มีความพร้อมใช้สูง (High Availability: HA) เพื่อให้บริการมีความเสถียรและไม่หยุดชะงัก

- การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment) ควรกำหนดขอบเขตการประเมิน ดังนี้

  - การประเมินนโยบายและแนวปฏิบัติ เพื่อป้องกันไม่ให้มีการเข้าถึงโดยไม่ได้รับอนุญาต ทั้งในเครือข่ายส่วนตัว (Private Network) และเครือข่ายสาธารณะ (Public Network)
  - การระบุทรัพย์สินที่ไม่ได้ลงทะเบียน
  - การระบุข้อผิดพลาดในการตั้งค่า
  - การป้องกันการเข้าถึงเครือข่าย

- การประเมินความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์ (Host Security Assessment)

  - ประเมินช่องโหว่อิงตามข้อมูลช่องโหว่ของแต่ละผลิตภัณฑ์ซึ่งประกาศโดยผู้ผลิต หรือจากช่องโหว่ที่เคยเกิดขึ้นมาแล้วจากข้อมูลข่าวกรอง (Threat Intelligence)
  - ขอบเขตการประเมินควรรวมถึงการเรียกข้อมูลระบบปฏิบัติการและแพตซ์ของแอปพลิเคชัน การระบุการกำหนดสิทธิในระบบไฟล์ที่ไม่ถูกต้อง การตรวจสอบนโยบายบัญชีและรหัสผ่าน การวิเคราะห์การตั้งค่าควบคุมต่าง ๆ (Configuration) เป็นต้น

(๒.๒) การพิจารณาดำเนินการตรวจสอบช่องโหว่สำหรับสภาพแวดล้อมที่เป็นระบบ ICS โดยผู้ดูแลระบบ หรือเจ้าของระบบงานต้องดำเนินการตรวจสอบช่องโหว่ด้วยตัวเอง ดังนี้

- ทบทวนการเชื่อมต่อกับเครือข่าย เพื่อระบุจุดการเข้าถึงทั้งหมดที่มีในปัจจุบัน ตามตัวอย่างภาคผนวก ๔
- ตรวจสอบความสอดคล้องของความต้องการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางรางกับการเปิดพอร์ต หรือบริการใด ๆ ในระบบที่สำคัญของผู้ให้บริการขนส่งทางราง
- วิเคราะห์ระบบ ICS เพื่อหาช่องโหว่จากข้อมูลที่ได้รับทราบ เช่น จากการประกาศช่องโหว่ของ CISA (CISA Adversaries) หรือจากฐานข้อมูลช่องโหว่แห่งชาติของ NIST (NIST National Vulnerability Database)
- ทบทวนกฎด้านความมั่นคงปลอดภัยไซเบอร์ เช่น กฎไฟร์วอลล์ เป็นต้น ตามตัวอย่างภาคผนวก ๒
- ทบทวนการตั้งค่า (Configuration) เช่น การจัดการบัญชี และรหัสผ่าน เป็นต้น ตามตัวอย่างภาคผนวก ๓
- ทบทวนตามรายการตรวจสอบ (Checklist) ที่หน่วยงานได้กำหนดไว้ หรือตามแนวปฏิบัติของเจ้าของผลิตภัณฑ์ หรือตามมาตรฐานขั้นต่ำด้านการตั้งค่าความปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง ตามตัวอย่างภาคผนวก ๕

- ติดตามรายการช่องโหว่เพื่อตรวจสอบ รวมถึงปรับปรุงรายการตรวจสอบให้เป็นปัจจุบัน เมื่อมีประกาศรายการช่องโหว่ใหม่ ๆ ที่เกี่ยวข้องกับระบบ ICS ที่หน่วยงานผู้ให้บริการขนส่งทางรางใช้งาน หรือเมื่อมาตรฐานได้รับการปรับปรุงและเผยแพร่

ในกรณีการใช้เครื่องมือสแกนหน่วยงานผู้ให้บริการขนส่งทางรางสามารถใช้การสแกนแบบพาสซีฟ (Passive) โดยตรวจสอบหรือวิเคราะห์ข้อมูลในเครือข่าย (Network Traffic) หรือแบบแอ็กทีฟ (Active) โดยสแกนหาช่องโหว่ที่ระบบ ICS โดยตรง ซึ่งก่อนการใช้เครื่องมือสแกนหน่วยงานผู้ให้บริการขนส่งทางราง ควรพิจารณาผลกระทบที่มีต่อส่วนประกอบของระบบ ICS ของหน่วยงานผู้ให้บริการขนส่งทางราง โดยพิจารณาดำเนินการดังนี้

- ดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง เมื่อมีการติดตั้งเครื่องมือสแกน หรือมีการตั้งค่าเครื่องมือสแกนใหม่ รวมถึงการตั้งค่าใหม่ต้องได้รับการอนุมัติ เพื่อพิจารณาผลกระทบต่อระบบ ICS เช่น ทำให้ระบบทำงานช้าลงหรือด้อยประสิทธิภาพลง
- สแกนระบบ ICS ในสภาพแวดล้อมที่ไม่เชื่อมต่อกับเครือข่าย หรือไม่เชื่อมต่อกับสภาพแวดล้อมการทำงานจริง โดยหน่วยงานผู้ให้บริการขนส่งทางรางอาจพิจารณาใช้ระบบสำรองที่สามารถทำงานแทนระบบ ICS หลัก ในเฉพาะกรณีที่ระบบมีความสำคัญต่อการดำเนินงานของหน่วยงานผู้ให้บริการขนส่งทางราง
- ตรวจสอบความเข้ากันได้ (Compatibility) ระหว่างเครื่องมือสแกนกับส่วนประกอบของระบบ ICS ควรได้รับการยืนยันจากผู้ขายระบบ ICS และส่วนประกอบโดยตรงของระบบหรือใช้เครื่องมือสแกนที่ผู้ขายแนะนำเท่านั้น

ในกรณีที่หน่วยงานผู้ให้บริการขนส่งทางรางดำเนินการสแกนเครือข่ายอื่นที่เชื่อมต่อกับเครือข่ายระบบ ICS หน่วยงานผู้ให้บริการขนส่งทางรางต้องดูแล เพื่อให้แน่ใจว่าการสแกนด้วยเครื่องมือจะไม่สแกนเครือข่ายระบบ ICS โดยไม่ได้ตั้งใจ

(๓) ขั้นตอนการประเมิน (Evaluation) โดยดำเนินการจัดหมวดหมู่ตามความรุนแรงของภัยคุกคาม และการจัดลำดับความสำคัญ (Prioritization) หลังจากที่ช่องโหว่ถูกค้นพบในระหว่างการสแกนช่องโหว่ ซึ่งขั้นตอนการจัดลำดับความสำคัญของช่องโหว่ด้านระบบสารสนเทศอาจใช้ Common Vulnerability Scoring System (CVSS) โดยระบุคะแนนเกี่ยวกับความรุนแรงของข้อบกพร่อง รวมถึงข้อมูลวิธีการหาประโยชน์จากข้อบกพร่อง

(๔) ขั้นตอนการรายงาน (Reporting) เป็นขั้นตอนที่ดำเนินการเมื่อการประเมินเสร็จสมบูรณ์ โดยรายละเอียดของรายงานจะระบุช่องโหว่ที่พบ มาตรการแก้ไขที่สามารถเลือกได้ รวมถึงเป็นหลักฐานในการดำเนินการประเมินช่องโหว่ของระบบ

(๕) ขั้นตอนการแก้ไข (Remediation) เป็นการดำเนินการแก้ไขช่องโหว่ หรือยอมรับความเสี่ยงหากไม่สามารถแก้ไขได้ โดยรายละเอียดในรายงานจะแสดงมาตรการแก้ไขสำหรับช่องโหว่ที่พบ ซึ่งช่องโหว่จะต้องได้รับการแก้ไข และอัปเดตแพตช์ตามระดับความวิกฤต และช่องโหว่ที่มีความวิกฤตสูงควรได้รับการแก้ไขทันที

(๖) ขั้นตอนการสแกนซ้ำ (Rescanning) เมื่อช่องโหว่ได้รับการแก้ไข และอัปเดตแพตช์แล้ว ต้องดำเนินการสแกนซ้ำ เพื่อตรวจสอบให้แน่ใจว่าไม่มีช่องโหว่เพิ่มเติม

๒. กำหนดให้ดำเนินการสร้างกระบวนการ เพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ เช่น ตรวจสอบสถานะของการแก้ไขช่องโหว่ และปรับปรุงรายงานการตรวจสอบช่องโหว่ และดำเนินการสแกนซ้ำหลังจากการแก้ไขช่องโหว่ รวมถึงจัดให้มีการสำรองข้อมูล เพื่อป้องกันความสูญเสียที่อาจเกิดขึ้นระหว่างการแก้ไขช่องโหว่ และกำหนดให้มีการเรียนรู้จากช่องโหว่ที่พบ เพื่อป้องกันไม่ให้เกิดขึ้นอีก เป็นต้น

๓. กำหนดให้มีการสแกนช่องโหว่ (Vulnerability Scanner) อย่างน้อยปีละ ๑ ครั้ง หรือขึ้นอยู่กับความสำคัญของบริการ หรือระบบที่ให้บริการตามระดับความเสี่ยงประเมินช่องโหว่ของบริการที่สำคัญและระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง โดยอ้างอิงตามหลักการบริหารความเสี่ยงของหน่วยงานผู้ให้บริการขนส่งทางราง อย่างน้อยปีละ ๑ ครั้ง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ และระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

๔. ประเมินช่องโหว่ของบริการที่สำคัญ และระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี โดยพิจารณาดำเนินการอย่างน้อย ดังนี้

๑) วิเคราะห์ผลกระทบของช่องโหว่ที่มีต่อระบบ และข้อมูล รวมถึงจัดลำดับความสำคัญของการแก้ไขช่องโหว่

๒) กำหนดหลักเกณฑ์ที่ชัดเจน เช่น Critical, High, Medium, Low เพื่อนำมากำหนดระดับเร่งด่วนในการแก้ไขช่องโหว่

๓) ดำเนินการอัปเดตแพตช์หรือเปลี่ยนแปลงการตั้งค่าอย่างเหมาะสม เพื่อแก้ไขช่องโหว่

๔) ดำเนินการทดสอบแพตช์ในระบบทดสอบก่อนนำไปใช้งานจริง (Patch Testing & Rollout Plan)

๕) จัดให้มีการบันทึกผลการดำเนินการบริหารจัดการช่องโหว่ตั้งแต่เริ่มต้น จนถึงการรายงานผลการติดตามการจัดการช่องโหว่

๕. กำหนดให้มีการทดสอบเจาะระบบ (Penetration Testing) โดยพิจารณาอย่างน้อยดังนี้

๑) พิจารณาจัดทำขั้นตอนสำหรับการทดสอบการเจาะระบบ (Penetration Testing Phases) ซึ่งประกอบด้วย ขั้นตอนดังนี้ การวางแผน การสำรวจ การโจมตี และการรายงาน

๒) พิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) สำหรับบริการที่สำคัญและระบบงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบ

๓) ตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๔) พิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ปีครั้ง ตามความจำเป็น เช่น มีการเปลี่ยนแปลงระดับความเสี่ยงเพิ่มขึ้นเกินกว่าระดับความเสี่ยงที่ยอมรับได้มีการเปลี่ยนแปลงลักษณะของภัยคุกคามทางไซเบอร์ เป็นต้น เพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ซึ่งในการดำเนินการทดสอบเจาะระบบอาจเกิดจากกรณี ดังนี้

- ก่อนทำการทดสอบระบบใหม่
- เพิ่มโครงสร้างพื้นฐาน เครือข่าย หรือแอปพลิเคชันใหม่
- อัพเกรดหรือการปรับเปลี่ยนที่สำคัญที่จะนำไปใช้กับโครงสร้างพื้นฐาน หรือแอปพลิเคชันของบริการที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี
- จัดตั้งสำนักงานแห่งใหม่
- ใช้แพตช์ใหม่ในการรักษาความมั่นคงปลอดภัย
- การเปลี่ยนแปลงนโยบายด้านการรักษาความมั่นคงปลอดภัย เป็นต้น

๕) ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ (Penetration Testers) ที่ทำการทดสอบเจาะระบบบนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditations and Certifications) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ

ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบต้องได้รับการรับรองมาตรฐานผู้ทดสอบระดับบริหารจัดการ และระดับปฏิบัติการที่ยอมรับ โดยทั่วไปมีดังต่อไปนี้

- ระดับบริหารจัดการ (Security Management level) เช่น
  (๑) Certified Information Systems Security Professional (CISSP)
  (๒) Certified Information Security Manager (CISM)
  (๓) Certified Information Systems Auditor (CISA)
- ระดับปฏิบัติการ (Penetration Tester Level) เช่น
  (๑) ประกาศนียบัตรการรับรองจากสถาบัน CompTIA เช่น CompTIA Pentest+ เป็นต้น
  (๒) ประกาศนียบัตรการรับรองจากสถาบัน EC-Council เช่น EC-Council’s Certified Penetration Testing Professional (CPENT), Certified Ethical Hacker (CEH), Licensed Penetration Tester (LPT) เป็นต้น
  (๓) ประกาศนียบัตรการรับรองจากสถาบัน ISACA เช่น CSX Cybersecurity Practitioner (CSX-P) เป็นต้น
  (๔) ประกาศนียบัตรการรับรองจากสถาบัน Mile๒ เช่น CERTIFIED Penetration Testing Engineer (C)PTE) เป็นต้น
  (๕) ประกาศนียบัตรการรับรองจากสถาบัน Council for Registered Ethical Security Testers (CREST) เช่น CREST Registered Penetration Tester, CREST Certified Web Application Tester, CREST Certified Infrastructure Tester เป็นต้น
  (๖) ประกาศนียบัตรการรับรอง จากสถาบัน Offensive Security เช่น OSCP, OSWP, OSCE, OSEE และ OSWE เป็นต้น

(๗) ประกาศนียบัตรการรับรองจากสถาบัน Global Information Assurance Certification (GIAC) เช่น GCIH, GMOB, GPEN, GXPN, GAWN และ GWAPT

๖) ตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมด โดยผู้ให้บริการทดสอบเจาะระบบดำเนินการภายใต้การดูแลของหน่วยงานผู้ให้บริการขนส่งทางราง

๗) จัดให้มีกระบวนการ เพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบและตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไข

๘) หากได้รับการร้องขอจาก กกม. หรือ สกมช. ให้ดำเนินการส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ ตามระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานผู้ให้บริการขนส่งทางรางไปยัง สกมช. หน่วยงานผู้ให้บริการขนส่งทางรางจะดำเนินการภายในกำหนด ๓๐ วัน นับแต่วันที่ได้รับหนังสือด้วย

๖. เมื่อการทดสอบแล้วเสร็จ (Post-testing Activity) ต้องดำเนินการตามขั้นตอนแก้ไข และติดตามช่องโหว่ เพื่อแก้ไขช่องโหว่ที่ได้พบ โดยทำการวิเคราะห์ผลลัพธ์จากการสแกนช่องโหว่ และดำเนินการจัดหามาตรการแก้ไข และจัดทำรายงานที่ระบุถึงช่องโหว่ของระบบ ช่องโหว่ของเครือข่าย และช่องโหว่อื่น ๆ พร้อมกับข้อแนะนำในการดำเนินการแก้ไข หรือลดผลกระทบโดยเปรียบเทียบการดำเนินการลดผลกระทบที่อาจเกิดขึ้นกับข้อกำหนดในการปฏิบัติงาน รวมถึงจัดเก็บไว้เป็นหลักฐานให้กับผู้ที่เกี่ยวข้อง เช่น ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) ผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูง (Chief Information Security Officer: CISO) และเจ้าหน้าที่ด้านการรักษาความมั่นคงปลอดภัย ตลอดจนเจ้าของระบบที่เกี่ยวข้องสามารถเข้าถึงได้

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการค้นหาและตรวจสอบช่องโหว่ โดยพิจารณาอย่างน้อยดังนี้

๑) ติดตามข้อมูลช่องโหว่จากมาตรฐาน หรือหน่วยงานสากลที่น่าเชื่อถือ เช่น CVE, NVD, CERT และ Vendor Advisory เป็นต้น

๒) ตรวจสอบข่าวสารเกี่ยวกับช่องโหว่ทางเทคนิคที่มีการประกาศบนเว็บไซต์ หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศของหน่วยงาน หรือจากศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ (ThaiCERT)

๓) กำหนดให้มีการควบคุมช่องโหว่ที่ยังไม่สามารถแก้ไขได้ทันที โดยพิจารณาอย่างน้อย ดังนี้

(๑) กำหนดมาตรการลดความเสี่ยง (Compensating Controls) เช่น ปิดพอร์ตชั่วคราว แยกระบบจากเครือข่ายหลัก หรือเปิดใช้งานระบบเฝ้าระวัง (IDS/IPS) เป็นต้น

(๒) ดำเนินการติดตามสถานะของช่องโหว่ที่ยังไม่ได้รับการแก้ไข หรือจัดการจนกว่าจะสามารถดำเนินการแก้ไขได้อย่างถาวร พร้อมทั้งจัดให้มีการรายงานการติดตามช่องโหว่ที่ยังไม่ได้รับการแก้ไข

(N) การจัดการผู้ให้บริการภายนอก (Third Party Management)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้ดำเนินการแยกประเภทห่วงโซ่อุปทานของผู้ให้บริการภายนอกด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Supply Chain) เช่น IT and cybersecurity service providers, Telecommunications service providers, Cloud platforms, OT hardware products, IoT /IIOT hardware products, IT hardware products (e.g., firewalls, computers, mobile devices), IT software products (e.g., enterprise software, cybersecurity software, database technologies, operating systems) และที่ไม่ใช่ด้านความมั่นคงปลอดภัยไซเบอร์ (Non-Cyber Supply Chain) เช่น Providers of consumables (e.g., stationery, catering, food), Office furniture (e.g., desks, chairs, cabinets), Contractors and service providers ที่ไม่ได้ให้บริการโดยตรงเกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น การบริหารจัดการอาคาร

๒. กำหนดให้ต้องดำเนินการกำกับดูแลการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอก อย่างต่อเนื่อง และสอดคล้องตามกรอบและกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานผู้ให้บริการขนส่งทางราง (IT Risk Management) เพื่อให้ความเสี่ยงอยู่ในระดับที่หน่วยงานยอมรับได้ และกำหนดให้มีระเบียบวิธีปฏิบัติที่ชัดเจนและเป็นลายลักษณ์อักษรครอบคลุมวัฏจักรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) ตั้งแต่การประเมินความเสี่ยง การคัดเลือกผู้ให้บริการภายนอก การจัดทำสัญญาหรือข้อตกลง การติดตามผลการปฏิบัติงานอย่างต่อเนื่องและการยกเลิก/สิ้นสุดสัญญาหรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓. กำหนดมีการจัดทำนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกอย่างชัดเจนเป็นลายลักษณ์อักษร และสอดคล้องกับนโยบายอื่นที่เกี่ยวข้องของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น นโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น ซึ่งการจัดทำนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกอาจเป็นนโยบายที่จัดทำขึ้นเฉพาะ หรืออาจจะกำหนดอยู่ในนโยบายอื่นที่มีอยู่แล้วของหน่วยงานผู้ให้บริการขนส่งทางราง

๔. นโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกควรครอบคลุมประเด็น ดังต่อไปนี้

๑) โครงสร้างการกำกับดูแล และบทบาทหน้าที่ของผู้เกี่ยวข้องในการกำกับดูแลและบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอก

๒) หลักเกณฑ์การจัดระดับความเสี่ยง และระดับความสำคัญของบริการ หรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง

๓) การบริหารจัดการความเสี่ยงที่ครอบคลุมวงจรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) และแนวทางการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ที่ครอบคลุมตามหลักการรักษาความลับ (Confidentiality) ความถูกต้องครบถ้วนของข้อมูลและความพร้อมใช้งาน (Availability)

๔) หลักเกณฑ์การขออนุมัติความเห็นชอบ และการรายงานต่อคณะกรรมการ หรือผู้บริหารระดับสูงที่ได้รับมอบหมาย ซึ่งหมายถึง กระบวนการที่หน่วยงานต้องดำเนินการเพื่อขออนุมัติจากผู้มีอำนาจ เช่น คณะกรรมการหรือผู้บริหารระดับสูงก่อนที่จะดำเนินการใด ๆ ที่เกี่ยวข้องกับการใช้บริการจากผู้ให้บริการภายนอก โดยจะต้องมีการรายงานรายละเอียดต่าง ๆ ที่เกี่ยวข้องกับการใช้บริการ เช่น ข้อมูลเกี่ยวกับบริการที่ให้ผู้ให้บริการภายนอกเข้าถึง ความเสี่ยงที่อาจเกิดขึ้น วิธีการจัดการความเสี่ยง และแนวทางการบริหารจัดการการเชื่อมต่อหรือการเข้าถึงข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งกระบวนการนี้ จะช่วยให้ผู้บริหารและคณะกรรมการสามารถตัดสินใจได้อย่างมีข้อมูลครบถ้วน และสามารถตรวจสอบความเหมาะสมของการใช้บริการภายนอกได้อย่างมีประสิทธิภาพ เพื่อให้มั่นใจว่าไม่มีความเสี่ยงที่อาจเกิดขึ้นจากการให้ผู้ให้บริการภายนอกเข้าถึงข้อมูลหรือระบบที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง

๕) การตรวจสอบการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๖) การเตรียมความพร้อมรับมือต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อหน่วยงานผู้ให้บริการขนส่งทางรางอย่างมีนัยสำคัญ เพื่อให้หน่วยงานผู้ให้บริการขนส่งทางรางสามารถดำเนินธุรกิจได้อย่างต่อเนื่อง ซึ่งรวมถึงการเตรียมข้อมูลให้พร้อมใช้สำหรับการดำเนินธุรกิจและการให้บริการแก่ผู้ใช้งานหรือผู้รับบริการของหน่วยงานผู้ให้บริการขนส่งทางรางได้อย่างต่อเนื่อง

๗) การคุ้มครองผู้ใช้งาน หรือผู้รับบริการของหน่วยงานผู้ให้บริการขนส่งทางราง

๕. นโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกต้องได้รับการอนุมัติจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย และได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ

๖. กำหนดให้มีการสื่อสารนโยบายให้ผู้ที่เกี่ยวข้องได้รับทราบอย่างทั่วถึง และควบคุมดูแลให้ผู้ที่เกี่ยวข้องปฏิบัติตามนโยบายอย่างเคร่งครัด

๗. จัดให้มีมาตรฐานและระเบียบวิธีปฏิบัติ เพื่อสนับสนุนการดำเนินการตามนโยบายการบริหารจัดการความเสี่ยงจากผู้ให้บริการภายนอกให้สอดคล้องกับระดับความเสี่ยง และระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง รวมถึงสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป

๘. การประเมินความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ต้องพิจารณาดำเนินการ ดังนี้

๑) ต้องประเมินความเสี่ยงและผลกระทบทั้งก่อนการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และเมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญ รวมถึงดำเนินการประเมินเป็นประจำอย่างน้อยปีละ ๑ ครั้ง โดยต้องมีผลการประเมินเป็นลายลักษณ์อักษร และคำนึงถึงความเสี่ยงดังต่อไปนี้

(๑) ความเสี่ยงด้านกลยุทธ์ (Strategic Risk) ซึ่งหมายถึง ความเสี่ยงที่เกิดขึ้นจากการตัดสินใจ หรือการดำเนินกลยุทธ์ที่ไม่เหมาะสม หรือการเปลี่ยนแปลงในสภาพแวดล้อมทางบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง ที่อาจส่งผลกระทบต่อความสามารถในการบรรลุเป้าหมายและวัตถุประสงค์ของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การเลือกใช้ผู้ให้บริการภายนอกที่ไม่ตรงกับเป้าหมาย และวัตถุประสงค์การดำเนินการของหน่วยงานผู้ให้บริการขนส่งทางราง หรือการเปลี่ยนแปลงของการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง

ที่ไม่สามารถตอบสนองต่อความต้องการ หรือคาดหวังของการเปลี่ยนแปลงที่เกิดขึ้นได้ ตัวอย่างของความเสี่ยงด้านกลยุทธ์ เช่น การเลือกใช้ผู้ให้บริการภายนอกที่ไม่สามารถปรับตัวได้ตามความต้องการของหน่วยงานผู้ให้บริการขนส่งทางรางหรือไม่สามารถพัฒนาเทคโนโลยีใหม่ ๆ ตามที่หน่วยงานผู้ให้บริการขนส่งทางรางต้องการ, การเปลี่ยนแปลงกลยุทธ์ของหน่วยงานผู้ให้บริการขนส่งทางรางที่ทำให้บริการจากผู้ให้บริการภายนอกไม่ตอบสนองต่อทิศทางใหม่ของหน่วยงานผู้ให้บริการขนส่งทางราง, ความไม่ตรงกับวิสัยทัศน์ระยะยาวของหน่วยงานผู้ให้บริการขนส่งทางรางจากการเลือกผู้ให้บริการภายนอก หรือพันธมิตรที่ไม่เหมาะสม

(๒) ความเสี่ยงจากการกำกับดูแล และบริหารจัดการผู้ให้บริการภายนอกที่ไม่ครอบคลุมทุกขั้นตอนที่ผู้ให้บริการภายนอกดำเนินการ

(๓) ความเสี่ยงด้านชื่อเสียง (Reputation Risk) เช่น ความขัดข้องของระบบ หรือบริการที่ดำเนินการร่วมกับผู้ให้บริการภายนอกอาจส่งผลกระทบต่อการให้บริการ รวมถึงชื่อเสียงและความน่าเชื่อถือของหน่วยงาน เป็นต้น

(๔) ความเสี่ยงด้านเทคโนโลยีสารสนเทศ และภัยคุกคามทางไซเบอร์ เช่น ระบบขัดข้องหรือหยุดบริการ โดยมีสาเหตุจากผู้ให้บริการภายนอก ระบบของผู้ให้บริการภายนอกมีช่องโหว่ด้านความปลอดภัยทำให้ข้อมูลเกิดการสูญหายหรือรั่วไหล ผู้ให้บริการภายนอกเข้าใช้งานด้วยสิทธิสูงเกินกว่าที่ได้รับอนุญาต การจัดเตรียมทรัพยากรระบบมีไม่เพียงพอต่อการใช้งาน เป็นต้น

(๕) ความเสี่ยงด้านกฎหมาย และกฎเกณฑ์ที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เช่น การปฏิบัติไม่ถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พระราชบัญญัติลิขสิทธิ์ และ The EU General Data Protection Regulation (GDPR) เป็นต้น

(๖) ความเสี่ยงของประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบธุรกิจ (Country /Cross Border Risk) เช่น การไม่สามารถเข้าถึงข้อมูลอันเนื่องมาจากการขัดข้องหรือการปิดกั้นเครือข่ายการสื่อสารระหว่างประเทศ เป็นต้น

(๗) ความเสี่ยงที่เกี่ยวข้องกับสัญญาหรือข้อตกลง เช่น ความไม่ครอบคลุม ความไม่ชัดเจน และความไม่ครบถ้วนสมบูรณ์ของสัญญาหรือข้อตกลง เป็นต้น

(๘) ความเสี่ยงจากการเปลี่ยนแปลงเทคโนโลยีของผู้ให้บริการหรือพันธมิตรทางธุรกิจ (Partner) และข้อจำกัดของหน่วยงานผู้ให้บริการขนส่งทางรางในการนำระบบหรือข้อมูลกลับมาดำเนินการ

(๙) ความเสี่ยงจากการกระจุกตัว (Concentration Risk) เช่น หน่วยงานที่มีภารกิจหน้าที่ในลักษณะเดียวกันมีการใช้บริการจากผู้ให้บริการภายนอกเพียงรายเดียว (Single Provider) เป็นต้น

(๑๐) ความเสี่ยงจากผู้ให้บริการภายนอกโดยมีผู้ว่าจ้างผู้อื่นมาดำเนินการแทน (Subcontractor) เช่น Subcontractor มีการปฏิบัติงานที่เกิดข้อบกพร่อง เป็นต้น

๒) ต้องจัดให้มีการควบคุมและบริหารจัดการความเสี่ยงที่สามารถครอบคลุมวัฏจักรการบริหารจัดการผู้ให้บริการภายนอก (Third Party Management Life Cycle) ตั้งแต่การคัดเลือก การจัดทำสัญญาหรือข้อตกลงการติดตามผลการปฏิบัติงานอย่างต่อเนื่อง ตลอดจนการยกเลิก/สิ้นสุดสัญญา หรือข้อตกลง รวมถึงการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๓) ต้องมีการกำหนดหลักเกณฑ์ที่ชัดเจนสำหรับการจัดระดับความเสี่ยง และระดับความสำคัญเพื่อวางแผนการจัดการความเสี่ยง

๔) ต้องจัดทำทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องให้ครอบคลุมครบถ้วนตามที่กำหนดในหัวข้อการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ข้อ ๑) จัดทำทะเบียนการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศ เพื่อให้หน่วยงานสามารถใช้ดำเนินการบริหารจัดการความเสี่ยง ติดตาม และตรวจสอบการปฏิบัติงานของผู้ให้บริการภายนอกได้ครบถ้วนและมีความต่อเนื่อง

๕) ดำเนินการประเมินความเสี่ยง โดยอาจพิจารณาใช้ทั้งการประเมินจากภายในและการประเมินจากภายนอก รวมถึงพิจารณาใช้ระบบสำหรับการประเมินความเสี่ยง และดำเนินการติดตามและประเมินผลการประเมินอย่างต่อเนื่องระหว่างการใช้บริการ ดังต่อไปนี้

(๑) การประเมินจากภายในหน่วยงาน (Internal Assessment) หมายถึง การรวบรวมข้อมูลจากบุคลากรภายในหน่วยงาน เช่น การสัมภาษณ์หรือการกรอกแบบสอบถาม โดยพิจารณาดำเนินการดังนี้

- จัดให้มีแพลตฟอร์มและมาตรฐานคำถามที่ชัดเจน (Standard Template) สำหรับสร้างแบบสอบถามที่สามารถปรับแต่งให้เหมาะสมกับบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น แบบสอบถามเกี่ยวกับความเสี่ยงที่เกิดจากการใช้บริการจากผู้ให้บริการภายนอก เป็นต้น
- จัดให้มีแบบสอบถามสำหรับเหตุการณ์เฉพาะ (Event-specific Questionnaires) โดยการสร้างแบบสอบถามที่เกี่ยวข้องกับเหตุการณ์ใหม่ ๆ ที่อาจเกิดขึ้น เช่น เมื่อมีข่าวภัยคุกคามใหม่ ๆ เช่น การค้นพบช่องโหว่ใหม่ ๆ การแก้ไขช่องโหว่ใหม่ ๆ ที่เกิดขึ้นของผู้ให้บริการภายนอก เป็นต้น

(๒) การประเมินจากภายนอกด้วยการตรวจสอบพื้นผิวการโจมตี (External Assessment with Attack Surface Testing) หมายถึง การตรวจสอบระบบจากภายนอกหน่วยงาน เพื่อหาจุดอ่อนที่อาจถูกโจมตี ซึ่งจะทำได้โดยวิธีที่ไม่เป็นการบุกรุก (Non - intrusive) ดังนี้

- ดำเนินการตรวจสอบพื้นผิวการโจมตี เช่น การค้นหาจากโดเมน หรือการตรวจสอบกลุ่ม IP Address ที่ใช้งานอยู่ในระบบ โดยตัวอย่างการสำรวจช่องโหว่ที่อาจเกิดขึ้น เช่น
  - ใบรับรอง TLS ที่ไม่มีความน่าเชื่อถือ
  - การขาด Web Application Firewall (WAF) ในระบบที่สำคัญ
  - การเปิดเผยข้อมูลในแอปพลิเคชันที่ไม่ได้รับการแพตช์
- ดำเนินการอัปเดตข้อมูลและฐานข้อมูลอย่างต่อเนื่อง เพื่อให้มั่นใจว่าได้ข้อมูลที่ถูกต้อง และทันสมัย
- พิจารณาใช้เครื่องมือที่สามารถตั้งค่าการแจ้งเตือน เมื่อมีการเปลี่ยนแปลงที่สำคัญหรือคะแนนความเสี่ยงลดลง

- ดำเนินการจัดกลุ่มหรือประเภทการประเมิน เพื่อให้การประเมินมีขอบเขตที่ชัดเจนและเป็นระเบียบ โดยการตรวจสอบพื้นผิวการโจมตีของผู้ให้บริการภายนอก หรือการได้รับข้อมูลจากผู้ให้บริการภายนอกเกี่ยวกับผลการตรวจสอบที่ดำเนินการ เช่น
- การประเมินพื้นผิวการโจมตีดิจิทัล (Digital Attack Surface) มุ่งเน้นการประเมินไปที่สินทรัพย์ดิจิทัลที่เข้าถึงได้จากอินเทอร์เน็ต เช่น เว็บแอปพลิเคชันและเว็บไซต์ (Web Applications & Websites) ระบบการเข้าถึงระยะไกล (Remote Access Systems) เป็นต้น
- การประเมินพื้นผิวการโจมตีทางกายภาพ (Physical Attack Surface) ซึ่งเป็นการประเมินความเสี่ยงทางกายภาพที่ผู้โจมตีสามารถใช้เพื่อเข้าถึงระบบดิจิทัลได้ เช่น การเข้าถึงอาคารโดยไม่ได้รับอนุญาตเพื่อติดตั้งอุปกรณ์ หรือการขโมยอุปกรณ์ เป็นต้น
- การประเมินพื้นผิวการโจมตีทางสังคม (Social/Human Attack Surface) ซึ่งเป็นการประเมินเกี่ยวข้องกับช่องโหว่ที่เกิดจากพฤติกรรมมนุษย์ รวมถึงการตรวจสอบข้อมูลที่เปิดเผยสาธารณะที่สามารถนำไปใช้ในการโจมตีแบบ Social Engineering เช่น Phishing, Spear Phishing เป็นต้น

๙. การคัดเลือกผู้ให้บริการภายนอก

๑) กำหนดให้มีระเบียบวิธีปฏิบัติและหลักเกณฑ์ในการพิจารณาคัดเลือกผู้ให้บริการภายนอกอย่างชัดเจนและเป็นลายลักษณ์อักษร โดยให้มีข้อมูลที่เพียงพอสำหรับการพิจารณาตัดสินใจเลือกใช้บริการและอนุญาตให้ผู้ให้บริการภายนอกเชื่อมต่อหรือเข้าถึงข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อให้สามารถทำการคัดเลือกผู้ให้บริการภายนอกที่มีความเหมาะสมตามวัตถุประสงค์สำหรับการดำเนินการของหน่วยงานผู้ให้บริการขนส่งทางราง

๒) การตัดสินใจเลือกใช้บริการที่ผู้ให้บริการภายนอกต้องเชื่อมต่อหรือเข้าถึงข้อมูลที่มีความเสี่ยงอย่างมีนัยสำคัญต้องได้รับความเห็นชอบจากคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

๓) กำหนดให้ดำเนินการประเมินศักยภาพของผู้ให้บริการภายนอก (Due Diligence) โดยการประเมินกระบวนการ การตรวจสอบ และประเมินความเหมาะสมของผู้ให้บริการภายนอกอย่างละเอียด เพื่อให้มั่นใจว่าผู้ให้บริการมีความสามารถและมีคุณสมบัติเหมาะสมในการให้บริการตามต้องการ ซึ่งควรมีการพิจารณาการประเมินให้ครอบคลุมตามระดับความสำคัญและระดับความเสี่ยงที่เกี่ยวข้องของการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกในประเด็นต่าง ๆ เช่น

(๑) ฐานะทางการเงิน ชื่อเสียง ความรู้ความเชี่ยวชาญ ประสบการณ์ และความสามารถในการให้บริการของผู้ให้บริการภายนอก

(๒) ธรรมาภิบาลและวัฒนธรรมภายในองค์กรของผู้ให้บริการภายนอก

(๓) การบริหารจัดการความเสี่ยง การควบคุมภายใน การตรวจสอบภายใน และการติดตามผลการปฏิบัติงาน

(๔) การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอก

(๕) การบริหารจัดการความต่อเนื่องทางธุรกิจ และความพร้อมรับมือจากภัยหรือเหตุการณ์ต่าง ๆ เช่น การตรจสอบจากการได้รับรองมาตรฐาน ISO หรือเอกสารรายงานการรับมือภัยคุกคามทางไซเบอร์

(๖) การปฏิบัติตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง และการปฏิบัติตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศ เช่น การเข้าตรวจสอบเอกสาร หลักฐาน หรือใบรับรองจากผู้ให้บริการภายนอกในการดำเนินการตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง หรือการได้รับการรองรับตามมาตรฐาน ISO/IEC ๒๗๐๐๑ เป็นต้น ซึ่งขอบเขตการรับรองตามมาตรฐานสากลของผู้ให้บริการภายนอกควรพิจารณาจากการรับรองการให้บริการในส่วนที่สำคัญ เช่น ศูนย์คอมพิวเตอร์ หรือ ได้รับการรับรองที่ครอบคลุมทั้งหน่วยงาน เป็นต้น

(๗) ปัจจัยภายนอกที่อาจกระทบต่อการให้บริการของผู้ให้บริการภายนอก เช่น ข้อจำกัดด้านกฎหมายของประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบธุรกิจ

(๘) การใช้เทคโนโลยีแบบเปิด (Open Technology) เพื่อให้สามารถนำระบบไปใช้งานหรือเชื่อมโยงกับระบบอื่นได้ (Interoperability) และสามารถลดข้อจำกัดในการย้าย หรือเปลี่ยนแปลงเทคโนโลยีของผู้ให้บริการ หรือพันธมิตร รวมถึงข้อจำกัดในการนำระบบหรือข้อมูลกลับมาดำเนินการเองภายใต้การดำเนินการของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น การใช้รูปแบบการรับส่งข้อมูลกับผู้ให้บริการภายนอกที่เป็นมาตรฐานการใช้เทคโนโลยีแบบเปิด (Open Standard หรือ Open Source) เป็นต้น

๑๐. การจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก

๑) กำหนดให้มีการจัดทำสัญญาหรือข้อตกลงการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกอย่างเป็นลายลักษณ์อักษร โดยอาจทำในรูปแบบของกระดาษ หรือโดยวิธีการทางอิเล็กทรอนิกส์ และจัดเก็บสัญญาหรือข้อตกลงดังกล่าวไว้ที่หน่วยงานผู้ให้บริการขนส่งทางรางเพื่อสามารถใช้เป็นหลักฐานตามกฎหมายและเป็นการเตรียมข้อมูลให้พร้อมสำหรับการตรวจสอบหรือเมื่อมีการร้องขอโดยสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒) กำหนดให้มีการระบุรายละเอียดและกำหนดเงื่อนไขที่สำคัญในสัญญาหรือข้อตกลงกับผู้ให้บริการภายนอกอย่างชัดเจน โดยต้องคำนึงถึงรายละเอียด ดังนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่อนุญาตให้เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง ตามความต้องการในการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยหน่วยงานผู้ให้บริการขนส่งทางรางต้องระบุรายละเอียด และสิทธิการเข้าถึงทรัพย์สินของบริการที่สำคัญ เช่น ไม่อนุญาตให้ผู้ให้บริการภายนอกประเภทที่เป็นผู้รับช่วงต่อเข้าถึงระบบงานหลักที่มีความเสี่ยงสูง

(ข) กำหนดภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง จากภัยคุกคามทางไซเบอร์ โดยต้องระบุรายละเอียดบทบาทหน้าที่ในการจัดการเทคโนโลยี การจัดการความเสี่ยงและการควบคุมทางไซเบอร์ (Managing Cyber Risks and Controls) เช่น หน่วยงานผู้ให้บริการขนส่งทางรางเป็นผู้ควบคุมการเข้าถึงข้อมูล และผู้ให้บริการภายนอกทำหน้าที่เป็นผู้ให้บริการหลักของบริการตามมาตรการที่กำหนด และต้องแจ้งหน่วยงานผู้ให้บริการขนส่งทางรางเมื่อมีการดำเนินการตามภาระหน้าที่ หรือเมื่อมีเหตุการณ์อื่นใดที่ก่อให้เกิดความเสี่ยงอย่างมีนัยสำคัญต่อหน่วยงานผู้ให้บริการขนส่งทางราง เป็นต้น

(ค) กำหนดให้มีการบริหารความเสี่ยงที่เกี่ยวข้องกับบริการ และห่วงโซ่อุปทานผลิตภัณฑ์ โดยระบุรายละเอียดการติดตาม และควบคุมความเสี่ยงจากการใช้บริการจากผู้ให้บริการภายนอก เช่น ผู้ให้บริการภายนอกต้องแจ้งการเปลี่ยนแปลง หรือเหตุการณ์ที่สำคัญให้รายงานปัญหา หรือเหตุการณ์ผิดปกติที่เกิดจากห่วงโซ่อุปทาน กำหนดให้มีข้อตกลงการเข้ารหัสที่สำคัญ และข้อมูลที่รับส่งผ่านระบบเครือข่ายคอมพิวเตอร์ เป็นต้น

(ง) สิทธิของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก เช่น กำหนดสิทธิของหน่วยงานผู้ให้บริการขนส่งทางราง หน่วยงานควบคุมและกำกับดูแล สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หรือผู้ตรวจสอบภายนอกที่ได้รับการแต่งตั้งจากหน่วยงานหรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ในการเข้าตรวจสอบการดำเนินงาน และการควบคุมภายในของผู้ให้บริการภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกของหน่วยงานผู้ให้บริการขนส่งทางราง ทั้งนี้ ควรพิจารณาระบุรายละเอียดอื่น ๆ ในข้อตกลงหรือสัญญา เช่น

- ขอบเขตการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก โดยระบุ รายละเอียด เช่น ความถี่ของการใช้บริการ เนื้อหาและรูปแบบของการใช้บริการ ระยะเวลาของการเชื่อมต่อตามสัญญา สถานที่ตั้งทางกายภาพของบริการ และบริการเสริม เช่น ซอฟต์แวร์หรือการสนับสนุนเทคโนโลยี อื่น ๆ การบำรุงรักษา และการบริการ
- การคุ้มครองข้อมูลส่วนบุคคลทั้งข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง และข้อมูลของผู้ใช้บริการของหน่วยงานผู้ให้บริการขนส่งทางราง โดยต้องกำหนดให้เป็นไปตามกฎหมายและกฎเกณฑ์ที่เกี่ยวข้อง เช่น ควรมีการจัดทำข้อตกลงเกี่ยวกับการใช้ หรือประมวลผลข้อมูลส่วนบุคคล (Data Processing Agreement: DPA) ให้สอดคล้องกับกฎหมายว่าด้วยการ คุ้มครองข้อมูลส่วนบุคคล
- มาตรฐานการปฏิบัติงานขั้นต่ำของผู้ให้บริการภายนอก เช่น มาตรฐานการควบคุมภายในมาตรฐานการรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) ต้องสอดคล้องกับมาตรฐานขั้นต่ำด้านการรักษาความมั่นคงปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น หากหน่วยงานผู้ให้บริการขนส่งทางรางได้รับการรับรองตาม ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๐๑๗ หรือ CSA-STAR หน่วยงานผู้ให้บริการขนส่งทางรางต้องดำเนินการกำหนดให้ผู้ให้บริการภายนอกได้รับการรับรองมาตรฐานในระดับใกล้เคียงกัน เป็นต้น
- แผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) สำหรับการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก โดยเฉพาะอย่างยิ่งสำหรับกรณีที่เกิดการหยุดชะงักของระบบ ซึ่งผู้ให้บริการภายนอกควรมีระบบการสื่อสารสำรอง เพื่อรองรับการดำเนินการของหน่วยงานผู้ให้บริการขนส่งทางรางให้สามารถดำเนินการได้ภายในระยะเวลาที่กำหนดหลักจากระบบหยุดชะงัก
- ข้อกำหนดในการดำเนินการทำลายข้อมูลเมื่อสิ้นสุดหรือยกเลิกการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น การกำหนดให้ผู้ให้บริการภายนอกต้องออกหนังสือรับรองการทำลายข้อมูลหลังจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลได้สิ้นสุดลง
- เงื่อนไขหรือสิทธิของหน่วยงานผู้ให้บริการขนส่งทางราง ในการขอเปลี่ยนแปลงยุติหรือยกเลิกสัญญาหรือข้อตกลง กรณีที่เกิดการเปลี่ยนแปลงหรือเกิดการละเมิดสัญญาหรือข้อตกลง เช่น

เมื่อผู้ให้บริการภายนอกมีการเปลี่ยน เจ้าของ การละเมิดความปลอดภัยหรือการรักษาความลับ หรือผู้ให้บริการภายนอกอยู่ระหว่างกระบวนการพิทักษ์ทรัพย์/การชำระบัญชี/การล้มละลาย เป็นต้น

๓) กรณีการใช้บริการงานด้านเทคโนโลยีสารสนเทศจากผู้ให้บริการภายนอก (IT Outsourcing) อย่างมีนัยสำคัญ โดยอาจมีผลกระทบต่อความเสี่ยงหรือผลลัพธ์ที่สำคัญที่สามารถส่งผลต่อการดำเนินงาน ความมั่นคงปลอดภัย หรือความสามารถในการปฏิบัติตามข้อกำหนดของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งควรสงวนสิทธิในการพิจารณาอนุมัติ ในกรณีผู้ให้บริการภายนอกว่าจ้างผู้รับเหมาช่วง (Subcontract) และข้อกำหนดที่ผู้ให้บริการภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง เช่น

- บริการที่อาจก่อให้เกิดผลกระทบต่อความมั่นคงปลอดภัย หากการใช้บริการจากผู้ให้บริการภายนอกเกี่ยวข้องกับข้อมูลหรือระบบที่สำคัญ เช่น ระบบที่ใช้จัดการข้อมูลผู้ใช้บริการ หรือข้อมูลทางการเงิน การให้ผู้รับเหมาช่วงเข้ามามีส่วนร่วมอาจเพิ่มความเสี่ยงในการเข้าถึงข้อมูลสำคัญ
- บริการที่เกิดความเสี่ยงด้านการดำเนินงาน หากผู้ให้บริการภายนอกมีการจ้างผู้รับเหมาช่วงในการ ดำเนินงานบางส่วน แต่ไม่สามารถควบคุมหรือประเมินการดำเนินการของผู้รับเหมาช่วงได้อย่างเต็มที่ อาจทำให้เกิดการปฏิบัติงานที่ไม่ได้มาตรฐานหรือล่าช้า ซึ่งมีผลกระทบต่อการให้บริการของหน่วยงานผู้ให้บริการขนส่งทางราง
- บริการที่อาจก่อให้เกิดผลกระทบต่อการควบคุมและการติดตาม การอนุญาตให้ผู้รับเหมาช่วงเข้ามาทำงานแทนผู้ให้บริการหลัก อาจทำให้หน่วยงานผู้ให้บริการขนส่งทางรางขาดการควบคุมและตรวจสอบการดำเนินการที่เกิดขึ้นภายใต้การทำงานของผู้รับเหมาช่วง
- การดำเนินการที่เกี่ยวข้องกับข้อกำหนดทางกฎหมาย และการปฏิบัติตามมาตรฐาน ซึ่งผู้ให้บริการภายนอกที่เลือกใช้ผู้รับเหมาช่วงต้องรับผิดชอบต่อการปฏิบัติตามข้อกำหนดกฎหมาย และมาตรฐานความมั่นคงปลอดภัยที่เกี่ยวข้อง เพื่อป้องกันปัญหาทางกฎหมายหรือข้อบังคับที่อาจเกิดขึ้นในภายหลัง

๔) ในกรณีที่ผู้ให้บริการภายนอกได้ว่าจ้างผู้รับเหมาช่วง (Subcontract) และผู้ให้บริการภายนอกมีสิทธิเข้าใช้บริการงานด้านเทคโนโลยีสารสนเทศที่สำคัญหน่วยงานผู้ให้บริการขนส่งทางราง ควรกำหนดสิทธิในการพิจารณาอนุมัติในกรณีผู้ให้บริการภายนอกว่าจ้างผู้รับเหมาช่วง (Subcontract) และแจ้งถึงข้อกำหนดที่ผู้ให้บริการภายนอกต้องรับผิดชอบต่อผลการปฏิบัติงานของผู้รับเหมาช่วง

๕) กรณีการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกที่ตั้งอยู่ในต่างประเทศ สัญญาหรือข้อตกลงในการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ควรพิจารณาถึงความเสี่ยงและอุปสรรคที่อาจเกิดขึ้นจากประเทศที่ผู้ให้บริการภายนอกตั้งอยู่หรือประกอบการดำเนินการตามภาระหน้าที่ของผู้ให้บริการภายนอก (Country Risk)

ทั้งนี้ ในการจัดทำสัญญาหรือข้อตกลงการใช้บริการหน่วยงานผู้ให้บริการขนส่งทางราง ควรมอบหมายให้ผู้ที่มีอำนาจตัดสินใจเข้าร่วมในการเจรจา โดยวัตถุประสงค์ของการเจรจาคือการมีข้อตกลงร่วมกัน และสอดคล้องกับการเปลี่ยนแปลงตามกฎหมายภายใต้เงื่อนไขที่ดีที่สุดสำหรับทั้งสองฝ่าย

๑๑. กำหนดให้สร้างกระบวนการในการตรวจสอบ ติดตามผลปฏิบัติงานอย่างต่อเนื่อง (Monitoring) เพื่อตรวจสอบความถูกต้องของผู้ให้บริการภายนอกในการดำเนินการให้สอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุเป็นเงื่อนไขในสัญญาที่ครอบคลุมการตรวจสอบการปฏิบัติ

ตามข้อกำหนดด้านความปลอดภัยทางไซเบอร์และข้อตกลงระดับการให้บริการ (Service Level Agreement) การตรวจสอบการเปลี่ยนแปลงสถานะต่างๆ ของผู้ให้บริการภายนอก เช่น การเงิน กฎหมาย ความเป็นเจ้าของ รวมถึงการตรวจสอบเรื่องการจัดการความเสี่ยงตามที่ระบุตามกรอบเวลาการแก้ไขข้อตกลงร่วมกัน ซึ่งกระบวนการตรวจสอบ ติดตามผู้ให้บริการภายนอก ควรพิจารณาให้มีขั้นตอน ดังนี้

๑) กำหนดผู้รับผิดชอบ และจัดการติดตามผลการปฏิบัติงานของผู้ให้บริการภายนอกอย่างต่อเนื่อง โดยพิจารณาตามระดับความเสี่ยงและระดับความสำคัญของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น กำหนดให้ผู้ให้บริการภายนอกรายงานผลการปฏิบัติงานอย่างสม่ำเสมอ กำหนดการประชุมติดตามอย่างสม่ำเสมอและต่อเนื่อง กำหนดการเข้าสังเกตการณ์การดำเนินงานของผู้ให้บริการภายนอก เป็นต้น

๒) กำหนดให้ผู้ให้บริการภายนอกรายงานเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อให้หน่วยงานผู้ให้บริการขนส่งทางราง รับทราบอย่างทันการณ์และสามารถประเมินผลกระทบที่มีต่อหน่วยงานผู้ให้บริการขนส่งทางราง และหากหน่วยงานผู้ให้บริการขนส่งทางรางประเมินแล้วพบว่าผลกระทบที่เกิดขึ้นมีผลต่อการดำเนินการของหน่วยงานผู้ให้บริการขนส่งทางรางอย่างมีนัยสำคัญ ต้องกำหนดให้หน่วยงานผู้ให้บริการขนส่งทางรางมีส่วนร่วมในการตัดสินใจแก้ไขเหตุการณ์ผิดปกติที่เกิดขึ้น

๓) ดำเนินการตรวจสอบความถูกต้องของผู้ให้บริการภายนอก โดยหน่วยงานผู้ให้บริการขนส่งทางราง ตามสิทธิ์การตรวจสอบที่กำหนดในข้อกำหนด โดยการพิจารณาวิธีการประเมินอย่างใดอย่างหนึ่งหรือใช้วิธีการร่วมกัน ดังนี้

- วิธีการประเมินตนเอง (Self–assessment) โดยการกำหนดให้ผู้ให้บริการภายนอกบันทึก ประเด็นปัญหาความเสี่ยง ข้อมูลความเสียหาย รวมถึงเหตุการณ์ผิดปกติที่เกิดขึ้นระหว่างการดำเนินงานด้วยตนเอง เพื่อให้หน่วยงานตรวจสอบและกำกับได้เมื่อมีการร้องขอ
- วิธีการประเมินโดยบุคคลที่สาม (Third-party Assessment) โดยให้หน่วยงานที่เป็นบุคคลที่สาม และมีความสามารถในการประเมินที่เป็นที่น่าเชื่อถือมาเป็นผู้ประเมินคุณภาพการดำเนินงานของผู้ให้บริการภายนอก
- วิธีการตรวจสอบผลิตภัณฑ์ โดยการทดสอบผลิตภัณฑ์ที่ผู้ให้บริการภายนอกใช้ในการดำเนินงาน เช่น การทดสอบความเร็วในการเชื่อมต่อของอุปกรณ์เครือข่าย การทดสอบการตรวจจับมัลแวร์ การตรวจสอบช่องโหว่ เป็นต้น

๔) ดำเนินการทบทวนการประเมินศักยภาพ การประเมินผลการปฏิบัติงาน และการประเมินความเสี่ยงของการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกทั้งในด้านประสิทธิภาพการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ และการปฏิบัติตามกฎหมาย เมื่อจะต่อสัญญาหรือเมื่อถึงรอบระยะเวลาที่หน่วยงานผู้ให้บริการขนส่งทางรางกำหนด รวมถึงควรดำเนินการทบทวนการประเมินอย่างน้อยปีละ ๑ ครั้ง รวมถึงให้รายงานผลการประเมินต่อคณะกรรมการหรือผู้บริหารระดับสูงที่ได้รับมอบหมาย

๑๒. การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง

๑) จัดให้มีมาตรฐานหรือระเบียบเกี่ยวกับการปฏิบัติว่าด้วยการยกเลิก และสิ้นสุดสัญญาหรือข้อตกลง เพื่อเป็นกรอบแนวทางการยกเลิกหรือสิ้นสุดสัญญาหรือข้อตกลง โดยคำนึงถึงความต่อเนื่องในการให้บริการและความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ซึ่งครอบคลุมถึงบทบาทหน้าที่ของคณะกรรมการและหน่วยงานที่เกี่ยวข้องกับ กระบวนการและการควบคุมภายใน เช่น การสำรองข้อมูลก่อนการยกเลิก การลบหรือการเรียกคืนทรัพย์สินสำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางกลับมาทำลาย เช่น กุญแจการเข้ารหัสข้อมูล และบัญชีผู้ใช้งาน เป็นต้น

๒) พิจารณาดำเนินการประเมินผล กระทบและความเสี่ยงที่อาจเกิดขึ้นจากการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง และดำเนินการตามมาตรฐาน หรือระเบียบเกี่ยวกับการปฏิบัติว่าด้วยการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง และกำหนดกลยุทธ์ และแผนงาน การยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลง (Exit Strategy and Exit Plan) ที่ชัดเจน เพื่อให้มั่นใจว่าการยกเลิกและการสิ้นสุดสัญญาหรือข้อตกลงนั้นเป็นไปอย่างมีประสิทธิภาพและได้เตรียมความพร้อมต่อผลกระทบที่อาจจะเกิดขึ้น เช่น การหยุดให้บริการของระบบที่ส่งผลกระทบกับผู้ใช้บริการ และการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เป็นต้น

๑๓. การเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ ในกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่ซึ่งอาจปรับเปลี่ยนระดับของรายละเอียด หรือความครอบคลุมของข้อตกลง และส่งผลต่อสัญญาปัจจุบันให้เกิดความเสี่ยงเพิ่มขึ้นและไม่สามารถยอมรับความเสี่ยงได้หน่วยงานผู้ให้บริการขนส่งทางราง ควรพิจารณาขอเจรจาแก้ไขข้อกำหนดของสัญญาเพิ่มเติม หรือขอแก้ไขรายละเอียด เพื่อให้สอดคล้องกับข้อกำหนดหรือความเสี่ยงที่เปลี่ยนแปลง และในการเจรจาต่อรองเงื่อนไขของสัญญาจ้างต้องทำความเข้าใจสิทธิและหน้าที่ความรับผิดชอบของแต่ละฝ่าย รวมถึงขอบเขตอำนาจในการเจรจาต่อรองในเงื่อนไขการบอกเลิกสัญญา หรือการรับผิดที่อาจตามมา และพิจารณารายละเอียดของขอบเขตงาน ความซับซ้อนในการดำเนินการ รวมถึงระยะเวลาในการดำเนินการที่เพิ่มขึ้น ซึ่งควรดำเนินการตรวจสอบจากที่ปรึกษาทางกฎหมายก่อนการเริ่มต้นเจรจาสัญญา

ในกรณีไม่สามารถตกลงกันได้ภายใต้เงื่อนไขใหม่อาจต้องพิจารณาจัดหาผู้ให้บริการรายอื่นมาดำเนินการในส่วนที่มีการเปลี่ยนแปลงแก้ไขต่อไป

๑๔. กำหนดให้ผู้ให้บริการภายนอกต้องมีมาตราการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและไซเบอร์ตามกรอบหลักการ ที่สำคัญ ๓ ประการ คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องครบถ้วน (Integrity) และการรักษาสภาพพร้อมใช้งาน (Availability) และสอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง (IT Security Policy) หรือมาตรฐานสากลด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เช่น ISO/IEC ๒๗๐๐๑, ISO/IEC ๒๗๐๑๗ เป็นต้น

ในกรณีที่มีการใช้บริการ Cloud Computing ต้องนำแนวปฏิบัติที่ดีของผู้ให้บริการ Cloud Computing มาเป็นแนวทางในการปฏิบัติงานและควบคุมดูแล เพื่อให้ระบบที่ใช้บริการ Cloud Computing มีความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ โดยต้องกำหนดให้บุคลากรที่เกี่ยวข้องในการปฏิบัติงานปฏิบัติตามแนวปฏิบัติด้านการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึง

เป็นไปตามมาตรฐานสากลทางด้านการป้องกัน และรับมือภัยคุกคามทางไซเบอร์ที่เป็นที่ยอมรับโดยทั่วไป และพิจารณาให้สอดคล้องตามระดับความเสี่ยง และระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง ซึ่งควรกำหนดมาตรการเพิ่มเติม ดังนี้

๑) จัดทำทะเบียนการใช้บริการ การเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง โดยพิจารณาดำเนินการ ดังนี้

(๑) จัดให้มีผู้รับผิดชอบในการจัดทำ และปรับปรุงทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้สามารถนำมาใช้ระบุความเสี่ยงจากการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอกได้อย่างชัดเจน และสามารถบริหารจัดการทรัพย์สินด้านเทคโนโลยีสารสนเทศได้อย่างปลอดภัยและทันการณ์

(๒) ทะเบียนการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก และทะเบียนทรัพย์สินด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง ควรครอบคลุมรายละเอียด ดังนี้

- ชื่อผู้ให้บริการภายนอก
- ประเภทของผู้ให้บริการภายนอก เช่น ประเภทที่อยู่ภายนอกกลุ่มของหน่วยงาน ประเภทที่อยู่ภายในกลุ่มของหน่วยงาน และ Regulator เป็นต้น
- ชื่อบริการ/ระบบงาน
- ลักษณะและขอบเขตของงาน
- ประเภทของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เช่น IT Outsourcing Cloud Computing บริการร่วมกับพันธมิตร การใช้บริการเครือข่ายสาธารณะ เป็นต้น
- ระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอก เข้าใช้ เชื่อมต่อหรือเข้าถึง
- ที่ตั้งศูนย์คอมพิวเตอร์หลักและสำรองข้อมูลของผู้ให้บริการภายนอกที่ประมวลผล จัดเก็บข้อมูล หรือดำเนินการใด ๆ ที่เกี่ยวข้องกับข้อมูลหรือระบบงานให้แก่หน่วยงานผู้ให้บริการขนส่งทางราง
- วันเริ่มต้นและวันสิ้นสุดสัญญาหรือข้อตกลงของการใช้บริการ การเชื่อมต่อหรือการเข้าถึง ข้อมูลจากผู้ให้บริการภายนอก
- การรับรองตามมาตรฐานสากลด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้อง (ถ้ามี)
- รายละเอียดทรัพย์สินที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล จากผู้ให้บริการภายนอก เช่น ข้อมูลที่นำไปจัดเก็บหรือประมวลผล ระดับชั้นความลับข้อมูล เป็นต้น

๒) การรักษาความมั่นคงปลอดภัยของข้อมูล (Information Security)

(๑) กำหนดให้ต้องแบ่งระดับความสำคัญของข้อมูล (Information Classification) ตามการบริหารจัดการทรัพย์สิน (Asset Management) ของกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ก่อนที่จะนำข้อมูลไปใช้ จัดเก็บหรือประมวลผลโดยผู้ให้บริการภายนอก โดยต้องพิจารณาจัดเก็บข้อมูล

หรือระบบสารสนเทศที่มีผลกระทบระดับสูงไว้ในประเทศ (Data Localization) ซึ่งอ้างอิงตามประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูล หรือระบบสารสนเทศ พ.ศ. ๒๕๖๖ และประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. ๒๕๖๗

(๒) เข้ารหัสข้อมูลที่อยู่ภายใต้การดูแลของผู้ให้บริการภายนอกให้เป็นไปตามนโยบายและมาตรฐานของหน่วยงานผู้ให้บริการขนส่งทางรางตามประเภทและระดับชั้นความลับของข้อมูล (Information Classification) ให้สอดคล้องกับนโยบาย และแนวปฏิบัติความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงพิจารณาการเข้ารหัสให้ครอบคลุมทั้งข้อมูลที่อยู่บนอุปกรณ์ที่ใช้ปฏิบัติงาน (Data at Endpoint) ข้อมูลที่อยู่ระหว่างการรับส่งผ่านเครือข่าย (Data in Transit) และข้อมูลที่อยู่บนระบบงานและสื่อบันทึกข้อมูล (Data at Rest) ซึ่งรวมถึงข้อมูลสำรอง

(๓) กำหนดให้มีการควบคุมทุกขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส (Lifecycle of Cryptographic Keys) ตั้งแต่ การสร้าง การจัดเก็บ การใช้งาน การสำรอง การเพิกถอน และการต่ออายุของกุญแจเข้ารหัสข้อมูล ภายใต้การดูแลของหน่วยงานผู้ให้บริการขนส่งทางราง

(๔) กำหนดให้หน่วยงานผู้ให้บริการขนส่งทางรางดำเนินการสร้างกุญแจการเข้ารหัสด้วยตนเอง ซึ่งในกรณีที่หน่วยงานผู้ให้บริการขนส่งทางรางไม่สามารถสร้างกุญแจการเข้ารหัสด้วยตนเอง หน่วยงานผู้ให้บริการขนส่งทางรางต้องกำหนดให้มีการควบคุมผู้ให้บริการภายนอกไม่ให้นำกุญแจการเข้ารหัสที่สร้างขึ้นโดยผู้ให้บริการภายนอกไปใช้ร่วมกับผู้ใช้บริการรายอื่น รวมถึงต้องทราบถึงรายละเอียดของระบบการบริหารจัดการกุญแจเข้ารหัสข้อมูลของผู้ให้บริการภายนอก ดังนี้

- ประเภทของกุญแจเข้ารหัสข้อมูล
- รายละเอียดของระบบ รวมถึงกระบวนการควบคุมการเข้ารหัสข้อมูลในแต่ละขั้นตอนตลอดวงจรการบริหารจัดการกุญแจการเข้ารหัส
- ข้อแนะนำการใช้งานและการควบคุมการเข้ารหัสข้อมูล

(๕) กำหนดให้มีการเก็บกุญแจการเข้ารหัสข้อมูลในอุปกรณ์รักษาความปลอดภัย เช่น Hardware Security Module (HSM) เป็นต้น และดูแลรักษาความปลอดภัยของอุปกรณ์ HSM ด้วยการจัดตั้งในโซนเครือข่ายที่มีความปลอดภัยและจำกัดการเชื่อมต่อกับระบบงานอื่นที่ไม่เกี่ยวข้อง

(๖) กำหนดให้มีการสอบทานการปฏิบัติงานการบริหารจัดการเข้ารหัสข้อมูลทั้งที่ดำเนินการภายใต้การดูแลของหน่วยงานผู้ให้บริการขนส่งทางราง และโดยผู้ให้บริการภายนอกให้ครอบคลุมการสอบทานช่องโหว่และความเสี่ยงของการเข้ารหัสข้อมูล โดยพิจารณาให้มีความปลอดภัยและมีความสอดคล้องกับมาตรฐานสากลที่ยอมรับโดยทั่วไป เช่น ใช้อัลกอริธึมการเข้ารหัส (Encryption Algorithm) และขนาดความยาวของกุญแจเข้ารหัสข้อมูลที่ได้รับการยอมรับ เป็นต้น

๓) การควบคุมการเข้าถึง (Access Control)

(๑) กำหนดกระบวนการจัดการและควบคุมการเบิกใช้สิทธิและการเข้าถึงระบบและข้อมูล ของหน่วยงานผู้ให้บริการขนส่งทางรางที่ชัดเจนเป็นลายลักษณ์อักษรเป็นไปตามนโยบายและแนวการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่กำหนด รวมทั้งตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป เช่น NIST, ISO/IEC๒๗๐๐๑ เป็นต้น

(๒) กำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้มีสิทธิเข้าใช้งานระบบ และผู้ใช้งานที่ได้รับสิทธิสูงสุด (Privilege Account) ให้ชัดเจน

(๓) ควบคุมดูแลการให้สิทธิแก่ผู้ให้บริการภายนอก โดยจำกัดสิทธิตามบทบาทหน้าที่และความจำเป็นในการใช้งาน รวมถึงมีการอนุมัติการเบิกใช้งาน เพื่อไม่ให้บุคคลใดบุคคลหนึ่งมีสิทธิปฏิบัติงานได้ตั้งแต่เริ่มกระบวนการจนจบกระบวนการ (Separation of Duties)

(๔) มีระบบหรือกระบวนการติดตามระหว่างการใช้งานบัญชีของผู้ใช้งานที่มีสิทธิสูงสุด รวมทั้งควรติดตามและสอบทานสถานะสิทธิและการใช้งานหรือการเข้าถึงระบบข้อมูลที่สอดคล้องกับความเสี่ยงและระดับของสิทธิ (Privilege Level) สม่ำเสมออย่างน้อยทุก ๖ เดือน เพื่อให้มั่นใจว่าการใช้งานสิทธิเป็นไปตามขอบเขต และความจำเป็นในการใช้งาน

(๕) กำหนดวิธีการระบุและพิสูจน์ตัวตนของผู้ใช้งานด้วยวิธีการที่รัดกุมเพียงพอและสอดคล้องกับนโยบายแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง

(๖) ในกรณีที่ผู้ให้บริการภายนอกต้องดำเนินการเชื่อมต่อ เพื่อเข้าถึงระบบงานของหน่วยงานผู้ให้บริการขนส่งทางรางผ่านช่องทางการเข้าถึงระบบงานระยะไกล (System Remote Access) ต้องมีการกำหนดกระบวนการบริหาร จัดการการเข้าถึงระยะไกลด้วยวิธีการที่ปลอดภัย ดังนี้

- มีการขออนุมัติก่อนการเข้าถึงระบบงานระยะไกล (System Remote Access)
- ผู้ใช้งานที่ได้รับสิทธิระดับสูง (Privilege Account) ให้ใช้เข้าถึงระบบงานเฉพาะกรณีที่มีความจำเป็น และภายในระยะเวลาที่อนุมัติเท่านั้น
- กำหนดให้มีการพิสูจน์ตัวตนของผู้ใช้งานแบบ Two-Factors Authentication และการเชื่อมต่อผ่าน Virtual Private Network (VPN)
- มีการควบคุมการเข้าใช้งาน โดยจำกัดการเข้าใช้งานเฉพาะอุปกรณ์ที่ได้รับอนุญาตเท่านั้น หรือใช้เทคโนโลยีเข้ามาบริหารจัดการเครื่องคอมพิวเตอร์แบบเสมือน (Virtual Desktops Infrastructure) เพื่อลดความเสี่ยงจากการติด Malware หรือการเข้าถึงระบบงานที่ไม่เหมาะสม
- สามารถระบุและสอบทานอุปกรณ์หรือระบบปลายทางที่มีการเชื่อมต่อกับระบบเครือข่ายของหน่วยงานผู้ให้บริการขนส่งทางรางแบบระยะไกลว่าเป็นอุปกรณ์ที่ได้รับอนุญาต
- มีการสอบทานการเข้าถึงระบบงานระยะไกล โดยบัญชีผู้ใช้งานที่ได้รับสิทธิระดับสูงด้วยบุคคล หรือหน่วยงานที่มีความเป็นอิสระและมีความรู้ความเชี่ยวชาญเพียงพอ

(๗) กำหนดให้มีการจัดเก็บบันทึกข้อมูลประวัติของการพิสูจน์ตัวตนและการเข้าถึง (Access Log) บันทึกการดำเนินงาน (Activity Log) อย่างน้อย ๙๐ วัน และจัดให้มีการสอบทานข้อมูลการบันทึกสม่ำเสมออย่างน้อยทุก ๖ เดือน ให้สอดคล้องกับความเสี่ยงและความสำคัญของระบบและข้อมูล

๔) การรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร (Communications Security)

(๑) กำหนดให้มีการรักษาความมั่นคงปลอดภัยไซเบอร์ในการรับส่งข้อมูลผ่านระบบเครือข่ายสื่อสารกับผู้ให้บริการภายนอกให้เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงให้เป็นไปตามมาตรฐานสากลที่ยอมรับโดยทั่วไป

(๒) กำหนดให้ผู้ให้บริการภายนอกมีระบบหรือกระบวนการสำหรับการคัดกรองข้อมูลที่ส่งผ่านระบบเครือข่าย (Traffic) ที่สามารถตรวจจับแจ้งเตือนและสามารถยับยั้งการบุกรุก หรือตอบโต้การโจมตีได้ โดยอัตโนมัติแบบต่อเนื่องบนระบบเครือข่ายให้เพียงพอเหมาะสมตามระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อ หรือเข้าถึงได้ ดังนี้

- เครื่องมือตรวจหาและแจ้งเตือน ที่สามารถยับยั้งการบุกรุก หรือตอบโต้การโจมตีได้โดยอัตโนมัติบนระบบเครือข่าย (Network Intrusion Detection and Prevention Systems: NIDPS)
- เครื่องมือป้องกันการโจมตีเว็บไซต์ (Web Application Firewall: WAF)
- มาตรการป้องกันการโจมตีแบบ Distributed Denial of Services (DDoS)
- ระบบป้องกัน ข้อมูลรั่วไหล (Data Leakage Prevention Systems: DLPS)
- ซอฟต์แวร์การตรวจจับไวรัส หรือมัลแวร์ ต่าง ๆ ที่อาจทำการบุกรุกเข้าสู่เครือข่าย

(๓) กรณีที่หน่วยงานใช้บริการ Cloud Computing ต้องกำหนดมาตรการที่ชัดเจนในการแยกแยะข้อมูลและแยกสภาพแวดล้อมบน Cloud ของหน่วยงานผู้ให้บริการขนส่งทางรางออกจากผู้ใช้บริการรายอื่นที่ใช้บริการจากผู้ให้บริการ Cloud เดียวกัน เช่น การแยกแยะสภาพแวดล้อมโดยการใช้ Virtual Private Cloud (VPC) หรือการสร้างบัญชีผู้ใช้แยกต่างหาก

๕) การบริหารจัดการการเปลี่ยนแปลง (Change Management)

(๑) จัดทำกระบวนการและแนวทางบริหารจัดการการเปลี่ยนแปลง โดยกำหนดให้ผู้ให้บริการ ภายนอก และผู้ที่ได้รับมอบหมายของหน่วยงานผู้ให้บริการขนส่งทางรางดำเนินการกำหนดกระบวนการและแนวทางร่วมกัน หรืออาจให้กระบวนการบริหารจัดการการเปลี่ยนของหน่วยงานผู้ให้บริการขนส่งทางรางที่มีอยู่มาบังคับใช้ร่วมกัน และดำเนินการสื่อสารให้ผู้ให้บริการภายนอกรับทราบ และปฏิบัติตามเพื่อให้สามารถประเมินผลกระทบ และเตรียมแนวทางรองรับผลกระทบที่จะเกิดขึ้น เช่น ผู้ให้บริการ Cloud Computing ต้องแจ้งหน่วยงานผู้ให้บริการขนส่งทางรางเมื่อผู้ให้บริการภายนอกต้องการเปลี่ยนแปลงระบบของผู้ให้บริการภายนอกและอาจส่งผลกระทบกับการให้บริการ

(๒) กำหนดให้ผู้ให้บริการภายนอกแจ้งการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่อาจมีผลกระทบกับการให้บริการของหน่วยงานผู้ให้บริการขนส่งทางราง โดยให้แจ้งล่วงหน้าในระยะเวลาที่กำหนด เพื่อให้หน่วยงานผู้ให้บริการขนส่งทางราง สามารถพิจารณาแนวทางการลดผลกระทบต่อการให้บริการระบบ และข้อมูลที่จะได้รับผลกระทบที่จะเกิดขึ้น

๖) การบริหารจัดการการตั้งค่าระบบ (System Configuration Management) ในกรณีที่ผู้ให้บริการภายนอกมีหน้าที่ตั้งค่าระบบงานหน่วยงานผู้ให้บริการขนส่งทางราง ต้องกำหนดมาตรฐานการตั้งค่าระบบงานให้ปลอดภัยเพียงพอ ตามมาตรฐานด้านความปลอดภัยด้านเทคโนโลยีสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น ค่า System Configuration ของระบบปฏิบัติการและการตั้งค่าความปลอดภัยของอุปกรณ์เครือข่าย เป็นต้น

๗) การบริหารจัดการขีดความสามารถของระบบ (Capacity Management)

(๑) กำหนดกระบวนการติดตาม ประเมินประสิทธิภาพและความเพียงพอของทรัพยากรด้านเทคโนโลยีสารสนเทศของการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูล โดยผู้ให้บริการภายนอกอย่างเพียงพอและต่อเนื่อง ตลอดจนรายงานผลการติดตามและประเมินให้แก่คณะกรรมการ หรือผู้บริหาร

ระดับสูงที่ได้รับมอบหมายทราบอย่างสม่ำเสมอ รวมถึงกำหนดแนวทางลดความเสี่ยงได้ทันการณ์ เช่น ติดตามและประเมินการใช้งานบริการของหน่วยงานเทียบกับทรัพยากรของระบบ และเครือข่ายของผู้ให้บริการ เช่น หน่วยประมวลผล (CPU) หน่วยความจำ (RAM) หรือความกว้างแถบความถี่ (Bandwidth) มีความพอเพียงในการใช้บริการหรือไม่

(๒) กำหนดตัวชี้วัดการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศ (Threshold และ Trigger) ในระดับต่าง ๆ และกำหนดกระบวนการรายงานและแจ้งเตือนปัญหาหรือเหตุการณ์ที่มีความผิดปกติที่เกิดจากการให้บริการหรือเชื่อมต่อกับผู้ให้บริการภายนอก รวมถึงกำหนดแนวทางการประสานงานกับหน่วยงานทั้งภายใน และภายนอกในกรณีเกิดเหตุขัดข้องให้เหมาะสมตามระดับความเสี่ยง และระดับความสำคัญของบริการ

๘) การจัดเก็บข้อมูลบันทึกเหตุการณ์ (Logging) ในกรณีที่หน่วยงานผู้ให้บริการขนส่งทางรางไม่สามารถเก็บข้อมูลบันทึกเหตุการณ์ได้ด้วยตนเอง เช่น การใช้บริการ Cloud Computing หน่วยงานผู้ให้บริการขนส่งทางรางต้องควบคุม และตรวจสอบให้ผู้ให้บริการภายนอกดำเนินการจัดเก็บข้อมูลให้ครบถ้วนเพียงพอ และปลอดภัย เพื่อใช้ในการติดตามตรวจสอบเกี่ยวกับร่องรอยการเข้าถึง และการใช้งานระบบหรือข้อมูลของผู้ใช้งาน รวมทั้งใช้เป็นหลักฐานการทำธุรกรรมทางอิเล็กทรอนิกส์ตามที่กฎหมายกำหนด

๙) การติดตามดูแลระบบและเฝ้าระวังภัยคุกคาม (Security Monitoring)

(๑) กำหนดให้ผู้ให้บริการภายนอกดำเนินการติดตามดูแลระบบและเฝ้าระวังภัยคุกคามอย่างต่อเนื่อง รวมทั้งมีการตรวจจับเหตุการณ์ที่ผิดปกติที่เกิดขึ้นอย่างมีนัยสำคัญกับระบบ หรือการบริการที่สำคัญ ซึ่งอาจส่งผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ทั้งในระดับระบบ (System) เครือข่าย (Network) และแอปพลิเคชัน (Application) เพื่อรับมือภัยคุกคามทางไซเบอร์ได้ทันการณ์

(๒) กำหนดให้มีการวิเคราะห์ข้อมูลบันทึกเหตุการณ์ (Logging) ของระบบ การบริการที่ใช้หรือเชื่อมต่อกับผู้ให้บริการภายนอก เพื่อให้สามารถป้องกันและตรวจจับการบุกรุกได้ทันการณ์

๑๐) การบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing)

(๑) กำหนดให้ผู้ให้บริการภายนอกมีการบริหารจัดการช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Management and Penetration Testing) ตามมาตรฐานสากลที่เป็นที่ยอมรับโดยทั่วไป และสอดคล้องกับนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศของหน่วยงานผู้ให้บริการขนส่งทางราง

(๒) ดำเนินการสอบทานขอบเขตและผลการทดสอบเจาะระบบของผู้ให้บริการภายนอก เพื่อให้มั่นใจว่าการทดสอบครอบคลุมระบบทั้งหมดที่หน่วยงานผู้ให้บริการขนส่งทางรางใช้บริการ หรือเชื่อมต่อกับผู้ให้บริการภายนอก และครอบคลุมภัยคุกคามทางไซเบอร์ที่สำคัญ

๑๑) กำหนดให้มีกระบวนการ หรือขั้นตอนการสำรองข้อมูล (Data Backup) ในกรณีที่หน่วยงานผู้ให้บริการขนส่งทางรางใช้บริการหรือเชื่อมต่อกับผู้ให้บริการภายนอก และมีการจัดเก็บข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง หรือข้อมูลผู้ใช้บริการของหน่วยงานผู้ให้บริการขนส่งทางราง โดยครอบคลุมเนื้อหา ดังนี้

- ขอบเขต และรายละเอียดของการสำรองข้อมูลและรอบเวลาสำรองข้อมูล

- วิธีการ หรือเทคโนโลยีการสำรองข้อมูลและรูปแบบข้อมูล (Data Format)
- ระยะเวลาในการเก็บรักษาข้อมูลสำรอง
- การตรวจสอบความถูกต้องครบถ้วนของข้อมูลสำรอง
- ขั้นตอนและวิธีการกู้ข้อมูล
- การทดสอบความสามารถในการกู้คืนข้อมูลจากอุปกรณ์สำรองข้อมูล (Restoration Test)
- สถานที่จัดเก็บข้อมูลสำรอง

๑๒) การบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศ (IT Incident Management)

(๑) ระบุหน้าที่และความรับผิดชอบของหน่วยงานผู้ให้บริการขนส่งทางราง และผู้ให้บริการภายนอกที่เกี่ยวกับการบริหารจัดการเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศอย่างชัดเจน ซึ่งต้องรวมถึงหน้าที่การกำหนดระดับความรุนแรงของเหตุการณ์ผิดปกติ และหน้าที่ของผู้ให้บริการภายนอกที่ต้องแจ้งให้ หน่วยงานผู้ให้บริการขนส่งทางรางทราบถึงเหตุการณ์ผิดปกติที่เกิดขึ้นและเกี่ยวข้องกับหน่วยงานผู้ให้บริการขนส่งทางรางภายในระยะเวลา ๒๔ ชม.

(๒) หากเหตุการณ์ผิดปกติที่เกิดขึ้นนั้นมีผลกระทบต่อการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางรางอย่างมีนัยสำคัญ ต้องดำเนินการร่วมกับผู้ให้บริการภายนอกเพื่อตัดสินใจแก้ไขเหตุการณ์ผิดปกติที่เกิดขึ้น

(๓) กำหนดให้ผู้ให้บริการภายนอกจัดให้มีช่องทาง ระบบ หรือเครื่องมือ เพื่อรองรับกรณีหน่วยงานผู้ให้บริการขนส่งทางรางตรวจพบและต้องการรายงานเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศให้ผู้ให้บริการภายนอกทราบ รวมถึงติดตามสถานการณ์และการแก้ไขของผู้ให้บริการภายนอกต่อเหตุการณ์ผิดปกติที่เกิดขึ้นได้อย่างทันการณ์

(๔) กำหนดให้ผู้ให้บริการภายนอกมีผู้ประสานงานอย่างเป็นทางการ เพื่อประสานงานกับหน่วยงานผู้ให้บริการขนส่งทางรางในการตอบสนองต่อเหตุการณ์ผิดปกติด้านเทคโนโลยีสารสนเทศได้อย่างทันการณ์

๑๓) การบริหารความต่อเนื่อง (Business Continuity Management)

(๑) กำหนดให้ผู้ให้บริการภายนอกจัดทำแผนความต่อเนื่อง (Business Continuity Plan) และแผนฟื้นฟูจากภัยพิบัติ (Disaster Recovery Plan) ที่ครอบคลุมถึงการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก เพื่อให้มีแนวทางรองรับต่อเหตุการณ์ที่อาจเกิดขึ้นและมีผลกระทบต่อการให้บริการอย่างมีนัยสำคัญ และสามารถดำเนินการให้บริการได้อย่างต่อเนื่อง

(๒) แผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติที่ผู้ให้บริการภายนอกจัดทำขึ้นต้องคำนึงถึงปัจจัยสำคัญ หรือความเสี่ยงที่อาจเกิดขึ้นและส่งผลต่อการหยุดชะงักจากการใช้บริการการเชื่อมต่อ หรือการเข้าถึงข้อมูลจากผู้ให้บริการภายนอก ผลกระทบที่มีต่อการดำเนินการตามภารกิจของหน่วยงานผู้ให้บริการขนส่งทางราง และการติดต่อสื่อสารระหว่างผู้ให้บริการภายนอกกับหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงการรายงานปัญหาหรือเหตุการณ์ผิดปกติให้คณะกรรมการ หรือผู้บริหารระดับสูงที่ได้รับมอบหมายทราบอย่างทันการณ์ตามความสำคัญ และระดับความรุนแรงหรือผลกระทบของเหตุการณ์

(๓) ประเมินและทดสอบการปฏิบัติตามแผนความต่อเนื่อง และแผนฟื้นฟูจากภัย พิบัติ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น ความสอดคล้องกันของขอบเขต คำนิยามและการกำหนดระยะเวลาที่สำคัญ เช่น ระยะเวลาการหยุดชะงักสูงสุดที่ยอมรับได้ (Maximum Tolerable Period of Disruption: MTPD) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective, RPO) เป็นต้น

(๔) กำหนดให้มีการเข้าร่วมทดสอบแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ในกรณีที่สามารถเข้าร่วมได้ เพื่อประเมินความพร้อมของผู้ให้บริการภายนอกในการกู้คืนระบบงานตามกรอบ MTPD, RTO และ RPO ที่กำหนดไว้

(๕) กำหนดให้มีการสื่อสารรายละเอียดแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ให้กับทีมบริหารจัดการในสภาวะวิกฤติ (Crisis Management Team) ของหน่วยงานผู้ให้บริการขนส่งทางรางได้รับทราบและเตรียมความพร้อมในการบริหารจัดการในส่วนที่เกี่ยวข้อง

(๖) ดำเนินการรวบรวมปัญหาที่พบระหว่างการทดสอบแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติกับผู้ให้บริการภายนอก ในกรณีที่ไม่ได้เข้าร่วมการซ้อมแผน ต้องกำหนดให้ผู้ให้บริการภายนอกจัดทำรายงานการซ้อมแผนความต่อเนื่อง และแผนฟื้นฟูจากภัยพิบัติส่งให้หน่วยงานผู้ให้บริการขนส่งทางรางตรวจสอบ และปรับปรุงแก้ไขร่วมกับผู้ให้บริการภายนอก

๑๕. กำหนดให้มีการตรวจสอบผู้ให้บริการภายนอกในส่วนที่เกี่ยวข้องกับการใช้บริการ การเชื่อมต่อหรือการเข้าถึงข้อมูลของหน่วยงาน เช่น ระบุเงื่อนไขในสัญญาหรือข้อตกลง เป็นต้น ซึ่งอาจเป็นการตรวจสอบจากหน่วยงานผู้ให้บริการขนส่งทางราง หรือดำเนินการแต่งตั้งหน่วยงานให้เข้าตรวจสอบแทนให้สอดคล้องกับระดับความเสี่ยงและระดับความสำคัญของบริการหรือข้อมูลที่เปิดให้ผู้ให้บริการภายนอกเข้าใช้ เชื่อมต่อหรือเข้าถึง โดยการใช้บริการการเชื่อมต่อหรือการเข้าถึงบริการหรือข้อมูลที่สำคัญควรได้รับการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อพบเหตุการณ์ผิดปกติเกิดขึ้นอย่างมีนัยสำคัญ

ในกรณีที่มีเหตุจำเป็นที่ทำให้ไม่สามารถดำเนินการตรวจสอบผู้ให้บริการภายนอกได้ ต้องระบุสิทธิหรือเงื่อนไขการตรวจสอบในสัญญาหรือข้อตกลง หรือดำเนินการตรวจสอบได้จากผลการตรวจสอบด้านเทคโนโลยีสารสนเทศของผู้ให้บริการภายนอกที่ได้รับการรับรองจากผู้ตรวจสอบภายนอกที่มีความเป็นอิสระและได้มาตรฐานสากล เช่น ผลการตรวจสอบตาม ISO/IEC ๒๗๐๐๑ หรือ CSA-STAR ที่ถูกรายงานให้คณะกรรมการ หรือผู้บริหารระดับสูงที่ได้รับมอบหมายรับทราบแล้ว

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการอบรม และสร้างความตระหนักด้านความปลอดภัยสำหรับบุคลากรของหน่วยงานผู้ให้บริการอย่างสม่ำเสมอเกี่ยวกับการบริหารจัดการผู้ให้บริการภายนอก

๒. ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกดำเนินการพัฒนาระบบควรพิจารณาข้อกำหนดด้านความมั่นคงปลอดภัย ในเรื่องดังนี้

๑) สิทธิในทรัพย์สินทางปัญญาสำหรับชุดคำสั่ง (Source Code) ในการพัฒนา

๒) การตรวจสอบด้านคุณภาพและความถูกต้องของระบบสารสนเทศ

๓) การตรวจสอบชุดคำสั่งที่ไม่พึงประสงค์

๔) ข้อจำกัดในการเปิดเผยข้อมูลขององค์กร

๕) มาตรฐานและคุณภาพการให้บริการด้านความมั่นคง

๖) การทดสอบระบบสารสนเทศ

๓. ในกรณีที่มีการจัดจ้างผู้ให้บริการภายนอกดำเนินการพัฒนาระบบไม่อนุญาตให้นำข้อมูลสำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น ข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลใช้ภายในเท่านั้น ไปใช้ในการทดสอบกับระบบงาน เพื่อป้องกันการรั่วไหลของข้อมูล เว้นแต่ได้รับการอนุมัติจากผู้บริหารที่มีอำนาจหน้าที่รับผิดชอบ หรือได้รับความยินยอมโดยชัดแจ้ง หรือมีการแจ้งเจ้าของข้อมูลส่วนบุคคลตามแต่กรณีไว้ก่อนแล้ว

๔. กำหนดให้มีการบริหารจัดการข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ โดยจัดทำข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับก่อนเริ่มดำเนินการใด ๆ ที่อาจมีการเปิดเผยข้อมูล และครอบคลุมเนื้อหาอย่างน้อย ดังนี้

๑) หน้าที่ความรับผิดชอบของผู้จัดทำข้อตกลง และผู้ที่ยินยอมรับทราบข้อตกลง

๒) ขอบเขตของข้อมูลที่ถือว่าเป็นความลับ เช่น ข้อมูลส่วนบุคคล ข้อมูล Source code ของระบบ ข้อมูลรายละเอียดโครงสร้างระบบเครือข่าย (Network diagram) หรือการตั้งค่าความปลอดภัย เป็นต้น

๓) ระยะเวลาการรักษาความลับ และระยะเวลาต่อเนื่องที่ต้องรักษาความลับหลังสิ้นสุดภาระหน้าที่ความรับผิดชอบ

๔) ข้อตกลงในการจำกัดการเปิดเผย การทำสำเนา และการส่งต่อข้อมูล

๕) บทลงโทษในกรณีละเมิดไม่ปฏิบัติตามข้อตกลง

๕. กำหนดให้มีการบริหารจัดเก็บ และควบคุมข้อตกลงการรักษาความลับ หรือการไม่เปิดเผยความลับอย่างน้อย ดังนี้

๑) ข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ที่ลงนามแล้ว ต้องถูกจัดเก็บในระบบการบริหารจัดการเอกสารขององค์กร (Document Control Management) โดยจัดเก็บแยกตามบุคคล/หน่วยงาน พร้อมระบุวันเริ่มต้น – สิ้นสุด และเลขอ้างอิง พร้อมทั้งกำหนดให้มีการควบคุมการเข้าถึงเอกสารข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ได้เฉพาะผู้มีสิทธิ์การเข้าถึงตามหน้าที่ความรับผิดชอบ พร้อมทั้งจัดให้มีการติดตามอายุของข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA)

๒) กำหนดให้มีการติดตาม และทบทวนสถานะของข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) อย่างสม่ำเสมอ เช่น อย่างน้อยปีละ ๑ ครั้ง

๓) กำหนดให้มีการติดตามการละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) โดยการกำหนดขั้นตอนการแจ้งเหตุละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับหรือปฏิบัติตามขั้นตอนการแจ้งเหตุละเมิดขององค์กร

๔) ในกรณีที่พบเหตุการณ์ละเมิดข้อตกลงการรักษาความลับหรือการไม่เปิดเผยความลับ (NDA) ต้องดำเนินการบันทึกเหตุการณ์ตามขั้นตอนการแจ้งเหตุละเมิดข้อตกลงการรักษาความลับ หรือการไม่เปิดเผยความลับ หรือปฏิบัติตามขั้นตอนการแจ้งเหตุละเมิดขององค์กร พร้อมทั้งดำเนินการลงโทษ และหามาตรการป้องกันการเกิดเหตุการณ์ซ้ำเดิม

(O) การแบ่งปันข้อมูล (Information Sharing)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. ต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูล เกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ในส่วนที่เกี่ยวกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และมาตรการบรรเทาผลกระทบใด ๆ ที่ดำเนินการ เพื่อตอบสนองต่อเหตุการณ์หรือภัยคุกคามดังกล่าวกับบุคคลที่ได้รับผลกระทบจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ หรือภัยคุกคามด้านความมั่นคงปลอดภัยไซเบอร์ (เช่น ผู้ใช้ ผู้รับเหมาที่ให้บริการแก่บริการที่สำคัญ และเจ้าของคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ที่จำเป็นต้องเชื่อมต่อกับบริการที่สำคัญ) เพื่อให้สามารถใช้มาตรการป้องกันที่จำเป็นได้

๒. การกำหนดขั้นตอนการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์และภัยคุกคามทางไซเบอร์ ควรประกอบไปด้วย

๑) กำหนดเป้าหมายและวัตถุประสงค์ของการแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ และภัยคุกคามไซเบอร์ ก่อนดำเนินการแบ่งปันข้อมูล

๒) จัดให้มีการระบุแหล่งที่มาของข้อมูลภัยคุกคาม (Identify Potential Sources) เช่น เป็นข้อมูลที่มาจากภายในหน่วยงาน แหล่งข้อมูลจากศูนย์ประสานงานด้านความมั่นคงปลอดภัยไซเบอร์ เครื่องมือที่ใช้ในการเก็บข้อมูล และตำแหน่งของเครื่องมือจัดเก็บข้อมูล

๓) จัดให้มีการระบุประเภทข้อมูลที่สามารถแบ่งปันได้ เช่น Indicator of Compromise (IOC) Tactics Techniques and Procedures (TTPs) เป็นต้น และกำหนดระดับความลับของข้อมูล

๔) ระบุขอบเขตผู้รับข้อมูล เช่น หน่วยงานภายในองค์กร ผู้ให้บริการที่เกี่ยวข้อง (Third Parties) พันธมิตรด้านความมั่นคงไซเบอร์ (Trusted Partners) หน่วยงานของรัฐ หน่วยงานกำกับดูแลหรือสาธารณะ (เฉพาะข้อมูลที่เปิดเผยได้) รวมถึงการเข้าถึงข้อมูล และเงื่อนไขการรักษาความลับ

๕) กำหนดมาตรการป้องกันความเป็นส่วนตัว เช่น ลบหรือปกปิดข้อมูลให้สามารถระบุตัวบุคคลได้ (PII) เพื่อปฏิบัติตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๖) กำหนดเกณฑ์การแบ่งปันข้อมูล (Sharing Designations) ตามระดับประเภทของข้อมูล (Traffic Light Protocol: TLP) ซึ่งมี ๕ ระดับ ดังนี้

ระดับชั้นข้อมูล (TLP)	**ข้อมูลในระดับความลับมาก**
คำอธิบาย ระดับชั้นข้อมูล	๑. เป็นข้อมูลที่ไม่สามารถเปิดเผยหรือเผยแพร่ได้ และจำกัดเฉพาะผู้ที่มีสิทธิได้รับข้อมูลเท่านั้น ๒. การนำไปใช้งานเมื่อข้อมูลมีความเกี่ยวข้องกับข้อมูลส่วนบุคคล หรือส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หรือภาครัฐ หากข้อมูลถูกนำไปใช้ในทางที่ผิด
การเปิดหรือเผยแพร่	ผู้ได้รับข้อมูลต้องไม่เปิดเผยหรือ เผยแพร่ข้อมูลให้กับบุคคลใด ๆ นอกเหนือจากที่ผู้ส่งข้อมูลได้ระบุไว
ตัวอย่างข้อมูล	● การรั่วไหลของข้อมูล (Data Breach) หรือการโจมตีเข้าถึงข้อมูลของลูกค้ารายบุคคล (Specific Customer) ● ข้อมูลส่วนบุคคล (Personal Identifiable Information) ● รหัสผ่าน Password ต่าง ๆ

	• Blocking Rules ที่เปิดเผยไม่ได้เพราะอาจมีผลกระทบอย่างรุนแรงต่อความสามารถในการปกป้องข้อมูลลูกค้า • ช่องโหว่ของระบบสารสนเทศของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ • Example of Attack Code สำหรับใช้ในการโจมตีช่องโหว่ของระบบข้อมูลของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ • ข้อมูลที่อาจทำให้ Attackers รู้ตัวว่าอยู่ระหว่างภายใต้การตรวจสอบ (Under Surveillance)
ระดับชั้นข้อมูล (TLP)	**ข้อมูลในระดับความลับ**
คำอธิบาย ระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่าง จำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงาน หรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สำหรับการสนับสนุนในการดำเนินการแก้ไขหรือป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ แต่อาจส่งผลกระทบต่อการดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หากถูกเผยแพร่ออกไปภายนอกหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูล
การเปิดหรือเผยแพร่	• ผู้ได้รับข้อมูลสามารถเปิดเผย หรือเผยแพร่ข้อมูลจำกัดเฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • ผู้ได้รับข้อมูลสามารถเปิดเผย หรือเผยแพร่ข้อมูลกับผู้ที่เกี่ยวข้องในหน่วยงานหรือหน่วยงานที่เกี่ยวข้องโดยตรงกับข้อมูล เพื่อปกป้องอันตรายที่อาจเกิดขึ้น • ผู้ส่งข้อมูลมีสิทธิที่จะระบุข้อจำกัดใน การเปิดเผยหรือเผยแพร่ข้อมูลเพิ่มเติม ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด
ตัวอย่างข้อมูล	• ขั้นตอนหรือการกระทำย่อย ๆ ที่ใช้เพื่อทำให้กลยุทธ์นั้นเป็นจริง เป็นส่วนหนึ่งของกลยุทธ์ที่ระบุว่าเราจะทำอย่างไรเพื่อให้บรรลุเป้าหมายที่วางไว้ Tactics Techniques and Procedures (TTPs) ของ Specific Attacker หรือ เฉพาะกลุ่มของ Threat Actors ที่มี TTP เป็นลักษณะเฉพาะเจาะจงในการโจมตีหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • Blocking Rules เช่น IP Blacklist หรือ WAF (Web Application Firewall) Rules ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น • Software Security Vulnerability (ช่องโหว่ความปลอดภัยของซอฟต์แวร์) ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงหรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูล

	สามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● Security Incident Information ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● System Logs ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● การโจมตีในรูปแบบต่าง ๆ ที่เกี่ยวข้องกับ Cybersecurity ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● ข้อมูลเกี่ยวกับ Identified (หรือ Acting) Botnet Networks ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับ ข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น ● ข้อมูลที่เตรียมทำเป็นข่าว ก่อนการแถลง ประกาศ หรือเปิดเผย (Press Releases Before Announcement) ซึ่งต้องการให้ผู้รับข้อมูลสามารถ เผยแพร่ข้อมูลเฉพาะภายในหน่วยงานหรือหน่วยงานของผู้มีสิทธิได้รับข้อมูลเท่านั้น
ระดับชั้นข้อมูล (TLP)	**ข้อมูลในระดับใช้ภายใน**
คำอธิบาย ระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้อย่างจำกัด ซึ่งผู้รับข้อมูลสามารถเผยแพร่ข้อมูลชนิดนี้ได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สำหรับ การสนับสนุนในการดำเนินการแก้ไขหรือ ป้องกันภัยคุกคามทางไซเบอร์ได้อย่างมี ประสิทธิภาพ แต่อาจส่งผลกระทบต่อ การดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หากถูกเผยแพร่ออกไปภายนอกหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูล

การเปิดหรือเผยแพร่	● ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่จำกัดเฉพาะเมื่อจำเป็นต้องรู้ (Need to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลกับหน่วยงาน หรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูล เพื่อปกป้องตนเอง หรือป้องกันอันตรายที่อาจเกิดขึ้น ● ผู้ส่งข้อมูลมีสิทธิที่จะระบุข้อจำกัดในการเปิดเผยหรือเผยแพร่ข้อมูลเพิ่มเติม ซึ่งผู้ได้รับข้อมูลจะต้องปฏิบัติตามโดยเคร่งครัด
ตัวอย่างข้อมูล	● ขั้นตอนหรือการกระทำย่อยๆ ที่ใช้เพื่อทำให้กลยุทธ์นั้นเป็นจริง เป็นส่วนหนึ่งของกลยุทธ์ที่ระบุว่าเราจะทำอย่างไรเพื่อให้บรรลุเป้าหมายที่วางไว้ Tactics Techniques and Procedures (TTPs) ของ Specific Attacker หรือ เฉพาะกลุ่มของ Threat Actors ที่มี TTP เป็นลักษณะเฉพาะเจาะจง ในการโจมตีหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็น ต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลนี้เท่านั้น ● Blocking Rules เช่น IP Blacklist หรือ WAF (Web Application Firewall) Rules ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● Software Security Vulnerability (ช่องโหว่ความปลอดภัยของซอฟต์แวร์) ที่มีข้อมูลเป็นลักษณะเฉพาะเจาะจงหรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● Security Incident Information ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● System Logs ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● การโจมตีในรูปแบบต่าง ๆ ที่เกี่ยวข้องกับ Cybersecurity ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับ

	หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● ข้อมูลเกี่ยวกับ Identified (หรือ Acting) Botnet Networks ที่สามารถระบุหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ ที่สามารถระบุหน่วยงาน หรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล หรือมีผลกระทบกับหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูล ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ข้อมูลได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น ● ข้อมูลที่เตรียมทำเป็นข่าว ก่อนการแถลง ประกาศ หรือเปิดเผย (Press Releases Before Announcement) ซึ่งต้องการให้ผู้รับข้อมูลสามารถเผยแพร่ ข้อมูลชนิดนี้ได้ เฉพาะเมื่อจำเป็นต้องรู้ (Need-to-know Basis) ภายในหน่วยงานหรือหน่วยงานหรือบุคคลที่เกี่ยวข้องโดยตรงกับข้อมูลเท่านั้น
ระดับชั้นข้อมูล (TLP)	**ข้อมูลในระดับเปิดเผยระหว่างหน่วยงานสมาชิก หรือกลุ่มบุคคลที่มีสิทธิ์เข้าถึงและเกี่ยวข้อง**
คำอธิบายระดับชั้นข้อมูล	๑. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่ได้จำกัด เฉพาะระหว่างหน่วยงานหรือหน่วยงานที่เป็นสมาชิกเท่านั้น ๒. เป็นข้อมูลที่เป็นประโยชน์กับสมาชิก ในการสร้างความตระหนักให้กับหน่วยงาน หรือผู้ที่เกี่ยวข้อง
การเปิดหรือเผยแพร่	● ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลเฉพาะระหว่างหน่วยงานหรือหน่วยงานของสมาชิกศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ ในด้านเดียวกับหน่วยงานเท่านั้น และต้องไม่เผยแพร่สู่สาธารณะ โดยการส่งต่อข้อมูลต้องไม่ใช้ช่องทางสาธารณะ ที่ทำให้ข้อมูลแพร่กระจายในวงกว้าง ● ในกรณีที่หน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลมีบริษัทใหญ่ หรือบริษัทย่อย หรือบริษัทร่วมหรือ บริษัทย่อยลำดับเดียวกัน ผู้ได้รับข้อมูลสามารถเปิดเผยหรือเผยแพร่ข้อมูลได้เฉพาะการนำข้อมูลที่ได้รับไปใช้ เพื่อวัตถุประสงค์ในการป้องกันภัยคุกคามทางไซเบอร์ของหน่วยงานหรือของ

	หน่วยงานของสมาชิกที่อยู่ในขอบเขต ของ สกมช. หรือหน่วยงานควบคุมหรือกำกับดูแล หรือภาคส่วนเท่านั้น เช่น บริษัท A เป็นบริษัทผู้ประกอบกิจการเกี่ยวกับบริการขนส่งทางรางเป็นสมาชิกของศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ บริษัท A สามารถนำข้อมูลที่อยู่ในระดับสีเขียวไปใช้ได้กับหน่วยงานหรือส่วนงานที่ IT Security Officer (หรือเทียบเท่า) ของบริษัท A รับผิดชอบเท่านั้น หากบริษัท A มีบริษัทใหญ่ชื่อบริษัท B ซึ่งไม่ได้อยู่ในภาคระบบการขนส่งทางรางและมีหน่วยงาน หรือส่วนงาน IT Security ของบริษัท B เองแล้วนั้น บริษัท A จะไม่สามารถ แชร์ข้อมูลที่อยู่ในระดับสีเขียวให้ บริษัท B ได้
ตัวอย่างข้อมูล	ข้อมูลทั่วไปเกี่ยวกับสถิติของ Cybersecurity Incidents ที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ ● ข้อมูลการวิเคราะห์สถิติหรือแนวโน้ม Malware หรือภัยคุกคามทางไซเบอร์เฉพาะกลุ่มอุตสาหกรรม ที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ ● รายชื่อ Websites, URLs, Hash ที่เป็นอันตราย (Malicious) หรือข้อมูลเกี่ยวกับ Indicator of Compromise (IoC) ที่สร้างโดย สกมช. หรือหน่วยงานควบคุม หรือกำกับดูแล หรือที่ไม่ใช่เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ ● ตัวอย่างมัลแวร์ (Malware Sample) ของหน่วยงานหรือหน่วยงานของผู้ได้รับข้อมูลหรือผู้ส่งข้อมูลที่ยังไม่มีการเผยแพร่สู่สาธารณะ ● ข้อมูลการติดต่อ สกมช. หรือหน่วยงานควบคุมหรือกำกับดูแล
ระดับชั้นข้อมูล (TLP)	**ข้อมูลในระดับเปิดเผยสู่สาธารณะ**
คำอธิบาย ระดับชั้นข้อมูล	๑. เป็นข้อมูลที่สามารถเปิดเผยหรือเผยแพร่สู่สาธารณะได้โดยไม่มีข้อจำกัด ๒. เป็นข้อมูลที่เปิดเผยหรือเผยแพร่สู่ สาธารณะแล้วไม่ส่งผลกระทบต่อการ ดำเนินงาน หรือความเป็นส่วนตัว หรือชื่อเสียงของบุคคล หน่วยงาน หรือภาครัฐใด ๆ ตลอดจนการเผยแพร่สู่สาธารณะต้องสอดคล้องกับหลักกฎหมายระหว่างประเทศ หรือกฎหมายภายในประเทศ ที่เกี่ยวข้อง
การเปิดหรือเผยแพร่	ผู้ได้รับข้อมูลสามารถเปิดเผยหรือ เผยแพร่ข้อมูลสู่สาธารณะได้ภายใต้หลักกฎหมาย ระหว่างประเทศ หรือกฎหมายภายในประเทศที่เกี่ยวข้อง
ตัวอย่างข้อมูล	● ข้อมูลที่เปิดเผยทั่วไปใน Public Domain ● รายชื่อ Websites, URLs, Hash ที่เป็นอันตราย (Malicious) หรือ ข้อมูลเกี่ยวกับ Indicator of Compromise (IoC) ที่สร้างโดย สกมช. กรมการขนส่งทางราง หรือหน่วยงานผู้ให้บริการขนส่งทางรางและกำหนดให้เป็นข้อมูลสาธารณะ หรือจากแหล่งข้อมูลสาธารณะ ● ตัวอย่างมัลแวร์ (Malware Sample) จากแหล่งข้อมูลสาธารณะ ● ข้อมูลที่เป็นข่าว หลังการแถลง, ประกาศ หรือเปิดเผย (Press Releases After Announcement)

๗) กำหนดช่องทางแบ่งปันที่ชัดเจน และปลอดภัย และใช้ช่องทางที่กำหนดในการแบ่งปันข้อมูลเท่านั้น เช่น ผ่าน CERT ระบบ Threat Intelligence Sharing Platform เป็นต้น

๘) กำหนดให้มีการจัดเก็บประวัติการแบ่งปันข้อมูลและผู้รับข้อมูล เพื่อให้สามารถตรวจสอบย้อนหลังได้ในกรณีที่ข้อมูลถูกนำไปใช้ไม่เหมาะสม

๓. กำหนดให้มีการอนุมัติการแบ่งปันข้อมูลก่อนทำข้อตกลงในการแบ่งปันข้อมูล จากผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมายในการอนุมัติการแบ่งปันข้อมูล รวมถึงขอความเห็นชอบในการดำเนินการทีมกฎหมายหรือผู้มีอำนาจในการทำสัญญา เจ้าหน้าที่ด้านการคุ้มครองข้อมูลส่วนบุคคลและผู้มีส่วนได้ส่วนเสียหลักอื่น ๆ ที่มีบทบาท ในการรวบรวม นำเข้า จัดเก็บ วิเคราะห์ เผยแพร่ หรือปกป้องข้อมูลภัยคุกคามทางไซเบอร์ รวมถึงกำหนดให้มีผู้ตรวจสอบข้อมูลก่อนดำเนินการแบ่งปันข้อมูล

๔. เมื่อได้รับการแจ้งเตือนด้านความมั่นคงปลอดภัยไซเบอร์หน่วยงานผู้ให้บริการขนส่งทางรางต้องดำเนินการพิจารณาว่าการแจ้งเตือนนั้น มาจากแหล่งที่เชื่อถือได้หรือไม่ เมื่อการแจ้งเตือนมาจากแหล่งที่ไม่รู้จักหรือไม่น่าเชื่อถือ หน่วยงานอาจต้องใช้เวลา ตรวจสอบข้อเท็จจริงมากขึ้น หรือขอการยืนยันที่เป็นอิสระ (Independent Confirmation) ก่อนที่จะดำเนินการ และหากการแจ้งเตือนมีความน่าเชื่อถือและเกี่ยวกับระบบ แอปพลิเคชัน หรือฮาร์ดแวร์ที่หน่วยงานผู้ให้บริการขนส่งทางรางเป็นเจ้าของหรือดำเนินการ หน่วยงานผู้ให้บริการขนส่งทางรางต้องกำหนดขั้นตอนในการตอบสนองต่อการแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ เพื่อแบ่งปันหรือเผยแพร่ข้อมูลการแจ้งเตือนความมั่นคงปลอดภัยไซเบอร์ให้สมาชิกในกลุ่ม ทราบถึงช่องโหว่ การใช้ประโยชน์ และปัญหาด้านความมั่นคงปลอดภัยอื่น ๆ ที่เกิดขึ้นใหม่ ข้อมูลที่มักปรากฏในการแจ้งเตือนด้านความมั่นคงปลอดภัยไซเบอร์ เช่น การแจ้งเตือนของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติและแถลงการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ และจัดทำรายงาน ซึ่งประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- ภาพรวมโดยย่อ/บทสรุปสำหรับผู้บริหารและคำอธิบายโดยละเอียด ซึ่งจะรวมถึงสิ่งบอกเหตุการณ์ต่าง ๆ
- แพลตฟอร์มที่ได้รับผลกระทบ (เช่น ระบบปฏิบัติการ แอปพลิเคชัน ฮาร์ดแวร์)
- ผลกระทบ (เช่น ระบบล่ม การขโมยข้อมูล การปล้นแอปพลิเคชัน)
- การจัดระดับความรุนแรง (เช่น Common Vulnerability Scoring System (CVSS))
- ตัวเลือกวิธีการลดผลกระทบ รวมถึงการแก้ไขถาวรหรือวิธีแก้ปัญหาชั่วคราว
- การอ้างอิงสำหรับข้อมูลเพิ่มเติม
- คำอธิบายรายละเอียดของข้อมูลการแจ้งเตือน (Alert Metadata) เช่น วันที่สร้าง และวันที่แก้ไขการแจ้งเตือน การรับทราบ

๕. กำหนดให้มีการจัดเก็บข้อมูลภัยคุกคามทางไซเบอร์ และจัดทำเป็นระเบียบฐานความรู้ โดยระบุข้อมูลดังนี้

- แหล่งที่มาของภัยคุกคามทางไซเบอร์ เช่น แหล่งเก็บข้อมูลแบบเปิด (Open Source) และหน่วยงานพันธมิตร
- กฎที่ควบคุมการใช้หรือการแบ่งปันสิ่งบอกเหตุการณ์

- วันที่หรือเวลาที่มีการรวบรวมสิ่งบอกเหตุการณ์
- ระยะเวลาที่ยังคงถือว่าสิ่งบอกเหตุการณ์ความถูกต้อง
- หน่วยงานหรือภาคส่วนที่เป็นเป้าหมายของการโจมตีที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- ช่องโหว่ด้านความมั่นคงปลอดภัยไซเบอร์ (Common Vulnerability Enumeration: CVE), แพลตฟอร์มฮาร์ดแวร์ ซอฟต์แวร์ และเฟิร์มแวร์ (Common Platform Enumeration: CPE), จุดอ่อนของซอฟต์แวร์หรือระบบคอมพิวเตอร์ (Common Weakness Enumeration: CWE), การตั้งค่า (Common Configuration Enumeration: CCE) ที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- กลุ่มหรือผู้คุกคามที่เกี่ยวข้องกับสิ่งบอกเหตุการณ์
- นามแฝงของผู้คุกคามที่เกี่ยวข้อง
- TTPs ที่ผู้คุกคามใช้กันทั่วไป
- แรงจูงใจหรือเจตนาของผู้คุกคามที่เกี่ยวข้อง
- บุคคลหรือประเภทของบุคคลที่ตกเป็นเป้าหมายในการโจมตีที่เกี่ยวข้อง
- ระบบที่เป็นเป้าหมายในการโจมตี

๖. กำหนดให้ระบุระยะเวลาการเก็บรักษาข้อมูล (Retention Requirement) ให้อยู่ในสภาพพร้อมใช้งาน ซึ่งแยกเป็นการจัดเก็บในระยะสั้น (ออนไลน์) และระยะยาว (ออฟไลน์) ในการจัดการและการเก็บรักษาข้อมูลอาจเปลี่ยนแปลงได้เมื่อข้อมูลภัยคุกคามถูกใช้ประกอบหลักฐาน ตัวอย่างเช่น หลักฐานที่ได้มาระหว่างการสืบสวนสอบสวนเหตุการณ์ภัยคุกคามใด ๆ ควรได้รับการรวบรวม และเก็บรักษาไว้โดยใช้แนวทางปฏิบัติที่ดีที่สุดในการเก็บรักษาข้อมูลตามข้อกำหนดของห่วงโซ่การครอบครองวัตถุพยาน (Chain of Custody) และกฎหมายอื่น ๆ ที่เกี่ยวข้องกับการส่งหลักฐาน โดยพิจารณาเทคนิคทางนิติวิทยาศาสตร์ที่เกี่ยวข้องกับห่วงโซ่การครอบครองวัตถุพยานและการรักษา ความสมบูรณ์ของข้อมูล (Preserving Information Integrity)

๗. การจัดทำและเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์ที่หน่วยงานผู้ให้บริการขนส่งทางรางพบและดำเนินการตอบสนองต่อภัยคุกคามนั้น โดยการจัดทำคำอธิบายรายละเอียดของข้อมูลภัยคุกคามทางไซเบอร์ (Metadata) ประกอบด้วยข้อมูลอย่างน้อย ดังนี้ แหล่งที่มา ประเภทข้อมูล เหตุการณ์ สถานะการดำเนินการจัดการ ข้อเสนอแนะการจัดการภัยคุกคาม และการปรับปรุงกฎการแบ่งปันข้อมูล เป็นต้น

ตัวอย่างจัดทำคำอธิบายรายละเอียดของข้อมูลภัยคุกคามทางไซเบอร์ (Metadata)

- การโจมตีแบบกระจายเพื่อให้ระบบปฏิเสธการให้บริการ (Distributed Denial of Service Attacks)
  - วันที่โจมตี(Attack Date)
  - บริการเป้าหมาย (Target Service)
  - เวลาเริ่มการโจมตี(Attack Start)
  - เวลาสิ้นสุดการโจมตี(Attack End)
  - ประเภทการโจมตี(Attack Type)
  - ปริมาณการโจมตี(Attack Volume)

- ผลกระทบจากการโจมตี(Attack Impact)
- สถานะการดำเนินการจัดการ
- ข้อเสนอแนะการจัดการภัยคุกคาม

- การประกาศขอความร่วมมือให้ช่วยกันจู่โจมแบบฟิชชิงหรือสเปียร์ฟิชชิง (Phishing or Spear Phishing Campaigns)
  - คำอธิบายการขอความร่วมมือให้ช่วยกันจู่โจม (Campaign Description)
  - ที่อยู่ผู้ส่ง (Sender Address)
  - ที่อยู่ IP ผู้ส่ง (Sender IP)
  - หัวข้ออีเมล (Email Subject)
  - ไฟล์แนบ/ ชื่อลิงก์/ แฮช (Attachment/ Link Name/ Hash)
  - รายละเอียดข้อมูลในแพ็คเก็ตของการจู่โจม (Payload) และสิ่งบอกเหตุการณ์การโจมตี (Indicators of Compromise: IOCs)
  - สถานะการดำเนินการจัดการ
  - ข้อเสนอแนะการจัดการภัยคุกคาม

๘. กำหนดให้มีการทบทวนกฎระเบียบ ข้อกำหนดของการแบ่งปันข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากปัจจัย ดังนี้

- การเปลี่ยนแปลงข้อกำหนดด้านกฎระเบียบหรือกฎหมาย
- การปรับปรุงนโยบายของหน่วยงาน
- บริบทขององค์กร เช่น โครงสร้างการดำเนินการขององค์กร
- การแนะนำแหล่งข้อมูลใหม่ ๆ
- การเปลี่ยนแปลงด้านการยอมรับความเสี่ยง
- การเปลี่ยนแปลงด้านกรรมสิทธิของข้อมูล
- การเปลี่ยนแปลงสภาพแวดล้อมของการดำเนินงาน
- การเปลี่ยนแปลงของภัยคุกคาม
- การควบรวม หรือการปรับเปลี่ยนของหน่วยงาน

ทั้งนี้ ในกรณีที่ สกมช. มีการประกาศกำหนดหลักเกณฑ์และวิธีการ แนวทางและรูปแบบในการแบ่งปันข้อมูล เพื่อความเป็นมาตรฐานในการปฏิบัติงาน และสามารถใช้ข้อมูลได้อย่างมีประสิทธิภาพ ให้ดำเนินการตามประกาศกำหนดนั้น

๙. กำหนดให้มีการให้ความรู้ความเข้าใจผู้รับผิดชอบในการแบ่งปันข้อมูล ให้สามารถดำเนินการตามแนวทางการแบ่งปันข้อมูลอย่างปลอดภัยอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

(P) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

แนวปฏิบัติที่ต้องดำเนินการตามกฎหมาย

๑. กำหนดให้มีการจัดทำแผนบริหารความต่อเนื่อง (BCP) เป็นกรอบการบริหารความต่อเนื่อง โดยใช้โมเดลวางแผน-ดำเนินการ-ตรวจสอบ-ปรับปรุง (Plan-Do-Check-Act Model) เพื่อการวางแผน การจัดทำ การดำเนินการ การติดตาม การทบทวน และการปรับปรุง ประสิทธิผลของแผนความต่อเนื่อง ดังนี้

(๑) ขั้นตอนการวางแผน (Plan) พิจารณาดำเนินการตามรายละเอียด ดังนี้

(๑.๑) ทำความเข้าใจบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงระบุประเด็นภายนอกและภายในที่อาจส่งผลกระทบต่อความสามารถในการดำเนินงานตามพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางรางอย่างต่อเนื่อง โดยพิจารณาจากประเด็นเหล่านี้

- วัตถุประสงค์ เป้าหมาย พันธกิจ และหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง
- การให้บริการของหน่วยงานผู้ให้บริการขนส่งทางราง
- จำนวนและประเภทของความเสี่ยงของหน่วยงานผู้ให้บริการขนส่งทางราง
- ความต้องการ และความคาดหวังของผู้ที่มีส่วนเกี่ยวข้องกับการบริหารความต่อเนื่อง
- กฎหมายและระเบียบที่หน่วยงานต้องปฏิบัติตาม

(๑.๒) หลังจากที่ดำเนินการวิเคราะห์บริบทของหน่วยงานผู้ให้บริการขนส่งทางรางเรียบร้อยแล้ว ให้ดำเนินการกำหนดขอบเขตของการดำเนินงานด้านความต่อเนื่อง และบันทึกขอบเขตในแผนบริหารความต่อเนื่อง โดยขอบเขตอาจระบุถึง

- ส่วนของหน่วยงานที่อยู่ในแผนบริหารความต่อเนื่อง รวมถึงระบุสถานที่ ขนาด ความซับซ้อนของการดำเนินการ เป็นต้น
- กระบวนการหรือบริการที่อยู่ในขอบเขตของการดำเนินการตามแผนบริหารความต่อเนื่อง

(๑.๓) กำหนดบทบาทของผู้บริหารที่ได้รับการแต่งตั้งหรือมอบหมายให้ดำเนินการด้านความต่อเนื่องจะประสบความสำเร็จได้ ซึ่งประกอบด้วยบทบาทหน้าที่อย่างนี้ดังนี้

(๑) กำกับดูแลให้มีการกำหนดนโยบายการจัดการความต่อเนื่อง และกำหนดให้การดำเนินการด้านความต่อเนื่องเป็นส่วนหนึ่งของการบริหารความเสี่ยงแบบองค์รวมขององค์กร รวมถึงจัดทำเป็นลายลักษณ์อักษร และได้รับการพิจารณาอนุมัติจากผู้บริหารระดับสูง

(๒) พิจารณาจัดสรรทรัพยากรที่พอเพียงต่อการดำเนินงานด้านความต่อเนื่อง

(๓) สื่อสารให้บุคลากรในหน่วยงานผู้ให้บริการขนส่งทางรางทุกคนตระหนักถึงความสำคัญของการดำเนินงานด้านความต่อเนื่องให้มีประสิทธิภาพ

(๔) ส่งเสริมให้มีการปรับปรุงการดำเนินงานตามแผนบริหารความต่อเนื่องอย่างสม่ำเสมอ

(๑.๔) ผู้บริหารระดับสูง หรือผู้ได้รับมอบหมายดำเนินการจัดทำนโยบายความต่อเนื่องที่เหมาะสมกับวัตถุประสงค์ของหน่วยงานผู้ให้บริการขนส่งทางรางและวัตถุประสงค์ในการบริหาร

ความต่อเนื่อง รวมถึงข้อกำหนดต่าง ๆ ที่เกิดจากการวิเคราะห์บริบทของหน่วยงานผู้ให้บริการขนส่งทางราง พร้อมทั้งจำให้อยู่ในรูปแบบที่เป็นเอกสาร และสื่อสารให้บุคลากรรับทราบ และพร้อมสำหรับการนำไปปฏิบัติ

(๑.๕) กำหนดบทบาทและความรับผิดชอบทีมตอบสนองต่อภัยคุกคาม เช่น ทีมเจ้าหน้าที่ความมั่นคงปลอดภัยไซเบอร์ ทีมสนับสนุนด้านเทคโนโลยีสารสนเทศ ทีมงานปฏิบัติการ (Operation Team) ทีมกฎหมาย และทีมสื่อสารประชาสัมพันธ์ โดยผู้บริหารระดับสูงดำเนินการมอบหมายความรับผิดชอบและอำนาจหน้าที่ให้แก่บุคลากรที่ได้รับการแต่งตั้ง และสื่อสารบทบาทหน้าที่ให้ผู้ปฏิบัติงาน และผู้ได้รับมอบหมายรับทราบปฏิบัติ

(๑.๖) ผู้บริหารระดับสูงดำเนินการแต่งตั้งคณะกรรมการบริหารความต่อเนื่อง ซึ่งประกอบด้วย หัวหน้าหน่วยงาน หัวหน้าส่วนงาน ผู้อำนวยการฝ่ายบริหารความเสี่ยง ผู้เชี่ยวชาญเฉพาะด้าน เป็นต้น เพื่อทำหน้าที่ดำเนินการบริหารความต่อเนื่อง ดังนี้

(๑) จัดทำระเบียบวิธีปฏิบัติและกระบวนการในการจัดการความต่อเนื่อง รวมถึงดูแลให้มีการนำไปปฏิบัติอย่างเหมาะสม

(๒) กำกับดูแลให้มีการกำหนดแผนความต่อเนื่องที่ครอบคลุมเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นและควรพิจารณาให้เหมาะสมสอดคล้องกับลักษณะการดำเนินภารกิจของหน่วยงานผู้ให้บริการขนส่งทางรางความซับซ้อนของเทคโนโลยีความเสี่ยงที่เกี่ยวข้อง และภัยคุกคามทางไซเบอร์ที่อาจจะเกิดขึ้น

(๓) พิจารณาขอบเขต ลักษณะวิกฤตการณ์และประเมินสถานการณ์ที่เกิดขึ้น

(๔) พิจารณาประกาศใช้แผนบริหารความต่อเนื่อง และดำเนินการแก้ไขเหตุการณ์ด้านความต่อเนื่องจนกว่าจะเข้าสู่สถานการณ์ปกติ

(๕) แต่งตั้งคณะทำงานย่อยเพื่อสนับสนุนการดำเนินงานได้ความความเหมาะสมและจำเป็น เช่น ทีมจัดการเหตุขัดข้อง ทีมกอบกู้ทรัพยากร

(๖) กำกับดูแลสนับสนุนและติดตามผลการใช้แผนบริหารความต่อเนื่อง เช่น

- ผลการจัดการความต่อเนื่องที่ครอบคลุมเหตุภัยคุกคามทางไซเบอร์
- ผลการทดสอบแผนบริหารความต่อเนื่อง
- ข้อมูลหรือปัญหาที่เกี่ยวข้องกับปัญหาหรือเหตุการณ์ที่ทำให้การดำเนินงานหยุดชะงัก รวมถึงภัยคุกคามทางไซเบอร์ที่เกิดขึ้น

(๗) กำหนดให้มีการฝึกซ้อมแผนบริหารความต่อเนื่อง และนำผลการซ้อมมาทบทวนนโยบาย ระเบียบวิธีปฏิบัติ การดำเนินงาน และแผนบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง ตามปีปฏิทิน

(๘) กำกับดูแลให้มีการจัดอบรมให้ความรู้แก่คณะกรรมการบริษัท ผู้บริหาร และบุคลากรที่ทำหน้าที่ ปฏิบัติงานตามแผนการบริหารความต่อเนื่องอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มีความรู้ความเข้าใจ และทักษะที่เพียงพอต่อการกำกับดูแล หรือปฏิบัติงาน

(๙) รายงานผลการปฏิบัติงานต่อผู้บริหารระดับสูง

(๑.๗) การวางแผนเพื่อการจัดทำแผนบริหารความต่อเนื่อง

(๑) กำหนดให้มีการพิจารณาผลการประเมินความเสี่ยงที่เกี่ยวข้องกับการวิเคราะห์บริบทของหน่วยงานผู้ให้บริการขนส่งทางราง และความต้องการของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งภายในและภายนอกมาประกอบการวางแผนการบริหารความต่อเนื่อง

(๒) การกำหนดวัตถุประสงค์ความต่อเนื่อง (Business Continuity Objectives) หน่วยงานควรกำหนดวัตถุประสงค์ความต่อเนื่อง (Business Continuity Objectives) ที่มีความสอดคล้องกับนโยบายความต่อเนื่อง รวมถึงสามารถวัดความสำเร็จของวัตถุประสงค์ได้ และตอบสนองต่อผลการวิเคราะห์บริบทของหน่วยงานผู้ให้บริการขนส่งทางราง และความต้องการของผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องทั้งภายในและภายนอก พร้อมทั้งกำหนดให้มีการบันทึกวัตถุประสงค์เป็นลายลักษณ์อักษร เพื่อใช้สื่อสารไปยังบุคลากรที่เกี่ยวข้อง และติดตามการดำเนินงาน ทั้งนี้ วัตถุประสงค์ควรมีเนื้อหาต่อไปนี้

ก) สิ่งที่ต้องทำ

ข) ทรัพยากรที่จำเป็น

ค) ผู้รับผิดชอบ

ง) กำหนดการที่ต้องทำให้เสร็จ

จ) วิธีการประเมินผลลัพธ์ของวัตถุประสงค์ที่กำหนดขึ้น

(๓) กำหนดให้มีการวางแผนสำหรับการเปลี่ยนแปลงการดำเนินการตามแผนการบริหารความต่อเนื่อง โดยต้องมีการวางแผนสำหรับการเปลี่ยนแปลง โดยพิจารณาหัวข้อ ดังนี้

ก) วัตถุประสงค์ของการเปลี่ยนแปลงและผลที่อาจเกิดตามมา

ข) ความสมบูรณ์ของการดำเนินงานตามแผนบริหารความต่อเนื่อง

ค) ความพร้อมของทรัพยากร

ง) การจัดสรรอำนาจหน้าที่และความรับผิดชอบ

(๑.๘) กำหนดให้มีวางแผน และจัดเตรียมทรัพยากรและกลไกสนับสนุนที่จำเป็น เพื่อให้บรรลุวัตถุประสงค์ในการบริหารความต่อเนื่อง รวมถึงการจัดเตรียมบุคลากรให้มีความรู้ และความตระหนักในการดำเนินการตามแผนบริหารความต่อเนื่อง

(๒) ขั้นตอนการดำเนินงาน (Do) เพื่อควบคุมให้เป็นไปตามแผนบริหารความต่อเนื่องและมีประสิทธิภาพ ควรพิจารณาดำเนินการ ดังนี้

(๒.๑) กำหนดให้ผู้ที่เกี่ยวข้องในการบริหารจัดการความต่อเนื่องปฏิบัติตามแผนการดำเนินการที่ได้วางไว้ และควบคุมกระบวนการที่จำเป็นต่อการบริหารความต่อเนื่อง เพื่อให้เป็นไปตามข้อกำหนด และสามารถบริหารจัดการความเสี่ยงที่อาจเกิดขึ้นควรกำหนดข้อมูลเพื่อให้การดำเนินการมีประสิทธิภาพอย่างน้อยดังนี้

ก) ข้อมูลและเวลาที่ต้องใช้สำหรับการดำเนินการบริหารจัดการความต่อเนื่องในแต่ละกระบวนการที่สำคัญ

ข) วิธีควบคุมกระบวนการที่สำคัญให้ได้ตามกำหนดเวลาของแต่ละกระบวนการ

ค) การเก็บรักษาเอกสารสารสนเทศตามขอบเขต เพื่อให้มั่นใจว่ากระบวนการต่าง ๆ ได้ดำเนินการตามแผนที่วางไว้

ง) ควบคุมการเปลี่ยนแปลงตามแผนบริหารความต่อเนื่อง และทบทวนผลที่ตามมาจากการเปลี่ยนแปลงที่ไม่คาดหมาย เพื่อเป็นการลดผลกระทบที่ไม่พึงประสงค์ใด ๆ

(๒.๒) ในกรณีที่มีการใช้บริการของผู้ให้บริการภายนอก ต้องดำเนินการให้มั่นใจว่ากระบวนการที่ดำเนินการโดยผู้ให้บริการภายนอก และห่วงโซ่อุปทานได้รับการควบคุม เช่น การสอบทานแผนบริหารความต่อเนื่องของผู้ให้บริการภายนอกที่เกี่ยวข้องกับการบริหารความต่อเนื่อง เพื่อพิจารณาความสอดคล้องกับแผนความต่อเนื่องของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งควรพิจารณาอย่างน้อย ดังนี้

ก) สอบทานความสอดคล้องกันของขอบเขต และคำนิยาม

ข) สอบทานการกำหนดระยะเวลาที่สำคัญ เช่น ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime: MTD) ระยะเวลาในการกู้คืนระบบ (Recovery Time Objective: RTO) และระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective: RPO)

(๒.๓) กำหนดให้มีการวิเคราะห์ผลกระทบต่อการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง (Business Impact Analysis: BIA) ซึ่งการวิเคราะห์ผลกระทบต่อการดำเนินการตามภารกิจหน้าที่ของ หน่วยงานผู้ให้บริการขนส่งทางราง (Business Impact Analysis: BIA) ช่วยให้หน่วยงานผู้ให้บริการขนส่งทางราง สามารถระบุลักษณะต่าง ๆ ของส่วนประกอบของระบบสารสนเทศ รวมทั้งภารกิจ หรือการดำเนินงานสำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางได้รับสนับสนุนจากระบบสารสนเทศ รวมถึงการพึ่งพาซึ่งกันและกันของระบบสารสนเทศและการดำเนินงานต่าง ๆ ของหน่วยงานผู้ให้บริการขนส่งทางราง

(๒.๔) การกำหนดกลยุทธ์ในการบริหารความต่อเนื่อง โดยนำผลลัพธ์จากการวิเคราะห์ผลกระทบต่อการดำเนินการตามภารกิจหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง (Business Impact Analysis: BIA) และการประเมินความเสี่ยงของหน่วยงานผู้ให้บริการขนส่งทางรางมาดำเนินการกำหนดกลยุทธ์ในการบริหารความต่อเนื่อง ให้ครอบคลุมการดำเนินการก่อน ระหว่าง และหลังการหยุดชะงักที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ซึ่งกลยุทธ์ในการบริหารความต่อเนื่อง มีการพิจารณาในประเด็นดังต่อนี้

ก) กลยุทธ์เป็นไปตามข้อกำหนดด้านเวลาและทรัพยากรที่ต้องใช้ในการกู้ระบบเพื่อแก้ไขเหตุการณ์ ตามแผนการบริหารความต่อเนื่อง เช่น ข้อกำหนดด้านระยะเวลาสูงสุดที่ยอมให้การดำเนินการของ หน่วยงานผู้ให้บริการขนส่งทางรางหยุดชะงัก เพื่อให้หน่วยงานผู้ให้บริการขนส่งทางรางสามารถดำเนินการได้อย่างต่อเนื่อง และสามารถฟื้นฟูบริการที่สำคัญให้อยู่ในสภาพพร้อมใช้งานได้ในระดับที่กำหนดภายในกรอบระยะเวลาที่กำหนด

ข) กลยุทธ์ที่สามารถการปกป้องการดำเนินงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง ให้สามารถดำเนินการได้ เช่น การกำหนดให้มีพื้นที่สำรองในการดำเนินงานที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง ในกรณีเกิดเหตุที่พื้นที่ให้บริการหลัก เป็นต้น

ค) กลยุทธ์ที่สามารถลดโอกาสที่จะเกิดการหยุดชะงักได้ เช่น การกำหนดให้มีระบบเครือข่ายสำรอง เพื่อป้องกันการหยุดชะงักในการให้บริการ เป็นต้น

ง) กลยุทธ์ที่สามารถลดระยะเวลาของการหยุดชะงัก เช่น กลยุทธ์ในการย้ายการทำงานไปที่ระบบสำรอง เป็นต้น

จ) กลยุทธ์ที่สามารถจำกัดผลกระทบของการหยุดชะงัก เช่น กลยุทธ์ในการสื่อสารและสร้างความสัมพันธ์กับผู้มีส่วนได้ส่วนเสียอยู่เสมอ เพื่อช่วยจำกัดผลกระทบของการหยุดชะงักที่มีต่อผู้รับบริการ เป็นต้น

ฉ) กลยุทธ์ที่สามารถรักษาทรัพยากรให้อยู่ในสภาพพร้อมใช้งานได้อย่างเพียงพอ เช่น การกำหนดให้มีเครื่องคอมพิวเตอร์สำรอง การเก็บข้อมูลสำคัญไว้ที่ศูนย์ข้อมูลสำรอง เป็นต้น

ช) กลยุทธ์ในการบริหารจัดการทรัพยากร โดยระบุความต้องการด้านทรัพยากรที่ต้องใช้ดำเนินการแก้ไขปัญหาด้านความต่อเนื่อง เช่น ทรัพยากรบุคคล ข้อมูล โครงสร้าง พื้นฐานทางกายภาพ เช่น อาคาร สถานที่ทำงาน หรือสิ่งอำนวยความสะดวกอื่น ๆ และระบบสาธารณูปโภคที่เกี่ยวข้อง อุปกรณ์และวัสดุสิ้นเปลือง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร การขนส่งและโลจิสติกส์ การเงิน และผู้ให้บริการภายนอก เป็นต้น

(๒.๕) การจัดทำแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP) ควรมีรายละเอียดอย่างน้อย ดังนี้

ก) ขอบเขต และวัตถุประสงค์ของแผนบริหารความต่อเนื่อง (Business Continuity Plan: BCP)

ข) ขั้นตอนการปฏิบัติงานและผู้รับผิดชอบการดำเนินการบริหารความต่อเนื่อง รวมถึงกำหนดหน้าที่และความรับผิดชอบของผู้ปฏิบัติงานแต่ละรายอย่างชัดเจน และจัดให้มีการสื่อสาร และซักซ้อมความเข้าใจถึงหน้าที่ที่ต้องปฏิบัติ ตลอดจนกำหนดรายละเอียดวิธีปฏิบัติงานที่สามารถเข้าใจและปฏิบัติตามได้

ค) ข้อมูลสนับสนุนที่จำเป็นต้องใช้ สำหรับการเรียกใช้งานแผนบริหารความต่อเนื่อง เช่น เกณฑ์และสิทธิ์การเรียกใช้งาน เป็นต้น

ง) ข้อมูลการพึ่งพา (Dependencies) เช่น ข้อมูลหน่วยงานภายนอก หรือผู้ให้บริการภายนอก รวมถึงข้อมูลการพึ่งพาซึ่งกันและกันของการดำเนินงานหรือบริการต่าง ๆ

จ) จัดให้มีทรัพยากรที่จำเป็นสำหรับการปฏิบัติงาน การสื่อสาร และการรายงาน เช่น การจัดหาหรือกำหนดบุคลากรที่จะปฏิบัติงานแทนทั้งระดับ พนักงานและผู้บริหาร แหล่งเงินทุน อุปกรณ์สำนักงาน คอมพิวเตอร์ เครื่องใช้สำนักงาน ระบบเทคโนโลยีสารสนเทศ เป็นต้น หรืออาจพิจารณาจัดตั้งศูนย์ปฏิบัติงานสำรอง (Alternate Site) เพื่อป้องกันผลกระทบจากเหตุฉุกเฉินที่เกิดขึ้นในบริเวณกว้าง

ฉ) กำหนดแนวทางในการสำรองข้อมูล (Backup System) เพื่อทำให้สามารถกู้คืนข้อมูลได้อย่างถูกต้องและรวดเร็ว โดยต้องมีความสอดคล้องกับระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objectives: RPO) โดยต้องกำหนดความถี่ในการสำรองข้อมูลให้เป็นไปตามนโยบายและแผนการบริหารความต่อเนื่องที่กำหนดขึ้น

ช) การกำหนดผู้ที่มีอำนาจตัดสินใจหรืออนุมัติประกาศใช้แผนบริหารความต่อเนื่อง ซึ่งทำหน้าที่ ตัดสินใจหรืออนุมัติประกาศใช้แผนบริหารความต่อเนื่อง ซึ่งควรเป็นคณะกรรมการ หรือผู้บริหารระดับสูง หรือเป็นผู้ที่ได้รับมอบอำนาจจากคณะกรรมการหรือผู้บริหารระดับสูงให้ปฏิบัติหน้าที่แทน

(๒.๖) กำหนดให้มีการดำเนินการซ้อมแผนบริหารความต่อเนื่อง อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ เพื่อตรวจสอบความถูกต้อง พร้อมทั้ง จับเวลาในการดำเนินการตามแผนบริหารความต่อเนื่อง เพื่อวัดประสิทธิผลของกลยุทธ์ที่กำหนดซึ่งการดำเนินการฝึกซ้อมแผนบริหารความต่อเนื่อง ควรมีการพิจารณา ดังนี้

ก) ความสอดคล้องกับวัตถุประสงค์ตามแผนการบริหารความต่อเนื่องที่กำหนดขึ้น

ข) กำหนดวิธีการฝึกซ้อมที่เหมาะสม มีเป้าหมายและวัตถุประสงค์ที่ชัดเจน เช่น หากใช้วิธีการฝึกซ้อมด้วยวิธีการแบบอิงการอภิปราย (Discussion-based Exercises) ต้องกำหนดสถานการณ์ (Scenarios) ที่เหมาะสม โดยจำลองจากสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นจริง ซึ่งอิงจากโครงสร้างพื้นฐานของ หน่วยงานผู้ให้บริการขนส่งทางราง เช่น อาคาร วัสดุอุปกรณ์ ระบบสารสนเทศต่าง ๆ และพิจารณานำช่องโหว่ที่อาจเป็นสาเหตุทำให้เกิดสถานการณ์ ฉุกเฉินมากำหนดเป็นสถานการณ์จำลอง และกำหนดบทบาทของมีผู้ที่มีส่วนเกี่ยวข้อง เพื่อเข้าร่วมฝึกซ้อม รวมถึงการเขียนบทสถานการณ์ต้องทำให้ผู้เข้าร่วมฝึกซ้อมได้ปฏิบัติการตอบโต้กับสถานการณ์ได้ฝึกตัดสินใจ ตอบสนองต่อเหตุการณ์ ซึ่งโจทย์สถานการณ์ต้องสามารถเชื่อมโยงกับการปฏิบัติของผู้เข้าร่วมฝึกในแต่ละบทบาท เป็นต้น

ค) การตรวจสอบประสิทธิภาพของกลยุทธ์และแนวทางแก้ไขตามแผนบริหารความต่อเนื่อง

จ) กำหนดให้มีการจัดทำรายงานหลังการฝึกอย่างเป็นทางการ ซึ่งประกอบด้วยผลลัพธ์ คำแนะนำ และการดำเนินการปรับปรุง

(๓) ขั้นตอนการติดตามและทบทวน (Check) เพื่อดำเนินการติดตามและทบทวนผลการปฏิบัติงานตามนโยบายและวัตถุประสงค์ในการบริหารความต่อเนื่อง และกำหนดให้มีการรายงานผลให้ฝ่ายบริหารทบทวน เพื่อกำหนด และอนุมัติการดำเนินการเพื่อแก้ไขและปรับปรุง รวมถึงต้องกำหนดให้มีการเก็บรักษาเอกสารรายงานผลการวิเคราะห์และประเมินผลการดำเนินการตามแผนบริหารความต่อเนื่อง ซึ่งควรพิจารณาให้มีการดำเนินการติดตาม และทบทวนอย่างน้อย ดังนี้

๑) กำหนดกระบวนการที่ต้องติดตามและวัดผลการดำเนินการตามแผนบริหารความต่อเนื่อง

๒) กำหนดวิธีการติดตาม การวัด การวิเคราะห์ และการประเมินผล ตามความเหมาะสม เช่น การจับเวลาขณะซ้อมแผน รวมถึงการจับเวลาการกู้คืนระบบหรือบริการ เป็นต้น

๓) กำหนดผู้ที่มีหน้าที่รับผิดชอบดำเนินการติดตาม และเก็บผลการดำเนินการ

๔) กำหนดผู้ที่มีหน้าที่รับผิดชอบวิเคราะห์และประเมินผลการติดตาม และกำหนดการการส่งผลการวิเคราะห์ และประเมินผล

(๔) ขั้นตอนการปรับปรุง (Act) ซึ่งเป็นขั้นตอนในการรักษาและปรับปรุงแผนบริหารความต่อเนื่อง โดยดำเนินการแก้ไขตามผลการทบทวนของฝ่ายบริหาร รวมถึงผลการประเมินและทบทวนขอบเขตและวัตถุประสงค์ของแผนบริหารความต่อเนื่อง ซึ่งควรพิจารณาดังนี้

(๔.๑) การดำเนินการปรับปรุง (Improvement)

๑) กำหนดช่วงเวลาสำหรับการดำเนินการปรับปรุงความไม่สอดคล้อง และดำเนินการแก้ไข (Nonconformity and Corrective Action) เมื่อเกิดสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง ซึ่งการกำหนดช่วงเวลาในการปรับปรุงหรือแก้ไขต้องเหมาะสมกับผลกระทบที่เกิดขึ้น ซึ่งควรพิจารณาให้มีการดำเนินการดังนี้

ก) ตอบสนองต่อสิ่งไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง โดยจัดให้มีการดำเนินการควบคุมและแก้ไข พร้อมทั้งจัดการกับผลที่ตามมา

ข) ประเมินความจำเป็นในการดำเนินการ เพื่อกำจัดสาเหตุที่แท้จริง (Root Cause) ของสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อไม่ให้เกิดขึ้นซ้ำ หรือไม่ให้เกิดขึ้นที่อื่น โดยหาสาเหตุ และพิจารณาว่ามีสิ่งที่ไม่เป็นไปตามข้อกำหนดที่คล้ายกันอาจเกิดขึ้นที่ใดได้อีก

ค) ทบทวนประสิทธิผลของการดำเนินการแก้ไขที่ได้ดำเนินการเรียบร้อยแล้ว

ง) หากมีความจำเป็น ต้องดำเนินการเปลี่ยนแปลงวิธีปฏิบัติหรือขั้นตอนการดำเนินการในการบริหารความต่อเนื่อง ต้องเก็บรักษาเอกสารข้อมูลที่ระบุรายละเอียดของสิ่งที่ไม่เป็นไปตามแผนการบริหารความต่อเนื่อง วัตถุประสงค์ในการบริหารความต่อเนื่อง หรือบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง รวมถึงการดำเนินการแก้ไข และผลลัพธ์ของการดำเนินการแก้ไขนั้น ๆ ไว้เพื่อเป็นหลักฐาน

(๔.๒) กำหนดให้มีการปรับปรุงอย่างต่อเนื่อง (Continual Improvement) เหมาะสมกับบริบทของหน่วยงานผู้ให้บริการขนส่งทางราง และปรับปรุงประสิทธิผลของการดำเนินงานตามแผนบริหารความต่อเนื่อง ทั้งเชิงคุณภาพและเชิงปริมาณ หลังจากพิจารณาผลการวิเคราะห์และการประเมินผล รวมถึงผลจากการทบทวนของผู้บริหาร

๒. กำหนดให้มีการวิเคราะห์ภัยคุกคาม หรืออันตรายที่จะเกิดต่อการดำเนินงานที่สำคัญต่อพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางราง โดยแยกกระบวนการดำเนินการพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางราง โดยดำเนินการวิเคราะห์ผลกระทบในการดำเนินการตามพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางราง (BIA) ซึ่งมี ๕ ขั้นตอน ดังนี้

๑) ระบุกระบวนการดำเนินการตามพันธกิจของหน่วยงานผู้ให้บริการขนส่งทางราง (BIA) โดยคำนึงถึงความสำคัญของกระบวนการ หรือบริการที่มีต่อบริการตามพันธกิจ และหน้าที่ของหน่วยงานผู้ให้บริการขนส่งทางราง เช่น (๑) บริการที่เกี่ยวข้องกับการควบคุมการเดินรถจากศูนย์กลาง (๒) บริการที่เกี่ยวข้องกับการส่งสัญญาณ การสื่อสาร และการส่งข้อมูล (๓) บริการขายตั๋วและสำรองที่นั่ง (๔) บริการที่เกี่ยวข้องกับการควบคุม กำกับดูแลและเก็บข้อมูลเป็นต้น

๒) พิจารณาผลกระทบจากการหยุดชะงักของกระบวนการหรือบริการที่สำคัญ

๓) กำหนดระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก (Maximum Tolerable Downtime) โดยระยะเวลาดังกล่าว ควรเป็นเวลาสูงสุดที่หน่วยงานที่เกี่ยวข้องกับกระบวนการในหน่วยงานผู้ให้บริการขนส่งทางราง สามารถยอมให้ระบบ หรือกระบวนการหยุดชะงักภายใต้เงื่อนไขที่ต้องดำเนินการตามภารกิจหรือการให้บริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางรางให้สามารถดำเนินการต่อไปได้

๔) กำหนดทรัพยากรของระบบที่จำเป็นต้องกู้คืนระบบ หรือกระบวนการที่จำเป็น เช่น สถานที่, บุคลากร, อุปกรณ์, ซอฟต์แวร์ ไฟล์ข้อมูลของระบบสารสนเทศ ส่วนประกอบของระบบ และเอกสารบันทึกข้อมูลสำคัญต่าง ๆ ที่เกี่ยวข้อง เพื่อให้หน่วยงานสามารถกลับมาดำเนินการหรือให้บริการที่สำคัญให้ได้ให้เร็วที่สุด

๕) ดำเนินการเชื่อมโยงทรัพยากรที่จำเป็นต่อการกู้คืนระบบกับกระบวนการ หรือบริการที่สำคัญของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อกำหนดระดับความสำคัญของทรัพยากร และเรียงลำดับการดำเนินการกู้คืนระบบ

แนวปฏิบัติสำหรับเป็นทางเลือกในการพิจารณาดำเนินการเพิ่มเติม (Option)

๑. กำหนดให้มีการจัดทำแนวปฏิบัติการบริหารจัดการสำรองข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) จัดทำแนวปฏิบัติการบริหารจัดการสำรองข้อมูล (Backup Policy) และแผนการดำเนินการสำรองข้อมูล (Backup Plan)

๒) กำหนดประเภทของข้อมูลที่ต้องสำรอง เช่น ข้อมูลสำคัญ (Critical Data), ข้อมูลส่วนบุคคล, ข้อมูลทางการเงิน เป็นต้น

๓) กำหนดความถี่ในการสำรองข้อมูล เช่น รายวัน รายสัปดาห์ หรือรายเดือน ตามระดับความสำคัญของข้อมูล (Backup Frequency)

๔) กำหนดพื้นที่การสำรองข้อมูล เช่น External Storage หรือ Cloud Backup เป็นต้น

๕) พิจารณาการสำรองข้อมูลแบบต่าง ๆ ตามความเหมาะสม เช่น สำรองข้อมูลทั้งหมด (Full Backup) สำรองเฉพาะข้อมูลที่เปลี่ยนแปลงตั้งแต่ครั้งล่าสุด (Incremental Backup) หรือสำรองข้อมูลที่เปลี่ยนแปลงตั้งแต่ Full Backup ครั้งล่าสุด (Differential Backup)

๒. กำหนดให้มีมาตรการด้านความปลอดภัยของข้อมูลสำรอง โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) เข้ารหัสข้อมูลสำรอง (Backup Encryption) ทั้งขณะจัดเก็บ (At Rest) และขณะส่งข้อมูล (In Transit)

๒) กำหนดสิทธิ์การเข้าถึงข้อมูลสำรองเฉพาะผู้มีอำนาจเท่านั้น (Access Control)

๓) จัดเก็บข้อมูลสำรองในสถานที่ปลอดภัย และพิจารณาการเก็บข้อมูลสำรองนอกสถานที่ (Offsite Backup) หรือในระบบ Cloud ที่มีมาตรฐานความปลอดภัยสูง

๔) ตั้งค่าการเก็บรักษาข้อมูล (Retention Policy) ให้สอดคล้องกับข้อกำหนดทางกฎหมายและนโยบายขององค์กร เช่น เก็บข้อมูลเป็นระยะเวลา ๕ ปี หรือ ๑๐ ปี เป็นต้น

๓. กำหนดให้มีการทดสอบและการกู้คืนข้อมูล โดยคำนึงถึงการพิจารณาอย่างน้อย ดังนี้

๑) กำหนดแผนการกู้คืนข้อมูล (Data Recovery Plan) ให้สอดคล้องกับแผนความต่อเนื่องทางธุรกิจ (BCP)

๒) ดำเนินการทดสอบการกู้คืนข้อมูล (Backup Restoration Test) อย่างสม่ำเสมอ เช่น ไตรมาสละ ๑ ครั้ง หรืออย่างน้อยปีละ ๑ ครั้ง

๓) บันทึกผลการทดสอบการกู้คืนข้อมูลเพื่อใช้ในการปรับปรุงกระบวนการ

กรณีตัวอย่าง

(กรณีที่ ๑) เมื่อเกิดเหตุการณ์ที่มีการบุกรุกจากภายนอก โดยประเมินแล้ว เหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืน ดังนี้

(๑) ตรวจสอบ log และการตั้งค่า Firewall เพื่อวิเคราะห์หาสาเหตุการเข้ามาและผลกระทบที่เกิดขึ้น

(๒) แจ้งให้ฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายรับทราบ

(๓) ดำเนินการการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ถูกบุกรุกเข้ามา

(กรณีที่ ๒) เมื่อเกิดเหตุการณ์ที่มีการมีการแพร่กระจายของไวรัส (Virus) มัลแวร์ (Malware) มัลแวร์เรียกค่าไถ่ หรือแรนซัมแวร์ (Ransomware) โดยประเมินแล้วเหตุการณ์มีผลกระทบต่อความมั่นคงปลอดภัยสารสนเทศ ให้ดำเนินการตามแผนกู้คืนดังนี้

(๑) ตัดการเชื่อมต่อทางเครือข่าย สำหรับเครื่องคอมพิวเตอร์ที่โดนมัลแวร์ (Malware) ระบบสำรองข้อมูล รวมถึงตัดการเชื่อมต่ออุปกรณ์จัดเก็บข้อมูลภายนอก และระบบสารสนเทศที่อยู่ในเครือข่ายเดียวกัน

(๒) แจ้งให้ฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายรับทราบ

(๓) ตรวจสอบเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่ายเดียวกับเครื่องที่ติดมัลแวร์ (Malware) เพื่อประเมินสถานการณ์ด้วยวิธีการดังนี้

- ตรวจสอบความผิดปกติภายในเครื่องคอมพิวเตอร์
- Full Scan ใน Anti-Virus และ Anti-Malware

(๔) ประสานเพื่อขอความช่วยเหลือไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เบอร์ติดต่อ ๐๒-๑๔๒๖๘๘๘ และศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ThaiCERT) ผ่านทางโทรศัพท์ เบอร์ติดต่อ ๐๒-๑๒๓๑๒๑๒

(๕) ปฏิบัติตามคำแนะนำของผู้เชี่ยวชาญ

(๖) กรณีเครื่อง Client ใช้คอมพิวเตอร์สำรอง ข้อมูลที่ถูกสำรองไว้ หรือข้อมูลบน Cloud ในการทำงาน โดยไม่ยุ่งเกี่ยวกับข้อมูลหรือเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ (Malware) จนกว่าการแก้ไขสถานการณ์จะสิ้นสุดลง

(๗) กรณีเครื่อง Server ดำเนินการกู้คืนข้อมูลจากอุปกรณ์ที่ได้ดำเนินการ Backup ไว้

(กรณีที่ ๓) การกลับสู่ภาวะปกติ

(๑) กรณี Client ทำการล้างเครื่องทั้งหมดแบบ Clean format ไม่ให้มีข้อมูลหลงเหลือใน Hard Disk ก่อนทำการลงเครื่องใหม่ ทั้งหมด

(๒) กรณี Server ทำการ Restore Backup Data, Application and Configuration

(๓) ดำเนินการ Test Restore

(๔) ตั้งค่าระบบ เพื่อให้ผู้ใช้งานสามารถใช้เข้าใช้งานได้ตามปกติ

(๕) ทดสอบความพร้อมใช้งานของระบบและความครบถ้วนของข้อมูลที่กู้คืน

(๖) รายงานผลการกู้คืนให้ฝ่ายเทคโนโลยีสารสนเทศ หรือฝ่ายที่ได้รับมอบหมายรับทราบ

๕.๔ การยกเว้น และการจัดหามาตรการทดแทนในการรับมือและปกป้องระบบ และข้อมูลของหน่วยงานผู้ให้บริการขนส่งทางราง

ในกรณีที่หน่วยงานผู้ให้บริการขนส่งทางราง ไม่สามารถปฏิบัติตามมาตรฐาน นโยบาย แนวปฏิบัติ ขั้นตอน หรือมาตรการปกป้องคุ้มครองระบบ และข้อมูลจากภัยคุกคามทางไซเบอร์ที่หน่วยงานผู้ให้บริการขนส่งทางรางได้กำหนดขึ้น เพื่อให้สอดคล้องกับกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการขนส่งทางรางฉบับนี้

ซึ่งการยกเว้นการปฏิบัติตามมาตรการป้องกันภัยไซเบอร์ที่กำหนดไว้ในมาตรฐานขั้นต่ำ หรือแนวทางปฏิบัติที่ ขร. กำหนด จะต้องดำเนินการพิจารณาอนุญาตเป็นรายกรณีเท่านั้น ภายใต้หลักการ ดังนี้

๑) การรักษาความมั่นคงปลอดภัยต้องไม่ลดลง โดยหน่วยงานผู้ให้บริการขนส่งทางราง ต้องแสดงให้เห็นว่ามาตรการทดแทนที่นำมาใช้สามารถรักษาความมั่นคงปลอดภัยเทียบเท่าหรือสูงกว่ามาตรการที่ได้รับการยกเว้น

๒) การยกเว้นต้องเป็นไป เพื่อแก้ไขข้อจำกัดที่จำเป็นทางเทคนิคหรือข้อจำกัดด้านงบประมาณหรือทรัพยากรที่ไม่สามารถหลีกเลี่ยงได้ และมาตรการที่กำหนดเดิมส่งผลกระทบอย่างมีนัยสำคัญต่อการปฏิบัติหน้าที่ หรือการให้บริการภายใต้บริการที่สำคัญ ๔ บริการ ตามกฎหมายกำหนดสำหรับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CII)

๓) การยกเว้นต้องเป็นทางเลือกสุดท้าย ซึ่งหน่วยงานผู้ให้บริการขนส่งทางรางต้องดำเนินการพิจารณาทุกทางเลือกในการปฏิบัติตามมาตรฐานหลักแล้ว แต่ไม่สามารถดำเนินการได้จริง

ทั้งนี้ หน่วยงานผู้ให้บริการขนส่งทางรางต้องจัดให้มีกระบวนการขออนุมัติยกเว้น (Exception) เพื่อประเมินความเสี่ยง และพิจารณาแนวทางควบคุมความเสี่ยงที่เพียงพอและเหมาะสมก่อนดำเนินการ ซึ่งหน่วยงานผู้ให้บริการขนส่งทางรางต้องกำหนดกระบวนการที่ประกอบด้วยเนื้อหาอย่างน้อย ดังนี้

๑. ต้องมีการกำหนดขอบเขตการขอยกเว้น โดยแบ่งประเภท ดังนี้

๑.๑ ข้อจำกัดทางเทคนิค เช่น ระบบเทคโนโลยีสารสนเทศที่ใช้งานมีความเก่า (Legacy System) หรือเป็นเทคโนโลยีเฉพาะที่ไม่รองรับการติดตั้งหรือปรับใช้มาตรการตามมาตรฐานที่กำหนด เช่น ไม่สามารถอัปเดตระบบปฏิบัติการเพื่อรองรับมาตรการควบคุมการเข้าถึงแบบใหม่ได้

๑.๒ ข้อจำกัดด้านงบประมาณ หรือทรัพยากร เช่น การปฏิบัติตามมาตรการนั้น ๆ ต้องใช้งบประมาณหรือทรัพยากรบุคคลผู้เชี่ยวชาญในระดับสูงมาก จนส่งผลกระทบต่อภารกิจหลักของหน่วยงานอย่างมีนัยสำคัญ ซึ่งในส่วนนี้ต้องมีเอกสารยืนยันความพยายามในการจัดหา และดำเนินการ

๑.๓ การมีมาตรการทดแทนที่มีประสิทธิภาพกว่า เช่น หน่วยงานมีมาตรการ หรือวิธีการปฏิบัติงานที่แตกต่างไปจากมาตรฐานที่กำหนด แต่ได้รับการพิสูจน์แล้วว่ามาตรการดังกล่าวมีระดับการป้องกันที่สูงกว่า หรือครอบคลุมความเสี่ยงได้ดีกว่า หรือเทียบเท่ามาตรการมาตรฐานที่ต้องการขอยกเว้นใช้มาตรการอื่นทดแทน

๒. กำหนดให้มีขั้นตอนการยื่นคำขอ และการพิจารณาอนุมัติการของยกเว้น และจัดหามาตรการอื่นทดแทน ประกอบด้วยขั้นตอน ดังนี้

๒.๑ การจัดทำข้อเสนอ โดยหน่วยงาน หรือส่วนงานที่ต้องการยกเว้นต้องจัดทำเอกสารประกอบด้วย

๑) มาตรการที่ต้องการยกเว้น

๒) เหตุผลและข้อจำกัดที่ไม่สามารถปฏิบัติตามได้

๓) กำหนดมาตรการทดแทน (Compensating Control) ที่จะนำมาใช้ และดำเนินการประเมินความเสี่ยง ในกรณีที่ใช้นำมาตรการทดแทนมาใช้งาน เพื่อให้สามารถยืนยันได้ว่ามาตรการทดแทนมีระดับการป้องกันที่เทียบเท่ากันกับมาตรการที่ขอยกเว้น

๔) นำเสนอผู้บริหารระดับสูงที่ทำหน้าที่บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Chief Information Security Officer: CISO) หรือเทียบเท่าที่ปฏิบัติหน้าที่เสมือน CISO ของหน่วยงานผู้ให้บริการขนส่งทางราง เพื่อขออนุมัติการยกเว้น

๕) นำมาตรการทดแทน และการยกเว้นที่ได้รับการอนุมัติสื่อสารให้กับผู้ปฏิบัติงานที่เกี่ยวข้อง และจัดเก็บหลักฐานการอนุมัติ และการกำหนดมาตรการอื่นทดแทนไว้เป็นหลักฐาน

๓. การกำหนดให้มีการทบทวน และตรวจสอบมาตรการทดแทนการจัดทำ

๑) กำหนดให้มีการทบทวนมาตรการทดแทนว่ายังดำเนินการอยู่อย่างมีประสิทธิภาพอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญของระบบ

๒) กำหนดให้มีการตรวจสอบมาตรการทดแทนว่ายังสามารถรักษาความมั่นคงปลอดภัยได้เทียบเท่า หรือข้อจำกัดที่เคยเป็นเหตุผลในการยกเว้นสิ้นสุดลง เช่น มีการอัปเกรดระบบใหม่ การยกเว้นจะถูกยกเลิก และหน่วยงาน หรือส่วนงานต้องปฏิบัติตามมาตรฐานหลักทันที

๓) กำหนดให้ต้องมีการรวบรวมรายละเอียดการยกเว้น และมาตรการทดแทนไว้ในแผนและรายงานการบริหารจัดการความเสี่ยงด้านไซเบอร์ที่ต้องส่งต่อ ขร. และ สกมช. ปีละ ๑ ครั้งตามระยะเวลาที่กฎหมายกำหนดภายในสามสิบวันนับแต่วันที่ดำเนินการแล้วเสร็จ (มาตรา ๕๔)

ภาคผนวก ๑ ตารางหัวข้อในการกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำสำหรับข้อมูลหรือระบบสารสนเทศ

มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับต่ำ			
(A) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)	●		
(B) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)	●		
(C) การจัดการทรัพย์สิน (Asset Management)	●		
(D) การควบคุมการเข้าถึง (Access Control)	●		
(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)	●		
(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)	●		
(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)	●		
(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)	●		
(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)	●		
มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับกลาง			
(A) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)		●	
(B) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)		●	
(C) การจัดการทรัพย์สิน (Asset Management)		●	
(D) การควบคุมการเข้าถึง (Access Control)		●	
(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)		●	
(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)		●	
(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)		●	
(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)		●	

มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศ	ระดับคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ของข้อมูลหรือระบบสารสนเทศ		
	ต่ำ	กลาง	สูง
(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)		●	
(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)		●	
(K) การเชื่อมต่อระยะไกล (Remote Connection)		●	
(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)		●	
มาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ สำหรับข้อมูลหรือระบบสารสนเทศมีคุณลักษณะความมั่นคงปลอดภัยไซเบอร์อยู่ในระดับสูง			
(A) การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Risk Assessment and Risk Management Strategy)			●
(B) แผนการรับมือภัยคุกคามทางไซเบอร์ (Incident Response Plan)			●
(C) การจัดการทรัพย์สิน (Asset Management)			●
(D) การควบคุมการเข้าถึง (Access Control)			●
(E) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)			●
(F) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)			●
(G) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)			●
(H) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)			●
(I) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)			●
(J) แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Audit Plan)			●
(K) การเชื่อมต่อระยะไกล (Remote Connection)			●
(L) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)			●
(M) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)			●
(N) การจัดการผู้ให้บริการภายนอก (Third Party Management)			●
(O) การแบ่งปันข้อมูล (Information Sharing)			●
(P) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)			●

ภาคผนวก ๒ ตัวอย่างรายการตรวจสอบการทบทวนกฎด้านความมั่นคงปลอดภัยไซเบอร์

รายการตรวจสอบการทบทวนกฎด้านความมั่นคงปลอดภัยไซเบอร์			
หมวดหมู่	**รายการตรวจสอบ(Configuration Item)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๑. ธรรมาภิบาลและความรับผิดชอบ (Governance & Accountability)			
๑.๑	นโยบายระบุความสำคัญสูงสุดของความปลอดภัย (Safety) และความพร้อมใช้งาน (Availability) ของ Operational Technology (OT) ก่อนความลับของข้อมูล (Confidentiality) หรือไม่	Yes/No	
๑.๒	มีการกำหนดบทบาทและความรับผิดชอบที่ชัดเจนระหว่างทีม Operational Technology (OT) และ Information Technology (IT) หรือไม่	Yes/No	
๑.๓	ผู้บริหารระดับสูง (Management Bodies) มีการอนุมัติและทบทวนมาตรการความเสี่ยงของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายอย่างสม่ำเสมอหรือไม่	Yes/No	
๑.๔	นโยบายการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายกำหนดสอดคล้องและรวมเข้ากับกรอบงานความมั่นคงปลอดภัยไซเบอร์ระดับองค์กร (IT) หรือไม่	Yes/No	
๒. การระบุและจัดการสินทรัพย์ (Asset Management Policy)			
๒.๑	นโยบายกำหนดให้มีการบำรุงรักษาบัญชีรายการทรัพย์สินของ Operational Technology (OT) ให้ถูกต้อง และเป็นปัจจุบันอย่างต่อเนื่อง รวมถึงประเมินระดับความสำคัญของทรัพย์สินหรือไม่	Yes/No	
๒.๒	นโยบายครอบคลุมถึงระบบ และอุปกรณ์ที่มีความสำคัญต่อความปลอดภัยของผู้ใช้บริการหรือไม่	Yes/No	
๒.๓	นโยบายระบุขั้นตอนการจัดการสินทรัพย์ที่สิ้นสุดอายุการใช้งาน (End of Life) หรือสิ้นสุดการสนับสนุน (End of Support) รวมถึงมีการบริหารจัดการความเสี่ยง และการปลดระวางอย่างปลอดภัยหรือไม่	Yes/No	
๓. การควบคุมการเข้าถึงและบัญชีผู้ใช้ (Access Control Policy)			
๓.๑	นโยบายบังคับใช้การควบคุมการเข้าถึงตามบทบาทหน้าที่ของผู้ใช้งาน และหลักการสิทธิ์น้อยที่สุด (Least Privilege) ของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายหรือไม่	Yes/No	
๓.๒	นโยบายกำหนดให้มีการใช้ Multi-Factor Authentication (MFA) สำหรับการเข้าถึงระยะไกล (Remote Access) และบัญชีสิทธิพิเศษ (Privileged Accounts) หรือไม่	Yes/No	

รายการตรวจสอบการทบทวนกฎด้านความมั่นคงปลอดภัยไซเบอร์			
หมวดหมู่	**รายการตรวจสอบ(Configuration Item)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๓.๓	นโยบายกำหนดให้มีการเปลี่ยนรหัสผ่านเริ่มต้น (Default Credentials) สำหรับอุปกรณ์ใหม่และอุปกรณ์ควบคุมทั้งหมดหรือไม่	Yes/No	
๓.๔	นโยบายระบุมาตรการควบคุมการเข้าถึงทางกายภาพ (Physical Access) ไปยังอุปกรณ์ของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายหรือไม่	Yes/No	
๔. การจัดการแพตช์และช่องโหว่ (Patch & Vulnerability Management Policy)			
๔.๑	นโยบายกำหนดวงจรการจัดการช่องโหว่ สำหรับระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายหรือไม่	Yes/No	
๔.๒	นโยบายระบุให้มีการทดสอบแพตช์ในสภาพแวดล้อมจำลอง (Testbed/Staging) ก่อนการใช้งานจริงในระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายหรือไม่	Yes/No	
๔.๓	นโยบายกำหนดการใช้มาตรการควบคุมชดเชย (Compensating Controls) สำหรับระบบ Legacy ที่ไม่สามารถแพตช์ได้หรือไม่	Yes/No	
๕. การแบ่งส่วนเครือข่ายและการควบคุมการสื่อสาร (Network Segmentation Policy)			
๕.๑	นโยบายบังคับใช้การแบ่งโซนและท่อ (Zone and Conduit) แยกออกจากโซน IT อย่างชัดเจน	Yes/No	
๕.๒	นโยบายกำหนดให้กฎไฟร์วอลล์ต้องเป็นไปตามหลักการ "Deny by Default" และต้องมีเอกสารการอนุมัติสำหรับทุกกฎ "Allow" หรือไม่	Yes/No	
๕.๓	นโยบายควบคุมการใช้สื่อแบบถอดได้ (Removable Media/USB) และกำหนดให้ต้องมีการตรวจสอบมัลแวร์ (Scanning) ก่อนเชื่อมต่อกับอุปกรณ์ กับระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายหรือไม่	Yes/No	
๖. การรับมือและกู้คืนเหตุการณ์ (Incident Response & Recovery Policy)			
๖.๑	นโยบายรับมือเหตุการณ์ (IRP) ให้ความสำคัญกับการแยก (Containment) และการกู้คืน (Recovery) เพื่อรักษาความปลอดภัยและการทำงานต่อเนื่องหรือไม่	Yes/No	
๖.๒	นโยบายกำหนดให้มีการฝึกซ้อมแผนรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ (Tabletop Exercise) ของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมายอย่างสม่ำเสมอหรือไม่	Yes/No	

รายการตรวจสอบการทบทวนกฎด้านความมั่นคงปลอดภัยไซเบอร์			
หมวดหมู่	**รายการตรวจสอบ(Configuration Item)**	**สถานะ การตรวจสอบ**	**หมายเหตุ**
๖.๓	นโยบายกำหนดให้มีการสำรองข้อมูล (Backup) และแผนการกู้คืน (Disaster Recovery) ของระบบภายใต้บริการทั้ง ๔ บริการที่สำคัญตามกฎหมาย และมีการทดสอบข้อมูลสำรองสม่ำเสมอหรือไม่	Yes/No	

ภาคผนวก ๓ ตัวอย่างรายการตรวจสอบการทบทวนการตั้งค่า (Configuration)

รายการตรวจสอบการทบทวนการตั้งค่า (Configuration) ของระบบ			
หมวดหมู่	**รายการตรวจสอบ (Configuration Item)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๑. การตั้งค่าอุปกรณ์ฮาร์ดแวร์ และซอฟต์แวร์			
๑.๑	มีการเปลี่ยนรหัสผ่านเริ่มต้น (Default Passwords) ของอุปกรณ์ควบคุมทั้งหมดหรือไม่	Yes/No	
๑.๒	มีการปิดใช้งานพอร์ต/บริการที่ไม่จำเป็นสำหรับอุปกรณ์ควบคุมหรือไม่ เช่น Web Server, Telnet, FTP เป็นต้น	Yes/No	
๒. เซิร์ฟเวอร์ (Server) หรือเวิร์คสเตชัน (Workstations)			
๒.๑	มีการใช้บัญชีผู้ใช้เฉพาะบุคคล (Individual Accounts) แทนบัญชีร่วม (Shared Accounts) หรือไม่	Yes/No	
๒.๒	มีการบังคับใช้การควบคุมการเข้าถึงตามบทบาท (Role-Based Access Control - RBAC) หรือไม่	Yes/No	
๒.๓	มีการติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์ (Antivirus/EDR) และมีการกำหนดค่าให้ทำงานในโหมดที่เข้ากันได้กับ OT หรือไม่	Yes/No	
๒.๔	มีการตั้งค่าระบบปฏิบัติการ (OS) ให้ล็อกหน้าจออัตโนมัติ (Screen Lock) และต้องใช้รหัสผ่านเมื่อไม่มีกิจกรรมหรือไม่	Yes/No	
๒.๕	มีการจำกัดการใช้ USB หรือสื่อแบบถอดได้ (Removable Media) ผ่านการตั้งค่านโยบายของระบบปฏิบัติการหรือไม่	Yes/No	
๓. การจัดการเครือข่ายและการแบ่งส่วน (Network Segmentation)			
๓.๑	มีการกำหนดค่ากฎไฟร์วอลล์ (Firewall Rules) เพื่อจำกัดการสื่อสารระหว่างโซน OT และ IT (หรือ DMZ) ตามหลักการที่จำเป็นต้องรู้ (Need-to-Know) หรือไม่	Yes/No	
๓.๒	มีการจำกัดการใช้โปรโตคอลที่ไม่ปลอดภัย (เช่น Telnet, FTP) ภายในเครือข่าย OT และใช้โปรโตคอลที่ปลอดภัยกว่า (เช่น SSH, SFTP) หรือไม่	Yes/No	
๓.๓	มีการควบคุมการเข้าถึงระยะไกล (Remote Access) ไปยังเครือข่าย OT ผ่าน VPN หรือ Jump Server และมีการใช้ MFA หรือไม่	Yes/No	
๓.๔	มีการกำหนดค่า Network Time Protocol (NTP) ให้ใช้เซิร์ฟเวอร์เวลาที่เชื่อถือได้ เพื่อความแม่นยำของการบันทึก Log หรือไม่	Yes/No	

รายการตรวจสอบการทบทวนการตั้งค่า (Configuration) ของระบบ			
หมวดหมู่	**รายการตรวจสอบ (Configuration Item)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๔. การบันทึกกิจกรรมและการตรวจสอบ (Logging & Monitoring)			
๔.๑	อุปกรณ์เครือข่ายและ Host สำคัญ (เช่น HMI, Server) มีการกำหนดค่าให้ส่ง Log ไปยังระบบรวบรวม Log (เช่น SIEM) หรือไม่	Yes/No	
๔.๒	มีการบันทึกกิจกรรมของผู้ดูแลระบบ (Admin) และการเปลี่ยนแปลงการตั้งค่า (Configuration Changes) ของอุปกรณ์ควบคุมหรือไม่	Yes/No	
๔.๓	มีการตรวจสอบการเข้าถึงที่ไม่สำเร็จซ้ำ ๆ (Failed Login Attempts) หรือการใช้โปรโตคอลที่ไม่ได้รับอนุญาตหรือไม่	Yes/No	
๕. การสำรองข้อมูลและการกู้คืน (Backup & Recovery Configuration)			
๕.๑	มีการสำรองข้อมูลอย่างสม่ำเสมอตามรอบที่กำหนดหรือไม่	Yes/No	
๕.๒	ข้อมูลสำรองถูกจัดเก็บในสถานที่ที่แยกจากกัน (Isolated/Offline) เพื่อป้องกันมัลแวร์เรียกค่าไถ่ (Ransomware) หรือไม่	Yes/No	
๕.๓	มีการจัดทำและทดสอบขั้นตอนการกู้คืน (Recovery Procedures) จากข้อมูลสำรองอย่างน้อยปีละครั้งหรือไม่	Yes/No	

ภาคผนวก ๔ ตัวอย่างรายการตรวจสอบการทบทวนการเชื่อมต่อกับเครือข่าย

รายการตรวจสอบการทบทวนการเชื่อมต่อกับเครือข่าย เพื่อระบุจุดการเข้าถึงทั้งหมด				
ลำดับ	**จุดเชื่อมต่อ / ช่องทางการเข้าถึง**	**รายการตรวจสอบ จุดควบคุมความปลอดภัย**	**สถานะ การตรวจสอบ**	**หมายเหตุ**
๑	ไฟร์วอลล์หลัก (IT/OT Firewall)	มีการกำหนดกฎ "Deny by Default" โดยอนุญาตเฉพาะพอร์ต/โปรโตคอล/IP ที่จำเป็นต่อภารกิจเท่านั้น	Yes/No	
๒	เซิร์ฟเวอร์ใน DMZ	กำหนดให้เซิร์ฟเวอร์ที่ต้องสื่อสารสองทาง (Dual-Homed) ต้องอยู่ในโซน DMZ ที่แยกส่วน และจำกัดการเข้าถึงอย่างเข้มงวด	Yes/No	
๓	การเชื่อมต่อจาก Cloud/Internet	ไม่มีการเชื่อมต่อโดยตรงจากอินเทอร์เน็ตสาธารณะเข้าสู่เครือข่ายของระบบภายใต้บริการ ๔ บริการตามที่กำหมายกำหนด โดยไม่ผ่านการควบคุมที่เข้มงวด	Yes/No	
๔	Remote Access Gateway	กำหนดให้บังคับใช้ Multi-Factor Authentication (MFA) สำหรับผู้ใช้งานระยะไกลทุกคน	Yes/No	
๕	สิทธิ์การเข้าถึงระยะไกล	จำกัดสิทธิ์การเข้าถึงให้เป็นไปตามหลัก Need-to-Know และกำหนดให้ต้องมีการ อนุมัติทุกครั้ง ก่อนการเชื่อมต่อ	Yes/No	
๖	พอร์ตสวิตช์ที่ไม่ได้ใช้งาน	พอร์ตเครือข่ายว่างบนสวิตช์ถูกปิดการใช้งาน (Disabled) และ/หรือถูกล็อคทางกายภาพแล้วหรือไม่	Yes/No	
๗	สื่อแบบถอดได้ (USB Drive, HDD)	มีนโยบายและมาตรการบังคับใช้ในการสแกนสื่อบันทึกแบบถอดได้ทั้งหมดก่อนนำมาใช้กับ เวิร์คสเตชัน (Workstations) เซิร์ฟเวอร์ (Server) หรืออุปกรณ์ควบคุมหรือไม่	Yes/No	
๘	เครือข่ายไร้สาย (WLAN/Access Points)	เครือข่าย Wi-Fi ที่ใช้ในพื้นที่ของระบบที่ให้บริการภายใต้บริการ ๔ บริการตามที่กำหมายกำหนดถูกแยกส่วน (Segmented) และจำกัดการเข้าถึงอย่างเคร่งครัดหรือไม่	Yes/No	

รายการตรวจสอบการทบทวนการเชื่อมต่อกับเครือข่าย เพื่อระบุจุดการเข้าถึงทั้งหมด				
ลำดับ	**จุดเชื่อมต่อ / ช่องทางการเข้าถึง**	**รายการตรวจสอบ จุดควบคุมความปลอดภัย**	**สถานะ การตรวจสอบ**	**หมายเหตุ**
๙	การเข้าถึงพื้นที่ควบคุม	พื้นที่ควบคุมถูกจำกัดการเข้าถึงตามหน้าที่ความรับผิดชอบ และมีระบบเฝ้าระวัง (CCTV) หรือไม่	Yes/No	

ภาคผนวก ๕ ตัวอย่างรายการตรวจสอบตามมาตรฐานขั้นต่ำด้านการตั้งค่าความปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง

รายการตรวจสอบตามมาตรฐานขั้นต่ำ ด้านการตั้งค่าความปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง			
รายการตรวจสอบ	**รายละเอียดที่ควรมี (สำหรับระบบ OT)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๑. รายการตรวจสอบการเฝ้าระวังและการตอบสนองต่อภัยคุกคาม			
การประเมินความเสี่ยง	ประเมินความเสี่ยง (Risk Assessment) ด้านความมั่นคงปลอดภัยไซเบอร์และช่องโหว่ของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดอย่างสม่ำเสมออย่างน้อยปีละหนึ่งครั้ง	Yes/No	
การระบุภัยคุกคาม	มีการระบุถึงภัยคุกคามทางไซเบอร์ที่เกี่ยวข้องกับบริการของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด	Yes/No	
การตรวจสอบและบันทึกเหตุการณ์	มีการเปิดใช้งานและเก็บรักษา บันทึกเหตุการณ์ (Logs) ที่สำคัญของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดเพื่อใช้ในการวิเคราะห์เมื่อเกิดเหตุการณ์ผิดปกติ	Yes/No	
แผนรับมือเหตุการณ์	มีแผนรับมือเหตุการณ์ (Incident Response Plan) ที่ครอบคลุมสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่อาจเกิดขึ้นกับระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด	Yes/No	
๒. รายการตรวจสอบการควบคุมการเข้าถึงและการยืนยันตัวตน (Access Control and Authentication)			
การระบุและยืนยันตัวตน	มีการกำหนดผู้ใช้งานแต่ละรายให้ ไม่ซ้ำกัน (Unique Identification) และต้องยืนยันตัวตนก่อนเข้าถึงระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด	Yes/No	
การใช้รหัสผ่านที่รัดกุม	มีการบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน (Password Complexity) และกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสม	Yes/No	
การใช้สิทธิพิเศษน้อยที่สุด	กำหนดสิทธิในการเข้าถึงให้เป็นไปตามหลักสิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege) โดยผู้ใช้งานและบริการ	Yes/No	

รายการตรวจสอบตามมาตรฐานขั้นต่ำ ด้านการตั้งค่าความปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง			
รายการตรวจสอบ	**รายละเอียดที่ควรมี (สำหรับระบบ OT)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
	ต้องได้รับสิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานเท่านั้น		
การยืนยันตัวตนแบบหลายปัจจัย (MFA)	พิจารณาใช้ MFA โดยเฉพาะสำหรับการเข้าถึงระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด จากเครือข่ายที่ไม่น่าเชื่อถือ (Untrust Networks) หรือการเชื่อมต่อระยะไกล (Remote Control)	Yes/No	
การแบ่งแยกหน้าที่	มีการกำหนดให้มีการ แบ่งแยกหน้าที่ (Separation of Duties) สำหรับการจัดการระบบที่สำคัญ เช่น ผู้ดูแลระบบ, ผู้อนุมัติการเปลี่ยนแปลง	Yes/No	
๓. รายการตรวจสอบการจัดการความมั่นคงปลอดภัยเครือข่ายและสภาปัตยกรรม (Network and Architecture Security)			
การแบ่งแยกเครือข่าย (Segmentation)	มีการ แบ่งแยกเครือข่าย ระหว่างระบบ Information Technology (IT) และระบบ Operational Technology (OT) ภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดอย่างชัดเจน และใช้ ไฟร์วอลล์ (Firewall) หรือเทคโนโลยีอื่นในการควบคุมการสื่อสารระหว่างโซน	Yes/No	
การควบคุมการเชื่อมต่อระยะไกล	การเชื่อมต่อระยะไกล (Remote Access) เข้าสู่ระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดต้องถูกควบคุมอย่างเข้มงวดและมีการกำหนดค่าที่เหมาะสม (Proper Configuration) เช่น การใช้ VPN และ MFA	Yes/No	
การประเมินช่องโหว่	ดำเนินการประเมินช่องโหว่ (Vulnerability Assessment) ของโฮสต์, เครือข่าย, และตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review) ของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด	Yes/No	

รายการตรวจสอบตามมาตรฐานขั้นต่ำ ด้านการตั้งค่าความปลอดภัยของหน่วยงานผู้ให้บริการขนส่งทางราง			
รายการตรวจสอบ	**รายละเอียดที่ควรมี (สำหรับระบบ OT)**	**สถานะการตรวจสอบ**	**หมายเหตุ**
๔. รายการตรวจสอบการทำให้ระบบมีความแข็งแกร่ง (System Hardening)			
การกำหนดค่าเริ่มต้นที่ปลอดภัย	อุปกรณ์และระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดทั้งหมดถูกตั้งค่าตามมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ที่หน่วยงานกำหนด	Yes/No	
การปิดบริการที่ไม่จำเป็น	ปิด (Disable) พอร์ต, โปรโตคอล, และบริการทั้งหมดที่ไม่จำเป็นต่อการทำงานของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดเพื่อลดช่องโหว่	Yes/No	
การจัดการแพตช์และอัปเดต	มีกระบวนการจัดการการอัปเดตระบบปฏิบัติการและซอฟต์แวร์ โดยเฉพาะอย่างยิ่งสำหรับอุปกรณ์ของระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนดที่มีความอ่อนไหว โดยต้องทดสอบและดำเนินการตามกระบวนการจัดการความเสี่ยงด้านความพร้อมใช้งาน (Availability)	Yes/No	
การจัดการสื่อเก็บข้อมูลแบบถอดได้	มีนโยบายควบคุมการใช้สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media) ในพื้นที่ระบบภายใต้ ๔ บริการที่สำคัญตามกฎหมายกำหนด เพื่อป้องกันมัลแวร์และการถ่ายโอนข้อมูลโดยไม่ได้รับอนุญาต	Yes/No	

ภาคผนวก ๖ เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

๑. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

๔. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

๕. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๓] ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

[๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ "ภัยคุกคามทางไซเบอร์" ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภาคผนวก ๗ เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ): โปรดระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์๔ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

ส่วนที่ ๑

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา: โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา: โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค. ข้อมูลการรับมือภัยคุกคาม
ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ) ☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ ☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม ☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว ☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ
ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว ☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว ☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว ☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว ☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ
ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี) โปรดระบุ

ส่วนที่ ๒

หมวด ง. รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)

วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การจู่โจม, ความผิดพลาดจากคนนอกองค์กร):

โปรดระบุ

บุคคล วิธี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ):

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

ง๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:

โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

ส่วนที่ ๒
หมวด ง. รายละเอียดภัยคุกคาม
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ ☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ ☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ) ☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ ☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ ☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Snifer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย ☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง ☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก ☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย ☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ ☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ ☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS) ☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ ☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น ☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ ☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility) ☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ
ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) โปรดระบุ
ง๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ
ง๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู
ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ
ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู
ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)
ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ
ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ
ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

ภาคผนวก ๘ ตัวอย่างแบบฟอร์มการร้องขอให้แก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)

<table>
<tr><td colspan="2">แบบฟอร์มการร้องขอให้แก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (Corrective Action Request: CAR)</td></tr>
<tr><td>การแก้ไขความไม่สอดคล้องหรือการไม่ปฏิบัติตาม
(Corrective Action Request: CAR)</td><td>CAR No. .....</td></tr>
<tr><td>หน่วยงาน / ผู้รับตรวจ : .....
ครั้งที่ตรวจ (Audit No.) ..... วันที่ตรวจ (Date:) .....
ผู้ตรวจ (Auditor) : .....</td><td>ประเภท NCR ☐ Major ☐ Minor
☐ Observation ☐ OFI
กฎหมาย/มาตรฐาน: ..... ข้อกำหนด/
รายการที่: .....</td></tr>
<tr><td colspan="2">๑. รายละเอียดความไม่สอดคล้องหรือการไม่ปฏิบัติตาม (สำหรับคณะผู้ตรวจประเมิน (Auditor))
.....
.....

ผู้ตรวจ (Auditor) : Date : .../.../.....</td></tr>
<tr><td colspan="2">๒. วิเคราะห์สาเหตุและแนวทางการ แก้ไข/ป้องกัน (สำหรับคณะทำงานหน่วยงานรัฐ หรือ CII)
วิเคราะห์สาเหตุ (Root Cause) (กรณีที่เป็น Major NC หรือ Minor NC) :
.....
.....

<table>
<tr><th>รายละเอียดการแก้ไข
(Action details)</th><th>วันที่เริ่มต้น
(Start Date)</th><th>วันที่คาดว่าจะแล้วเสร็จ
(Expected Due Date)</th><th>วันที่เสร็จจริง
(Finish Date)</th><th>สอบทานโดย
(Verified by)</th></tr>
<tr><td><u>การแก้ไขเบื้องต้น (Correction)</u>
.....</td><td></td><td></td><td></td><td></td></tr>
<tr><td><u>การแก้ไขโดยไม่ให้เกิดซ้ำ (Corrective Action)</u>
กิจกรรมย่อย ๑.
.....
กิจกรรมย่อย ๒.
.....</td><td></td><td></td><td></td><td></td></tr>
</table>
ผู้ดำเนินการแก้ไข : ..... Date : ...../...../.....</td></tr>
</table>

๓. พิจารณาความเหมาะสมของแนวทางการแก้ไข (สำหรับคณะผู้ตรวจประเมิน (Auditors) หรือกรรมการบริหารของหน่วยงานผู้ให้บริการขนส่งทางราง)

ความเห็น ☐ เห็นชอบ ☐ ไม่เห็นชอบ

รายละเอียด

.....

ผู้ให้ความเห็นชอบ : ..... Date : ..../..../....

Remark: โปรดส่งกลับให้ผู้ตรวจสอบหรือผู้รับผิดชอบ ภายใน .../.../...

ต้องส่งต่อให้ ☐ สกมช. (ส่งต่อ กกม.)..../..../.... ☐ กรมการขนส่งทางราง (ขร.) ..../..../....

☐ อื่น ๆ โปรดระบุ.....

☐ **ส่งให้** กกม. พิจารณา ภายใน .../... /.... (สำหรับ สกมช.)

☐ **ส่งให้** ขร. พิจารณา ภายใน .../... /.... (สำหรับ ขร.)

๔. พิจารณาความเหมาะสมของแนวทางการแก้ไข (สำหรับ กกม. หรือ ขร.)

ความเห็น ☐ อนุมัติ ☐ ไม่อนุมัติ

รายละเอียด .....

ให้ดำเนินการแก้ไขให้แล้วเสร็จภายใน .../.../...

ผู้ให้ความเห็นชอบ : ..... Date : .../.../...

๕. พิจารณาผลการแก้ไข (สำหรับคณะผู้ตรวจประเมิน (Auditors) หรือกรรมการบริหารหน่วยงาน CII)

สถานะการดำเนินการ ☐ ดำเนินการเรียบร้อย ☐ ดำเนินการยังไม่แล้วเสร็จ

.....

.....

ผู้ให้ความเห็นชอบ : ..... Date : .../.../...

๖. ส่งผลการแก้ไขให้ กกม. หรือ ขร.

ส่งให้ สกมช. ภายใน ..../..../....

ส่งให้ ขร. ภายใน ..../..../....

ภาคผนวก ๙ ตารางเปรียบเทียบกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (NIST Cybersecurity Framework ๒.๐) กับกรอบการบริหารจัดการความมั่นคงปลอดภัยของสารสนเทศ (Information Security Management System - ISMS)

ฟังก์ชันของ NIST CSF ๒.๐	ความหมายโดยย่อ	ISO ๒๗๐๐๑:๒๐๒๒ Control Reference
GOVERN (GV)	การกำหนดกลยุทธ์ นโยบาย และการบริหารความเสี่ยงระดับองค์กร	Clause ๔ (Context) Clause ๕ (Leadership) Clause ๖ (Planning)
IDENTIFY (ID)	การทำความเข้าใจทรัพย์สิน ข้อมูล และความเสี่ยงทางไซเบอร์ขององค์กร	Clause ๘.๒ (Risk Assessment) A.๕ (Organizational) A.๕.๙ (Inventory of information and other associated)
PROTECT (PR)	การใช้มาตรการเพื่อปกป้องระบบและข้อมูลไม่ให้เกิดภัยคุกคาม	A.๘ (Technological) A.๘.๓ (Information access restriction) A.๘.๒๔ (Use of cryptography)
DETECT (DE)	การเฝ้าระวังและค้นหาเหตุการณ์ผิดปกติที่อาจเกิดขึ้น	A.๘.๑๖ (Monitoring activities) Clause ๙.๑ (Monitoring, measurement, analysis and evaluation)
RESPOND (RS)	การดำเนินการเมื่อเกิดเหตุภัยคุกคามขึ้นแล้ว เพื่อจำกัดผลกระทบ	A.๕.๒๔ - A.๕.๒๘ (Incident Management)
RECOVER (RC)	การกู้คืนระบบและข้อมูลให้กลับมาใช้งานได้ตามปกติ	A.๕.๒๙ (Information security during disruption) A.๕.๓๐ (ICT readiness for business continuity)

ภาคผนวก ๑๐ ตารางเปรียบเทียบข้อกำหนดมาตรฐาน TS ๕๐๗๐๑ ฟังก์ชันของมาตรฐาน NIST Cybersecurity Framework ๒.๐

หลักการของมาตรฐาน TS ๕๐๗๐๑	หน้าที่หลักของ NIST (CSF)	โดเมน/กิจกรรมที่สอดคล้องกันใน NIST CSF ๒.๐ (Categories / Subcategories)
การประเมินภัยคุกคามและความเสี่ยง	Identify (ID) Govern (GV)	GV.SC (Supply Chain Risk Management) ID.AM (Asset Management) ID.AM-๐๑ (Inventory) ID.AM-๐๘ (Inventory Criticality) ID.RA (Risk Assessment) ID.RA-๐๓ (Risk Identify) ID.RA-๐๔ (Business & Safety Impact Analysis)
การปกป้องฟังก์ชันสำคัญ	Protect (PR)	PR.DS (Data Security) PR.DS-๐๑ (Data Protection) PR.DS-๑๐ (Integrity PR.IR (Technology Infrastructure Resilience) PR.IR-๐๓ (Resilience)
การควบคุมการเข้าถึง	Protect (PR)	PR.AA (Identity Management, Authentication, and Access Control) PR.AA-๐๑ (User Management) PR.AA-๐๓ (Multi-Factor Authentication) PR.AA-๐๕ (Physical Access)
การตรวจติดตามและการตอบสนองต่อเหตุการณ์	Detect (DE) Respond (RS)	DE.CM (Continuous Monitoring) DE.CM-๐๑ (Operational Technology) DE.CM-๐๙ (Remote Maintenance Access) RS.MA (Incident Management) RS.MA-๐๒ (SOP) RS.MI (Incident Mitigation) RS.MI-๐๒ (Containment)
การทดสอบและการประเมินความปลอดภัย	Identify (ID) Protect (PR)	ID.RA (Risk Assessment - Vulnerability) PR.PS (Platform Security) PR.PS-๐๒ (Baseline Configuration)
การติดตามและการตรวจสอบ	Detect (DE) Govern (GV) Identify (ID)	DE.AE (Adverse Event Analysis) GV.OV (Oversight) ID.IM (Lessons Learned)

ภาคผนวก ๑๑ ตารางเปรียบเทียบข้อกำหนดมาตรฐาน EN ๕๐๑๒๘ ฟังก์ชันของมาตรฐาน NIST Cybersecurity Framework

หลักการของ EN ๕๐๑๒๘ (เน้น Software Safety และ Quality)	**หน้าที่หลักของ NIST (CSF)**	**โดเมน/กิจกรรมที่สอดคล้องกันใน NIST CSF ๒.๐ (Categories / Subcategories)**
การจัดการความเสี่ยง (Risk Management)	Identify (ID) Govern (GV)	GV.RM (Risk Management) ID.RA (Risk Assessment) GV.SC (Supply Chain Risk Management)
กระบวนการพัฒนาซอฟต์แวร์ (Software Development Process)	Protect (PR)	PR.DS (Data Security) PR.PS (Platform Security) ID.AM (Asset Management)
การประกันคุณภาพซอฟต์แวร์ (Software Quality Assurance)	Govern (GV) Protect (PR)	GV.AT (Improvement) PR.DS (Data Security)
การทดสอบและการตรวจสอบ (Testing and Verification)	Protect (PR) Detect (DE)	PR.PS (Platform Security) DE.CM (Continuous Monitoring)
การจัดการการเปลี่ยนแปลงและการบำรุงรักษา (Change Management and Maintenance)	Protect (PR)	PR.PS (Platform Security)
การควบคุมการเข้าถึงและความปลอดภัย (Access Control and Security)	Protect (PR)	PR.AA (Identity Management, Authentication, and Access Control)

ภาคผนวก ๑๒ ตารางเปรียบเทียบข้อกำหนดมาตรฐาน IEC ๖๒๔๔๓ ฟังก์ชันของมาตรฐาน NIST Cybersecurity Framework ๒.๐

การเปรียบเทียบข้อกำหนดพื้นฐาน ๗ ข้อของมาตรฐาน IEC ๖๒๔๔๓ กับฟังก์ชันหลัก ๖ ฟังก์ชันตามมาตรฐาน NIST Cybersecurity Framework ๒.๐ มีรายละเอียด ดังนี้

No.	IEC ๖๒๔๔๓	Govern	Identify	Protect	Detect	Respond	Recover
๑	IAC	✓	✓	✓			
๒	UC	✓	✓	✓	✓		
๓	SI			✓	✓	✓	✓
๔	DC	✓	✓	✓	✓	✓	
๕	RDF			✓	✓		
๖	TRE	✓			✓	✓	✓
๗	RA		✓	✓	✓	✓	✓

๑. Identification and Authentication Control (IAC)

หมายถึง การระบุและรับรองอัตลักษณ์ของผู้ใช้งาน (มนุษย์), กระบวนการ (Software processes) และอุปกรณ์ (Devices) ก่อนอนุญาตให้เข้าถึงระบบ สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Govern
  - GV.PO (Policy)
  - GV.SC (Supply Chain Risk Management)
- Identify
  - ID.AM (Asset Management)
- Protect
  - PR.AA (Identity Management, Authentication, and Access Control)
  - PR.AT (Awareness and Training)

๒. Use Control (UC)

หมายถึง การบังคับใช้สิทธิ์การใช้งาน (Authorization) เพื่อให้มั่นใจว่าผู้ใช้หรืออุปกรณ์ทำได้เฉพาะสิ่งที่ได้รับอนุญาตเท่านั้น (Least Privilege) สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Govern
  - GV.PO (Policy)
- Identify
  - ID.AM (Asset Management)
- Protect
  - PR.AA (Identity Management, Authentication, and Access Control)
  - PR.DS (Data Security)

- Detect
    - DE.CM (Continuous Monitoring)

๓. System Integrity (SI)

หมายถึง การปกป้องความสมบูรณ์ของระบบ (Software, Firmware, Information) เพื่อป้องกันการแก้ไขเปลี่ยนแปลงโดยไม่ได้รับอนุญาต สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Protect
    - PR.PS (Platform Security)
    - PR.DS (Data Security)
- Detect
    - DE.CM (Continuous Monitoring)
    - DE.AE (Adverse Event Analysis)
- Respond
    - RS.MA (Incident Analysis)
    - RS.MI (Incident Mitigation)
- Recover
    - RC.RP (Recovery Planning)

๔. Data Confidentiality (DC)

หมายถึง การรับประกันว่าข้อมูลสำคัญ (เช่น ข้อมูลการผลิต, ทรัพย์สินทางปัญญา) จะไม่ถูกเปิดเผยต่อผู้ไม่มีสิทธิ์ สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Govern
    - GV.OC (Organizational Context)
- Identify (การระบุ)
    - ID.AM (Asset Management)
    - ID.RA (Risk Assessment)
- Protect
    - PR.DS (Data Security)
    - PR.AA (Access Control)
- Detect
    - DE.AE (Adverse Event Analysis)
- Respond
    - RS.CO (Incident Communication)

๕. Restricted Data Flow (RDF)

หมายถึง การแบ่งโซนเครือข่าย (Network Segmentation) และการควบคุมทิศทางการไหลของข้อมูล (Zone & Conduit) เพื่อจำกัดวงความเสียหาย สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Protect
    - PR.AA (Access Control)
    - PR.PS (Platform Security)
- Detect
    - DE.CM (Continuous Monitoring)
    - DE.AE (Adverse Event Analysis)

๖. Timely Response to Events (TRE)

หมายถึง ความสามารถของระบบและองค์กรในการตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยอย่างรวดเร็วและมีประสิทธิภาพ สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Govern
    - GV.PO (Policy)
- Detect
    - DE.AE (Adverse Event Analysis)
    - DE.CM (Continuous Monitoring)
- Respond
    - RS.MA (Incident Analysis)
    - RS.MI (Incident Mitigation)
    - RS.CO (Incident Communication)
- Recover
    - RC.RP (Recovery Planning)

๗. Resource Availability (RA)

หมายถึง การรับประกันว่าระบบควบคุมอุตสาหกรรมจะพร้อมใช้งานเสมอ แม้ในขณะถูกโจมตี (Resilience / DoS Protection) สอดคล้องกับฟังก์ชัน NIST CSF ๒.๐ ดังนี้

- Identify
    - ID.RA (Risk Assessment)
- Protect
    - PR.DS (Data Security)
    - PR.PS (Platform Security)
- Detect
    - DE.AE (Adverse Event Analysis)
- Respond
    - RS.MI (Incident Mitigation)
- Recover
    - RC.RP (Recovery Planning)