กรมการขนส่งทางราง
Department of Rail Transport

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กองยุทธศาสตร์และแผนงาน

514/1 Lan Luang Rd.,
Si Yaek Maha Nak,
Dusit, Bangkok 10300

https://www.drt.go.th/

Facebook/DRT.OfficialFanpage

สารบัญ

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และไปในทิศทางเดียวกัน

กรมการขนส่งทางราง (ขร.) ในฐานะหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล จึงจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

๑.๒ วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์พร้อมทั้งนำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโลยีสารสนเทศของ ขร. ให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

๑.๓ ขอบเขต

เอกสารฉบับนี้ครอบคลุมตามกรอบและวิธีปฏิบัติสำหรับด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๔ คำนิยาม

๑) หน่วยงาน หรือ องค์กร	หมายถึง	กรมการขนส่งทางราง หรือ ขร.
๒) คณะกรรมการ	หมายถึง	คณะกรรมการการรักษาความมั่นคงปลอดภัยทางไซเบอร์
๓) ดัชนีชี้วัดความเสี่ยงที่สำคัญ	หมายถึง	เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือนเพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์ และความเสี่ยงในอนาคตและเตรียมมาตรการการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

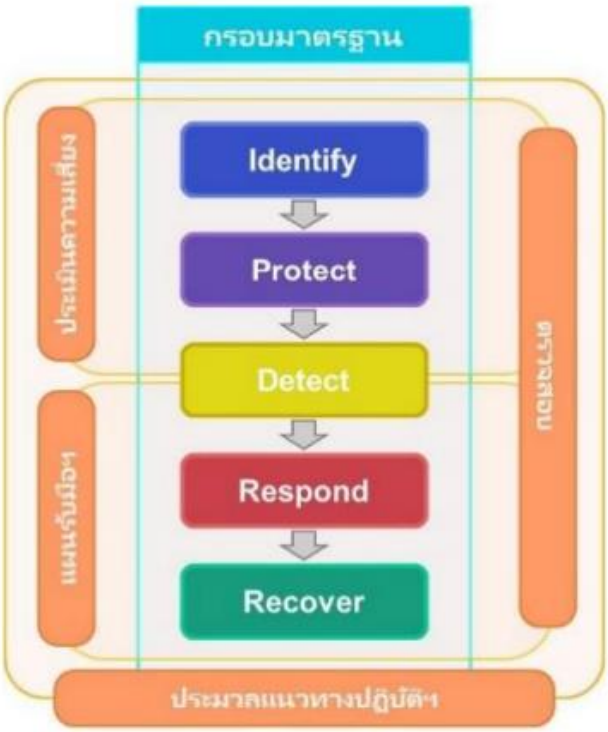
๔) คอมไพเลอร์	หมายถึง	โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรมเป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น
๕) แพตช์	หมายถึง	โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟแวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟแวร์ ผู้พัฒนาซอฟแวร์หลายรายได้เผยแพร่แพตช์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตช์ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update
๖) Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
๗) Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
๘) Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
๙) ผู้ใช้งาน	หมายถึง	ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของ ขร.
๑๐) บุคคลภายนอก	หมายถึง	บุคคลจากหน่วยภานอกภายนอกที่เข้ามาประชุมหรือปฏิบัติงานร่วมกับสำนักงาน
๑๑) หน่วยงานภายนอก	หมายถึง	หน่วยงานภายนอกที่สำนักงานอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสำนักงาน

		โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล
๑๐) สิทธิ์ของผู้ใช้งาน	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
๑๑) ผู้ดูแลระบบ	หมายถึง	ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน
๑๒) สินทรัพย์	หมายถึง	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและ ไม่มีตัวตน อันมีมูลค่าคุณค่าสำหรับหน่วยงาน
๑๓) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การขออนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย
๑๔) ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ

บทที่ ๒
แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑ การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔ สามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้



รูปที่ ๑-๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒ กิจกรรมตามกรอบมาตรฐาน

รายละเอียดของแต่ละกิจกรรมมีดังนี้

๑) Identify คือ การระบุและเข้าใจถึงบริทบต่าง ๆ เพื่อการบริหารจัดการความเสี่ยงที่เกิดขึ้นแก่ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

๒) Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน

๓) Detect คือ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๔) Response คือ มาตรการเผชิญเหตุ เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

๕) Recover คือ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามไซเบอร์

ข้อ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management) ดำเนินการดังนี้

๑.๑.๑ จัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญและดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน

๑.๑.๒ ระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๓ มีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ ให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy) ดำเนินการดังนี้

๑.๒.๑ ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยงโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

(ข) คำอธิบายของความเสี่ยง (Description of the Risk)

(ค) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

(ง) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

(ฉ) การจัดการความเสี่ยง (Risk Treatment)

(ง) เจ้าของความเสี่ยง (Risk Owner)

(ฉ) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

(ช) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๒.๒ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับประเมินความเสี่ยง ที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑.๒.๓ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑.๒.๔ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ การระบุโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

๑.๒.๕ วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญโดยมีการบริหารจัดการความเสี่ยง ดังนี้

(๑) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่า หรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๒) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ดำเนินการดังนี้

๑.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นงคงปลอดภัยแห่งชาติ สำนักพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) หรือจากแหล่งอื่นที่น่าเชื่อถือ เป็นต้น

๑.๓.๒ ประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยงของ ขร. เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ

๑.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของโฮสต์

(ข) การประเมินความมั่นคงปลอดภัยของเครือข่าย

(ค) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม

๑.๓.๔ การประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อ หรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญ การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชั่น การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

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

๑.๓.๖ ตรวจสอบขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชั่นของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๗ ดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ ครั้ง หรือตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ ก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

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

๑.๓.๙ การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของ ขร.

๑.๓.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

ทั้งนี้ ขร. กำหนดให้กลุ่มเทคโนโลยีสารสนเทศจัดให้มีการตรวจประเมินช่องโหว่และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบสารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยเร่งด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบต้องดำเนินการแก้ไขให้แล้วเสร็จโดยไม่ชักช้าหรือไม่เกินกว่า ๗ วัน นับจากวันที่ได้รับแจ้งจากกลุ่มเทคโนโลยีสารสนเทศ พร้อมทั้งรายงานผลการแก้ไขกลับมายังกลุ่มเทคโนโลยีสารสนเทศเพื่อทราบและดำเนินการตรวจสอบการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบที่ไม่อาจปิดช่องโหว่ได้ พร้อมกำหนดมาตรการชดเชยหรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่ทางเทคนิคนั้น หรือในกรณีที่มีความจำเป็นอาจต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายพิจารณาและให้ความเห็นชอบ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ดำเนินการดังนี้

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของ ขร.

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระกวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานทางสารสนเทศ ของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทางธุรกิจของ ขร. และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(ง) สิทธิของ ขร. ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

ข้อ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Asset Control) ดำเนินการดังนี้

๒.๑.๑ การเข้าถึงบริการที่สำคัญของ ขร. ถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒.๑.๒ ให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของ ขร. ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๒.๑.๓ เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ เช่น USB พอร์ตอนุกรม และ การเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้นและทำภายใต้การดูแลของ ขร.

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ดำเนินการดังนี้

๒.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชั่น และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) ของบริการที่สำคัญ

๒.๒.๒ มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) มีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้

(ก) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

(ข) การแบ่งแยกหน้าที่ (Separation of Duties)

(ค) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

(ง) การลบบัญชีที่ไม่ได้ใช้

(จ) การลบบริการและแอปพลิเคชั่นที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชั่นสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application

(ฉ) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

(ช) การป้องกันมัลแวร์ (Malware)

(ซ) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

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

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

๒.๒.๕ จัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ

๒.๓ การเชื่อมต่อระยะไกล (Remote Connection) ดำเนินการดังนี้

๒.๓.๑ ตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญได้จัดให้มีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญ ต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

(ก) เปิดใช้งานการเชื่อมต่อไปยัง หรือจากไซต์ระยะไกล เมื่อจำเป็นเท่านั้น

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

(ค) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

(ง) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญ เว้นแต่จะได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

(จ) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อบันทึกข้อมูลแบบถอดได้ (Removable Storage Media) ดำเนินการดังนี้

๒.๔.๑ กำหนดการควบคุมการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญ โดยการปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น กรณีที่ต้องการใช้งานให้แจ้งขึ้นทะเบียนสื่อบันทึกข้อมูล และขออนุมัติการเชื่อมต่อเป็นรายกรณีพร้อมทั้งมีการตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญ

๒.๔.๒ เข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญบนสื่อบันทึกข้อมูลถอดได้

๒.๕ การสร้างความตระนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) ดำเนินการดังนี้

การสร้างความตระหนักรู้ด้านความปลอดภัยไซเบอร์ (Cybersecurity Awareness) บทบาทหน้าที่ความรับผิดชอบ กฎหมายว่าด้วยความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติ มาตรฐาน และขั้นตอนที่เกี่ยวกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ การประชาสัมพันธ์และสื่อสารผ่านช่องทางต่าง ๆ ที่ ขร. กำหนดให้พนักงาน ผู้ให้บริการภายนอก ผู้ใช้งานที่เป็นหน่วยงานภายนอก ที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญสารสนเทศได้ และมีการทบทวนการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

ประโยชน์ที่ได้รับจากการทำ Security Awareness

บุคลากรที่มีความรู้ด้านการรักษาความมั่นคงปลอดภัย สามารถใช้งานทรัพยากรสารสนเทศขององค์กรได้ถูกต้อง ปลอดภัย ป้องกันภัยคุกคามและแจ้งเหตุผิดปกติให้องค์กรสามารถยับยั้งความเสียหายได้ทันท่วงที

ลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทุกรูปแบบ เช่น Phishing Email Ransomware เว็บไซต์อันตรายโฆษณาชวนเชื่อ หรือกลอุบายต่าง ๆ จากผู้ไม่ประสงค์ดีต่อองค์กร

ทรัพย์สินปลอดภัย ข้อมูลเป็นความลับ เมื่ออัตราการถูกโจมตีลดลง ความปลอดภัยของทรัพย์สินรวมถึงข้อมูลความลับต่าง ๆ ก็เพิ่มขึ้น

เกิดความเชื่อมั่นด้านความปลอดภัย ผู้ใช้บริการและคู่ค้าทางธุรกิจจะไว้วางใจที่จะทำงานร่วมกับองค์กรมากขึ้น

การใช้งานคอมพิวเตอร์

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย

๑. ควรมีการแยก User ใช้งานกันของแต่ละบุคคล

๒. ควร Logout เมื่อไม่อยู่หน้าเครื่องคอมพิวเตอร์

๓. ควรติดตั้ง Anti-Malware และมีการ Update อย่างสม่ำเสมอ

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

๖. ไม่ควรจด Password และติด Password ไว้ที่หน้าจอ

๗. มีการใช้ Password ที่ดี และไม่ควรบอก Password แก่ผู้อื่น

การใช้เกี่ยวกับรหัสผ่าน (Password)

การใช้รหัสผ่าน (Password) ที่ดี คือ

๑. มีความซับซ้อน เช่น ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)

๒. มีความยาวของ Password อย่างน้อย ๘ ตัวอักษร

๓. ควรหลีกเลี่ยงการใช้ Common password หรือ Default password หรือสิ่งที่สามารถคาดเดาได้ง่าย เช่น password,๑๒๓๔๕๖,วันเกิด,หมายเลขโทรศัพท์

๔. มีการเปลี่ยน Password อย่างสม่ำเสมอ

๕. ใช้ Multi Factor Authentication ในกรณีที่สามารถใช้งานได้

๖. ไม่ควรใช้ Password ซ้ำกันในแต่ละระบบ

๗. ไม่ควรบอก Password แก่ผู้อื่น

การใช้อีเมล (E-mail)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. ไม่เปิด E-mail ที่น่าสงสัย หรือผู้ส่งที่ไม่ชัดเจน

๒. ไม่เปิดไฟล์แนบจาก E-mail ที่น่าสงสัย หรือผู้ส่งไม่ชัดเจน

๓. ไม่คลิก Link ใน E-mail โดยไม่มีการตรวจเช็ค

๔. เรื่องที่มีความสำคัญก่อนทำธุรกรรมต่าง ๆ ควรมีการเช็คผ่านทางช่องทางอื่น ๆ เพิ่มเติม

การใช้เว็บไซต์ (Website)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. ไม่เข้าเว็บไซต์ที่ได้รับจากช่องทางที่ไม่แน่ชัด เช่น จากการแชร์ผ่านช่องทาง Social ต่าง ๆ

๒. ไม่ควรทำการบันทึก Password ต่าง ๆ บน Browser

๓. เว็บไซต์สำหรับทำธุรกรรมที่สำคัญ หรือต้องมีการกรอกข้อมูลที่สำคัญต้องมี SSL และใช้งานผ่าน HTTPS เท่านั้น

๔. ใช้ Browser ที่ผู้ใช้งานทั่วไปนิยมใช้งาน เช่น Google Chrome Mozilla Firefox เป็นต้น

๕. ควรมีการ Update Version ของ Browser อย่างสม่ำเสมอ

๖. ในกรณีเครื่องคอมพิวเตอร์ที่ใช้งานไม่ใช่เครื่องส่วนตัวควรใช้งาน Browser ในโหมด Safe Web Browsing

๗. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

การใช้เกี่ยวกับข้อความ (Messaging)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. ไม่ควรบันทึก Password ไว้ที่โปรแกรม

๒. กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

๓. มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

๔. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

ในด้านเกี่ยวกับการประชุม (Conference)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. ใช้สถานที่เหมาะสมกับการ Conference

๒. ในการประชุม Conference ควรมีแต่ผู้ที่เกี่ยวข้อง

๓. แชร์เอกสารต่าง ๆ อย่างระมัดระวัง

๔. ใช้โปรแกรมที่ผู้ใช้งานทั่วไปนิยมใช้งาน

๕. มีการ Update Version ของโปรแกรม Conference อย่างสม่ำเสมอ

๖. ควรมีการขออนุญาตผู้เข้าร่วมประชุม Conference ก่อนที่จะบันทึกภาพและเสียงในการประชุม

การใช้ที่เก็บข้อมูล (Cloud Storage)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. แยก User ในการใช้งานของแต่ละบุคคล

๒. ควรกำหนดผู้เข้าถึงไฟล์ได้เท่าที่จำเป็นเท่านั้น

๓. ปิดการเข้าถึงไฟล์ หรือปิดการแชร์ไฟล์เมื่อไม่มีความจำเป็น

๔. ควรติดตั้ง Anti-Malware และ update อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

๖. มีการตั้ง Password ที่ดี และไม่บอก Password แก่ผู้อื่น

การใช้ WIFI

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. ไม่ควรใช้งาน WIFI ที่เปิดให้ใช้บริการแบบไม่มีรหัสผ่าน

๒. หลีกเลี่ยงการใช้งาน WIFI ที่ไม่รู้ที่มาในการให้บริการ

การใช้โทรศัพท์ (Mobile)

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. เปิดการใช้งาน PIN/Password, Face scan หรือ Fingerprint ในการเข้าใช้งานอุปกรณ์

๒. ไม่ติดตั้ง Application ที่น่าสงสัยหรือไม่รู้แหล่งที่มา

๓. กำหนด Application permission ให้เหมาะสม

๔. มีการ Update Patch ระบบปฏิบัติการ (OS) อย่างสม่ำเสมอ

๕. มีการ Update Version ของโปรแกรมบนเครื่องอย่างสม่ำเสมอ

การใช้ Internet Connection

สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ

๑. เปลี่ยน Default Password ของ Router ที่มาจากโรงงาน

๒. เปลี่ยน SSID และรหัสผ่านของ WIFI ที่กำหนดมาจากผู้ให้บริการ

๓. กำหนดผู้ที่สามารถเข้าใช้งาน Internet เท่าที่จำเป็น

ข้อ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๓.๑.๑ มีกลไกและกระบวนการเพื่อตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๑.๒ จัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๓.๑.๓ วิเคราะห์ภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของ ขร. หรือไม่

๓.๑.๔ ทบทวนกลไกและกระบวนการ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

ข้อ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ดำเนินการดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity incident Response Plan)

จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ การสื่อสาร การฝึกซ้อม การทบทวน และปรับปรุงตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๔.๒ แผนการสื่อสารในสภาวะวิกฤต (Crisis Communication Plan)

จัดทำแผนการสื่อสารในสภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ และฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ ครั้ง

๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

มีการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ ครั้ง เพื่อรับมือกับสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

ข้อ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์ (Recover)

๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

๕.๑.๑ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของ ขร. สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของ ขร. เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น

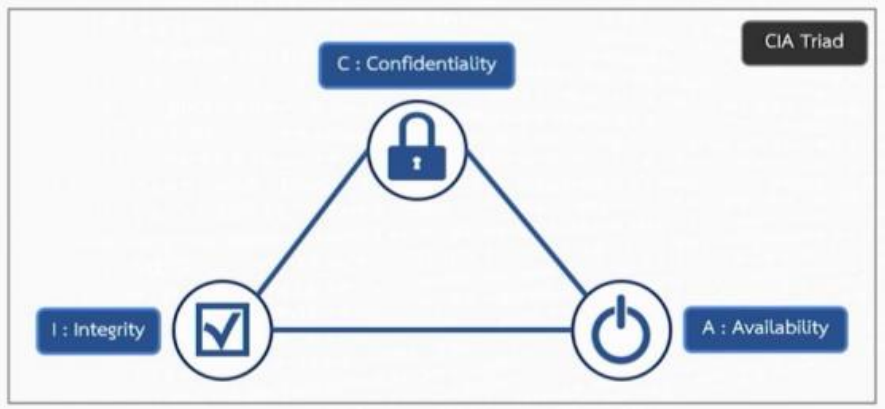
๕.๑.๒ จัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) และกำหนดบริการสำคัญที่ส่งผลกระทบต่อความต่อเนื่องทางธุรกิจ (Business Impact Analysis : BIA)

๕.๑.๓ บริหารแผนความต่อเนื่องทางธุรกิจ (Business Impact Analysis : BIA)

๕.๑.๔ ฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๒.๓ ความปลอดภัยสำหรับสารสนเทศ (Information Security)

การรักษาความปลอดภัยข้อมูล คือ การรักษาความปลอดภัยข้อมูลจากการเข้าถึง การแก้ไข และการขโมยข้อมูลโดยไม่ได้รับอนุญาตระหว่าง การประมวลผล การจัดเก็บ และการส่ง รักษาความปลอดภัยข้อมูลจัดการกับเอกสารข้อมูลทุกรูปแบบทรัพย์สินทางดิจิทัล ทรัพย์สินทางปัญญาในจิตใจของผู้คนและการสื่อสารทางวาจาและการมองเห็น วัตถุประสงค์ของการรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับองค์ประกอบที่สำคัญของการรักษาความลับ โดยทั่วไปเรียกว่า CIA Triad ประกอบด้วย



รูปที่ ๑-๒ องค์ประกอบที่สำคัญของการรักษาความลับ (CIA Triad)

Confidentiality หรือ การรักษาความลับของข้อมูล คือ การที่ระบุสิทธิในการเข้าถึงข้อมูลกับผู้ที่สามารถเข้าถึงได้ในแต่ละชุดข้อมูลตามลำดับของชั้นความลับที่กำหนดไว้ ตัวอย่างเช่น

- ข้อมูลส่วนเงินเดือนของพนักงานในองค์กร จัดเป็น ความลับสูงสุด ผู้ที่สามารถเข้าถึงได้ คือ บุคลากรของทรัพยากรบุคคลเท่านั้น
- เบอร์โทรของคนในองค์กร จัดเป็น ข้อมูลภายในเท่านั้น ผู้ที่สามารถเข้าถึงได้ คือ บุคลากรทุกคนในองค์กร

Integrity หรือ การรักษาความถูกต้องของข้อมูล คือ การที่ระบุสิทธิของการแก้ไขข้อมูล และการรักษาความถูกต้องของข้อมูลให้มีความถูกต้องอย่างต่อเนื่อง เช่น

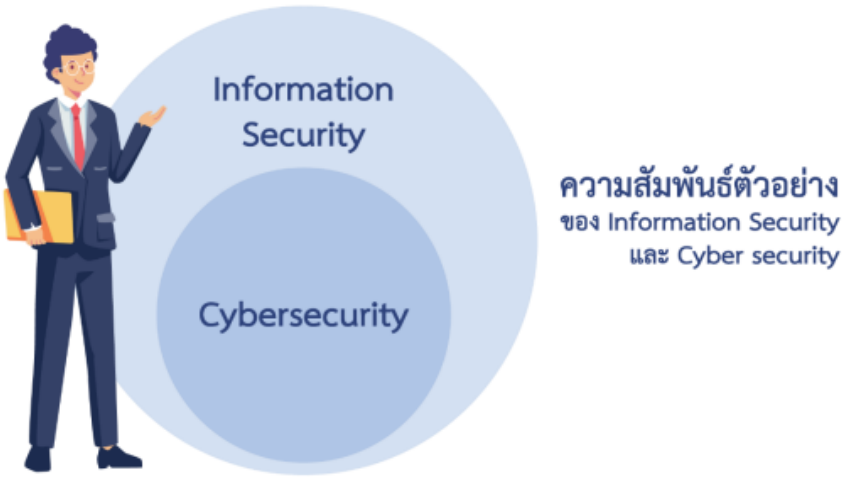
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

Availability หรือ ความพร้อมใช้งานของข้อมูล คือ การที่ข้อมูลพร้อมให้เข้าถึงใช้งานได้ตลอดเวลา รักษาความต่อเนื่องในการให้บริการข้อมูล เช่น

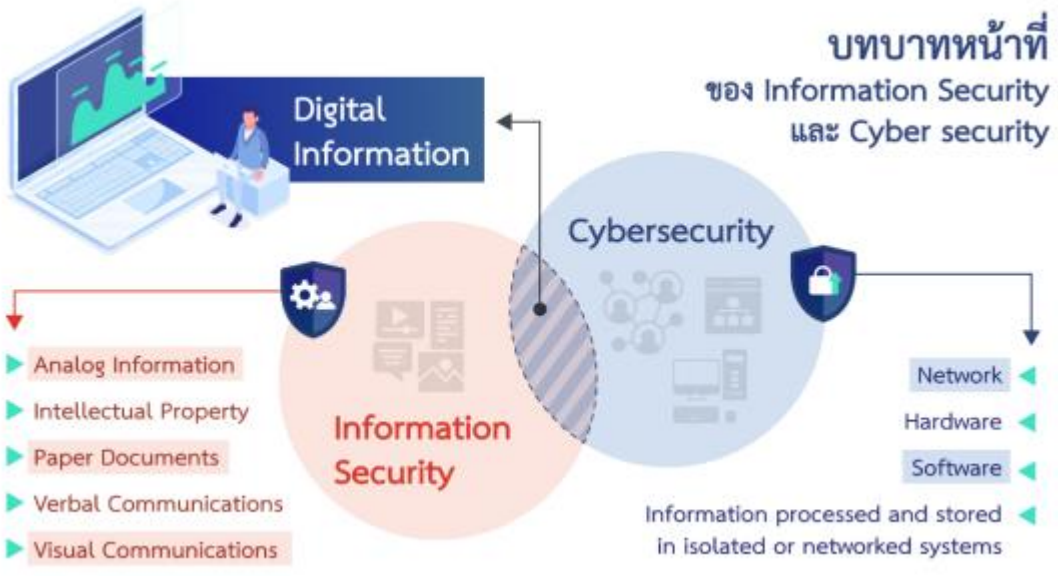
- ข้อมูลของธนาคารด้านการเงิน เช่น ข้อมูลบัญชีธนาคาร
- ข้อมูลที่อยู่บนระบบคอมพิวเตอร์

ความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security)

ความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) คือ การนำเครื่องมือทางด้านเทคโนโลยีและกระบวนการที่รวมถึงวิธีการปฏิบัติที่ถูกออกแบบไว้เพื่อป้องกัน และรับมือที่อาจจะถูกโจมตีเข้ามายังอุปกรณ์ เครือข่าย โครงสร้างพื้นฐานทางสารสนเทศ ปัจจุบันหน่วยงานภาครัฐ และภาคเอกชนได้เริ่มให้ความสำคัญในเรื่องของความมั่นคงปลอดภัยทางไซเบอร์มากยิ่งขึ้น เนื่องจากเป้าหมายในการโจมตีมีความหลากหลายมากยิ่งขึ้น รวมถึงรูปแบบของการโจมตีทางด้านไซเบอร์มีความหลากหลาย และสร้างความเสียหายให้กับองค์กร



รูปที่ ๑-๓ ความสัมพันธ์ตัวอย่างของ Information Security และ Cyber Security



รูปที่ ๑-๔ บทบาทหน้าที่ของ Information Security และ Cyber Security

ระบบการจัดความปลอดภัยของข้อมูล (ISMS)

ระบบการจัดการความปลอดภัยข้อมูล ISMS เป็นวิธีการอย่างเป็นระบบสำหรับการจัดตั้ง การดำเนินการ ติดตาม ตรวจสอบ ดูแล และปรับปรุงองค์กรความปลอดภัยของข้อมูลเพื่อบรรลุวัตถุประสงค์ทางธุรกิจ ซึ่งขึ้นอยู่กับความเสี่ยงการประเมิน และระดับการยอมรับความเสี่ยงขององค์กรที่ออกแบบมาเพื่อรักษาและจัดการความเสี่ยงอย่างมีประสิทธิภาพ

วงจรบริหารงานคุณภาพ (Plan-Do-Check-Act)

วงจรบริหารงานคุณภาพ ประกอบไปด้วย ๔ ขั้นตอน Plan-Do-Check-Act เป็นกระบวนการที่ใช้ปรับปรุงการทำงานขององค์กรอย่างเป็นระบบ โดยมีเป้าหมายเพื่อแก้ปัญหา และเกิดการพัฒนาอย่างต่อเนื่อง (Continuous improvement)

PDCA ประกอบด้วย ๔ ขั้นตอน ดังนี้

๑) วางแผน (Plan) : กำหนดนโยบาย วัตถุประสงค์ กระบวนการ และขั้นตอนที่เกี่ยวข้องกับการบริหารความเสี่ยง และการปรับปรุงความปลอดภัยของข้อมูลเพื่อให้ได้ผลลัพธ์ที่สอดคล้องกัน นโยบายและวัตถุประสงค์ขององค์กร

๒) ปฏิบัติ (Do) : ดำเนินการ และดำเนินการตามนโยบาย การควบคุมกระบวนการ และขั้นตอนของระบบการจัดการ

๓) ตรวจสอบ (Check) : ตรวจสอบและวัดกระบวนการ และประสิทธิภาพ ISMS ต่อนโยบาย วัตถุประสงค์ และข้อกำหนดสำหรับ ISMS และรายงานผลลัพธ์

๔) ปรับปรุง (Act) : ใช้การดำเนินการเพื่อปรับปรุงประสิทธิภาพ ISMS อย่างต่อเนื่อง ดำเนินการแก้ไขและป้องกันตามผลการตรวจสอบภายใน และการตรวจสอบของฝ่ายบริหาร หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องเพื่อปรับปรุงระบบดังกล่าวอย่างต่อเนื่อง

รูปที่ ๑-๕ วงจรบริหารงานคุณภาพ (Plan-Do-Check-Act)

กระบวนการทั่วไป

- วิธีการควบคุมเอกสาร
- การประเมินความเสี่ยง
- การสื่อสารภายใน
- การจัดการความเสี่ยง
- กระบวนการความรู้ความสามารถ

๒.๔ รูปแบบภัยคุกคามของ Cybersecurity

ในปัจจุบันมีภัยคุกคามหลายประเภท และเป็นภัยคุกคามที่มีความอันตรายแตกต่างกันไป เช่น

๑) Malware คือ ซอฟต์แวร์หรือโค้ดประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมา เพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูลไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus), เวิร์ม (Worms) และ โทรจัน (Trojans)

๒) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้ เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware .เว็บไซต์ส่วนใหญ่ที่โดน Hack เพื่อแก้ไขโค้ด ส่วนมากจะเป็นเว็บไซต์ประเภท CMS (Content Management System)

๓) Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail SMS เว็บไซต์ หรือ ช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๔) Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น

- Code ของเว็บไซต์ เช่น CMS
- Web Server หรือ Database Server

วิธีการโจมตีที่นิยมใช้

- Cross-Site Scripting
- SQL Injection
- Path Traversal

๕) Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความ หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail SMS เว็บไซต์ หรือช่องทาง Social โดยเป็นการส่งจำนวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

๖) DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์,ระบบการให้บริการ หรือ ระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๗) Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชั่น หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชั่น หรือผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

ผลกระทบ

- ข้อมูลสำคัญส่วนตัว หรือขององค์กรโดนนำไปเผยแพร่
- ในบางกรณีมีการเรียกค่าไถ่ของข้อมูล
- สร้างผลกระทบต่อชื่อเสียงและความน่าเชื่อถือขององค์กร

๘) Insider threat คือ ภัยที่เกิดจากภายในบุคลากร ภายในองค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำ ทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

๙) Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมาย หรือดำเนินการบางอย่างที่ถูกโปรแกรมเขียนไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้ว จะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์ เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

วิธีการป้องกัน

- สำรองข้อมูลเป็นประจำ โดยทำการแยกเก็บไฟล์สำรองข้อมูล
- ควรติดตั้ง Anti-Malware และมีการ update อย่างสม่ำเสมอ
- ก่อนเปิดไฟล์ต่าง ๆ ที่ได้รับมา ควรมีความตระหนักก่อนที่จะทำการเปิด

๑๑) Cryptojacking คือ วิธีการที่ Hacker เข้ามาเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

บทที่ ๓
แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑ แนวปฏิบัติ

๓.๑.๑ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง โดยมีขอบเขตในการตรวจสอบดังนี้

(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ

(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)

(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติ และคณะกรรมการประกาศกำหนด

๓.๑.๒ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดตามมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๓.๑.๓ ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑. เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบ โดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้

(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ

(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๓.๑.๓ (ก.)

๓.๑.๔ ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลา ที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย

๓.๑.๕ เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม.หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.

๓.๒ ความคาดหวังในการตรวจสอบ

๓.๒.๑ มีความถูกต้องแม่นยำ การตรวจสอบควรดำเนินการอย่างครอบคลุมและถูกต้องตามมาตรฐานสากลเพื่อให้ได้ข้อมูลที่สะท้อนถึงสถานะของการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กรอย่างแท้จริง

๓.๒.๒ มีวัตถุประสงค์ การตรวจสอบควรดำเนินการอย่างเป็นกลางและปราศจากอคติ เพื่อให้ได้ข้อเสนอแนะและคำแนะนำที่เป็นประโยชน์ต่อการพัฒนาการรักษาความมั่นคงปลอดภัยไซเบอร์ขององค์กร

๓.๒.๓ ความทันต่อเหตุการณ์ การตรวจสอบควรติดตามความเปลี่ยนแปลงของภัยคุกคามทางไซเบอร์อยู่เสมอเพื่อให้คำแนะนำที่สอดคล้องกับสถานการณ์ปัจจุบัน

๓.๒.๔ ความสามารถในการตอบสนองต่อภัยคุกคามอย่างรวดเร็วและมีประสิทธิภาพ

๓.๒.๕ ความสามารถในการระบุและแก้ไขช่องโหว่ก่อนที่จะถูกใช้ประโยชน์

๓.๒.๖ ความสามารถในการติดตามพฤติกรรมของผู้โจมตี

๓.๒.๗ ความสามารถในการระบุและประเมินความเสี่ยงด้านความปลอดภัยไซเบอร์ขององค์กร

๓.๓ หลักในการตรวจสอบ

การตรวจสอบควรยึดหลักการต่อไปนี้เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้เพื่อช่วยให้ผู้ตรวจสอบซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน

ก. ความซื่อสัตย์ (Integrity): รากฐานของความเป็นมืออาชีพ

- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจนและครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบ และความเที่ยงธรรมของข้อสรุปการตรวจสอบ

- ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ
- ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี
- รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๓.๔ วัตถุประสงค์ในการตรวจสอบ

๓.๔.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๓.๔.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๓.๔.๓ เพื่อระบุช่องโหว่ การตรวจสอบ ควรหาช่องโหว่ต่าง ๆ ของระบบ เพื่อช่วยในการปรับปรุง แก้ไขและปิดเส้นทางในการเข้ามาเจาะระบบ

๓.๔.๔ เพื่อประเมินความเสี่ยงด้านความปลอดภัยของข้อมูล

๓.๔.๕ เพื่อเสนอแนวทางการปรับปรุงความปลอดภัยของข้อมูล

๓.๕ ขอบเขตการตรวจสอบ

การตรวจสอบจะครอบคลุมสิ่งต่อนี้

ขอบเขต (Audit Subject)	คำอธิบาย (Description)
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรคลอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๓.๖ แนวทางการตรวจสอบ (Audit Approach)

การตรวจสอบควรใช้แนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

๓.๖.๑ การปฏิบัติตามข้อกำหนด คือ ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรองหรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๓.๖.๒ ตามความเสี่ยง คือ ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๓.๗ ข้อค้นพบการตรวจสอบ (Audit Finding)

๓.๗.๑ ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

๓.๗.๒ เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

๓.๗.๓ เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม

๓.๗.๔ เน้นแนวปฏิบัติ (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

องค์ประกอบ (Attributes)	**คำอธิบาย (Description)**
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/กฎ/เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (root cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ(ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๓.๘ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

๓.๘.๑ ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

๓.๘.๒ ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๓.๙ รูปแบบรายงานของการตรวจสอบ (Audit Report Format)

รายงานการตรวจสอบควรมีอย่างน้อยดังนี้

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๓.๔ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๓.๕ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่งคำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ค. วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๓.๗ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๓.๘ ของเอกสารนี้

๓.๑๐ ขั้นตอนปฏิบัติในการตรวจสอบ (Audit Process)

๓.๑๐.๑ วิธีการประชุมก่อนตรวจประเมิน (Opening meeting)

๓.๑๐.๑.๑ ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๓.๑๐.๑.๒ ผู้ตรวจสอบและคณะทำงานของ ขร. ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

- เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ
- การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ
- การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร
- การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ
- ยืนยันแผนการตรวจสอบ

๓.๑๐.๑.๓ ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานหน้าที่ตอบข้อซักถามและจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑๐.๑.๔ ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ
- ข้อเสนอแนะในการปรับปรุง
- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

๓.๑๐.๑.๕ ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๓.๑๐.๑.๖ คณะทำงานรับทราบผลการตรวจสอบ

๓.๑๐.๑.๗ ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับในการตรวจสอบ ระยะเวลาไม่น้อยกว่า ๙๐ วัน ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และที่แก้ไขเพิ่มเติม

๓.๑๐.๑.๘ คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๓.๑๐.๑.๙ คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๓.๑๐.๑.๑๐ ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

๓.๑๐.๒ วิธีการเก็บหลักฐานการตรวจสอบ (Audit evidence)

ผู้ตรวจสอบมีสิทธิ์ที่จะยืนยันในการเข้าถึงแหล่งข้อมูลทั้งหมดที่มีอยู่ในองค์กรที่ได้รับการตรวจสอบ เพื่อให้สามารถประเมินการควบคุมที่ประกาศได้อย่างเพียงพอ

ตัวอย่างบางส่วนของแหล่งข้อมูล :

- บันทึก (Records) : บันทึกการเข้าใช้ห้องเซิร์ฟเวอร์ที่มอบให้โดยการเข้าถึงระบบบัตรแม่เหล็ก บันทึกผู้เข้าชม
- เอกสาร (Documents) : นโยบายความปลอดภัย คู่มือพนักงาน
- การสัมภาษณ์ (Interviews) : การสัมภาษณ์ผู้ดูแลระบบเครือข่าย การสัมภาษณ์กลุ่มบุคลากร
- ฐานข้อมูลและเว็บไซต์ (Database and website) : ฐานข้อมูลพนักงานขององค์กรและอินทราเน็ต
- ตัวบ่งชี้ (Indicators) : แดชบอร์ดเกี่ยวกับตัวบ่งชี้เกี่ยวกับเหตุการณ์ด้านความปลอดภัย
- การกำหนดค่าระบบ (System configurations) : การกำหนดค่าไฟร์วอลล์ที่แสดงว่าการเข้าถึงเว็บไซต์ต้องห้ามถูกปิดกั้น
- การสังเกต (Observation) : การสังเกตว่าห้องเซิร์ฟเวอร์ถูกล็อค โดยมีการควบคุม

๓.๑๑ ทักษะของการเป็นผู้ตรวจสอบ (Auditing Skills)

๓.๑๑.๑ สมบัติของผู้ตรวจสอบ (Personal behavior)

- มีใบรับรองตามมาตรฐานสากลที่เกี่ยวข้อง เช่น Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), IRCA ISO/IEC ๒๗๐๐๑ Lead Auditor, Certified Information Security Manager (CISM), CompTIA Security+, SANS/GIAC Certified (Various)
- มีจริยธรรม เช่น ยุติธรรม จริงใจ ซื่อสัตย์
- ใจกว้าง เช่น เปิดเปิดรับฟังความคิดเห็นต่างของผู้อื่น
- มีชั้นเชิง เช่น มีไหวพริบในการติดต่อบุคคล
- ช่างสังเกต เช่น การสังเกตสภาพแวดล้อมต่าง ๆ
- เฉลียวฉลาด เช่น สามารถเข้าใจสถานการณ์ต่าง ๆ ได้
- รอบรู้ เช่น พร้อมปรับตัวเข้ากับสถานการณ์ต่าง ๆ ได้
- ยืนหยัด เช่น แน่วแน่ และมุ่งมั่นที่จะบรรลุวัตถุประสงค์
- เฉียบขาด เช่น สามารถทำข้อสรุปต่าง ๆ ได้ทัน
- พึ่งพาตนเองได้ เช่น ทำหน้าที่ได้อย่างเป็นอิสระ
- ดำเนินงานด้วยความอดทน เช่น สามารถดำเนินงานได้อย่างมีความรับผิดชอบ มีจริยธรรม
- เปิดรับการปรับปรุง เช่น ยินดีที่จะเรียนรู้สิ่งใหม่ ๆ
- มีความอ่อนไหวทางวัฒนธรรม เช่น เชื่อฟัง ยอมรับในวัฒนธรรมของผู้รับตรวจ
- ให้ความร่วมมือ เช่น มีปฏิสัมพันธ์กับผู้อื่น

๓.๑๑.๒ ความรู้และทักษะของผู้ตรวจสอบ (Knowledge and skills)

- เข้าใจถึงประเภทของความเสี่ยงที่เกี่ยวข้องกับการตรวจสอบ
- วางแผน และจัดการงานอย่างมีประสิทธิผล
- ตรวจสอบภายในตามตารางเวลาที่กำหนด
- จัดลำดับความสำคัญ และให้ความสำคัญในเรื่องต่าง ๆ
- สื่อสารอย่างมีประสิทธิผล ทั้งทางวาจา และลายลักษณ์อักษร
- เก็บข้อมูลผ่านการสัมภาษณ์ การฟัง การสังเกตการณ์ และการทบทวนเอกสาร
- เข้าใจความเหมาะสมของการใช้เทคนิคการสุ่ม
- รักษาความลับของข้อมูล