แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
กรมบังคับคดี

สารบัญ

หัวข้อ	หน้า
บทที่ ๑ บทนำ	๑
๑.๑ หลักการและเหตุผล	๑
๑.๒ วัตถุประสงค์	๑
๑.๓ ขอบเขต	๑
๑.๔ คำนิยาม	๑
บทที่ ๒ แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษามั่นคงปลอดภัยไซเบอร์	๓
๒.๑ การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๓
๒.๒ กิจกรรมตามกรอบมาตรฐาน	๓
๒.๓ ความปลอดภัยสำหรับสารสนเทศ (Information Security)	๑๖
๒.๔ รูปแบบภัยคุกคามของ Cybersecurity	๑๘
บทที่ ๓ แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์	๒๑
๓.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๒๑
๓.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๒๑
๓.๓ แผนการรับมือภัยคุกคามทางไซเบอร์	๒๒
๓.๔ การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์	๒๒

บทที่ ๑
บทนำ

๑.๑ หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของประเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยทางไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และไปในทิศทางเดียวกัน กรมบังคับคดี ในฐานะหน่วยงานของรัฐ จึงจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความปลอดภัยทางไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ และประกาศคณะกรรมการกำกับดูแล ด้านความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.๒๕๖๔

๑.๒ วัตถุประสงค์

เพื่อกำหนดกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์พร้อมทั้งนำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโนโลยีสารสนเทศของกรมบังคับคดี ให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน

๑.๓ ขอบเขต

เอกสารฉบับนี้ครอบคลุมตามกรอบและวิธีปฏิบัติสำหรับด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ใช้กับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๑.๔ คำนิยาม

๑) หน่วยงาน หรือ องค์กร หมายถึง กรมบังคับคดี

๒) คณะกรรมการ หมายถึง คณะทำงานด้านเทคโนโลยีสารสนเทศของกรมบังคับคดี

๓) ดัชนีชี้วัดความเสี่ยงที่สำคัญ หมายถึง เครื่องมือที่ใช้วัดกิจกรรมที่อาจจะทำให้องค์กรมีความเสี่ยงที่เพิ่มขึ้น ช่วยติดตามความเสี่ยงพร้อมทั้งเป็นสัญญาณเตือน เพื่อให้หน่วยงานสามารถคาดการณ์เหตุการณ์และความเสี่ยงในอนาคต และเตรียมมาตรการการป้องกันก่อนเกิดเหตุการณ์ความเสียหาย

๔) คอมไพเลอร์ หมายถึง โปรแกรมแปลโปรแกรม ตัวแปลโปรแกรมเป็นโปรแกรมคอมพิวเตอร์ที่ทำหน้าที่แปลงชุดคำสั่งภาษาคอมพิวเตอร์หนึ่งไปเป็นชุดคำสั่งที่มีความหมายเดียวกันในภาษาคอมพิวเตอร์อื่น

๕) แพตซ์ หมายถึง โปรแกรมที่ใช้ในการปรับปรุงแก้ไขซอฟแวร์ โดยส่วนใหญ่จะอยู่ในลักษณะของไฟล์ และใช้เพื่อแก้ไขช่องโหว่เรื่องความมั่นคงปลอดภัย หรือเพื่อเพิ่มความสามารถของซอฟแวร์ ผู้พัฒนาซอฟแวร์หลายราย ได้เผยแพร่แพตซ์ออกมาเป็นระยะ เช่น บริษัท Microsoft จะเผยแพร่แพตซ์ ที่แก้ไขช่องโหว่ของซอฟต์แวร์ผ่านระบบ Windows Update

๖) Recovery Time Objective (RTO) หมายถึง ระยะเวลาในการกู้คืนระบบ

๗) Recovery Point Objective (RPO) หมายถึง ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย

๘) Maximum Tolerance Period หมายถึง ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงัก of Disruption (MTPD) เพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงัก หรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด

๙) ผู้ใช้งาน หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของกรมบังคับคดี

๑๐) บุคคลภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่เข้ามาประชุมหรือปฏิบัติงานร่วมกับกรมบังคับคดี

๑๑) หน่วยงานภายนอก หมายถึง หน่วยงานภายนอกที่กรมบังคับคดีอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูล หรือทรัพย์สินต่าง ๆ ของกรมบังคับคดี โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๒) สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของกรมบังคับคดี

๑๓) ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบงาน

๑๔) สินทรัพย์ หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตน อันมีมูลค่าคุณค่าสำหรับกรมบังคับคดี

๑๕) การเข้าถึงหรือควบคุม หมายถึง การขออนุญาต การกำหนดสิทธิ หรือการใช้งานสารสนเทศมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานระบบสารสนเทศและระบบเครือข่าย

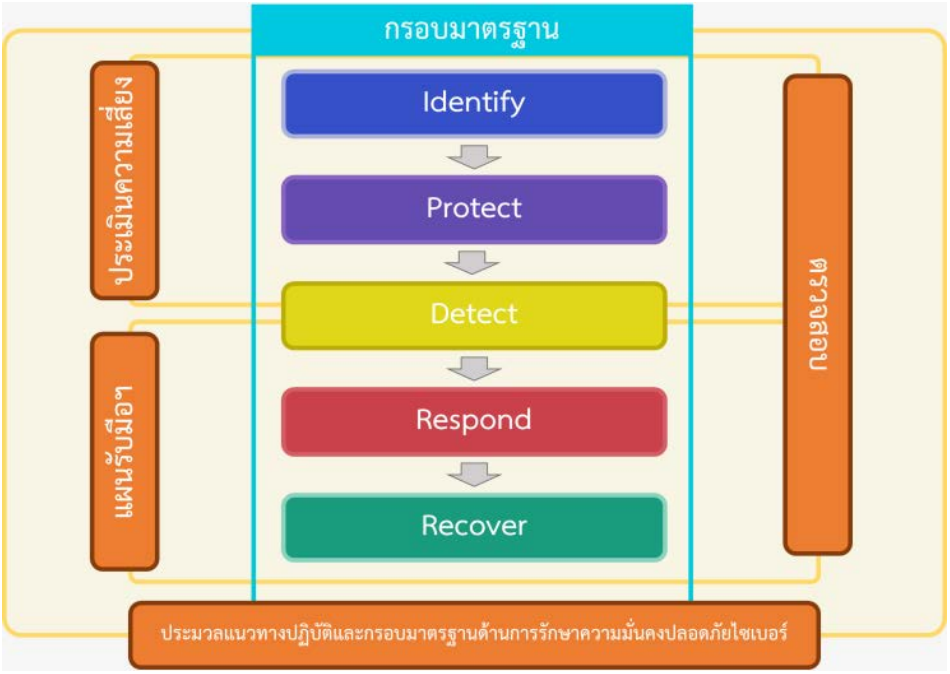
๑๖) ความมั่นคงปลอดภัย หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องด้านสารสนเทศครบถ้วนและสภาพพร้อมใช้งานของระบบเทคโนโลยีสารสนเทศ

บทที่ ๒
แนวปฏิบัติตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒.๑ การปฏิบัติเพื่อให้สอดคล้องตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยทางไซเบอร์ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยทางไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ สามารถสรุปกิจกรรมการดำเนินการต่าง ๆ ดังต่อไปนี้

รูปที่ ๑ กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์



๒.๒ กิจกรรมตามกรอบมาตรฐาน

รายละเอียดของแต่ละกิจกรรมมีดังนี้

๑) Identify คือ การระบุและเข้าใจถึงบริบทต่าง ๆ เพื่อการบริหารจัดการความเสี่ยงที่เกิดขึ้นแก่ระบบคอมพิวเตอร์ ข้อมูลที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล

๒) Protect คือ การวางมาตรฐานควบคุมเพื่อปกป้องระบบของหน่วยงาน

๓) Detect คือ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์

๔) Response คือ มาตรการเผชิญเหตุ เมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์

๕) Recover คือ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

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 ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญที่กระทบต่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามเกณฑ์ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) และจัดทำทะเบียนประเมินความเสี่ยงโดยมีรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทความเสี่ยง/กิจกรรม

(ข) ปัจจัยความเสี่ยง

(ค) กิจกรรมในการควบคุม

(ง) ความสำคัญ

(ฉ) ระยะเวลา

(ง) หน่วยงานที่รับผิดชอบ

๑.๒.๒ กำหนดปัจจัยต่าง ๆ ที่เกี่ยวข้องกับประเมินความเสี่ยงที่เกิดขึ้นจากปัจจัยภายนอก อาทิ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

๑.๒.๓ ปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๑.๒.๔ กำหนดเกณฑ์การประเมินความเสี่ยง ได้แก่ การระบุโอกาสการเกิดขึ้นของเหตุการณ์ความเสี่ยง การระบุผลกระทบของเหตุการณ์ความเสี่ยง และระดับความเสี่ยงที่ยอมรับได้

๑.๒.๕ วิเคราะห์และประเมินความเสี่ยงต่อทรัพย์สินสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการเปลี่ยนแปลงทรัพย์สินของระบบสารสนเทศที่สำคัญโดยมีการบริหารจัดการความเสี่ยงดังนี้

(๑) จัดทำแผนการลดความเสี่ยงโดยพิจารณาถึงลำดับความสำคัญในการดำเนินการ ค่าใช้จ่าย ความคุ้มค่าหรือประโยชน์ที่ได้รับ และผู้รับผิดชอบในการดำเนินการ

(๒) นำเสนอแผนการลดความเสี่ยงต่อผู้บังคับบัญชาเพื่อพิจารณาและให้ข้อคิดเห็นตามความจำเป็น

(๓) ผู้บังคับบัญชาสั่งการให้ดำเนินการตามแผนและรายงานผลการดำเนินการให้ได้รับทราบเป็นระยะ ๆ จนกระทั่งเสร็จสิ้น

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ดำเนินการดังนี้

๑.๓.๑ ติดตามและตรวจสอบช่องโหว่ทางเทคนิคที่มีการประกาศจากเว็บไซต์หรือแหล่งข้อมูลของเจ้าของผลิตภัณฑ์ต่าง ๆ ที่มีการใช้งานบนระบบสารสนเทศ หรือจากแหล่งข้อมูลของศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (ThaiCERT) หรือจากแหล่งอื่นที่น่าเชื่อถือ เป็นต้น

๑.๓.๒ ประเมินช่องโหว่ของบริการที่สำคัญโดยอ้างอิงตามหลักการบริหารความเสี่ยงของกรมบังคับคดี เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญ

๑.๓.๓ การตรวจสอบขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย

(ก) การประเมินความมั่นคงปลอดภัยของเครื่องคอมพิวเตอร์แม่ข่าย และระบบที่ให้บริการ

(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) รวมถึงการทดสอบเจาะระบบของเครื่องคอมพิวเตอร์แม่ข่าย เครือข่าย และระบบงานของบริการที่สำคัญโดยเฉพาะอย่างยิ่ง ทุกระบบที่มีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

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

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

๑.๓.๙ การทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบจะต้องดำเนินการภายใต้การควบคุมดูแลของกรมบังคับคดี

๑.๓.๑๐ ติดตาม ปรับปรุง และแก้ไข ตามข้อเสนอแนะจากผลการทดสอบเจาะระบบและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่ พร้อมทั้งตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอแล้ว โดยเฉพาะอย่างยิ่งช่องโหว่ในระดับวิกฤติ และระดับสูง

ทั้งนี้ กรมบังคับคดี กำหนดให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดให้มีการตรวจประเมินช่องโหว่และทดสอบเจาะระบบตามแนวทางที่ได้กำหนดไว้เบื้องต้น และกรณีที่มีการตรวจพบช่องโหว่บนระบบ

สารสนเทศต้องแจ้งให้ผู้รับผิดชอบระบบสารสนเทศปรับปรุงและแก้ไขช่องโหว่โดยเร่งด่วน โดยเฉพาะอย่างยิ่งช่องโหว่ที่มีความรุนแรงระดับวิกฤตและระดับสูง โดยผู้รับผิดชอบต้องดำเนินการแก้ไขให้แล้วเสร็จโดยเร็วหรือไม่เกินกว่า ๗ วัน นับจากวันที่ได้รับแจ้งจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมทั้งรายงานผลการแก้ไขกลับมายังศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและดำเนินการตรวจสอบการแก้ไขปรับปรุง หากไม่สามารถดำเนินการแก้ไขช่องโหว่ได้ ผู้รับผิดชอบระบบสารสนเทศต้องชี้แจงความจำเป็นและเหตุผลประกอบ พร้อมกำหนดมาตรการชดเชยหรือการดำเนินการเพื่อลดความเสี่ยงของช่องโหว่ทางเทคนิคนั้น หรือในกรณีที่มีความจำเป็นอาจต้องปิดการให้บริการระบบสารสนเทศนั้นเป็นการชั่วคราวในระหว่างที่ยังไม่ได้ดำเนินการแก้ไขช่องโหว่ โดยเสนอผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารหรือผู้ที่ได้รับมอบหมายพิจารณาและให้ความเห็นชอบ

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management) ดำเนินการดังนี้

๑.๔.๑ แจ้งผู้ให้บริการภายนอกได้รับทราบถึงความรับผิดชอบ (Responsible) และภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ไม่ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญของกรมบังคับคดี

๑.๔.๒ ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระกวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานทางสารสนเทศของผู้ให้บริการภายนอกในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

(ก) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญตามความต้องการทำงธุรกิจของกรมบังคับคดี และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

(ข) ภาระหน้าที่ของผู้ให้บริการภายนอกในการปกป้องบริการที่สำคัญ

(ค) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

(ง) สิทธิของกรมบังคับคดี ในการตรวจสอบความมั่นคงปลอดภัยทางไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ สร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยทางไซเบอร์ตามเงื่อนไขที่ระบุในสัญญา

๑.๔.๔ ดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับที่เกี่ยวข้อง

ข้อ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Asset Control) ดำเนินการดังนี้

๒.๑.๑ การเข้าถึงบริการที่สำคัญของกรมบังคับคดีถูกจำกัดไว้ที่

(ก) บุคลากร และกิจกรรมที่ได้รับอนุญาต

(ข) อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาต

๒.๑.๒ ให้แต่ละบุคลากร กิจกรรมและกระบวนการที่ได้รับอนุญาตให้เข้าถึงบริการที่สำคัญของกรมบังคับคดี ต้องจัดให้มีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ

๒.๑.๓ เก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญ และตรวจสอบบันทึกเหล่านี้เพื่อหากิจกรรมที่ผิดปกติเป็นประจำ

ความสม่ำเสมอในการตรวจสอบบันทึกเหล่านี้ควรสอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว

๒.๑.๔ ตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ เช่น USB พอร์ตอนุกรม และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น และทำภายใต้การดูแลของกรมบังคับคดี

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening) ดำเนินการดังนี้

๒.๒.๑ สร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชั่น และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ (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) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใด 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 กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของกรมบังคับคดีมีมาตรการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของกรมบังคับคดีต้องปฏิบัติตามแนวทางปฏิบัติ ดังนี้

๑) เปิดใช้งานการเชื่อมต่อระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น

๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)

๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)

๔) มีเทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two-Factor Authentication) กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างสม่ำเสมอ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของกรมบังคับคดีเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น แล็ปท็อป กับบริการที่สำคัญของกรมบังคับคดีโดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด เช่น พอร์ต USB ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของกรมบังคับคดี

๒.๔.๒ กรมบังคับคดีมีการเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของกรมบังคับคดีบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ กรมบังคับคดีมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cybersecurity Awareness) ดำเนินการดังนี้

๒.๕.๑ กรมบังคับคดีมีการเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางไซเบอร์และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งานในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๕.๒ กรมบังคับคดีมีการจัดทำ ปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบันและมีการเผยแพร่ผ่านช่องทางที่เหมาะสม

๒.๕.๓ กรมบังคับคดีมีการจัดฝึกอบรมการใช้งานระบบสารสนเทศให้มีความปลอดภัยอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒.๕.๔ กรมบังคับคดีมีการสร้างความตระหนัก (Awareness Program) เรื่องการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ

๒.๕.๕ กรมบังคับคดีมีการจัดให้มีการฝึกอบรมและพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมและเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์กับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

ประโยชน์ที่ได้รับจากการทำ Security Awareness

๑. บุคลากรที่มีความรู้ด้านการรักษาความมั่นคงปลอดภัย สามารถใช้งานทรัพยากรสารสนเทศขององค์กรได้ถูกต้อง ปลอดภัย ป้องกันภัยคุกคามและแจ้งเหตุผิดปกติให้องค์กรสามารถยับยั้งความเสียหายได้ทันท่วงที

๒. ลดความเสี่ยงที่อาจเกิดขึ้นจากภัยคุกคามทุกรูปแบบ เช่น Phishing Email Ransomware เว็บไซต์อันตรายโฆษณาชวนเชื่อ หรือกลอุบายต่าง ๆ จากผู้ไม่ประสงค์ดีต่อองค์กร

๓. ทรัพย์สินปลอดภัย ข้อมูลเป็นความลับ เมื่ออัตราการถูกโจมตีลดลง ความปลอดภัยของทรัพย์สินรวมถึงข้อมูลความลับต่าง ๆ ก็เพิ่มขึ้น

๔. เกิดความเชื่อมั่นด้านความปลอดภัย ผู้ใช้บริการและคู่ค้าทางธุรกิจจะไว้วางใจที่จะทำงานร่วมกับองค์กรมากขึ้น

กรมบังคับคดี ได้มีการดำเนินการด้าน Security Awareness ให้กับการปฏิบัติงานเจ้าหน้าที่กรมบังคับคดี ดังนี้

การควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑. การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่อนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของหน่วยงาน ดังนั้นผู้ใช้ต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพ

(๒) โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน

(๔) การตั้งชื่อเครื่องคอมพิวเตอร์จะต้องกำหนดโดยเจ้าหน้าที่ของศูนย์เท่านั้น

(๕) ห้ามคัดลอกโปรแกรมต่างๆ ที่ติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานซึ่งมีลิขสิทธิ์ถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๖) การเคลื่อนย้ายจุดติดตั้งหรือตรวจซ่อมคอมพิวเตอร์จะต้องดำเนินการโดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเท่านั้น

(๗) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๘) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ใช้งานอยู่

(๙) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์โดยปฏิบัติ ดังนี้

- ไม่นำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์
- ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

๒. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์

(๑) เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัสให้กับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้ต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Thumb Drive ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๓) ผู้ใช้ต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานเสมอ

(๔) ผู้ใช้ต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๓. การสำรองข้อมูลและการกู้คืน

เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องรับผิดชอบในการสำรองข้อมูล และเก็บรักษาข้อมูล เมื่อผู้ใช้นำเครื่องคอมพิวเตอร์มาทำการตรวจสอบ ซ่อมแซม และหากทำการตรวจสอบซ่อมแซมจนเครื่องคอมพิวเตอร์สามารถใช้งานได้ตามปกติเป็นที่เรียบร้อยแล้ว ก็ต้องทำการเคลื่อนย้ายข้อมูลกลับไปให้คงเดิม

การใช้เกี่ยวกับรหัสผ่าน (Password)

มีการกำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password user) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือกลุ่มเหมือนกัน

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล (Save Password)

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาทุก ๆ ๑๘๐ วัน หรือเปลี่ยนรหัสผ่านทันทีเมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานต่างๆ ที่ตนใช้งาน

(๑๔) หลีกเลี่ยงการใช้รหัสผ่านเดิมเมื่อเปลี่ยนรหัสผ่านใหม่

(๑๕) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป

การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

(๑) เจ้าหน้าที่ในสังกัด หากต้องการติดต่องานราชการหรือติดต่อกับบุคคลภายนอก ให้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน หรือของส่วนราชการที่กำหนดให้เท่านั้น ห้ามนำไปใช้ติดต่อในเรื่องส่วนตัว และห้ามติดต่องานราชการผ่านระบบจดหมายอิเล็กทรอนิกส์ของเว็บไซต์ผู้ให้บริการอื่น

(๒) สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบ ผู้ใช้ทุกคนจะต้องทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

(๓) ห้ามผู้ใช้ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติของระบบจดหมายอิเล็กทรอนิกส์

(๔) ผู้ใช้ต้องระมัดระวังการใช้งานจดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และมาแสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์

(๕) ผู้ใช้ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(๖) ผู้ใช้ต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของหน่วยงาน เพื่อการทำงานของหน่วยงานเท่านั้น

(๗) หลังจากใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น และทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(๘) ผู้ใช้ต้องทำการตรวจเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

(๙) ผู้ใช้ต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

(๑๐) ห้ามผู้ใช้ใช้ข้อความที่ไม่สุภาพหรือรับ-ส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงาน ทำให้เกิดความแตกแยกระหว่างองค์กรผ่านทางจดหมายอิเล็กทรอนิกส์ และต้องระบุชื่อผู้รับและหัวข้อให้ชัดเจน

(๑๑) หลีกเลี่ยงการส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่านบัญชีผู้ใช้งาน หมายเลขบัตรประชาชน ผ่านจดหมายอิเล็กทรอนิกส์

(๑๒) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ต้องระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๑๓) ผู้ใช้ต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

(๑๔) ผู้ใช้ต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

(๑๕) ผู้ใช้ต้องย้ายจดหมายอิเล็กทรอนิกส์ที่จำเป็นต้องนำมาใช้ในภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อป้องกันผู้อื่นแอบเข้าไปแอบอ่านจดหมายได้

(๑๖) ไม่จัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

(๑๗) การใช้งานระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน จะถือว่าผู้ที่เข้าใช้บริการรับทราบ ทำความเข้าใจและยอมรับนโยบายจดหมายอิเล็กทรอนิกส์ของหน่วยงานแล้ว

การใช้งานเว็บไซต์ (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)

(๑) สิ่งที่ควรปฏิบัติเพื่อความปลอดภัย คือ ไม่ควรบันทึก Password ไว้ที่โปรแกรม

(๒) กรณีไม่ใช่เครื่องคอมพิวเตอร์ส่วนตัว ไม่ควรบันทึกไฟล์ต่าง ๆ ไว้บนเครื่อง

(๓) มีความตระหนักก่อนเปิด Link หรือ ไฟล์ต่าง ๆ ที่ได้รับมา

(๔) มีการ Update Version ของโปรแกรมอย่างสม่ำเสมอ

การประชุม (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

การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless)

(๑) ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย

(๒) ผู้ดูแลระบบจะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ผู้ดูแลระบบเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่

(๕) ผู้ดูแลระบบต้องกำหนดค่าของการใช้งานให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

(๖) ผู้ดูแลระบบต้องมีการแยก VLAN ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๗) ผู้ดูแลระบบต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในหน่วยงาน

(๘) ผู้ดูแลระบบต้องใช้ซอฟท์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

การใช้โทรศัพท์ (Mobile)

การใช้โทรศัพท์มือถืออย่างปลอดภัยเป็นสิ่งสำคัญ เพราะโทรศัพท์มือถือมีข้อมูลส่วนบุคคลและข้อมูลที่อาจเป็นอันตรายหากถูกเข้าถึงโดยไม่ชอบด้วยวิธีต่างๆ

(๑) ป้องกันด้วยรหัสผ่าน: ตั้งรหัสผ่านที่แข็งแกร่งเพื่อป้องกันการเข้าถึงโดยไม่ชอบด้วยและเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ ไม่ควรใช้รหัสผ่านที่ซ้ำกับที่ใช้ในบัญชีอื่นๆ

(๒) อัปเดตซอฟต์แวร์และแอปพลิเคชัน: รักษาระบบปฏิบัติการและแอปพลิเคชันบนโทรศัพท์มือถือให้เป็นเวอร์ชันล่าสุดเสมอ เพื่อป้องกันช่องโหว่ความปลอดภัยที่อาจถูกใช้ในการโจมตี

(๓) ใช้แอปพลิเคชันที่มีความปลอดภัย: ควรใช้แอปพลิเคชันจากที่มั่นคงและไม่สร้างความเสี่ยงต่อความปลอดภัย เช่น ใช้ที่มีการตรวจสอบและการอัปเดตตามปกติ

(๔) ปิดการใช้งานบริการที่ไม่จำเป็น: ปิดการใช้งานบริการที่ไม่จำเป็นเช่น Bluetooth, NFC หรือ Wi-Fi ที่ไม่ได้ใช้งานเพื่อลดความเสี่ยงจากการโจมตี

(๕) หลีกเลี่ยงการเชื่อมต่อกับเครือข่าย Wi-Fi สาธารณะ: หากไม่จำเป็น ควรหลีกเลี่ยงการใช้เครือข่าย Wi-Fi สาธารณะที่ไม่มีการรักษาความปลอดภัยที่เพียงพอ

(๖) ระวังการคลิกลิงก์และแนบไฟล์: อย่าเปิดลิงก์หรือแนบไฟล์จากแหล่งที่ไม่น่าเชื่อถือ เพราะอาจเป็นการโจมตีด้วยซอฟต์แวร์มัลแวร์

(๗) สำรองข้อมูลและตรวจสอบความปลอดภัย: สำรองข้อมูลสำคัญอยู่บ่อยๆ และตรวจสอบการตั้งค่าความปลอดภัยของโทรศัพท์เป็นประจำ

ข้อ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Treat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านไซเบอร์ที่ยอมรับได้ตามที่กำหนดไว้ โดยกรมบังคับคดีมีกระบวนการในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังนี้

๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ มีกระบวนการในการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่ตรวจพบ

๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของกรมบังคับคดี

๓.๔ ต้องดำเนินการตรวจสอบกลไกและกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

ข้อ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ดำเนินการดังนี้

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) กรมบังคับคดีมีการจัดทำการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ กรมบังคับคดีมีการจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๔.๒.๒ กรมบังคับคดีมีการตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์มหรือช่องทางการเผยแพร่ที่เหมาะสม เช่น สื่อดั้งเดิมและโซเชียลมีเดียสำหรับการเผยแพร่ข้อมูล

๔.๒.๓ กรมบังคับคดีมีการตรวจสอบแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ กรมบังคับคดีมีการดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผล ในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

ข้อ ๕ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery) เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือเมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์หน่วยงานควรกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าวควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้น

๕.๑ กรมบังคับคดีมีการจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมบังคับคดี สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงาน เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อย ดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และระบบสารสนเทศโดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงัก ลำดับความสำคัญในการกู้คืนระบบ เป็นต้น

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่อง มีการควบคุมดูแล การแก้ไขและกู้คืนระบบ เมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และระบบสารสนเทศ

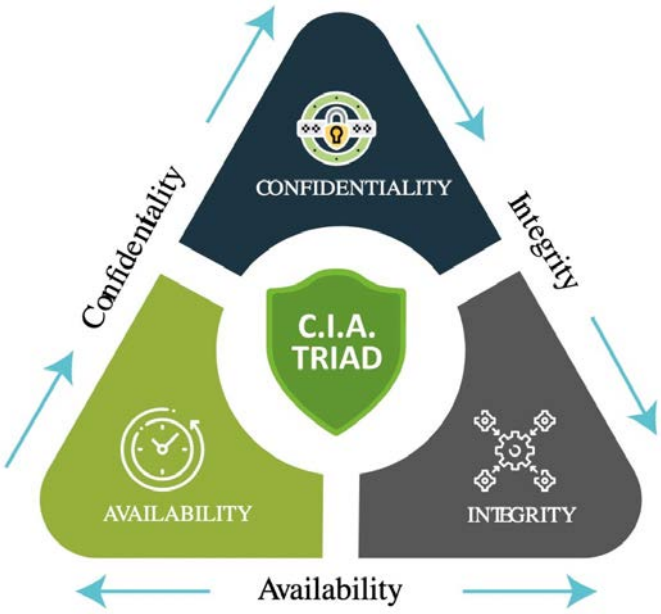
๕.๒ กรมบังคับคดีมีการตรวจสอบให้แน่ใจว่ามีการฝึกซ้อมแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) กรมบังคับคดีจะดำเนินการจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการให้คณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมทราบทุกระยะ

๒.๓ ความปลอดภัยสำหรับสารสนเทศ (Information Security)

การรักษาความปลอดภัยข้อมูล คือ การรักษาความปลอดภัยข้อมูลจากการเข้าถึง การแก้ไข และการขโมยข้อมูลโดยไม่ได้รับอนุญาตระหว่าง การประมวลผล การจัดเก็บ และการส่ง รักษาความปลอดภัยข้อมูล จัดการ กับเอกสารข้อมูลทุกรูปแบบทรัพย์สินทางดิจิทัล ทรัพย์สินทางปัญญาในจิตใจของผู้คนและการสื่อสารทางวาจา และการมองเห็นวัตถุประสงค์ของการรักษาความปลอดภัยข้อมูลที่เกี่ยวข้องกับองค์ประกอบที่สำคัญของการรักษาความลับ โดยทั่วไปเรียกว่า CIA Triad ประกอบด้วย

รูปที่ 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)

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

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 ดำเนินการแก้ไข และป้องกันตามผลการตรวจสอบภายใน และการตรวจสอบของฝ่ายบริหาร หรือข้อมูลอื่น ๆ ที่เกี่ยวข้องเพื่อปรับปรุงระบบดังกล่าวอย่างต่อเนื่อง

รูปที่ ๓ 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 โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมาชื่อเรียก Malware นั้น ครอบคลุมถึง ไวรัส (Virus) เวิร์ม (Worms) และ โทรจัน (Trojans)

๒) Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทาเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์ โดยการใส่โค้ดที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง 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 โดยเป็นการส่งจานวนมาก หรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญ หรือก่อกวน

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

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

<u>ผลกระทบ</u>

- 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 เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมเขียนไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๑๐) Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้ว จะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์ เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

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
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๓.๑ แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กรมบังคับคดีมีการตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยทางไซเบอร์โดยคณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม รับรองอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์

กรมบังคับคดีมีการกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยทางไซเบอร์ ซึ่งมีการกำหนด เรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์และมีการจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์โดยจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้

๓.๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงานบุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๓.๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ยอมรับได้

๓.๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ที่ยอมรับได้

๓.๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ต่อคณะอนุกรรมการ ตามรอบการประชุมของคณะอนุกรรมการมีการทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยทางไซเบอร์ ความเสี่ยงมาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓.๓ แผนการรับมือภัยคุกคามทางไซเบอร์

กรมบังคับคดีมีการดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๓.๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้อง

๓.๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของกรมบังคับคดี หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์

๓.๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยทางไซเบอร์

กรมบังคับคดีต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยทางไซเบอร์ไปยังคณะอนุกรรมการด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรมอย่างน้อย ดังนี้

๓.๔.๑ แนวนโยบายหรือแนวปฏิบัติด้านในการรักษาความมั่นคงปลอดภัยทางไซเบอร์

๓.๔.๒ เหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) ที่ตรวจพบ และผลดำเนินการในการตรวจสอบเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident) (ถ้ามี)

๓.๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)

๓.๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

๓.๔.๕ การพัฒนาบุคลากรด้านความมั่นคงปลอดภัยทางไซเบอร์

๓.๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยทางไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น