ประกาศกรมสอบสวนคดีพิเศษ
เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ ของกรมสอบสวนคดีพิเศษ
พ.ศ. ๒๕๖๘

จัดทำโดย ศูนย์สารสนเทศ
กองเทคโนโลยีสารสนเทศและศูนย์ข้อมูลการตรวจสอบ

ประกาศกรมสอบสวนคดีพิเศษ
เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษ
พ.ศ. ๒๕๖๘

ด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามมาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว เพื่อให้มาตรฐานความปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษสอดคล้องกับมาตรฐานสากล

อาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม ประกอบมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กรมสอบสวนคดีพิเศษจึงออกประกาศมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้ เรียกว่า “ประกาศกรมสอบสวนคดีพิเศษ เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ กรณีที่มีการแก้ไขเพิ่มเติมมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ โดยคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติที่แตกต่างไปจากที่กำหนดไว้ในประกาศนี้ ให้ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสอบสวนคดีพิเศษถือปฏิบัติตามที่ได้มีการแก้ไข หรือเพิ่มเติม นั้น

ข้อ ๔ ให้ใช้มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษแนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๖ กันยายน พ.ศ. ๒๕๖๘

พันตำรวจตรี
(ยุทธนา แพรดำ)
อธิบดีกรมสอบสวนคดีพิเศษ

สารบัญ

สารบัญ (ต่อ)

บัญชีแนบท้ายประกาศกรมสอบสวนคดีพิเศษ
เรื่อง มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์
ของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘
****

๑. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ตามมาตรา ๔๔ ได้กำหนดให้หน่วยงานของรัฐ จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว กรมสอบสวนคดีพิเศษในฐานะหน่วยงานรัฐ จึงได้ดำเนินการจัดทำมาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษ โดยกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรืออย่างร้ายแรงต่อระบบสารสนเทศ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมสอบสวนคดีพิเศษ สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

๓. ขอบเขตการใช้

มาตรฐานและแนวปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษฉบับนี้มีผลบังคับใช้ครอบคลุมข้อมูล และระบบสารสนเทศของกรมสอบสวนคดีพิเศษ

๔. คำนิยาม

หน่วยงาน	หมายถึง	กรมสอบสวนคดีพิเศษ
Recovery Time Objective (RTO)	หมายถึง	ระยะเวลาในการกู้คืนระบบ
Recovery Point Objective (RPO)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย
Maximum Tolerance Period of Disruption (MTPD)	หมายถึง	ระยะเวลาสูงสุดที่ยอมให้ธุรกิจหยุดชะงักเพื่อรองรับการดำเนินธุรกิจอย่างต่อเนื่องของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และรองรับการเกิดเหตุการณ์ผิดปกติต่าง ๆ ที่อาจส่งผลให้เกิดการหยุดชะงักหรือเกิดความเสียหายต่อระบบ เช่น ภัยคุกคามการทำงานได้ตามปกติให้เร็วที่สุด
Business Continuity Plan	หมายถึง	แผนบริหารความต่อเนื่องทางธุรกิจ

๕. การจัดทำมาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกรมสอบสวนคดีพิเศษ มี ๒ ส่วน ดังนี้

ส่วนที่ ๑
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวปฏิบัติ

๑. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบอย่างน้อย ดังนี้

๑) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานโดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้

๒.๑ การประเมินความเสี่ยง (Risk Assessment)

๑) การระบุความเสี่ยง (Risk Identification)

ระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

๒) การวิเคราะห์ความเสี่ยง (Risk Analysis)

เข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๓) การประเมินค่าความเสี่ยง (Risk Evaluation)

ประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจรวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒.๒ การจัดการความเสี่ยง (Risk Treatment)

มีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้

๒.๓ ติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

มีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๒.๔ การรายงานความเสี่ยง (Risk Reporting)

รายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะอนุกรรมการ ตามรอบการประชุมของคณะอนุกรรมการ

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๓. แผนการรับมือภัยคุกคามทางไซเบอร์

หน่วยงานต้องดำเนินการจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

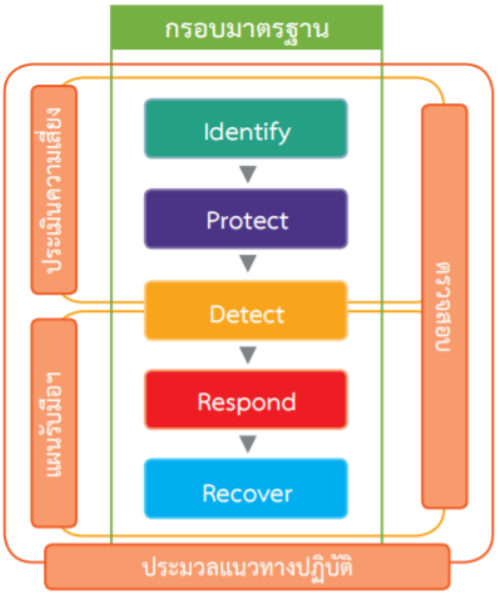
๓.๑ จัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๓.๒ ตรวจสอบแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้อง

๓.๓ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๓.๔ ทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงาน หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๓.๕ ฝึกซ้อมการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. การรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์

หน่วยงานต้องรายงานสถานการณ์เกี่ยวกับด้านความมั่นคงปลอดภัยไซเบอร์มายังคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์ของกระทรวงยุติธรรม อย่างน้อยดังนี้

๔.๑ แนวนโยบายหรือแนวปฏิบัติด้านในการรักษาความมั่นคงปลอดภัยไซเบอร์

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

๔.๓ การดำเนินการเพื่อทำให้ระบบความมั่นคงปลอดภัยมีความแข็งแกร่ง (Hardening)

๔.๔ การดำเนินการทางกฎหมายที่เกี่ยวข้องในการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Security Incident)

๔.๕ การพัฒนาด้านบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

๔.๖ การรายงานปัญหาและอุปสรรคที่เกิดขึ้นในด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการแก้ไขปัญหาที่เกิดขึ้น

ส่วนที่ ๒
มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๑ การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)

๑.๑ การจัดการทรัพย์สิน (Asset Management)

การจัดเก็บรายละเอียดข้อมูลของอุปกรณ์ด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ทั้งหมดของระบบเพื่อใช้ในการวางแผนและการบริหารด้านความมมั่งคงปลอดภัยทางไซเบอร์

๑.๑.๑ หน่วยงานต้องมีทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินด้านเทคโนโลยีสารสนเทศของฮาร์ดแวร์ (Hardware) และ ซอฟต์แวร์ (Software) และดูแลรักษาทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยทะเบียนทรัพย์สินแต่ละประเภทต้องมีข้อมูลอย่างน้อย ดังนี้

๑) ชื่อ/คำอธิบายของทรัพย์สิน
๒) ประเภทของอุปกรณ์/ยี่ห้อ
๓) ฟังก์ชันที่สำคัญของทรัพย์สิน
๔) ชื่อระบบปฏิบัติการ (Operation System) และเวอร์ชัน
๕) การระบุลำดับความสำคัญของทรัพย์สิน
๖) เจ้าของและ/หรือผู้ดำเนินการของทรัพย์สิน
๗) ตำแหน่งทางกายภาพของทรัพย์สิน
๘) การขึ้นต่อกันของทรัพย์สิน

๑.๑.๒ หน่วยงานต้องมีทะเบียนทรัพย์สินข้อมูล (Data Inventory) ที่ระบุข้อมูลที่เก็บไว้ภายในระบบสารสนเทศโดยจะต้องมีการกำหนดชั้นความลับของข้อมูล (Data Classification) เพื่อให้สามารถกำหนดสิทธิในการเข้าถึงข้อมูลได้อย่างปลอดภัย

๑.๑.๓ หน่วยงานต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญของหน่วยงานและระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)

๑.๑.๔ หน่วยงานต้องมีการตรวจสอบทะเบียนทรัพย์สินอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญของหน่วยงานให้ปรับปรุงทะเบียนทรัพย์สินดังกล่าวด้วย

๑.๑.๕ หน่วยงานต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ในข้อ ๑.๑ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๑.๑.๖ หน่วยงานต้องดำเนินการจัดทำแผนผังเครือข่าย (Network Diagram) ของหน่วยงานและปรับปรุงให้เป็นปัจจุบัน

๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

การประเมินความเสี่ยงด้านความความมั่นคงปลอดภัยไซเบอร์เพื่อเป็นการเตรียมความพร้อมในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่อาจจะเกิดขึ้นกับหน่วยงาน พร้อมทั้งหาแนวทางในการรับมือเพื่อลดความเสียหายที่จะเกิดกับหน่วยงาน

๑.๒.๑ หน่วยงานต้องประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยต้องมีข้อมูลอย่างน้อย ดังนี้

๑) กำหนดหน้าที่และความรับผิดชอบในการบริหารและจัดการความเสี่ยง

๒) ระบุความเสี่ยงที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ (IT-related risk)

๓) ประเมินความเสี่ยงที่ครอบคลุมถึงโอกาสหรือความถี่ที่จะเกิดความเสี่ยง และผลกระทบที่จะเกิดขึ้น เพื่อจัดลำดับความสำคัญในการบริหารจัดการความเสี่ยง

๔) กำหนดวิธีการหรือเครื่องมือในการบริหาร และจัดการความเสี่ยงให้อยู่ในระดับที่องค์กรยอมรับได้

๑.๒.๒ หน่วยงานต้องปรับปรุงทะเบียนความเสี่ยงทุกครั้งหลังการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ทะเบียนความเสี่ยงต้องจัดทำเอกสาร โดยมีรายละเอียดอย่างน้อยดังต่อไปนี้

๑) วันที่ระบุความเสี่ยง (Date the Risk is Identified)

๒) คำอธิบายของความเสี่ยง (Description of the Risk)

๓) โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)

๔) ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)

๕) การจัดการความเสี่ยง (Risk Treatment)

๖) เจ้าของความเสี่ยง (Risk Owner)

๗) สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)

๘) ความเสี่ยงที่เหลือ (Residual Risk)

๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

เป็นการประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing) ทางด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานที่ครอบคลุมทั้งฮาร์ดแวร์ (Hardware) และซอฟต์แวร์ (Software) ว่ามีช่องโหว่ใดบ้างที่มีผลกระทบต่อความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน เพื่อให้หน่วยงานทราบถึงจุดอ่อนด้านความมั่นคงปลอดภัย และแก้ไขก่อนที่จะเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบสารสนเทศของหน่วยงาน

๑.๓.๑ หน่วยงานต้องดำเนินการประเมินช่องโหว่ของอุปกรณ์ของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัย และการควบคุมโดยครอบคลุมบริการที่สำคัญของหน่วยงาน ซึ่งเป็น

๑) ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)

๒) ระบบที่ใช้ควบคุมเครื่องจักรในอุตสาหกรรม (Industrial Control System: ICS)

๑.๓.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการประกอบด้วย

๑) การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)

๒) การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)

๓) การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)

๑.๓.๓ หน่วยงานต้องทำการประเมินช่องโหว่ของบริการที่สำคัญของหน่วยงาน เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและควบคุมก่อนที่จะทำการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อหรือดำเนินการเปลี่ยนแปลงระบบที่สำคัญใด ๆ กับบริการที่สำคัญของหน่วยงาน

การเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี

๑.๓.๔ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) บริการที่สำคัญของหน่วยงานโดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเทอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย

๑.๓.๕ หน่วยงานต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญของหน่วยงาน โดยเฉพาะอย่างยิ่งทุกระบบที่เป็นมีการเชื่อมต่ออินเทอร์เน็ตโดยตรง (Internet Facing)

๑.๓.๖ หน่วยงานควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของหน่วยงานก่อนที่จะทำการทดสอบระบบใหม่หรือการเปลี่ยนแปลงระบบที่สำคัญ เช่น โมดูลเสริม การปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

การจัดให้มีการกำกับดูแลการบริหารจัดการความเสี่ยงจากการใช้บริการการเชื่อมต่อหรือการเข้าถึงข้อมูลจากบุคคลภายนอก โดยประกอบด้วยการกำหนดบทบาทหน้าที่และความรับผิดชอบของผู้ให้บริการภายนอก

๑.๔.๑ หน่วยงานต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใดๆ ก็ตาม ในส่วนของบริการที่สำคัญของหน่วยงาน

๑.๔.๒ หน่วยงานต้องมีข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการ ของผู้ให้บริการภายนอก ในข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก ข้อกำหนดต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้

๑) ประเภทของผู้ให้บริการภายนอกที่เข้าถึงทรัพย์สินของบริการที่สำคัญของหน่วยงาน ตามความต้องการทางธุรกิจขององค์กร และโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒) ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องบริการที่สำคัญของหน่วยงานจากภัยคุกคามทางไซเบอร์

๓) ความเสี่ยงที่เกี่ยวข้องกับบริการและห่วงโซ่อุปทานผลิตภัณฑ์

๔) สิทธิ์ของหน่วยงานในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของผู้ให้บริการภายนอก

๑.๔.๓ หน่วยงานควรพิจารณาสร้างกระบวนการตรวจสอบความถูกต้องของผู้ให้บริการภายนอกว่าสอดคล้องกับข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ในเงื่อนไขของสัญญา ตัวอย่างเช่น การตรวจสอบโดยบุคคลที่สาม และการตรวจสอบผลิตภัณฑ์

๑.๔.๔ หน่วยงานควรพิจารณาดำเนินการเจรจาต่อรองเงื่อนไขของสัญญาจ้างให้สอดคล้องกับกรณีที่มีข้อกำหนดทางกฎหมายหรือข้อบังคับใหม่

หัวข้อที่ ๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

๒.๑ การควบคุมการเข้าถึง (Access Control)

การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๑ หน่วยงานต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย อย่างน้อยดังนี้

๑) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๓) การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่าย

๔) การควบคุมการเข้าถึงระบบงานและแอปพลิเคชัน

๕) การบริหารจัดการการเข้าถึงด้านระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน

๒.๑.๒ หน่วยงานต้องกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของหน่วยงาน ให้สอดคล้องกับหน้าที่ความรับผิดชอบของเจ้าหน้าที่

๒.๑.๓ หน่วยงานต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึงและช่องทางการเข้าถึง

๒.๑.๔ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญของหน่วยงาน (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดยทางสารสนเทศเท่านั้น

๒.๑.๕ หน่วยงานต้องเก็บรักษาบันทึกของการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของหน่วยงาน

๒.๑.๖ ในการเข้าถึงระบบสารสนเทศของหน่วยงานต้องมีการเข้ารหัส Transaction ที่มีความปลอดภัย เช่น Secure Socket Layer (SSL) หรือ Transport Layer Security (TLS) เป็นต้น โดยต้องใช้ใบรับรอง (Certificate) ที่มีความปลอดภัย

๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๒.๒.๑ หน่วยงานต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญของหน่วยงาน

๒.๒.๒ หน่วยงานต้องจัดทำมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัย อย่างน้อยดังต่อไปนี้

๑) สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)

๒) การแบ่งแยกหน้าที่ (Separation of Duties)

๓) การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน

๔) การลบบัญชีที่ไม่ได้ใช้

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

๖) การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน

๗) การป้องกันมัลแวร์ (Malware)

๘) การปรับปรุงซอฟต์แวร์และแพตช์ (Patch) ความมั่นคงปลอดภัยของระบบ อย่างทันการณ์และเหมาะสม

๒.๒.๓ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ก่อนที่จะมีทรัพย์สินใดๆ เชื่อมต่อ หรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของหน่วยงาน

๒.๒.๔ หน่วยงานต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standard) ของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์

๒.๒.๕ หน่วยงานต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญของหน่วยงาน

๒.๓ การเชื่อมต่อระยะไกล (Remote Control)

๒.๓.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญของหน่วยงานมีมาตรการรักษาความมั่นคงปลอดภัยไซเบอร์ที่มีประสิทธิภาพ เพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต

๒.๓.๒ สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญของหน่วยงานต้องปฏิบัติตามแนวทางปฏิบัติดังต่อไปนี้

๑) เปิดใช้งานการเชื่อมต่อไซต์ระยะไกล เมื่อจำเป็นและได้รับการอนุญาตเท่านั้น

๒) ควรใช้งานโปรโตคอลที่ปลอดภัย เช่น Internet Protocol Security (IPSEC)

๓) ต้องทำการเชื่อมต่อระยะไกลผ่านช่องทางระบบเครือข่ายเสมือน Virtual Private Network (VPN)

๔) ในกรณีที่เป็นไปได้ ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง เช่น การยืนยันตัวตนแบบสองปัจจัย (Two Factor Authentication) , กำหนดระยะเวลาในการเปลี่ยนรหัสผ่านตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานหรืออย่างสม่ำเสมอ

๕) ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น

๖) ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญของหน่วยงานเว้นแต่จะได้รับอนุญาต

๗) จำกัดการไหลของข้อมูลเฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อ

๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๒.๔.๑ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวดในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญของหน่วยงาน โดยใช้มาตรการอย่างน้อย ดังนี้

๑) ในกรณีที่มีฟังก์ชันให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น

๒) ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาตเท่านั้น

๓) ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของหน่วยงาน

๒.๔.๒ หน่วยงานต้องเข้ารหัสข้อมูลที่ละเอียดอ่อนทั้งหมดของบริการที่สำคัญของหน่วยงานบนสื่อบันทึกข้อมูลแบบถอดได้

๒.๔.๓ หน่วยงานต้องมีการกำหนดวิธีการที่ปลอดภัยในการทำลายสื่อบันทึกข้อมูลแบบถอดได้เพื่อป้องกันการรั่วไหลของข้อมูล

๒.๕ การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๒.๕.๑ หน่วยงานต้องเผยแพร่ ประชาสัมพันธ์ เกี่ยวกับแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๕.๒ หน่วยงานต้องจัดทำ ปรับปรุงคู่มือการใช้งานระบบสารสนเทศให้เป็นปัจจุบัน และมีการเผยแพร่ผ่านช่องทางที่เหมาะสมของหน่วยงาน

๒.๕.๓ หน่วยงานต้องจัดฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๒.๕.๔ หน่วยงานต้องสร้างความตระหนัก (awareness program) เรื่องการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ความเสี่ยงด้านเทคโนโลยีสารสนเทศ การใช้งานระบบอย่างปลอดภัย ให้แก่บุคลากรทุกระดับ

๒.๕.๕ หน่วยงานควรจัดให้มีการฝึกอบรมและพัฒนาความรู้ความเชี่ยวชาญให้ครอบคลุมและเพียงพอต่อการปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศกับเจ้าหน้าที่ที่ดูแลระบบสารสนเทศ

๒.๖ การแบ่งปันข้อมูล (Information Sharing)

หน่วยงานต้องกำหนดขั้นตอนเพื่อแบ่งปันข้อมูลเกี่ยวกับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์และภัยคุกคามทางไซเบอร์ โดยต้องรายงานต่อคณะอนุกรรมการด้านความมั่นคงปลอดภัยไซเบอร์กระทรวงยุติธรรม

หัวข้อที่ ๓ มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring) การตรวจสอบการกระทำหรือการดำเนินการใดๆ โดยมิชอบ โดยใช้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ ซึ่งมีจุดมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลที่เกี่ยวข้อง เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านเทคโนโลยีสารสนเทศที่ยอมรับได้ที่กำหนดไว้ โดยหน่วยงานต้องมีกระบวนการในการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ ดังต่อไปนี้

๓.๑ มีกระบวนการในการตรวจจับเหตุการณ์ผิดปกติที่กระทบต่อความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ มีกระบวนการในการจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ

๓.๓ มีกระบวนการในการระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับบริการที่สำคัญของหน่วยงาน

๓.๔ ต้องดำเนินการตรวจสอบกลไกและกระบวนการเฝ้าระวังภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่างๆ ยังคงมีประสิทธิภาพ

หัวข้อที่ ๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) ซึ่งมีแผนเกี่ยวข้องกับการตรวจพบภัยคุกคามทางไซเบอร์ จำนวน ๒ แผน ดังนี้

๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

หน่วยงานต้องมีการจัดทำการสื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อย ปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมี ประสิทธิภาพและประสิทธิผล

๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๔.๒.๑ หน่วยงานต้องจัดทำแผนการสื่อสารในภาวะวิกฤตเพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๔.๒.๒ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤต

๑) จัดตั้งทีมสื่อสารในภาวะวิกฤตเพื่อเปิดใช้งานในช่วงวิกฤต

๒) ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง

๓) ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท

๔) ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน

๕) ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล

๔.๒.๓ หน่วยงานต้องตรวจสอบแผนการสื่อสารในภาวะวิกฤตรวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต

๔.๒.๔ หน่วยงานต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

หัวข้อที่ ๕ มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

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

๕.๑ หน่วยงานต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan: BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของหน่วยงาน สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงักเนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริงเพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานเช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะเวลาที่สำคัญ Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น โดยมีรายละเอียดอย่างน้อยดังนี้

๕.๑.๑ จัดลำดับความสำคัญของความเสี่ยงด้านความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศโดยต้องพิจารณาจากปัจจัยที่สำคัญ เช่น ผลกระทบของการหยุดชะงัก ระยะเวลาที่ยอมรับได้ของการหยุดชะงักลำดับความสำคัญในการกู้คืนระบบ

๕.๑.๒ จัดทำแผนกู้คืนภาวะวิกฤต สำหรับกระบวนการดำเนินงานของหน่วยงานที่ใช้ทรัพย์สินสารสนเทศที่มีระดับการป้องกันความมั่นคงปลอดภัย “สูง” หรือ “สูงสุด” เพื่อให้มั่นใจว่าสามารถดำเนินงานได้อย่างต่อเนื่องมีการควบคุมดูแลการแก้ไขและกู้คืนระบบเมื่อเกิดเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยทางไซเบอร์และสารสนเทศ

๕.๒ หน่วยงานต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม (Business Continuity Plan: BCP) อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง เพื่อประเมินประสิทธิภาพของ (Business Continuity Plan: BCP) ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๓ ในกรณีตรวจพบภัยคุกคามทางไซเบอร์ (Cyber Security Incident) หน่วยงานต้องจัดทำรายงานภัยคุกคามทางไซเบอร์ (Incident Report) โดยรายงานความคืบหน้าของการดำเนินการให้คณะอนุกรรมการทราบทุกระยะ

ภาคผนวก ก

แผนการตรวจสอบ
ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (INTRODUCTION)

การตรวจสอบความมั่นคงปลอดภัยไซเบอร์จะต้องดำเนินการอย่างน้อยปีละหนึ่ง หรือความถี่ที่สูงกว่านั้นตามที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน) กำหนดในกรณีใดกรณีหนึ่ง และดำเนินการโดยผู้ตรวจสอบที่ได้รับอนุมัติหรือแต่งตั้งโดยหน่วยงาน

๒. วัตถุประสงค์ (PURPOSE)

เอกสารฉบับนี้มีวัตถุประสงค์เพื่อกำหนดความคาดหวังในการตรวจสอบ และใช้เป็นแนวทางสำหรับผู้ตรวจสอบที่ได้รับการอนุมัติ หรือได้รับการแต่งตั้งเพื่อทำการตรวจสอบความมั่นคงปลอดภัยไซเบอร์

เอกสารนี้ไม่ได้หมายถึงแหล่งข้อมูลที่ละเอียดถี่ถ้วนสำหรับการดำเนินการตรวจสอบการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

ในกรณีที่การตรวจสอบความมั่นคงปลอดภัยไซเบอร์ไม่มีหัวข้อใดที่กำหนดในเอกสารนี้ ผู้ตรวจสอบควรใช้ดุลยพินิจเยี่ยงผู้ประกอบวิชาชีพและระบุสถานการณ์ดังกล่าวในรายงานการตรวจสอบ

๓. กลุ่มเป้าหมาย (AUDIENCE)

กลุ่มเป้าหมายของเอกสารนี้:

ก. ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ และ

ข. ผู้มีส่วนได้ส่วนเสีย (เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบและผู้ขาย หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล ฯลฯ) ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

๔. ขอบเขต (SCOPE)

เอกสารนี้ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๕. การอนุมัติผู้ตรวจสอบ (AUDITOR APPROVAL)

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหน่วยงานและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด ใบสมัครจะถือว่าสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาโดยหน่วยงาน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

เกณฑ์การพิจารณามี ๒ ประการ ได้แก่ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (audit firm/team) และผู้ตรวจสอบ (auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง:

ก. ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์ และ

ข. ควรมีความสามารถทางเทคนิคที่จำเป็น (เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้ และประสบการณ์ที่เกี่ยวข้อง) เพื่อดำเนินการตรวจสอบ

ทั้งนี้ หน่วยงานอาจพิจารณาแตกต่างกันไปตามที่หน่วยงานเห็นสมควร ในประเด็นต่อไปนี้

(๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน

(๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น

ในกรณีผู้ตรวจสอบของหน่วยงานที่ลงทะเบียนแล้วลาออกจากการเป็นพนักงานก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงพนักงานที่ลงทะเบียนไว้ ให้หน่วยงานแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่การเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๖. ความคาดหวังในการตรวจสอบ (AUDIT EXPECTATIONS)

ส่วนนี้กำหนดความคาดหวังในการตรวจสอบ มีวัตถุประสงค์เพื่อช่วยให้ผู้อ่านเข้าใจว่าควรดำเนินการและรายงานการตรวจสอบความมั่นคงปลอดภัยไซเบอร์อย่างไร

สกมช. ได้ระบุความคาดหวังในการตรวจสอบไว้ ๗ ด้านในหัวข้อ ๖.๑ ถึง ๖.๗

๖.๑ หลักการตรวจสอบ (Principles of Auditing)

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): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ

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

๖.๒ วัตถุประสงค์ในการตรวจสอบ

วัตถุประสงค์ของการตรวจสอบ คือ:

ก. ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

ข. ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๖.๓ ขอบเขตการตรวจสอบ (Audit Scope)

การตรวจสอบจะครอบคลุมสิ่งต่อไปนี้:

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

๖.๔ แนวทางการตรวจสอบ (Audit Approach)

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

ก. การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ข. ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๖.๕ ข้อค้นพบการตรวจสอบ (Audit Finding)

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้:

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม และ

ง. เน้นแนวปฏิบัติที่ดี (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะต่อไปนี้ของข้อค้นพบการตรวจสอบอย่างชัดเจน

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ

องค์ประกอบ (Attributes)	คำอธิบาย (Description)
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

๖.๖ สรุปผลการตรวจสอบ (Audit Conclusion)

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

ก. ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

๖.๗ รูปแบบรายงานการตรวจสอบ (Audit Report Format)

รายงานการตรวจสอบควรมีอย่างน้อยดังต่อไปนี้:

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารนี้

เนื้อหา	คำอธิบาย
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย(Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๖.๕ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๖.๖ ของเอกสารนี้

๗. ขั้นตอนการปฏิบัติในการตรวจสอบ

๑. ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

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

๒. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

- ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ
- ระดับความไม่สอดคล้องของข้อตรวจพบ

- ข้อเสนอแนะในการปรับปรุง
- สรุปผลการตรวจสอบ
- กำหนดการตรวจติดตาม (ถ้ามี)

๔. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๕. คณะทำงานรับทราบผลการตรวจสอบ

๖. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับในการตรวจสอบ

๗. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๘. คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๙. ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

๘. เอกสารอ้างอิง

- GUIDELINES FOR AUDITING CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, JANUARY ๒๐๒๐
- Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guidelines_for_auditing_critical_information_infrastructure.pdf
- ISO ๑๙๐๑๑:๒๐๑๘ Guidelines for auditing management systems, ISO, July ๒๐๑๘
- Link: https://www.iso.org/standard/๗๐๐๑๗.html

ภาคผนวก ข

แผนบริหารความเสี่ยง

ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. บทนำ (INTRODUCTION)

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ด้วยความก้าวหน้าทางเทคโนโลยีอย่างรวดเร็ว ภูมิทัศน์ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนไป และความเป็นดิจิทัลที่เพิ่มขึ้น หน่วยงานต่าง ๆ อาจเผชิญกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่มากขึ้น ซึ่งอาจส่งผลกระทบในทางลบต่อหน่วยงานและวัตถุประสงค์ทางธุรกิจ ดังนั้นจึงมีความจำเป็นสำหรับหน่วยงานในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) (เรียกว่า "การประเมินความเสี่ยง" (Risk Assessment)) เป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ:

- ระบุเหตุการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้เจ้าหน้าที่มีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่เจ้าหน้าที่ดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๑.๒ ปัญหาทั่วไปที่สังเกตได้

ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่งก็ประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกตเห็น ได้แก่

ก. การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

ข. การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุมความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่างเทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยงทำให้เกิดพฤติกรรม “รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัยว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

ค. การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

ง. การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้ อาจไม่ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

จ. จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต (PURPOSE, AUDIENCE & SCOPE)

๒.๑ วัตถุประสงค์ของเอกสาร

เพื่อให้ทราบแนวทางการดำเนินการ กำกับดูแล ตรวจสอบเกี่ยวกับการบริหารจัดการ และเผยแพร่ความรู้ความเข้าใจเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๒.๒ กลุ่มเป้าหมายและขอบเขต (Audience & Scope)

เอกสารนี้มีขึ้นเพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

- ผู้มีส่วนได้ส่วนเสีย (Stakeholders) ได้แก่ ผู้บริหารระดับสูง หน่วยงานภายในกรมสอบสวนคดีพิเศษ ผู้อำนวยการกอง หัวหน้ากลุ่ม/ส่วน ผู้ดูแลระบบ เจ้าหน้าที่ที่ปฏิบัติงานภายในหน่วยงาน
- ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน
- ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๓. สร้างบริบทความเสี่ยง (ESTABLISH RISK CONTEXT)

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมินความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๓.๑ กำหนดความเสี่ยง (Define Risk)

การกำหนดคำนิยามทั่วไปของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สำหรับวัตถุประสงค์ของแนวทางฉบับนี้ ความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ:

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน; และ
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง เหตุการณ์ใด ๆ ในระหว่างที่ผู้คุกคาม (Threat Actor) ใช้เวกเตอร์ภัยคุกคาม (การกระทำโดยระบุจุดทั้งหมดที่สามารถเข้าถึงระบบคอมพิวเตอร์หรือเครือข่าย (เรียกว่า เวกเตอร์การโจมตี (Threat Vector)) กระทำต่อทรัพย์สินในลักษณะที่อาจก่อให้เกิดอันตราย ในบริบทของการรักษาความมั่นคงปลอดภัยไซเบอร์ เหตุการณ์ภัยคุกคามสามารถระบุได้ด้วยกลวิธี เทคนิค และขั้นตอน (Tactics, Techniques and Procedures (TTP)) ที่ใช้โดยผู้คุกคาม

ช่องโหว่ (Vulnerability)

ช่องโหว่หมายถึงจุดอ่อนในการออกแบบ การนำไปใช้ และการดำเนินงานของทรัพย์สินหรือการควบคุมภายในของกระบวนการ

ความน่าจะเป็น (Likelihood)

ความน่าจะเป็น หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

ผลกระทบ (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ:

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตาราง : การยอมรับความเสี่ยง (Risk Tolerance Description)

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันที ทางเลือกที่เป็นไปได้ คือ กลยุทธ์การลดระดับความเสี่ยงหรือการถ่ายโอนจำเป็นต้องดำเนินการทันที
Medium	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้ กลยุทธ์การรักษาที่มุ่งลดระดับความเสี่ยงควรได้รับการพัฒนาและดำเนินการใน ๓ - ๖ เดือนข้างหน้า
Low	ความเสี่ยงระดับนี้สามารถยอมรับได้หากไม่มีกลยุทธ์การจัดการความเสี่ยงที่สามารถดำเนินการได้ง่ายและประหยัด ความเสี่ยงจะต้องได้รับการติดตามเป็นระยะเพื่อให้แน่ใจว่ามีการตรวจพบการเปลี่ยนแปลงของสถานการณ์และดำเนินการอย่างเหมาะสม

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

การกำหนดความรับผิดชอบและแบ่งอำนาจหน้าที่มีวัตถุประสงค์เพื่อลดความเสี่ยงของหน่วยงาน และให้ผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในการวิเคราะห์ความเสี่ยง การประเมินความเสี่ยงและการควบคุมความเสี่ยง โดยกำหนดหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศดังต่อไปนี้

หัวหน้าหน่วยงาน (Head of Organization)

เจ้าหน้าที่อาวุโสระดับสูงสุด (Highest-level Senior Official) ภายในหน่วยงานที่มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

เจ้าของกระบวนการธุรกิจ (Business Owner)

เจ้าหน้าที่อาวุโสระดับสูงสุดของหน่วยธุรกิจ (Business Unit) ที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากิจกรรมทางธุรกิจบรรลุเป้าหมายทางธุรกิจ หรือแบ่งปันข้อกังวลเกี่ยวกับผลกระทบที่มีต่อธุรกิจในกรณีที่ระบบมีการหยุดชะงัก

ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งหน่วยงาน ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและธุรกิจในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชัน เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมทางธุรกิจ พวกเขาควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดีและสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบในการดำเนินการและการบำรุงรักษาการควบคุมความมั่นคงปลอดภัยไซเบอร์ในระบบที่สนับสนุนกิจกรรมทางธุรกิจ โดยบุคคลดังกล่าวควรระบุภัยคุกคามที่อาจเกิดขึ้นกับระบบ กำหนดแนวคิดเกี่ยวกับสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ กำหนดโอกาสเสี่ยง ตลอดจนแนะนำมาตรการที่เหมาะสมเพื่อจัดการกับภัยคุกคามหรือการโจมตีที่ระบุ

๔. การประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

การประเมินความเสี่ยงนั้นเกี่ยวกับการระบุความเสี่ยงที่เฉพาะเจาะจงกับสภาพแวดล้อม และการกำหนดระดับของความเสี่ยงที่ระบุ ขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ การระบุความเสี่ยง (Risk Identification) การวิเคราะห์ความเสี่ยง (Risk Analysis) และการประเมินความเสี่ยง (Risk Evaluation)

รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๔.๑ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

จากการวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมสอบสวนคดีพิเศษ สามารถแยกประเภทความเสี่ยงออกเป็น ๙ หมวดหมู่ (Risk Cluster) ดังนี้

๑) การโจมตีด้วยมัลแวร์ (Malware Attacks)
๒) การโจมตีด้วยฟิชชิง (Phishing Attacks)
๓) ภัยคุกคามจากบุคคลภายใน (Insider Threats)
๔) การละเมิดข้อมูล (Data Breaches)
๕) การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)
๖) ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)
๗) ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)
๘) ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)
๙) การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)

ในการระบุความเสี่ยงสามารถจำแนกข้อมูลเกี่ยวกับชื่อความเสี่ยง (Risk Cluster) ภัยคุกคาม (Threat) ช่องโหว่ (Vulnerability) และผลกระทบ/ผู้ได้รับผลกระทบ โดยจะแสดงรายละเอียดต่าง ๆ ตามตารางด้านล่างดังนี้

ตาราง : แสดงรายละเอียดความเสี่ยง (Description of risk) แยกตามลักษณะของความเสี่ยงแต่ละด้าน

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
๑. การโจมตีด้วยมัลแวร์ (Malware Attacks)	๑. มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงด้วยมัลแวร์	๑. ไม่มีระบบหรือมาตรการควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ในหน่วยงาน	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. มีการติดมัลแวร์ที่มาจากการใช้อุปกรณ์ USB Storage หรือสื่อเก็บข้อมูลภายนอก	๒. ไม่มีการติดตั้งหรืออัปเดตโปรแกรมป้องกันไวรัสเมื่อใช้อุปกรณ์ USB Storage	
	๓. ไฟล์แนบในอีเมลมีฟิชชิงและแฝงด้วยมัลแวร์	๓. ขาดระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งาน อีเมลที่มีไฟล์แนบ	
	๔. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ฝังด้วยมัลแวร์	๔. เจ้าหน้าที่ขาดความรู้ในการติดตั้งไฟล์หรือเว็บไซต์ที่มีความเสี่ยงไซเบอร์	
	๕. เจ้าหน้าที่เข้าถึงโฆษณาออนไลน์ (Malvertising) ตามเว็บต่างๆ ที่พาไปยังเว็บไซต์ที่มีมัลแวร์	๕. ไม่มีระบบกรองเว็บไซต์ ที่ป้องกันมัลแวร์และอัปเดตเป็นประจำ	
๒. การโจมตีด้วยฟิชชิง (Phishing Attacks)	๑. การรับอีเมลที่มีฟิชชิงหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน	๑. ขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่ไม่สามารถแยกแยะอีเมลหรือเว็บไซต์ปลอมได้	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. Spear Phishing ที่กำหนดเป้าหมายเจาะจงบุคคลหรือหน่วยงาน หลุดเข้ามาในระบบ	๒. ไม่มีระบบตรวจจับอีเมลฟิชชิง เช่น ไม่มีการใช้ตัวกรองอีเมลเพื่อบล็อกอีเมลที่เป็นอันตราย	
	๓. มีการรับส่งลิงก์ที่มีฟิชชิงผ่าน SMS หรือโซเชียลมีเดีย	๓. การใช้รหัสผ่านซ้ำหรือไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้ซ้ำในหลายระบบ	
	๔. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าล็อกอินของหน่วยงานหรือบริการออนไลน์	๔. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
	๕. ถูกระบบโทรศัพท์ปลอม (Call center) หลอกขอข้อมูลส่วนตัว	๕. ไม่มีกระบวนการยืนยันการสื่อสารที่ปลอดภัย เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมลหรือข้อความ	
๓. ภัยคุกคามจากบุคคลภายใน (Insider Threats)	๑. การใช้งานข้อมูลโดยใช้อำนาจมิชอบ เช่น เจ้าหน้าที่ที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	๑. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น เจ้าหน้าที่บางคนได้รับสิทธิ์เข้าถึงข้อมูลมากเกินความจำเป็น	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. การรั่วไหลของข้อมูลโดยเจตนา เช่น เจ้าหน้าที่ที่ไม่พอใจหน่วยงานส่งข้อมูลสำคัญให้คู่แข่งหรือบุคคลภายนอก	๒. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ผิดปกติในระบบของเจ้าหน้าที่	
	๓. กระทำผิดพลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญหรือแชร์ข้อมูลให้บุคคลที่ไม่เกี่ยวข้อง	๓. ขาดการฝึกอบรมเกี่ยวกับการปกป้องข้อมูล เช่น เจ้าหน้าที่ไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	
	๔. การใช้บัญชีที่ถูกยึดหรือถูกแฮ็ก (Inactive users) เช่น บัญชีของเจ้าหน้าที่ที่ถูกยึดหรือแฮ็กมีการนำไปใช้ในการกระทำที่ไม่เหมาะสม	๔. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากหน่วยงาน เช่น บัญชีของเจ้าหน้าที่ที่ลาออกยังคงสามารถเข้าถึงระบบได้	
	๕. มีการปลอมตัวเป็นบุคคลภายใน เช่น บุคคลภายนอกแฝงตัวเข้ามาในหน่วยงานผ่านการร่วมมือของเจ้าหน้าที่ภายใน	๕. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการคัดลอกหรือส่งออก	
๔. การละเมิดข้อมูล (Data Breaches)	๑. มีการแฮ็กระบบเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้า หรือข้อมูลทางการเงิน	๑. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่อ่อนแอ	๒. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นผลเปิดช่องโหว่ให้ถูกโจมตี	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
	๓. มีการรั่วไหลของข้อมูลผ่านเจ้าหน้าที่ (โดยเจตนาหรือไม่เจตนา)	๓. การตั้งรหัสผ่านที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้รหัสผ่านซ้ำกันในหลายระบบ	
	๔. มีการส่งข้อมูลสำคัญผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมลที่ไม่มีการเข้ารหัส	๔. ขาดระบบตรวจสอบการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	
	๕. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	๕. ขาดการตรวจสอบกิจกรรมในระบบ เช่น ไม่มีการตรวจสอบกิจกรรมที่น่าสงสัยในระบบหรือการแจ้งเตือน	
๕. การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	๑. มีการดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่แฝงแรนซัมแวร์ผ่านอีเมลฟิชชิง	๑. การขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่เปิดไฟล์แนบที่เป็นอันตรายจากอีเมลฟิชชิง	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	๒. ซอฟต์แวร์และระบบปฏิบัติการที่ไม่ได้อัปเดต เช่น ระบบหรือซอฟต์แวร์ มีช่องโหว่ที่เปิดให้แรนซัมแวร์เข้าถึงได้	
	๓. มีการใช้ Remote Desktop Protocol (RDP) ที่ไม่ได้ตั้งค่าความปลอดภัย	๓. การขาดการสำรองข้อมูล (Backup) เช่น ไม่มีระบบสำรองข้อมูลที่สามารถกู้คืนได้เมื่อถูกโจมตี	
	๔. มีการแอบแฝงแรนซัมแวร์ในอุปกรณ์ USB Storage หรืออุปกรณ์พกพาอื่นๆ	๔. การตั้งค่าความปลอดภัยของ RDP ที่ไม่เหมาะสม เช่น เปิดใช้งาน RDP โดยไม่มีการควบคุมการเข้าถึงที่เข้มงวด	
	๕. มีการกระจายแรนซัมแวร์ผ่านเครือข่ายที่เชื่อมโยงกับหน่วยงาน	๕. การขาดระบบป้องกันมัลแวร์ที่มีประสิทธิภาพ เช่น ไม่มีซอฟต์แวร์ป้องกันแรนซัมแวร์ที่สามารถตรวจจับและบล็อกการโจมตี	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
๖. ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)	๑. มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้จำหน่าย (๓rd Party/Suppliers) ที่ไม่ได้มีการควบคุมความปลอดภัยอาจทำให้ข้อมูลของหน่วยงานรั่วไหล	๑. การขาดกระบวนการตรวจสอบผู้จำหน่าย (๓rd Party/Suppliers) เช่น ไม่มีการตรวจสอบความปลอดภัยของผู้จำหน่าย (๓rd Party/Suppliers) ก่อนเซ็นสัญญา	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. มีการโจมตีผ่านซัพพลายเชน (Supply Chain Attacks) เช่น ผู้โจมตีใช้ช่องโหว่ของซัพพลายเออร์เพื่อเข้าถึงระบบหน่วยงาน	๒. ไม่มีข้อตกลงด้านความปลอดภัย (Security SLA) เช่น ขาดข้อตกลงที่กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัย	
	๓. พบว่าผู้จำหน่ายขาดการปฏิบัติตามกฎระเบียบ เช่น ผู้จำหน่ายไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดด้านความปลอดภัย เช่น ISO ๒๗๐๐๑, ๒๗๐๑๘, ๒๗๗๐๑	๓. การเข้าถึงระบบที่ไม่เหมาะสม: ผู้จำหน่ายได้รับสิทธิ์เข้าถึงระบบมากเกินความจำเป็น	
	๔. การพึ่งพาผู้จำหน่ายที่ไม่มีความมั่นคงในการบริการ เช่น ความล้มเหลวของผู้จำหน่าย อาทิ การหยุดให้บริการ อาจส่งผลกระทบต่อธุรกิจ	๔. ขาดการเฝ้าระวังความปลอดภัยของผู้จำหน่าย เช่น ไม่มีการติดตามการปฏิบัติงานของผู้จำหน่ายในด้านความปลอดภัย	
	๕. การแชร์ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้มีการป้องกัน เช่น การส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีการเข้ารหัส	๕. การแชร์ข้อมูลกับผู้จำหน่ายหลายๆ ราย ทำให้ยิ่งแชร์ข้อมูลกับผู้จำหน่ายมากๆ ความเสี่ยงที่ข้อมูลจะรั่วไหลก็ยิ่งสูง	
๗. ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)	๑. ถูกการโจมตีแบบ DDoS (Distributed Denial of Service) เช่น การส่งคำขอจำนวนมากเพื่อทำให้เครือข่ายหยุดทำงาน	๑. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น การตั้งค่าเราเตอร์หรือไฟร์วอลล์ที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. ถูกการโจมตีแบบ Man-in-the-Middle (MitM) เช่น การดักฟังข้อมูลระหว่างการสื่อสารผ่านเครือข่าย	๒. ไม่มีการแยกเครือข่าย (Network Segmentation) เช่น ขาดการแยกเครือข่ายสำคัญออกจากเครือข่ายทั่วไป (VLAN)	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
	๓. ถูกการโจมตีแบบ Phishing ผ่านเครือข่าย เช่น การส่งลิงก์ฟิชชิงหรือไฟล์ที่เป็นอันตรายผ่านอีเมลหรือเครือข่าย	๓. ขาดระบบตรวจจับและป้องกันภัยคุกคาม เช่น ไม่มีการติดตั้ง IDS/IPS (Intrusion Detection/Prevention Systems)	
	๔. มีการใช้ช่องโหว่ของโปรโตคอลเครือข่าย เช่น การโจมตีผ่านโปรโตคอล อาทิ DNS Spoofing หรือ ARP Poisoning	๔. การใช้โปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet ที่ไม่มีการเข้ารหัส	
	๕. มีการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรืออุปกรณ์ที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายของหน่วยงาน	๕. ไม่มีการควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการตรวจสอบอุปกรณ์หรือผู้ใช้ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน	
๘. ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)	๑. มีการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรือผู้ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่สำคัญได้ อาทิ ศูนย์ข้อมูลหรือเซิร์ฟเวอร์รูมหรือดาต้าเซ็นเตอร์	๑. การขาดระบบควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการกำหนดสิทธิ์หรือการยืนยันตัวตนก่อนเข้าถึงพื้นที่สำคัญ	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. มีการขโมยหรือสูญหายของอุปกรณ์ เช่น อุปกรณ์สำคัญต่างๆ อาทิ เซิร์ฟเวอร์ ฮาร์ดไดรฟ์ แล็ปท็อป ถูกขโมยหรือสูญหาย	๒. ไม่มีการเฝ้าระวังด้วยกล้องวงจรปิด (CCTV) เช่น ขาดระบบเฝ้าระวังหรือการตรวจสอบเหตุการณ์ที่เกิดขึ้นในพื้นที่สำคัญ	
	๓. มีการก่อวินาศกรรม (Sabotage) เช่น การทำลายทรัพย์สินหรือระบบโดยบุคคลภายในหรือบุคคลภายนอก	๓. ไม่มีระบบป้องกันการก่อวินาศกรรม เช่น ขาดการออกแบบหรือมาตรการป้องกันการก่อวินาศกรรม	
	๔. เกิดภัยธรรมชาติ (Natural Disasters) เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหวที่ส่งผลกระทบต่ออุปกรณ์และข้อมูลสำคัญ	๔. ไม่มีระบบป้องกันภัยธรรมชาติ เช่น ขาดการออกแบบหรือมาตรการป้องกันภัยธรรมชาติ อาทิ การป้องกันน้ำท่วม	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	ผลกระทบ/ผู้ได้รับผลกระทบ
	๕. มีการขโมยข้อมูลผ่านการเข้าถึงทางกายภาพ เช่น การเชื่อมต่อกับพอร์ต USB หรือเครือข่ายโดยตรงในหน่วยงาน เพื่อขโมยข้อมูล	๕. การเก็บรักษาอุปกรณ์สำคัญในที่ไม่ปลอดภัย เช่น อุปกรณ์สำคัญถูกเก็บไว้ในพื้นที่ที่เข้าถึงได้ง่าย	
๙. การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)	๑. มีการส่งข้อมูลโดยไม่ได้ตั้งใจ เช่น การส่งข้อมูลสำคัญไปยังผู้รับผิดคนหรือแพลตฟอร์มที่ไม่ปลอดภัย	๑. การขาดการควบคุมการเข้าถึงข้อมูล เช่น ไม่มีการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	- ผู้ใช้งาน - ผู้ดูแลระบบงาน - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย
	๒. มีการขโมยข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจหรือบุคคลภายนอกขโมยข้อมูลเพื่อผลประโยชน์ส่วนตัว	๒. การไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บหรือรับส่งกัน ไม่มีการเข้ารหัส	
	๓. มีการละเมิดข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัย เช่น การรั่วไหลของข้อมูลที่ส่งผ่าน Wi-Fi หรือเครือข่ายที่ไม่มีการเข้ารหัส	๓. ขาดนโยบายและกระบวนการจัดการข้อมูล เช่น ไม่มีการกำหนดนโยบายในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคล	
	๔. ถูกการโจมตีแบบ Phishing เช่น ผู้โจมตีใช้ฟิชชิงเพื่อเข้าถึงข้อมูลสำคัญผ่านอีเมลหรือข้อความ	๔. การขาดระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention - DLP) เช่น ไม่มีการใช้ระบบเพื่อตรวจจับและป้องกันการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	
	๕. มีการติดมัลแวร์หรือแรนซัมแวร์ เช่น มีการใช้มัลแวร์เพื่อดึงข้อมูลหรือขัดขวางการเข้าถึงข้อมูล	๕. อุปกรณ์และบัญชีทรัพย์สินที่ไม่ได้รับการควบคุม เช่น อุปกรณ์พกพาหรือบัญชีผู้ใช้งานที่ไม่ได้ใช้งานยังสามารถเข้าถึงข้อมูลได้	

๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น และ

(๒) ผลกระทบ (Impact) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

ระดับโอกาสที่จะเกิดเหตุการณ์ (Likelihood)		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	โอกาสเกิดขึ้นได้ทุกวัน หรือทุกสัปดาห์
๔	สูง	โอกาสเกิดขึ้นได้ภายในระยะเวลา ๑ เดือน
๓	ปานกลาง	โอกาสเกิดขึ้นได้ภายในระยะเวลา ๑ ปี
๒	น้อย	โอกาสเกิดขึ้นได้ภายในระยะเวลา ๒-๕ ปี
๑	น้อยมาก	โอกาสเกิดขึ้นได้ภายในระยะเวลา ๕ ปี

ระดับความรุนแรง (Impact) ของผลกระทบ		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	เกิดความสูญเสียต่อระบบ สารสนเทศ ที่สำคัญทั้งหมด และ เกิดความเสียหายอย่าง ร้ายแรงต่อ ความปลอดภัยของข้อมูลต่างๆ
๔	สูง	เกิดความสูญเสียต่อระบบ สารสนเทศ ที่สำคัญบางส่วน และระบบความปลอดภัย ซึ่ง ส่งผลต่อความถูกต้องของข้อมูล
๓	ปานกลาง	ระบบมีปัญหาและมีความสูญเสีย ไม่มาก สามารถใช้งานได้ต่อเนื่อง
๒	น้อย	เกิดเหตุการณ์ในบางระบบที่ แก้ไขได้ในทันที
๑	น้อยมาก	เกิดเหตุการณ์ที่ไม่มีนัยสำคัญ

ตาราง : การวิเคราะห์ความเสี่ยง (Risk Analysis)

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
๑. การโจมตีด้วยมัลแวร์ (Malware Attacks)	๑. มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงด้วยมัลแวร์	๑. ไม่มีระบบหรือมาตรการควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ในหน่วยงาน	๑	๔
	๒. มีการติดมัลแวร์ที่มาจากการใช้อุปกรณ์ USB Storage หรือสื่อเก็บข้อมูลภายนอก	๒. ไม่มีการติดตั้งหรืออัปเดตโปรแกรมป้องกันไวรัสเมื่อใช้อุปกรณ์ USB Storage	๓	๔
	๓. ไฟล์แนบในอีเมล์มีฟิชชิงและแฝงด้วยมัลแวร์	๓. ขาดระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งาน อีเมลที่มีไฟล์แนบ	๓	๔
	๔. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ฝังด้วยมัลแวร์	๔. เจ้าหน้าที่ขาดความรู้ในการติดตั้งไฟล์หรือเว็บไซต์ที่มีความเสี่ยงไซเบอร์	๑	๔
	๕. เจ้าหน้าที่เข้าถึงโฆษณาออนไลน์ (Malvertising) ตามเว็บต่างๆ ที่พาไปยังเว็บไซต์ที่มีมัลแวร์	๕. ไม่มีระบบกรองเว็บไซต์ ที่ป้องกันมัลแวร์และอัปเดตเป็นประจำ	๓	๔
๒. การโจมตีด้วยฟิชชิง (Phishing Attacks)	๑. การรับอีเมลที่มีฟิชชิงหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน	๑. ขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่ไม่สามารถแยกแยะอีเมลหรือเว็บไซต์ปลอมได้	๓	๔
	๒. Spear Phishing ที่กำหนดเป้าหมายเจาะจงบุคคลหรือหน่วยงาน หลุดเข้ามาในระบบ	๒. ไม่มีระบบตรวจจับอีเมลฟิชชิง เช่น ไม่มีการใช้ตัวกรองอีเมลเพื่อบล็อกอีเมลที่เป็นอันตราย	๒	๔
	๓. มีการรับส่งลิงก์ที่มีฟิชชิงผ่าน SMS หรือโซเชียลมีเดีย	๓. การใช้รหัสผ่านซ้ำหรือไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้ซ้ำในหลายระบบ	๒	๔
	๔. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าล็อกอินของหน่วยงานหรือบริการออนไลน์	๔. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	๑	๔

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
	๕. ถูกระบบโทรศัพท์ปลอม (Call center) หลอกขอข้อมูลส่วนตัว	๕. ไม่มีกระบวนการยืนยันการสื่อสารที่ปลอดภัย เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมลหรือข้อความ	๓	๔
๓. ภัยคุกคามจากบุคคลภายใน (Insider Threats)	๑. การใช้งานข้อมูลโดยใช้อำนาจมิชอบ เช่น เจ้าหน้าที่ที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	๑. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น เจ้าหน้าที่บางคนได้รับสิทธิ์เข้าถึงข้อมูลมากเกินความจำเป็น	๑	๓
	๒. การรั่วไหลของข้อมูลโดยเจตนา เช่น เจ้าหน้าที่ที่ไม่พอใจหน่วยงานส่งข้อมูลสำคัญให้คู่แข่งหรือบุคคลภายนอก	๒. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ผิดปกติในระบบของเจ้าหน้าที่	๓	๓
	๓. กระทำผิดพลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญหรือแชร์ข้อมูลให้บุคคลที่ไม่เกี่ยวข้อง	๓. ขาดการฝึกอบรมเกี่ยวกับการปกป้องข้อมูล เช่น เจ้าหน้าที่ไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	๓	๓
	๔. การใช้บัญชีที่ถูกยึดหรือถูกแฮ็ก (Inactive users) เช่น บัญชีของเจ้าหน้าที่ที่ถูกยึดหรือแฮ็กมีการนำไปใช้ในการกระทำที่ไม่เหมาะสม	๔. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากหน่วยงาน เช่น บัญชีของเจ้าหน้าที่ที่ลาออกยังคงสามารถเข้าถึงระบบได้	๑	๓
	๕. มีการปลอมตัวเป็นบุคคลภายใน เช่น บุคคลภายนอกแฝงตัวเข้ามาในหน่วยงานผ่านการร่วมมือของเจ้าหน้าที่ภายใน	๕. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการคัดลอกหรือส่งออก	๑	๓
๔. การละเมิดข้อมูล (Data Breaches)	๑. มีการแฮ็กระบบเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้า หรือข้อมูลทางการเงิน	๑. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	๒	๓

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
	๒. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่อ่อนแอ	๒. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นผลเปิดช่องโหว่ให้ถูกโจมตี	๒	๓
	๓. มีการรั่วไหลของข้อมูลผ่านเจ้าหน้าที่ (โดยเจตนาหรือไม่เจตนา)	๓. การตั้งรหัสผ่านที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้รหัสผ่านซ้ำกันในหลายระบบ	๓	๓
	๔. มีการส่งข้อมูลสำคัญผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมลที่ไม่มีการเข้ารหัส	๔. ขาดระบบตรวจสอบการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	๒	๓
	๕. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	๕. ขาดการตรวจสอบกิจกรรมในระบบ เช่น ไม่มีการตรวจสอบกิจกรรมที่น่าสงสัยในระบบหรือการแจ้งเตือน	๒	๓
๕. การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	๑. มีการดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่แฝงแรนซัมแวร์ผ่านอีเมลฟิชชิง	๑. การขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่เปิดไฟล์แนบที่เป็นอันตรายจากอีเมลฟิชชิง	๓	๕
	๒. ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	๒. ซอฟต์แวร์และระบบปฏิบัติการที่ไม่ได้อัปเดต เช่น ระบบหรือซอฟต์แวร์ มีช่องโหว่ที่เปิดให้แรนซัมแวร์เข้าถึงได้	๓	๕
	๓. มีการใช้ Remote Desktop Protocol (RDP) ที่ไม่ได้ตั้งค่าความปลอดภัย	๓. การขาดการสำรองข้อมูล (Backup) เช่น ไม่มีระบบสำรองข้อมูลที่สามารถกู้คืนได้เมื่อถูกโจมตี	๒	๕
	๔. มีการแอบแฝงแรนซัมแวร์ในอุปกรณ์ USB Storage หรืออุปกรณ์พกพาอื่นๆ	๔. การตั้งค่าความปลอดภัยของ RDP ที่ไม่เหมาะสม เช่น เปิดใช้งาน RDP โดยไม่มีการควบคุมการเข้าถึงที่เข้มงวด	๓	๕

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
	๕. มีการกระจายแรนซัมแวร์ผ่านเครือข่ายที่เชื่อมโยงกับหน่วยงาน	๕. การขาดระบบป้องกันมัลแวร์ที่มีประสิทธิภาพ เช่น ไม่มีซอฟต์แวร์ป้องกันแรนซัมแวร์ที่สามารถตรวจจับและบล็อกการโจมตี	๓	๕
๖. ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)	๑. มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้จำหน่าย (๓rd Party/Suppliers) ที่ไม่ได้มีการควบคุมความปลอดภัยอาจทำให้ข้อมูลของหน่วยงานรั่วไหล	๑. การขาดกระบวนการตรวจสอบผู้จำหน่าย (๓rd Party/Suppliers) เช่น ไม่มีการตรวจสอบความปลอดภัยของผู้จำหน่าย (๓rd Party/Suppliers) ก่อนเซ็นสัญญา	๑	๓
	๒. มีการโจมตีผ่านซัพพลายเชน (Supply Chain Attacks) เช่น ผู้โจมตีใช้ช่องโหว่ของซัพพลายเออร์เพื่อเข้าถึงระบบหน่วยงาน	๒. ไม่มีข้อตกลงด้านความปลอดภัย (Security SLA) เช่น ขาดข้อตกลงที่กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัย	๑	๓
	๓. พบว่าผู้จำหน่ายขาดการปฏิบัติตามกฎระเบียบ เช่น ผู้จำหน่ายไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดด้านความปลอดภัย เช่น ISO ๒๗๐๐๑, ๒๗๐๑๘, ๒๗๗๐๑	๓. การเข้าถึงระบบที่ไม่เหมาะสม: ผู้จำหน่ายได้รับสิทธิ์เข้าถึงระบบมากเกินความจำเป็น	๑	๓
	๔. การพึ่งพาผู้จำหน่ายที่ไม่มีความมั่นคงในการบริการ เช่น ความล้มเหลวของผู้จำหน่าย อาทิ การหยุดให้บริการ อาจส่งผลกระทบต่อธุรกิจ	๔. ขาดการเฝ้าระวังความปลอดภัยของผู้จำหน่าย เช่น ไม่มีการติดตามการปฏิบัติงานของผู้จำหน่ายในด้านความปลอดภัย	๒	๓
	๕. การแชร์ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้มีการป้องกัน เช่น การส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีการเข้ารหัส	๕. การแชร์ข้อมูลกับผู้จำหน่ายหลายๆ ราย ทำให้ยิ่งแชร์ข้อมูลกับผู้จำหน่ายมากๆ ความเสี่ยงที่ข้อมูลจะรั่วไหลก็ยิ่งสูง	๒	๓
๗. ความเสี่ยงด้านความปลอดภัยของ	๑. ถูกการโจมตีแบบ DDoS (Distributed Denial of Service) เช่น การส่งคำขอจำนวนมากเพื่อทำให้เครือข่ายหยุดทำงาน	๑. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น การตั้งค่าเราเตอร์หรือไฟร์วอลล์ที่ไม่ปลอดภัย	๓	๓

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
เครือข่าย (Network Security Risks)	๒. ถูกการโจมตีแบบ Man-in-the-Middle (MitM) เช่น การดักฟังข้อมูลระหว่างการสื่อสารผ่านเครือข่าย	๒. ไม่มีการแยกเครือข่าย (Network Segmentation) เช่น ขาดการแยกเครือข่ายสำคัญออกจากเครือข่ายทั่วไป (VLAN)	๒	๓
	๓. ถูกการโจมตีแบบ Phishing ผ่านเครือข่าย เช่น การส่งลิงก์ฟิชชิงหรือไฟล์ที่เป็นอันตรายผ่านอีเมลหรือเครือข่าย	๓. ขาดระบบตรวจจับและป้องกันภัยคุกคาม เช่น ไม่มีการติดตั้ง IDS/IPS (Intrusion Detection/Prevention Systems)	๓	๓
	๔. มีการใช้ช่องโหว่ของโปรโตคอลเครือข่าย เช่น การโจมตีผ่านโปรโตคอล อาทิ DNS Spoofing หรือ ARP Poisoning	๔. การใช้โปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet ที่ไม่มีการเข้ารหัส	๒	๓
	๕. มีการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรืออุปกรณ์ที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายของหน่วยงาน	๕. ไม่มีการควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการตรวจสอบอุปกรณ์หรือผู้ใช้ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน	๒	๓
๘. ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)	๑. มีการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรือผู้ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่สำคัญได้ อาทิ ศูนย์ข้อมูลหรือเซิร์ฟเวอร์รูมหรือดาต้าเซ็นเตอร์	๑. การขาดระบบควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการกำหนดสิทธิ์หรือการยืนยันตัวตนก่อนเข้าถึงพื้นที่สำคัญ	๑	๓
	๒. มีการขโมยหรือสูญหายของอุปกรณ์ เช่น อุปกรณ์สำคัญต่างๆ อาทิ เซิร์ฟเวอร์ ฮาร์ดไดรฟ์ แล็ปท็อป ถูกขโมยหรือสูญหาย	๒. ไม่มีการเฝ้าระวังด้วยกล้องวงจรปิด (CCTV) เช่น ขาดระบบเฝ้าระวังหรือการตรวจสอบเหตุการณ์ที่เกิดขึ้นในพื้นที่สำคัญ	๑	๓
	๓. มีการก่อวินาศกรรม (Sabotage) เช่น การทำลายทรัพย์สินหรือระบบโดยบุคคลภายในหรือบุคคลภายนอก	๓. ไม่มีระบบป้องกันการก่อวินาศกรรม เช่น ขาดการออกแบบหรือมาตรการป้องกันการก่อวินาศกรรม	๑	๓

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)
	๔. เกิดภัยธรรมชาติ (Natural Disasters) เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหวที่ส่งผลกระทบต่ออุปกรณ์และข้อมูลสำคัญ	๔. ไม่มีระบบป้องกันภัยธรรมชาติ เช่น ขาดการออกแบบหรือมาตรการป้องกันภัยธรรมชาติ อาทิ การป้องกันน้ำท่วม	๒	๓
	๕. มีการขโมยข้อมูลผ่านการเข้าถึงทางกายภาพ เช่น การเชื่อมต่อกับพอร์ต USB หรือเครือข่ายโดยตรงในหน่วยงาน เพื่อขโมยข้อมูล	๕. การเก็บรักษาอุปกรณ์สำคัญในที่ไม่ปลอดภัย เช่น อุปกรณ์สำคัญถูกเก็บไว้ในพื้นที่ที่เข้าถึงได้ง่าย	๓	๓
๙. การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)	๑. มีการส่งข้อมูลโดยไม่ได้ตั้งใจ เช่น การส่งข้อมูลสำคัญไปยังผู้รับผิดคนหรือแพลตฟอร์มที่ไม่ปลอดภัย	๑. การขาดการควบคุมการเข้าถึงข้อมูล เช่น ไม่มีการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	๑	๓
	๒. มีการขโมยข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจหรือบุคคลภายนอกขโมยข้อมูลเพื่อผลประโยชน์ส่วนตัว	๒. การไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บหรือรับส่งกัน ไม่มีการเข้ารหัส	๒	๓
	๓. มีการละเมิดข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัย เช่น การรั่วไหลของข้อมูลที่ส่งผ่าน Wi-Fi หรือเครือข่ายที่ไม่มีการเข้ารหัส	๓. ขาดนโยบายและกระบวนการจัดการข้อมูล เช่น ไม่มีการกำหนดนโยบายในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคล	๑	๓
	๔. ถูกการโจมตีแบบ Phishing เช่น ผู้โจมตีใช้ฟิชชิงเพื่อเข้าถึงข้อมูลสำคัญผ่านอีเมลหรือข้อความ	๔. การขาดระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention - DLP) เช่น ไม่มีการใช้ระบบเพื่อตรวจจับและป้องกันการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	๓	๓
	๕. มีการติดมัลแวร์หรือแรนซัมแวร์ เช่น มีการใช้มัลแวร์เพื่อดึงข้อมูลหรือขัดขวางการเข้าถึงข้อมูล	๕. อุปกรณ์และบัญชีทรัพย์สินที่ไม่ได้รับการควบคุม เช่น อุปกรณ์พกพาหรือบัญชีผู้ใช้งานที่ไม่ได้ใช้งานยังสามารถเข้าถึงข้อมูลได้	๓	๕

๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินค่าความเสี่ยง จะพิจารณาจากปัจจัยจากขั้นตอนที่ผ่านมาได้แก่ โอกาสที่ภัยคุกคามที่เกิดขึ้นทำให้ระบบขาดความมั่นคง, ระดับผลกระทบหรือความรุนแรงของภัยคุกคามที่มีต่อระบบและประสิทธิภาพของแผนการควบคุมความปลอดภัยของระบบ การวัดระดับความเสี่ยงมีการกำหนดแผนภูมิความเสี่ยงที่ได้จาก การพิจารณาจัดระดับความสำคัญของความเสี่ยงจากโอกาสที่จะเกิดความเสี่ยง และผลกระทบที่เกิดขึ้น และขอบเขตของระดับความเสี่ยงที่สามารถยอมรับได้

ผลกระทบของความเสี่ยง						
	๕	๕	๑๐	๑๕	๒๐	๒๕
	๔	๔	๘	๑๒	๑๖	๒๐
	๓	๓	๖	๙	๑๒	๑๕
	๒	๒	๔	๖	๘	๑๐
	๑	๑	๒	๓	๔	๕
		๑	๒	๓	๔	๕
		โอกาสที่จะเกิดความเสี่ยง				

เกณฑ์ที่ใช้วัดค่าเฉลี่ยของระดับความเสี่ยง (Risk Level)

พื้นที่สี	ระดับความเสี่ยง	ระดับคะแนนความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง/คำอธิบาย
	ต่ำ	๑ – ๕.๐	ยอมรับความเสี่ยงได้ (มีแผนรองรับ) **คำอธิบาย :** ต้องติดตามเป็นระยะ แต่ยังไม่ต้องมีการดำเนินการใด ๆ เพิ่มเติม
	ปานกลาง	๕.๑ – ๙.๔	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม) **คำอธิบาย :** เป็นความเสี่ยงปานกลาง ดังนั้นต้องมีการติดตามและอาจมีมาตรการป้องกัน
	สูง	๙.๕ – ๑๒.๔	ควบคุมความเสี่ยงได้ (มีแผนควบคุมความเสี่ยง) **คำอธิบาย :** เป็นความเสี่ยงสูง ต้องมีการดำเนินการบางอย่างเพื่อลดความเสี่ยง
	สูงมาก	๑๒.๕ – ๒๕	ถ่ายโอนความเสี่ยง **คำอธิบาย :** เป็นความเสี่ยงขั้นวิกฤติ ต้องมีการดำเนินการโดยทันทีและมีการวางแผนจัดการความเสี่ยง

ตาราง : การประเมินความเสี่ยง (Risk Evaluation)

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
๑. การโจมตีด้วยมัลแวร์ (Malware Attacks)	๑. มีการดาวน์โหลดไฟล์จากเว็บไซต์ที่ไม่น่าเชื่อถือ ซึ่งอาจแฝงด้วยมัลแวร์	๑. ไม่มีระบบหรือมาตรการควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ในหน่วยงาน	๑	๔	๔	๘.๘
	๒. มีการติดมัลแวร์ที่มาจากการใช้อุปกรณ์ USB Storage หรือสื่อเก็บข้อมูลภายนอก	๒. ไม่มีการติดตั้งหรืออัปเดตโปรแกรมป้องกันไวรัสเมื่อใช้อุปกรณ์ USB Storage	๓	๔	๑๒	
	๓. ไฟล์แนบในอีเมล์มีฟิชชิงและแฝงด้วยมัลแวร์	๓. ขาดระบบหรือมาตรการหรือนโยบายการควบคุมการใช้งานอีเมลที่มีไฟล์แนบ	๓	๔	๑๒	
	๔. การติดตั้งซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ที่ฝังด้วยมัลแวร์	๔. เจ้าหน้าที่ขาดความรู้ในการติดตั้งไฟล์หรือเว็บไซต์ที่มีความเสี่ยงไซเบอร์	๑	๔	๔	
	๕. เจ้าหน้าที่เข้าถึงโฆษณาออนไลน์ (Malvertising) ตามเว็บต่างๆ ที่พาไปยังเว็บไซต์ที่มีมัลแวร์	๕. ไม่มีระบบกรองเว็บไซต์ ที่ป้องกันมัลแวร์ และอัปเดตเป็นประจำ	๓	๔	๑๒	
๒. การโจมตีด้วยฟิชชิง (Phishing Attacks)	๑. การรับอีเมลที่มีฟิชชิงหลอกให้ผู้ใช้กรอกข้อมูลสำคัญ เช่น รหัสผ่าน หรือข้อมูลทางการเงิน	๑. ขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่ไม่สามารถแยกแยะอีเมลหรือเว็บไซต์ปลอมได้	๓	๔	๑๒	๘.๘

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	๒. Spear Phishing ที่กำหนดเป้าหมายเจาะจงบุคคลหรือหน่วยงาน หลุดเข้ามาในระบบ	๒. ไม่มีระบบตรวจจับอีเมลฟิชชิง เช่น ไม่มีการใช้ตัวกรองอีเมลเพื่อบล็อกอีเมลที่เป็นอันตราย	๒	๔	๘	
	๓. มีการรับส่งลิงก์ที่มีฟิชชิงผ่าน SMS หรือโซเชียลมีเดีย	๓. การใช้รหัสผ่านซ้ำหรือไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้ซ้ำในหลายระบบ	๒	๔	๘	
	๔. เข้าเว็บไซต์ปลอมที่เลียนแบบหน้าล็อกอินของหน่วยงานหรือบริการออนไลน์	๔. ขาดการใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) เช่น ระบบไม่มีการยืนยันตัวตนเพิ่มเติมสำหรับการเข้าถึงข้อมูลสำคัญ	๑	๔	๔	
	๕. ถูกระบบโทรศัพท์ปลอม (Call center) หลอกขอข้อมูลส่วนตัว	๕. ไม่มีกระบวนการยืนยันการสื่อสารที่ปลอดภัย เช่น ขาดนโยบายการยืนยันตัวตนของผู้ส่งอีเมลหรือข้อความ	๓	๔	๑๒	
๓. ภัยคุกคามจากบุคคลภายใน (Insider Threats)	๑. การใช้งานข้อมูลโดยใช้อำนาจมิชอบ เช่น เจ้าหน้าที่ที่มีสิทธิ์เข้าถึงข้อมูลสำคัญอาจนำข้อมูลไปใช้โดยไม่ได้รับอนุญาต	๑. การควบคุมสิทธิ์การเข้าถึงที่ไม่เหมาะสม เช่น เจ้าหน้าที่บางคนได้รับสิทธิ์เข้าถึงข้อมูลมากเกินความจำเป็น	๑	๓	๓	๕.๔

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	๒. การรั่วไหลของข้อมูลโดยเจตนา เช่น เจ้าหน้าที่ที่ไม่พอใจหน่วยงานส่งข้อมูลสำคัญให้คู่แข่งหรือบุคคลภายนอก	๒. ขาดระบบตรวจสอบพฤติกรรม เช่น ไม่มีการติดตามกิจกรรมที่ผิดปกติในระบบของเจ้าหน้าที่	๓	๓	๙	
	๓. กระทำผิดพลาดโดยไม่ได้ตั้งใจ เช่น การลบข้อมูลสำคัญหรือแชร์ข้อมูลให้บุคคลที่ไม่เกี่ยวข้อง	๓. ขาดการฝึกอบรมเกี่ยวกับการปกป้องข้อมูล เช่น เจ้าหน้าที่ไม่เข้าใจถึงความสำคัญของการปกป้องข้อมูล	๓	๓	๙	
	๔. การใช้บัญชีที่ถูกยึดหรือถูกแฮ็ก (Inactive users) เช่น บัญชีของเจ้าหน้าที่ที่ถูกยึดหรือแฮ็กมีการนำไปใช้ในการกระทำที่ไม่เหมาะสม	๔. ไม่มีการจัดการบัญชีผู้ใช้งานที่ออกจากหน่วยงาน เช่น บัญชีของเจ้าหน้าที่ที่ลาออกยังคงสามารถเข้าถึงระบบได้	๑	๓	๓	
	๕. มีการปลอมตัวเป็นบุคคลภายใน เช่น บุคคลภายนอกแฝงตัวเข้ามาในหน่วยงานผ่านการร่วมมือของเจ้าหน้าที่ภายใน	๕. ไม่มีการเข้ารหัสข้อมูลสำคัญ เช่น ข้อมูลที่สำคัญไม่ได้รับการป้องกัน ทำให้ง่ายต่อการคัดลอกหรือส่งออก	๑	๓	๓	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
๔. การละเมิดข้อมูล (Data Breaches)	๑. มีการแฮ็กระบบเพื่อเข้าถึงข้อมูลสำคัญ เช่น ข้อมูลลูกค้าหรือข้อมูลทางการเงิน	๑. การขาดการเข้ารหัสข้อมูล (Encryption) เช่น ข้อมูลสำคัญไม่ได้รับการเข้ารหัสทั้งในขณะส่งและจัดเก็บข้อมูล	๒	๓	๖	๖.๖
	๒. มีการละเมิดข้อมูลจากการตั้งรหัสผ่านที่อ่อนแอ	๒. ระบบที่ไม่ได้อัปเดต (Outdated Systems) เช่น ระบบปฏิบัติการและซอฟต์แวร์ที่ไม่ได้อัปเดตเป็นผลเปิดช่องโหว่ให้ถูกโจมตี	๒	๓	๖	
	๓. มีการรั่วไหลของข้อมูลผ่านเจ้าหน้าที่ (โดยเจตนาหรือไม่เจตนา)	๓. การตั้งรหัสผ่านที่ไม่ปลอดภัย เช่น ผู้ใช้ตั้งรหัสผ่านที่เดาง่ายหรือใช้รหัสผ่านซ้ำกันในหลายระบบ	๓	๓	๙	
	๔. มีการส่งข้อมูลสำคัญผ่านช่องทางที่ไม่ปลอดภัย เช่น อีเมลที่ไม่มีการเข้ารหัส	๔. ขาดระบบตรวจสอบการเข้าถึง (Access Control): ไม่มีการควบคุมสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	๒	๓	๖	
	๕. มีการโจมตีผ่าน API หรือระบบที่ไม่ได้รับการตรวจสอบความปลอดภัย	๕. ขาดการตรวจสอบกิจกรรมในระบบ เช่น ไม่มีการตรวจสอบกิจกรรมที่น่าสงสัยในระบบหรือการแจ้งเตือน	๒	๓	๖	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
๕. การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	๑. มีการดาวน์โหลดไฟล์หรือซอฟต์แวร์ที่แฝงแรนซัมแวร์ผ่านอีเมลฟิชชิง	๑. การขาดการฝึกอบรมเจ้าหน้าที่ เช่น เจ้าหน้าที่เปิดไฟล์แนบที่เป็นอันตรายจากอีเมลฟิชชิง	๓	๕	๑๕	๑๔
	๒. ถูกการโจมตีโดยใช้ช่องโหว่ในระบบหรือซอฟต์แวร์ที่ไม่ได้อัปเดต	๒. ซอฟต์แวร์และระบบปฏิบัติการที่ไม่ได้อัปเดต เช่น ระบบหรือซอฟต์แวร์ มีช่องโหว่ที่เปิดให้แรนซัมแวร์เข้าถึงได้	๓	๕	๑๕	
	๓. มีการใช้ Remote Desktop Protocol (RDP) ที่ไม่ได้ตั้งค่าความปลอดภัย	๓. การขาดการสำรองข้อมูล (Backup) เช่น ไม่มีระบบสำรองข้อมูลที่สามารถกู้คืนได้เมื่อถูกโจมตี	๒	๕	๑๐	
	๔. มีการแอบแฝงแรนซัมแวร์ในอุปกรณ์ USB Storage หรืออุปกรณ์พกพาอื่นๆ	๔. การตั้งค่าความปลอดภัยของ RDP ที่ไม่เหมาะสม เช่น เปิดใช้งาน RDP โดยไม่มีการควบคุมการเข้าถึงที่เข้มงวด	๓	๕	๑๕	
	๕. มีการกระจายแรนซัมแวร์ผ่านเครือข่ายที่เชื่อมโยงกับหน่วยงาน	๕. การขาดระบบป้องกันมัลแวร์ที่มีประสิทธิภาพ เช่น ไม่มีซอฟต์แวร์ป้องกันแรนซัมแวร์ที่สามารถตรวจจับและบล็อกการโจมตี	๓	๕	๑๕	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
๖. ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)	๑. มีการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตจากผู้จำหน่าย (๓rd Party/Suppliers) ที่ไม่ได้มีการควบคุมความปลอดภัยอาจทำให้ข้อมูลของหน่วยงานรั่วไหล	๑. การขาดกระบวนการตรวจสอบผู้จำหน่าย (๓rd Party/Suppliers) เช่น ไม่มีการตรวจสอบความปลอดภัยของผู้จำหน่าย (๓rd Party/Suppliers) ก่อนเซ็นสัญญา	๑	๓	๓	๔.๒
	๒. มีการโจมตีผ่านซัพพลายเชน (Supply Chain Attacks) เช่น ผู้โจมตีใช้ช่องโหว่ของซัพพลายเออร์เพื่อเข้าถึงระบบหน่วยงาน	๒. ไม่มีข้อตกลงด้านความปลอดภัย (Security SLA) เช่น ขาดข้อตกลงที่กำหนดบทบาทและความรับผิดชอบด้านความปลอดภัย	๑	๓	๓	
	๓. พบว่าผู้จำหน่ายขาดการปฏิบัติตามกฎระเบียบ เช่น ผู้จำหน่ายไม่ปฏิบัติตามมาตรฐานหรือข้อกำหนดด้านความปลอดภัย เช่น ISO ๒๗๐๐๑, ๒๗๐๑๘, ๒๗๗๐๑	๓. การเข้าถึงระบบที่ไม่เหมาะสม: ผู้จำหน่ายได้รับสิทธิ์เข้าถึงระบบมากเกินความจำเป็น	๑	๓	๓	
	๔. การพึ่งพาผู้จำหน่ายที่ไม่มีความมั่นคงในการบริการ เช่น ความล้มเหลวของผู้จำหน่าย	๔. ขาดการเฝ้าระวังความปลอดภัยของผู้จำหน่าย เช่น ไม่มี	๒	๓	๖	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	อาทิ การหยุดให้บริการ อาจส่งผลกระทบต่อธุรกิจ	การติดตามการปฏิบัติงานของผู้จำหน่ายในด้านความปลอดภัย				
	๕. การแชร์ข้อมูลระหว่างกันกับผู้จำหน่ายที่ไม่ได้มีการป้องกัน เช่น การส่งข้อมูลสำคัญผ่านช่องทางที่ไม่มีการเข้ารหัส	๕. การแชร์ข้อมูลกับผู้จำหน่ายหลายๆ ราย ทำให้ยิ่งแชร์ข้อมูลกับผู้จำหน่ายมากๆ ความเสี่ยงที่ข้อมูลจะรั่วไหลก็ยิ่งสูง	๒	๓	๖	
๗. ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)	๑. ถูกการโจมตีแบบ DDoS (Distributed Denial of Service) เช่น การส่งคำขอจำนวนมากเพื่อทำให้เครือข่ายหยุดทำงาน	๑. การตั้งค่าความปลอดภัยที่ไม่เหมาะสม เช่น การตั้งค่าเราเตอร์หรือไฟร์วอลล์ที่ไม่ปลอดภัย	๓	๓	๙	๗.๒
	๒. ถูกการโจมตีแบบ Man-in-the-Middle (MitM) เช่น การดักฟังข้อมูลระหว่างการสื่อสารผ่านเครือข่าย	๒. ไม่มีการแยกเครือข่าย (Network Segmentation) เช่น ขาดการแยกเครือข่ายสำคัญออกจากเครือข่ายทั่วไป (VLAN)	๒	๓	๖	
	๓. ถูกการโจมตีแบบ Phishing ผ่านเครือข่าย เช่น การส่งลิงก์ฟิชชิงหรือไฟล์ที่เป็นอันตรายผ่านอีเมลหรือเครือข่าย	๓. ขาดระบบตรวจจับและป้องกันภัยคุกคาม เช่น ไม่มีการติดตั้ง IDS/IPS (Intrusion Detection/Prevention Systems)	๓	๓	๙	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	๔. มีการใช้ช่องโหว่ของโปรโตคอลเครือข่าย เช่น การโจมตีผ่านโปรโตคอล อาทิ DNS Spoofing หรือ ARP Poisoning	๔. การใช้โปรโตคอลที่ล้าสมัย เช่น FTP หรือ Telnet ที่ไม่มีการเข้ารหัส	๒	๓	๖	
	๕. มีการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรืออุปกรณ์ที่ไม่ได้รับอนุญาตเชื่อมต่อกับเครือข่ายของหน่วยงาน	๕. ไม่มีการควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการตรวจสอบอุปกรณ์หรือผู้ใช้ที่เชื่อมต่อกับเครือข่ายของหน่วยงาน	๒	๓	๖	
๘. ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)	๑. มีการเข้าถึงพื้นที่โดยไม่ได้รับอนุญาต เช่น บุคคลภายนอกหรือผู้ไม่ได้รับอนุญาตสามารถเข้าถึงพื้นที่สำคัญได้ อาทิ ศูนย์ข้อมูลหรือเซิร์ฟเวอร์รูมหรือดาต้าเซ็นเตอร์	๑. การขาดระบบควบคุมการเข้าถึง (Access Control) เช่น ไม่มีการกำหนดสิทธิ์หรือการยืนยันตัวตนก่อนเข้าถึงพื้นที่สำคัญ	๑	๓	๓	๔.๘
	๒. มีการขโมยหรือสูญหายของอุปกรณ์ เช่น อุปกรณ์สำคัญต่างๆ อาทิ เซิร์ฟเวอร์	๒. ไม่มีการเฝ้าระวังด้วยกล้องวงจรปิด (CCTV) เช่น ขาดระบบเฝ้าระวังหรือการตรวจสอบเหตุการณ์ที่เกิดขึ้นในพื้นที่สำคัญ	๑	๓	๓	

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	ฮาร์ดไดรฟ์ แล็ปท็อป ถูกขโมยหรือสูญหาย					
	๓. มีการก่อวินาศกรรม (Sabotage) เช่น การทำลายทรัพย์สินหรือระบบโดยบุคคลภายในหรือบุคคลภายนอก	๓. ไม่มีระบบป้องกันการก่อวินาศกรรม เช่น ขาดการออกแบบหรือมาตรการป้องกันการก่อวินาศกรรม	๑	๓	๓	
	๔. เกิดภัยธรรมชาติ (Natural Disasters) เช่น น้ำท่วม ไฟไหม้ หรือแผ่นดินไหวที่ส่งผลกระทบต่ออุปกรณ์และข้อมูลสำคัญ	๔. ไม่มีระบบป้องกันภัยธรรมชาติ เช่น ขาดการออกแบบหรือมาตรการป้องกันภัยธรรมชาติ อาทิ การป้องกันน้ำท่วม	๒	๓	๖	
	๕. มีการขโมยข้อมูลผ่านการเข้าถึงทางกายภาพ เช่น การเชื่อมต่อกับพอร์ต USB หรือเครือข่ายโดยตรงในหน่วยงานเพื่อขโมยข้อมูล	๕. การเก็บรักษาอุปกรณ์สำคัญในที่ไม่ปลอดภัย เช่น อุปกรณ์สำคัญถูกเก็บไว้ในพื้นที่ที่เข้าถึงได้ง่าย	๓	๓	๙	
๙. การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)	๑. มีการส่งข้อมูลโดยไม่ได้ตั้งใจ เช่น การส่งข้อมูลสำคัญไปยังผู้รับผิดคนหรือแพลตฟอร์มที่ไม่ปลอดภัย	๑. การขาดการควบคุมการเข้าถึงข้อมูล เช่น ไม่มีการกำหนดสิทธิ์การเข้าถึงข้อมูลที่เหมาะสม	๑	๓	๓	๖.๖

ความเสี่ยง (Risk Cluster)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	โอกาสที่จะเกิด (Likelihood)	ความรุนแรง (Impact)	ระดับความเสี่ยง (Risk Level)	ค่าเฉลี่ยของระดับความเสี่ยง (Risk level)
	๒. มีการขโมยข้อมูลโดยเจตนา เช่น พนักงานที่ไม่พอใจหรือบุคคลภายนอกขโมยข้อมูลเพื่อผลประโยชน์ส่วนตัว	๒. การไม่มีการเข้ารหัสข้อมูล เช่น ข้อมูลที่จัดเก็บหรือรับส่งกันไม่มีการเข้ารหัส	๒	๓	๖	
	๓. มีการละเมิดข้อมูลผ่านเครือข่ายที่ไม่ปลอดภัย เช่น การรั่วไหลของข้อมูลที่ส่งผ่าน Wi-Fi หรือเครือข่ายที่ไม่มีการเข้ารหัส	๓. ขาดนโยบายและกระบวนการจัดการข้อมูล เช่น ไม่มีการกำหนดนโยบายในการจัดการข้อมูลสำคัญและข้อมูลส่วนบุคคล	๑	๓	๓	
	๔. ถูกการโจมตีแบบ Phishing เช่น ผู้โจมตีใช้ฟิชชิงเพื่อเข้าถึงข้อมูลสำคัญผ่านอีเมลหรือข้อความ	๔. การขาดระบบป้องกันข้อมูลรั่วไหล (Data Loss Prevention - DLP) เช่น ไม่มีการใช้ระบบเพื่อตรวจจับและป้องกันการถ่ายโอนข้อมูลที่ไม่ได้รับอนุญาต	๓	๓	๓	
	๕. มีการติดมัลแวร์หรือแรนซัมแวร์ เช่น มีการใช้มัลแวร์เพื่อดึงข้อมูลหรือขัดขวางการเข้าถึงข้อมูล	๕. อุปกรณ์และบัญชีทรัพย์สินที่ไม่ได้รับการควบคุม เช่น อุปกรณ์พกพาหรือบัญชีผู้ใช้งานที่ไม่ได้ใช้งานยังสามารถเข้าถึงข้อมูลได้	๓	๕	๑๕	

๕. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้วขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของกรมสอบสวนคดีพิเศษ

๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้ โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในกรมสอบสวนคดีพิเศษจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม หน่วยงานควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่าตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคาแพง

เมื่อกรมสอบสวนคดีพิเศษเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยงหรือการลดผลกระทบจากความเสี่ยง

ตาราง : แผนจัดการความเสี่ยง (Risk Treatment Plan)

ความเสี่ยง (Risk Cluster)	ค่าเฉลี่ยระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	ตัวเลือกการตอบสนอง (Risk Treatment)	แผนจัดการความเสี่ยง (Risk Treatment Plan)
๑. การโจมตีด้วยมัลแวร์ (Malware Attacks)	๘.๘	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- ติดตั้งและอัปเดตโปรแกรมป้องกันมัลแวร์ - ควบคุมการดาวน์โหลดและติดตั้งซอฟต์แวร์ - ควบคุมการใช้งาน USB และอุปกรณ์พกพา - อัปเดตระบบปฏิบัติการและซอฟต์แวร์ - การให้ความรู้และฝึกอบรมเจ้าหน้าที่ - ใช้ระบบกรองเนื้อหาและตรวจจับ - สร้างระบบสำรองข้อมูล (Backup) - การจำลองและทดสอบการโจมตี - ใช้เครื่องมือความปลอดภัยแบบครบวงจร (Security Suites) - นโยบายการจัดการเหตุการณ์ (Incident Reporting)
๒. การโจมตีด้วยฟิชชิง (Phishing Attacks)	๘.๘	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- การให้ความรู้และฝึกอบรมเจ้าหน้าที่ - ติดตั้งตัวกรองอีเมล (Email Filtering) - ใช้การยืนยันตัวตนแบบหลายปัจจัย (MFA) - สร้างนโยบายรหัสผ่านที่เข้มงวด - ตรวจสอบและควบคุมการเข้าถึงเว็บไซต์ - จัดทำกระบวนการยืนยันตัวตนของการสื่อสาร - ใช้เครื่องมือ SIEM (Security Information and Event Management) - การจำลองและทดสอบช่องโหว่ - นโยบายการจัดการเหตุการณ์ (Incident Reporting)

ความเสี่ยง (Risk Cluster)	ค่าเฉลี่ยระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	ตัวเลือกการตอบสนอง (Risk Treatment)	แผนจัดการความเสี่ยง (Risk Treatment Plan)
๓. ภัยคุกคามจากบุคคลภายใน (Insider Threats)	๕.๔	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- การกำหนดสิทธิ์การเข้าถึง (Access Control) - การเฝ้าระวังพฤติกรรมของผู้ใช้งาน (User Behavior Analytics - UBA) - การฝึกอบรมเจ้าหน้าที่ - การจัดการบัญชีผู้ใช้งาน - การเข้ารหัสข้อมูลสำคัญ - การเฝ้าระวังและแจ้งเตือนเหตุการณ์ - นโยบายและกระบวนการตรวจสอบความปลอดภัย - สร้างโปรแกรม Insider Threat Program (ITP)
๔. การละเมิดข้อมูล (Data Breaches)	๖.๖	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- การเข้ารหัสข้อมูล (Encryption) - อัปเดตระบบและซอฟต์แวร์ (Patch Management) - กำหนดนโยบายรหัสผ่านที่เข้มงวด - การควบคุมการเข้าถึง (Access Control) - ระบบตรวจสอบและแจ้งเตือนภัยคุกคาม - การฝึกอบรมเจ้าหน้าที่ - ใช้ระบบสำรองข้อมูล (Backup) - ทดสอบช่องโหว่และการโจมตีจำลอง - การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan) - นโยบายการควบคุม API (Application Programming Interfaces) และการบูรณาการระบบ

ความเสี่ยง (Risk Cluster)	ค่าเฉลี่ยระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	ตัวเลือกการตอบสนอง (Risk Treatment)	แผนจัดการความเสี่ยง (Risk Treatment Plan)
๕. การโจมตีด้วยแรนซัมแวร์ (Ransomware Attacks)	๑๔	ถ่ายโอนความเสี่ยง	ถ่ายโอนความเสี่ยง	- การติดตั้งและอัปเดตซอฟต์แวร์ป้องกันแรนซัมแวร์ - อัปเดตซอฟต์แวร์และระบบปฏิบัติการ - การสำรองข้อมูลอย่างสม่ำเสมอ - การตั้งค่าความปลอดภัยของ RDP - การฝึกอบรมเจ้าหน้าที่ - การกรองอีเมลและเว็บ - การใช้เทคโนโลยีการจำกัดสิทธิ์ - ติดตั้งระบบตรวจจับและตอบสนองภัยคุกคาม - ใช้การเข้ารหัสข้อมูล - การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)
๖. ความเสี่ยงจากผู้จำหน่ายภายนอก (Third-Party Vendor Risks)	๔.๒	ยอมรับความเสี่ยงได้ (มีแผนรองรับ)	ยอมรับ (Accept)	- การตรวจสอบความปลอดภัยก่อนเลือกผู้จำหน่าย - การจัดทำข้อตกลงด้านความปลอดภัย (Security SLA) - การจัดการสิทธิ์การเข้าถึง (Access Control) - การติดตามและเฝ้าระวังผู้จำหน่าย (Vendor Monitoring) - การแบ่งชั้นข้อมูลที่แชร์กับผู้จำหน่าย - การประเมินความเสี่ยงของซัพพลายเชน - การควบคุมการเข้าถึงข้อมูล - การจัดทำแผนรับมือเหตุการณ์ร่วมกับผู้จำหน่าย - การทบทวนและปรับปรุงกระบวนการบริหารจัดการผู้จำหน่าย

ความเสี่ยง (Risk Cluster)	ค่าเฉลี่ยระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	ตัวเลือกการตอบสนอง (Risk Treatment)	แผนจัดการความเสี่ยง (Risk Treatment Plan)
๗. ความเสี่ยงด้านความปลอดภัยของเครือข่าย (Network Security Risks)	๗.๒	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- การติดตั้งไฟร์วอลล์ (Firewall) - การใช้ระบบตรวจจับและป้องกันภัยคุกคาม (IDS/IPS) - การเข้ารหัสการสื่อสารในเครือข่าย - การแยกเครือข่าย (Network Segmentation) - การควบคุมการเข้าถึง (Access Control) - การใช้ VPN (Virtual Private Network) - การอัปเดตอุปกรณ์เครือข่ายและระบบปฏิบัติการ - การตรวจสอบและเฝ้าระวังเครือข่าย - การป้องกันการโจมตี DDoS - การฝึกอบรมเจ้าหน้าที่ - การกำหนดนโยบายการใช้งานเครือข่าย (Network Policy) - การตรวจสอบอุปกรณ์ในเครือข่าย
๘. ความเสี่ยงด้านความปลอดภัยทางกายภาพ (Physical Security Risks)	๔.๘	ยอมรับความเสี่ยงได้ (มีแผนรองรับ)	ยอมรับ (Accept)	- การติดตั้งระบบควบคุมการเข้าถึงทางกายภาพ - การเฝ้าระวังด้วยกล้องวงจรปิด (CCTV) - การป้องกันภัยธรรมชาติ - การจัดเก็บอุปกรณ์สำคัญในที่ปลอดภัย - การกำหนดนโยบายการเข้าถึงพื้นที่สำคัญ - การเฝ้าระวังและตรวจสอบเหตุการณ์ - การฝึกอบรมพนักงานด้านความปลอดภัย - การจัดทำแผนรับมือเหตุการณ์ฉุกเฉิน - การตรวจสอบความปลอดภัยทางกายภาพเป็นระยะ - การประกันภัย

ความเสี่ยง (Risk Cluster)	ค่าเฉลี่ยระดับความเสี่ยง	กลยุทธ์ในการจัดการความเสี่ยง	ตัวเลือกการตอบสนอง (Risk Treatment)	แผนจัดการความเสี่ยง (Risk Treatment Plan)
๙. การสูญหายหรือการรั่วไหลของข้อมูล (Data Loss or Data Leakage)	๖.๖	ยอมรับความเสี่ยงได้ (มีมาตรการติดตาม)	ลดความเสี่ยง (Mitigate)	- การเข้ารหัสข้อมูล (Data Encryption) - การตั้งค่าและควบคุมสิทธิ์การเข้าถึง (Access Control) - การใช้ระบบป้องกันการรั่วไหลของข้อมูล (Data Loss Prevention - DLP) - การสร้างนโยบายการจัดการข้อมูล (Data Governance) - การสำรองข้อมูล (Backup) - การใช้ระบบตรวจจับและแจ้งเตือนแบบเรียลไทม์ - การควบคุมการใช้งานอุปกรณ์พกพา (Mobile Device Management - MDM) - การฝึกอบรมพนักงาน (Employee Training) - การตั้งค่าความปลอดภัยของเครือข่าย - การจัดทำแผนรับมือเหตุการณ์ (Incident Response Plan)

เอกสารอ้างอิง

- GUIDE TO CONDUCTING CYBERSECURITY RISK ASSESSMENT FOR CRITICAL INFORMATION INFRASTRUCTURE, Cyber Security Agency of Singapore, FEBRUARY ๒๐๒๑
- Link: https://www.csa.gov.sg/docs/default-source/csa/documents/legislation_supplementary_references/guide-to-conducting-cybersecurity-risk-assessment-for-cii.pdf
- NIST SP ๘๐๐-๓๐ Rev. ๑ Guide for Conducting Risk Assessments, NIST, September ๒๐๑๒
- Link: https://csrc.nist.gov/publications/detail/sp/๘๐๐-๓๐/rev-๑/final
- ISO ๓๑๐๐๐:๒๐๑๘(en) Risk management — Guidelines, ISO, FEBRUARY ๒๐๑๘
- Link: https://www.iso.org/obp/ui/#iso:std:iso:๓๑๐๐๐:ed-๒:v๑:en
- ISO/IEC ๒๗๐๐๕:๒๐๑๘ Information technology — Security techniques — Information security risk management, ISO/IEC, July ๒๐๑๘
- Link: https://www.iso.org/standard/๗๕๒๘๑.html

ภาคผนวก ค

แผนรับมือภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมสอบสวนคดีพิเศษฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์

รวมทั้งเพื่อให้เป็นไปตามประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖ และประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖ ด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นในกรมสอบสวนคดีพิเศษ โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใต้กรมสอบสวนคดีพิเศษ การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมสอบสวนคดีพิเศษ

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมสอบสวนคดีพิเศษ รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ มีหน้าที่ทบทวนและขออนุมัติแผนรับมือแผนรับมือฯ ฉบับนี้ ถึงผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ของกรมสอบสวนคดีพิเศษ

๕. หน้าที่ในการดำเนินการตามแผน

ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ กรมสอบสวนคดีพิเศษ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยให้ทุกหน่วยงานภายในกรมสอบสวนคดีพิเศษเป็นหน่วยงานสนับสนุนในการดำเนินการตามแผนรับมือฯ

๖. รายละเอียดการบังคับใช้เอกสาร

๖.๑ รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control and review)	
ผู้จัดทำเอกสาร (Author)	นางสาวสุปราณี ลาภโภคาชัย
ผู้ดำเนินการตามเอกสาร (Owner)	ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ
วันที่จัดทำเอกสาร (Date created)	๙ กันยายน ๒๕๖๘
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	นางจิตลัดดา เสียงใส
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	๙ กันยายน ๒๕๖๘
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ของกรมสอบสวนคดีพิเศษ
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	xx กันยายน ๒๕๖๙

๖.๒ การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
-	-	-	-

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๗.๑ ประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖

๗.๒ ประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖

๗.๓ นโยบายการใช้งานเว็บไซต์กรมสอบสวนคดีพิเศษ

๗.๔ นโยบายการคุ้มครองข้อมูลส่วนบุคคลของกรมสอบสวนคดีพิเศษ

๘. นิยาม

๑) เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

๒) เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๓) ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๔) เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ นามสกุล / ช่องทางการติดต่อสื่อสาร	ระยะเวลาในการปฏิบัติงาน	หน้าที่	ความรับผิดชอบ
๑	พันตำรวจโท อนุรักษ์ โรจนนิรันดร์กิจ ตำแหน่ง : รองอธิบดีกรมสอบสวนคดีพิเศษ E-mail : anurak@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๔ ๘๗๕ ๓๔๘๕	๒๔ ชั่วโมง/ ๗ วัน	ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูง	ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูง กรมสอบสวนคดีพิเศษ
๒	นายพิพัฒน์ เพ็ญภาค ตำแหน่ง : ผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ E-mail : pipat@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๔ ๗๕๑ ๖๕๒๕	๒๔ ชั่วโมง/ ๗ วัน	ผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ	ผู้บริหารด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสอบสวนคดีพิเศษ
๓	นายพัลลภ เกิดเทพ ตำแหน่ง : รองผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ E-mail : panlop_k@dsi.go.th หมายเลขโทรศัพท์ : ๐๖๑ ๓๙๘ ๑๐๒๓	๒๔ ชั่วโมง/ ๗ วัน	รองผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ	ผู้บริหารด้านเทคโนโลยีสารสนเทศและการสื่อสารของกรมสอบสวนคดีพิเศษ
๔	นายนิติภัทร แสงพัฒน์ ตำแหน่ง : ผู้อำนวยการศูนย์สารสนเทศ E-mail : nitipat_sa@dsi.go.th หมายเลขโทรศัพท์ : ๐๖๓ ๒๐๓ ๙๖๒๒	๒๔ ชั่วโมง/ ๗ วัน	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

กรมสอบสวนคดีพิเศษใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อ นามสกุล / รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	นายนิติภัทร แสงพัฒน์ ตำแหน่ง : ผู้อำนวยการศูนย์สารสนเทศ E-mail : nitipat_sa@dsi.go.th หมายเลขโทรศัพท์ : ๐๖๓ ๒๐๓ ๙๖๒๒	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นางจิตลัดดา เสียงใส ตำแหน่ง : นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ E-mail : jitladda_sie@dsi.go.th หมายเลขโทรศัพท์ : ๐๙๘ ๘๕๓ ๖๗๗๓ นางสาวสุปราณี ลาภโภคาชัย ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : supranee_lap@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๑ ๘๘๐ ๕๓๕๑	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นายพงศ์บัณฑิต ชัยชาญ ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : pongbandit_ch@dsi.go.th หมายเลขโทรศัพท์ : ๐๙๔ ๙๖๕ ๑๔๑๙ นางสาวกานทิพย์ โพธิ์อ่อน ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : kantip_pho@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๙ ๐๕๒ ๕๐๐๔	เจ้าหน้าที่รับมือฯ (Incident lead)	ทำหน้าที่ช่วยเหลือศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	นายธัมมจิต รุจนวงศ์ ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : thammajit_rou@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๕ ๘๑๓ ๕๕๕๔	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๑	นายภัทรดนัย รุจิชัยกุล ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : pattharadanai_ruj@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๒ ๗๙๙ ๒๐๘๘	เจ้าหน้าที่ศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๒	นางสาวกานทิพย์ โพธิ์อ่อน ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : kantip_pho@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๙ ๐๕๒ ๕๐๐๔ นางสาวสุปราณี ลาภโภคาชัย ตำแหน่ง : เจ้าหน้าที่คดีพิเศษชำนาญการ E-mail : supranee_lap@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๑ ๘๘๐ ๕๓๕๑	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘
๓	นายภูวนัย แสงพล ตำแหน่ง : เจ้าหน้าที่คดีพิเศษปฏิบัติการ E-mail : puwanai_san@dsi.go.th หมายเลขโทรศัพท์ : ๐๘๕ ๓๐๕ ๘๕๒๑ นายวีรภัทร จิระสุนทร ตำแหน่ง : นักวิชาการคอมพิวเตอร์ปฏิบัติการ E-mail : werapat_jir@dsi.go.th หมายเลขโทรศัพท์ : ๐๙๕ ๐๔๐ ๓๖๔๕	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘
๔	ผู้อำนวยการกองกฎหมาย	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่เป็นที่ปรึกษากฎหมายที่เกี่ยวข้อง
๕	ผู้อำนวยการกลุ่มตรวจสอบภายใน	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๘

ลำดับ	ชื่อ นามสกุล	หน้าที่	ความรับผิดชอบ
๖	เลขานุการกรม	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ด้านการสื่อสารองค์กรและประชาสัมพันธ์ข่าวสาร

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

ลำดับ	ชื่อ นามสกุล / ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) E-mail : saraban@ncsa.or.th หมายเลขโทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘	สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	
๒	นายโกมล พรมเพ็ง ตำแหน่ง รองปลัดกระทรวงยุติธรรม หัวหน้ากลุ่มภารกิจด้านอำนวยความยุติธรรม สำนักงานปลัดกระทรวงยุติธรรม หมายเลขโทรศัพท์ : ๐ ๒๑๔๑ ๕๑๐๖	รองปลัดกระทรวงยุติธรรมที่กำกับดูแล	หน่วยงานกำกับดูแล
๓	นายไตรยฤทธิ์ เตมหิวงศ์ ตำแหน่ง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง สำนักงานปลัดกระทรวงยุติธรรม หมายเลขโทรศัพท์ : ๐ ๒๑๔๑ ๕๑๑๗	คณะอนุกรรมการด้านไซเบอร์ของกระทรวงยุติธรรม	หน่วยงานกำกับดูแล
๔	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ E-mail : thaicert@ncsa.or.th หมายเลขโทรศัพท์ : ๐ ๒๑๑๔ ๓๕๓๑	THAI-CERT	

๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

(๑) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๙.๒ รายงานสถานการณ์ต่อผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ

(๒) ผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ พิจารณาการดำเนินการและรายงานเหตุการณ์ต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ของกรมสอบสวนคดีพิเศษ โดยอาจพิจารณาร่วมกับทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘ และหน่วยงานภายในอื่น ๆ ที่เกี่ยวข้อง

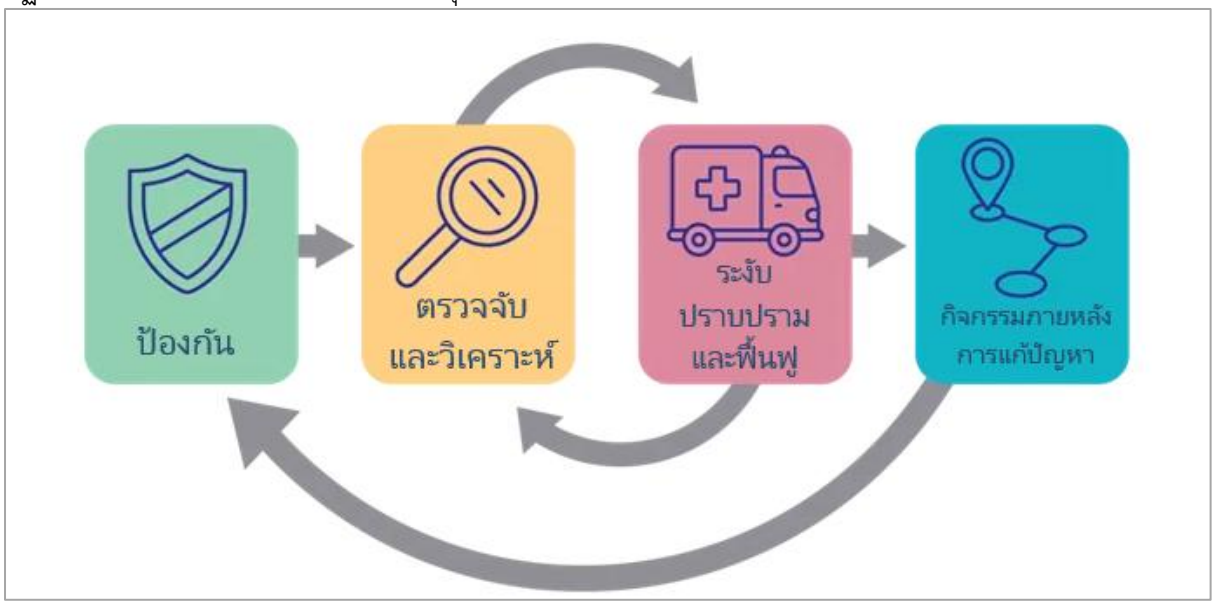
(๓) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) ของกรมสอบสวนคดีพิเศษ พิจารณาการดำเนินการและรายงานเหตุการณ์ต่ออธิบดีกรมสอบสวนคดีพิเศษ โดยอาจพิจารณาร่วมกับผู้อำนวยการกองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ และหน่วยงานภายในอื่น ๆ ที่เกี่ยวข้อง

(๔) อธิบดีกรมสอบสวนคดีพิเศษ พิจารณาการดำเนินการและรายงานเหตุการณ์ต่อปลัดกระทรวงยุติธรรม หรือหน่วยงานภายนอกอื่น ๆ ที่เกี่ยวข้อง

๑๐. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมกากำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ รวมถึงประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖

ในการนี้ การดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling) สามารถแบ่งขั้นตอนการดำเนการออกได้เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ โดยมีรายละเอียดดังนี้



ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling)

๑๐.๑ ขั้นตอนการเตรียมการ (preparation)

เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็นการตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๙.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่

ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายละเอียดตามข้อ ๙.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๓.๑) การจัดเตรียมข้อมูลและอุปกรณ์ให้พร้อม ต้องจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์

(๓.๒) การตั้งค่าระบบต่าง ๆ ให้ปลอดภัยเป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องเครื่องแม่ข่าย มีการปิดช่องโหว่และทำการแพตช์ระบบมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention เป็นต้น

(๔) จัดเตรียมข้อมูลและอุปกรณ์ในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ ได้แก่

- รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รายละเอียดตามข้อ ๙.๒
- ช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์แจ้งศูนย์สารสนเทศ กองเทคโนโลยีและศูนย์ข้อมูลการตรวจสอบ
- ช่องทางการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(๕) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ ได้แก่

- จัดเตรียมสถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูลและพยายวัตถุอื่น ๆ ที่สำคัญ โดยใช้ห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)
- การตั้งค่าระบบต่าง ๆ ให้ปลอดภัยเป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องเครื่องแม่ข่าย มีการปิดช่องโหว่และทำการแพตช์ระบบมีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention เป็นต้น

(๖) จัดทำแนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ชองกรมสอบสวนคดีพิเศษ

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของกรมสอบสวนคดีพิเศษ (รายละเอียดปรากฏตามภาคผนวก ๑)

นอกจากนี้ หน่วยงานต้องดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๒ <u>ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์</u>

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(๑) จัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้น หรืออาจเกิดขึ้นกับหน่วยงาน โดยรูปแบบการโจมตีที่ควรจัดเตรียมแนวทางรับมือไว้นั้น อาจพิจารณาได้จาก Attack Vector ที่หน่วยงานมี เช่น มีการอนุญาตให้ใช้งานอุปกรณ์แบบถอดได้ (External/Removable Media) ซึ่งมีความเสี่ยงต่อการเผยแพร่มัลแวร์ หรือมีการให้บริการเว็บไซต์ที่เสี่ยงต่อการโจมตีแบบ Cross-site scripting เป็นต้น

(๒) ดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(๓) ดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (Functional impact) ผลกระทบต่อข้อมูล (Information impact) และความสามารถในการกู้คืน (Recoverability effort) เป็นต้น

เกณฑ์การประเมินระดับของภัยคุกคาม

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
ต่ำ (Low)	ส่งผลกระทบต่อหน่วยงานในวงจำกัด เช่น เกิดการหยุดชะงักของการให้บริการเล็กน้อย หรือกระทบแค่หน่วยงานเดียว สามารถกู้คืนโดยใช้ทรัพยากรที่มีได้ ความเสียหายทางการเงินต่ำ ไม่ส่งผลกระทบต่อชื่อเสียงหรือความเชื่อมั่นของสาธารณะ หรือไม่เกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแล	แก้ไขภายใน ๗๒ ชั่วโมง
ปานกลาง (Medium)	ส่งผลกระทบต่อหน่วยงานในระดับปานกลาง เช่น เกิดการหยุดชะงักของการให้บริการที่ยาวนานขึ้น กระทบหลายหน่วยงาน สามารถกู้คืนได้แต่ต้องมีการจัดหาทรัพยากรเพิ่ม มีความเสียหายทางการเงินมากขึ้น เริ่มส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับไม่ร้ายแรง	แก้ไขภายใน ๔๘ ชั่วโมง
สูง (High)	ส่งผลกระทบอย่างมากต่อหน่วยงาน เช่น ระบบสารสนเทศบางส่วนถูกทำลาย การดำเนินงานหยุดชะงักอย่างมากในช่วงเวลาหนึ่ง เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก ข้อมูลสำคัญจำนวนมากสูญหาย ความเสียหายทางการเงินสูง ส่งผลกระทบอย่างมากต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงาน ด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับร้ายแรง	แก้ไขภายใน ๒๔ ชั่วโมง

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
สูงมาก (Extreme)	ส่งผลกระทบอย่างร้ายแรงต่อหน่วยงาน เช่น มีภัยคุกคามต่อชีวิต ระบบสารสนเทศหลักถูกทำลาย การดำเนินงานทั้งหมดหยุดชะงักจนต้องปิดการให้บริการ ไม่สามารถทำการกู้คืนได้ ข้อมูลสำคัญจำนวนมากสูญหายและถูกนำไปเผยแพร่ต่อสาธารณะ ความเสียหายทางการเงินสูงมาก ส่งผลกระทบอย่างรุนแรงต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับวิกฤติ	แก้ไขภายใน ๔ ชั่วโมง

(๔) จัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

(๕) จัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยมีการบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอน ตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุ ตลอดถึงระยะเวลาที่ใช้ระงับเหตุด้วย ทั้งนี้ การบันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ โดยระบุวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม รายละเอียดตามแบบฟอร์ม (รายละเอียดปรากฏตามภาคผนวก ๓)

(๖) กรณีหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ ดังนี้

(๖.๑) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการแจ้งตามกฎหมาย หรือนำส่งข้อมูลที่มีรายละเอียดเทียบเท่ากับแบบฟอร์ม ก๑ (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(๖.๒) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(๖.๓) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัย

ไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

นอกจากนี้ หน่วยงานต้องดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าว ควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

(๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

(๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

(๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๑.๑) ดำเนินการตามนโยบายการใช้งานระบบป้องกันการโจมตีทางไซเบอร์หรือมัลแวร์สำหรับเครื่องคอมพิวเตอร์อย่างเคร่งครัด

(๑.๒) ดำเนินการตามนโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล และนโยบายการใช้งานเครื่องคอมพิวเตอร์ แบบพกพาอย่างเคร่งครัด

(๑.๓) ดำเนินการจัดหาซอฟต์แวร์ป้องกันการโจมตีทางไซเบอร์แบบคอร์ปอเรต ให้เพียงพอต่อจำนวนบุคลากรของกรมสอบสวนคดีพิเศษ

(๑.๔) ดำเนินการสำรองข้อมูลของระบบสารสนเทศ เพื่อป้องกันเหตุฉุกเฉินอย่างสม่ำเสมอ

(๒) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

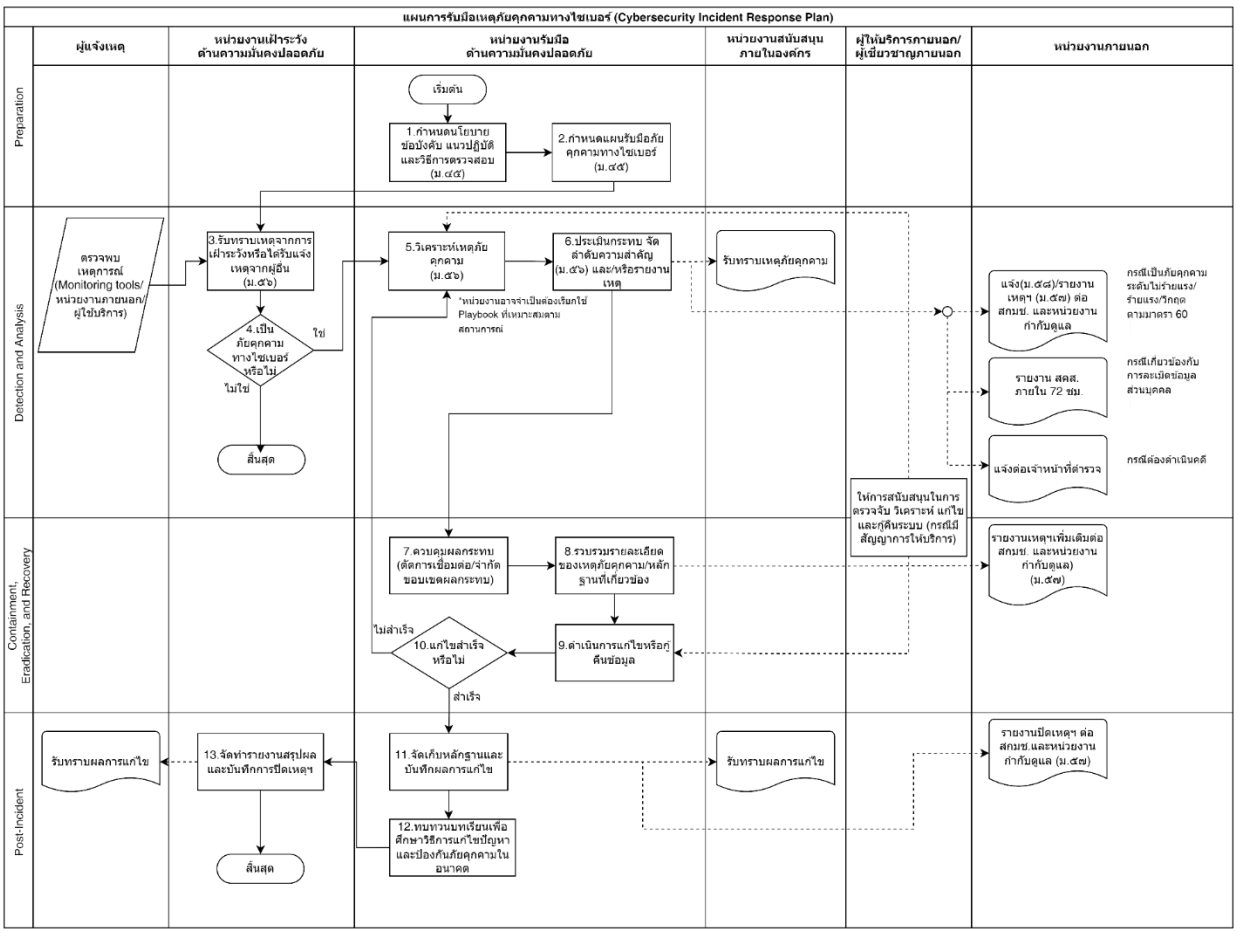
๑๐.๕ <u>การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident handling Checklist)</u>

จัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) เพื่อเป็นแนวทางและการตรวจทานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ (รายละเอียดปรากฏตามภาคผนวก ๕)

ภาคผนวก ๑ - ๕

ภาคผนวก ๑
แผนการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท

๑. แผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)



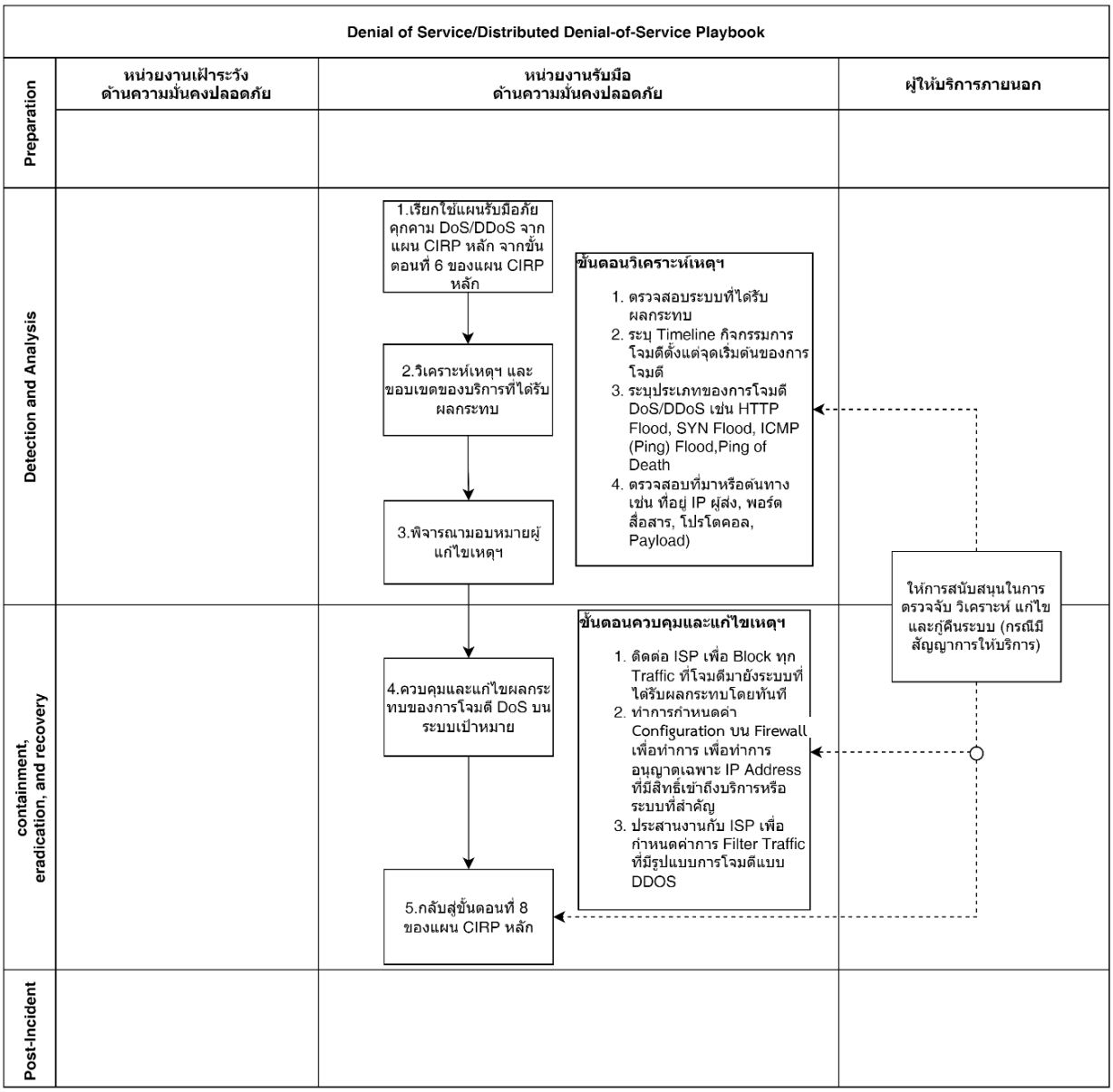
คำอธิบายแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการเตรียมการ (preparation)		
๑	กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหารของหน่วยงานกำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา ๑๓ วรรคหนึ่ง (๔))
๒	กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ โดยระบุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอนและวิธีการในการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ กำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มีการทดสอบแผนรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๓	รับทราบเหตุจากการเฝ้าระวังหรือได้รับแจ้งเหตุจากผู้อื่น (ม.๕๖)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ได้รับทราบเหตุจากการเฝ้าระวัง (Monitoring tools) หรือได้รับแจ้งเหตุจากผู้อื่นที่ตรวจพบเหตุการณ์ เช่น หน่วยงานภายนอกหรือผู้ใช้บริการ
๔	เป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาเหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
๕	วิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม ข้อมูล จำนวนระบบ บริการ หรือสินทรัพย์ที่ได้รับผลกระทบ
๖	ประเมินกระทบ และจัดลำดับความสำคัญ (ม.๕๖)	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการประเมินกระทบ และจัดลำดับความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคามทางไซเบอร์ **หมายเหตุ:** หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์ ๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานต่าง ๆ ■ กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤต ตามมาตรา ๖๐ หน่วยงานต้องแจ้งเหตุภัยคุกคาม (มาตรา ๕๘) (แบบฟอร์ม ก.๑ หรือมีข้อมูลเทียบเท่า) และ/หรือรายงานเหตุภัยคุกคาม (มาตรา ๕๗)

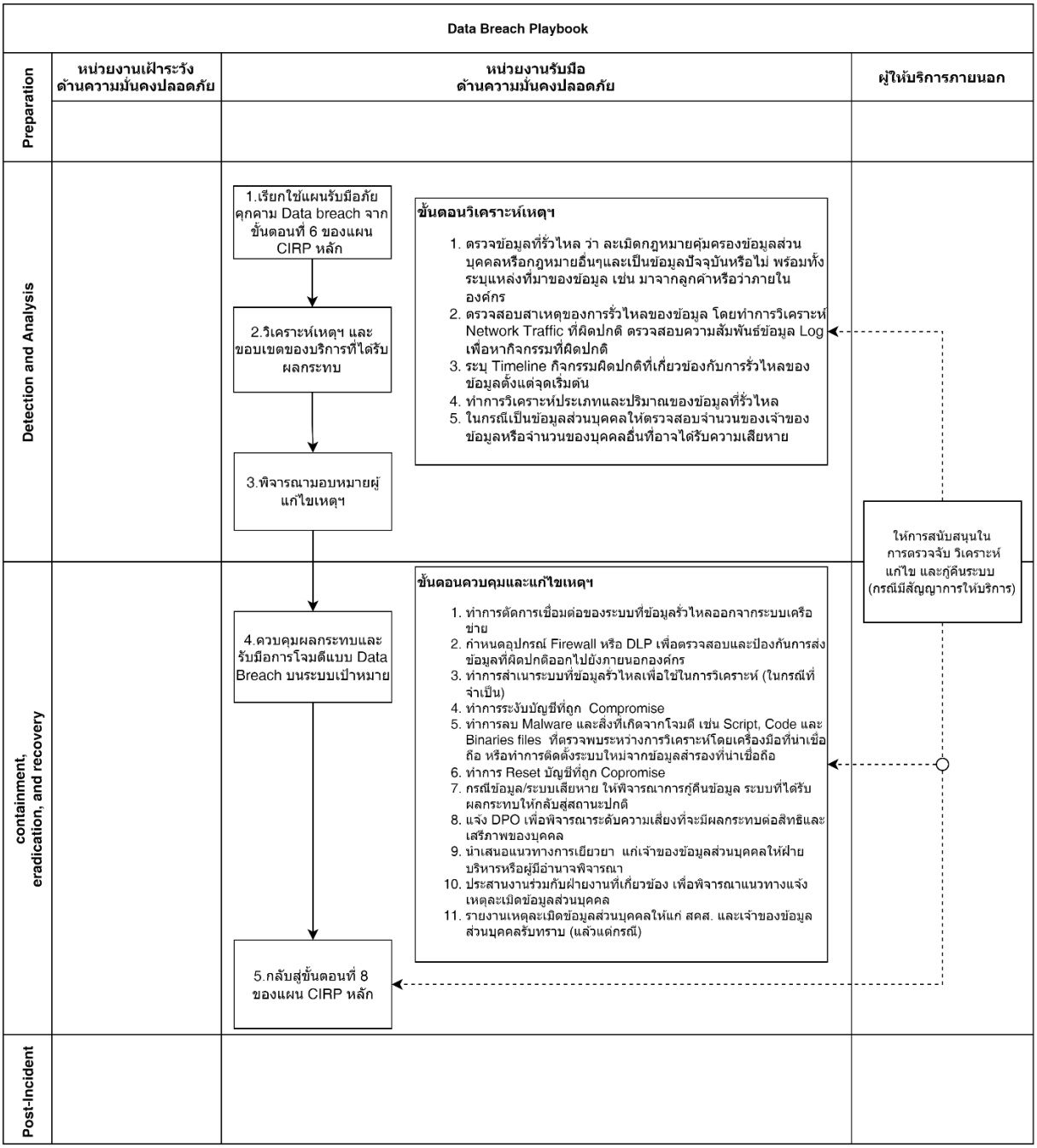
ลำดับ	หัวข้อ	คำอธิบาย
		(แบบฟอร์ม ก.๒) ต่อ สกมช. และหน่วยงานกำกับดูแล ■ กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. ■ กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้นเหตุนั้นเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้องแจ้งไปยังเจ้าหน้าที่ตำรวจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๗	ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำการกำจัดสาเหตุ (Eradicate the incident) กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ
๘	รวบรวมรายละเอียดของเหตุภัยคุกคาม/หลักฐานที่เกี่ยวข้อง	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึกเหตุการณ์ และดำเนินการจัดเก็บรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน ๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๙	ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
๑๐	แก้ไขสำเร็จหรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาว่าระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ ให้ดำเนินการต่อที่ขั้นตอนที่ ๑๑ หากยังไม่สามารถแก้ไขได้ ให้ดำเนินการขั้นตอนที่ ๕ ซ้ำเพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง

ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๑๑	จัดเก็บหลักฐานและบันทึกผลการแก้ไข	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ๒. บันทึกผลการแก้ไขเหตุภัยคุกคามและวิธีการแก้ไขเพื่อจัดเก็บเป็นบทเรียน ๓. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๑๒	ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไขปัญหา และป้องกันภัยคุกคามในอนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนดแนวทางในการป้องกันการเกิดเหตุซ้ำ หรือป้องกันภัยคุกคาม อื่น ๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
๑๓	จัดทำรายงานสรุปผลและบันทึกการปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงานสรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไขไปยังผู้เกี่ยวข้องให้รับทราบ

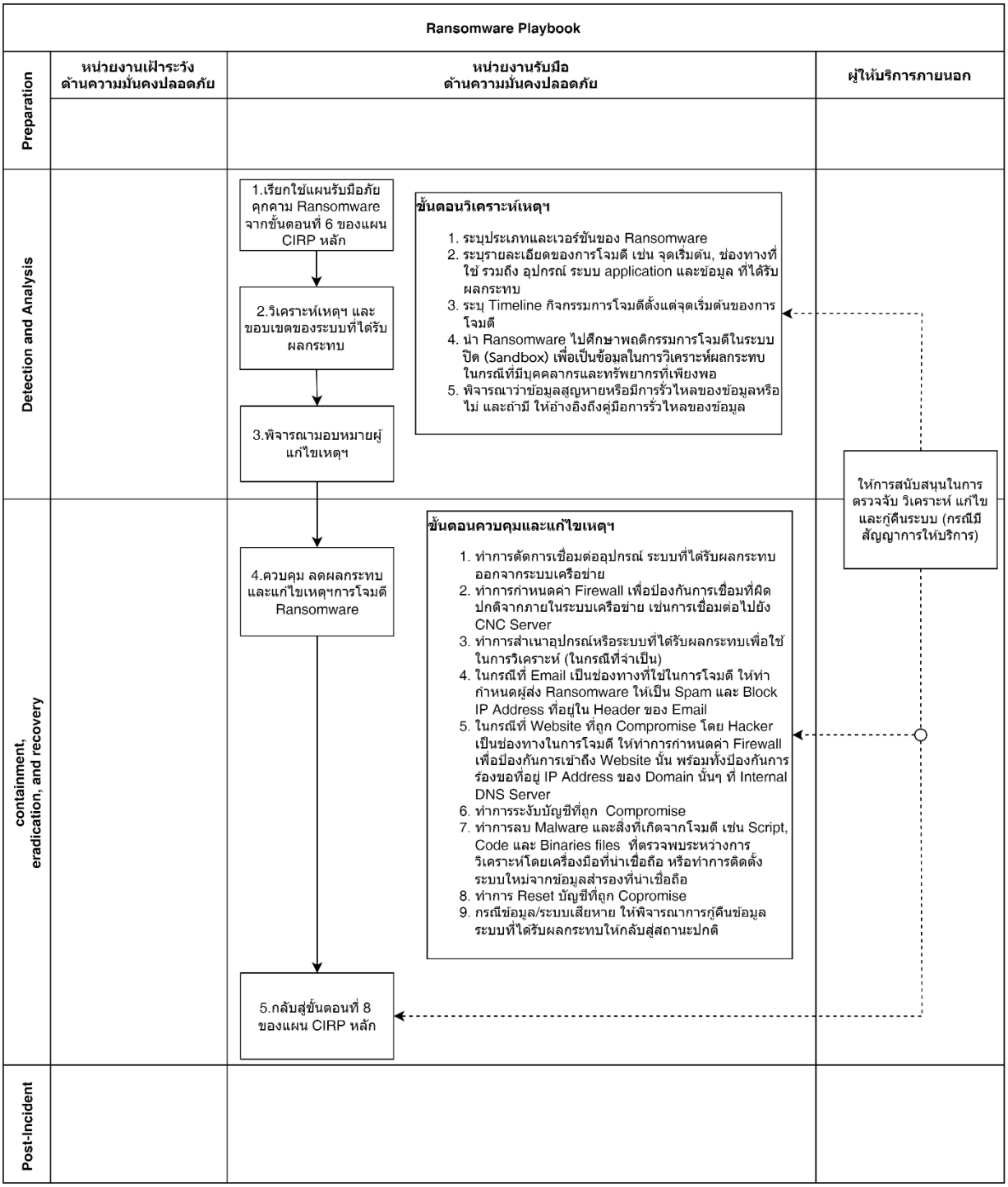
๒. ขั้นตอนการรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook)



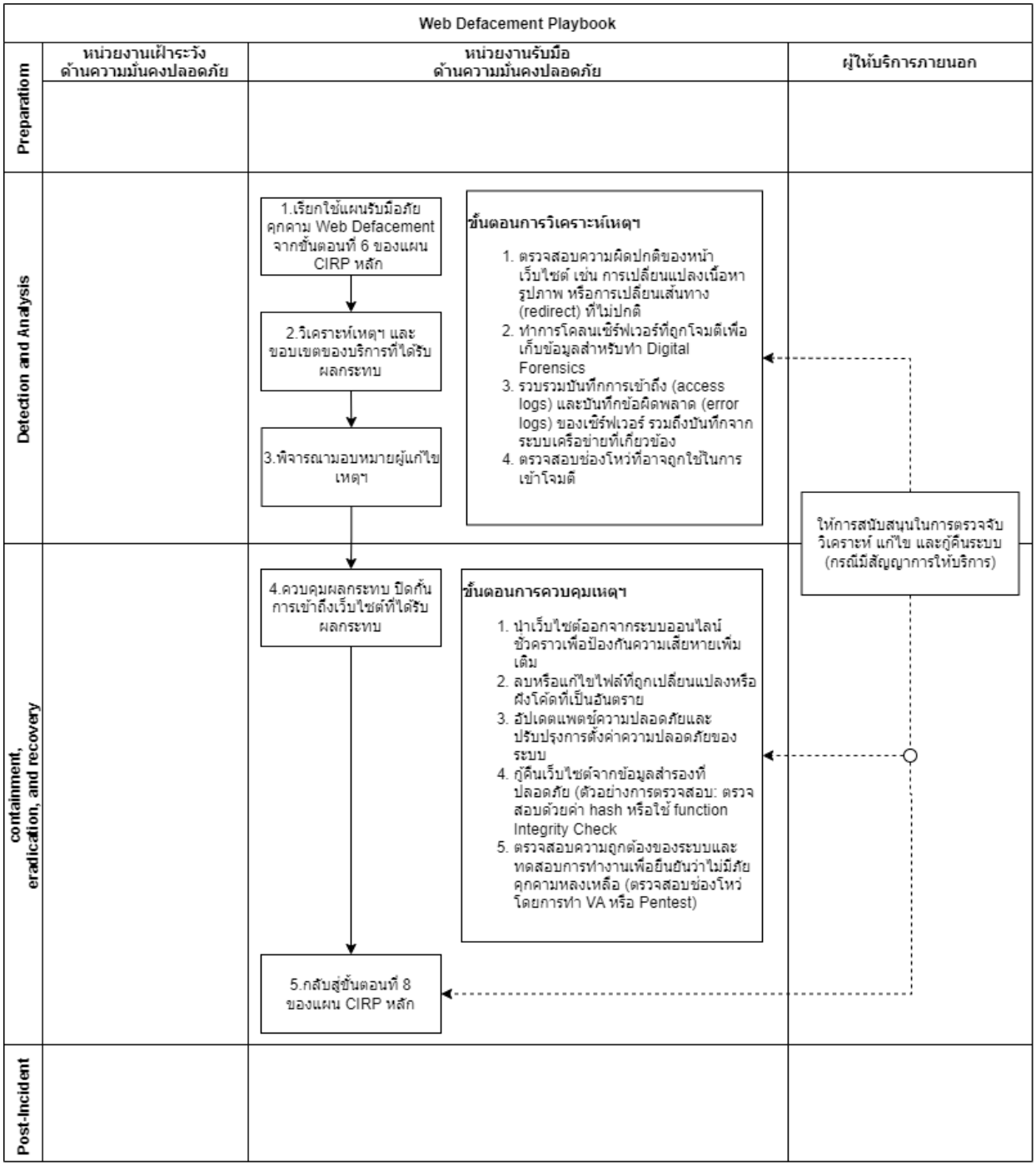
๓. ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)



๔. ขั้นตอนการรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook)



๕. ขั้นตอนการรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook)



ภาคผนวก ๒

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๓

ตัวอย่าง : บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง ๑๒/๑/๖๖ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก ๔

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

๑. ข้อมูลการประสานงาน

ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม

วันที่และเวลาที่แจ้ง

๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม

๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล ตำแหน่งงาน

ชื่อหน่วยงาน อีเมล

โทรศัพท์ (ที่ทำงาน / มือถือ)

๔. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

๕. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[1] ในระดับใด (มาตรา ๖๐)

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

☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

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

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

[1] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.) : โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี) :** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[๒] ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[2] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

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

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

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์):

โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

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

โปรดระบุ

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

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) : โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[๓]

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

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

ทรัพย์สินที่ได้รับผลกระทบ	จำนวน
เครื่องแม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตซ์ (Switch) /เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[๔]

ระดับภัยคุกคาม	จำนวน
ไม่ร้ายแรง	
ร้ายแรง	
วิกฤต (ก)	
วิกฤต (ข)	

[3] หมวดหมู่ตามข้อ 1 ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.2564

[4] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

ภาคผนวก ๕

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่น ๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

เอกสารอ้างอิง

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide
- ACSC Cyber Incident Response Plan Guidance
- ประกาศกระทรวงยุติธรรม เรื่อง มาตรฐานและแนวทางปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ของกระทรวงยุติธรรม พ.ศ. ๒๕๖๖
- ประกาศกรมสอบสวนคดีพิเศษ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมสอบสวนคดีพิเศษ พ.ศ. ๒๕๖๖

จัดทำโดย ศูนย์สารสนเทศ

กองเทคโนโลยีสารสนเทศและศูนย์ข้อมูลการตรวจสอบ

กรมสอบสวนคดีพิเศษ