ประกาศกรมส่งเสริมอุตสาหกรรม
เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
ของกรมส่งเสริมอุตสาหกรรม
พ.ศ. ๒๕๖๙

เพื่อให้การปฏิบัติงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรม เป็นไปอย่างมีประสิทธิภาพสอดคล้องกับมาตรฐานสากล อาศัยอำนาจมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเทคโนโลยีดิจิทัลของกรมส่งเสริมอุตสาหกรรมเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีดิจิทัลในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ กรมส่งเสริมอุตสาหกรรม จึงออกประกาศ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศกรมส่งเสริมอุตสาหกรรม เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรม”

ข้อ ๒ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรม เป็นไปตามเอกสารแนบท้ายประกาศ

ข้อ ๓ ให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนและปรับปรุงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้มีความทันสมัยเป็นปัจจุบัน และเป็นมาตรฐานที่ยอมรับ อย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๑๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นางสาวณัฏฐิญา เนตยสุภา)
อธิบดีกรมส่งเสริมอุตสาหกรรม

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
(Guideline and Cybersecurity Framework)
ของกรมส่งเสริมอุตสาหกรรม
ประจำปี พ.ศ. ๒๕๖๙

คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อันเป็นข้อกำหนดขั้นต่ำ ในการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญ หรือร้ายแรงต่อระบบสารสนเทศ เพื่อให้การรักษาความปลอดภัยไซเบอร์ปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ สอดคล้องกับมาตรฐานสากล

กรมส่งเสริมอุตสาหกรรม เป็นหน่วยงานที่มุ่งมั่นขับเคลื่อนด้วยข้อมูลและเทคโนโลยีดิจิทัล เพื่อพัฒนาอุตสาหกรรมและวิสาหกิจไทยให้เติบโตในเศรษฐกิจและสังคมโลกยุคใหม่อย่างมั่นคง และยกระดับการบริหารจัดการและการบริการสู่องค์กรดิจิทัล มีมาตรการรักษาความมั่นคงปลอดภัยในการเข้าใช้ข้อมูลและระบบงานดิจิทัล เพื่อให้การกำกับดูแลการบริหารงานด้านเทคโนโลยีดิจิทัลเป็นไปอย่างมีประสิทธิภาพ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมอุตสาหกรรม จึงได้จัดทำเอกสารฉบับนี้ เพื่อให้กรมส่งเสริมอุตสาหกรรม มีรูปแบบรวมถึงขั้นตอนปฏิบัติ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ทั้งนี้ เพื่อใช้เป็นแนวทางสำหรับผู้ใช้งานข้อมูล ระบบสารสนเทศ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของหน่วยงาน ตระหนักถึงความมั่นคงปลอดภัยไซเบอร์ ปฏิบัติตามมาตรการด้านการรักษาความมั่นคงปลอดภัยที่มีการกำหนดตามเอกสารฉบับนี้

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมส่งเสริมอุตสาหกรรม
เมษายน ๒๕๖๙

สารบัญ

สารบัญ (ต่อ)

ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Guideline and Cybersecurity Framework)

๑. บทนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้กำหนดให้มีการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อันเป็นข้อกำหนดขั้นต่ำในการดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รวมทั้งกำหนดมาตรการในการประเมินความเสี่ยง การตอบสนองและรับมือกับภัยคุกคามทางไซเบอร์ เมื่อมีภัยคุกคามทางไซเบอร์ หรือเหตุการณ์ที่ส่งผลกระทบหรืออาจก่อให้เกิดผลกระทบหรือความเสียหายอย่างมีนัยสำคัญหรืออย่างร้ายแรงต่อระบบสารสนเทศของกรมส่งเสริมอุตสาหกรรม

กรมส่งเสริมอุตสาหกรรม ในฐานะหน่วยงานของรัฐที่เป็นองค์กรพัฒนาอุตสาหกรรมและวิสาหกิจไทยให้เติบโตในเศรษฐกิจและสังคมโลกยุคใหม่อย่างมั่นคง จึงจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ถือปฏิบัติ โดยอ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ จากสำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรมปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล เพื่อสนับสนุนการดำเนินงานของสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

๒. วัตถุประสงค์

เพื่อกำหนดกรอบแนวคิดและวิธีปฏิบัติของระบบบริหารจัดการความมั่นคงปลอดภัยทางไซเบอร์และนำไปใช้ในการดำเนินงานและการจัดการระบบงานเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรม ให้มีประสิทธิภาพและเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล และเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๓. ขอบเขต

เอกสารนี้ครอบคลุมกรอบและวิธีปฏิบัติสำหรับงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สำหรับสารสนเทศที่สำคัญของกรมส่งเสริมอุตสาหกรรม

๔. คำนิยาม

๑. หน่วยงาน หรือ องค์กร	หมายถึง	กรมส่งเสริมอุตสาหกรรม หรือ กสอ.
๒. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)	หมายถึง	ผู้ที่อธิบดีกรมส่งเสริมอุตสาหกรรม มอบหมายให้รับผิดชอบสั่งการและกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมอุตสาหกรรม
๓. ผู้ให้บริการภายนอก	หมายถึง	บุคคลหรือนิติบุคคลผู้ให้บริการภายนอก ซึ่งเป็นผู้ให้บริการด้านเทคโนโลยีสารสนเทศ หรือเป็นผู้ที่มีการเชื่อมต่อกับระบบเทคโนโลยีสารสนเทศของ กสอ. หรือเป็นผู้ที่สามารถเข้าถึงข้อมูลสำคัญของ กสอ. หรือข้อมูลของผู้ใช้บริการที่ควบคุมดูแลโดย กสอ. ได้
๔. ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรม โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้ง คุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
๕. เหตุภัยคุกคามทางไซเบอร์ (Cyber incident)	หมายถึง	เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
๖. ไฟร์วอลล์ (Firewall)	หมายถึง	เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
๗. ผลกระทบ (Impact)	หมายถึง	ขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๘. ความน่าจะเป็น (Likelihood)	หมายถึง	ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่งๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับปัจจัยต่างๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ
๙. ช่องโหว่ (Vulnerability)	หมายถึง	ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต
๑๐. โปรแกรมประสงค์ร้าย (Malware)	หมายถึง	โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอนคอมพิวเตอร์ (Worm) หรือม้าโทรจัน (Trojan Horse) หรือฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

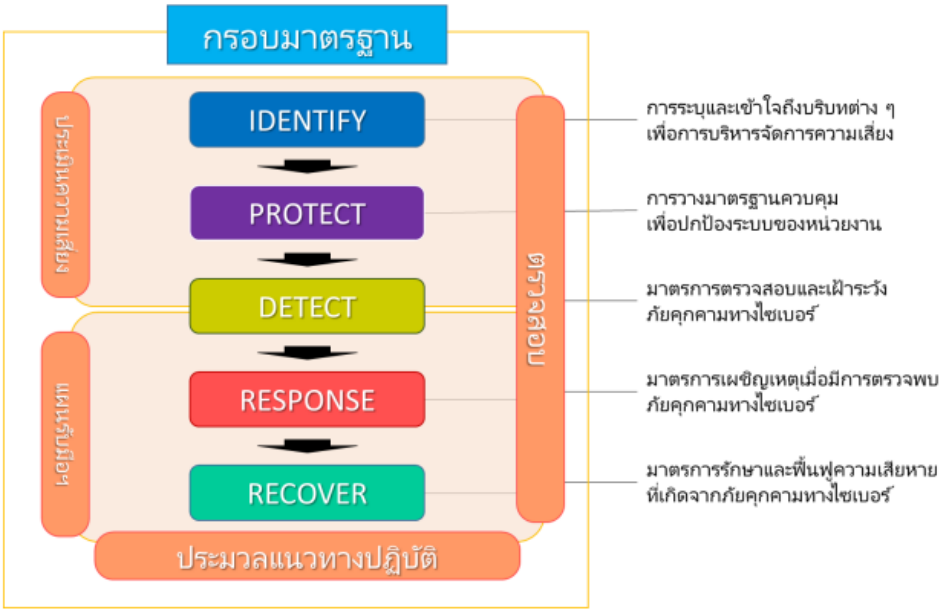
๕. การจัดทำประมวลแนวทางปฏิบัติ

การดำเนินการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ฉบับนี้ เป็นไปตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ โดยมีองค์ประกอบ ดังนี้

๑. แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. แผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

องค์ประกอบที่ ๑ แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางปฏิบัติ

๑.๑ การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยกรมส่งเสริมอุตสาหกรรม เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรม ซึ่งมีเกณฑ์การพิจารณา ดังนี้

๑. ไม่อยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน

๒. มีความสามารถทางเทคนิคที่จำเป็น เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ของกรมส่งเสริมอุตสาหกรรม

๑.๒ ความคาดหวังในการตรวจสอบ

กรมส่งเสริมอุตสาหกรรมได้ระบุความคาดหวังในการตรวจสอบไว้ ๗ ประการ ดังนี้

๑.๒.๑ หลักการตรวจสอบ

รูปที่ ๒ หลักการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

การตรวจสอบควรยึดหลักการต่อไปนี้

ก. ความถูกต้องครบถ้วน (Integrity)
- ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ
- ทำให้แน่ใจว่ามีความสามารถในขณะดำเนินการตรวจสอบ
- ดำเนินการตรวจสอบอย่างเป็นกลาง
- ทำให้แน่ใจว่ามีความยุติธรรมและเป็นกลางในการติดต่อทั้งหมด ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

ข. การนำเสนออย่างยุติธรรม (Fair Presentation): การรายงานตามความเป็นจริงและถูกต้อง
- ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง
- รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ
- ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจน และครบถ้วน

ค. การปฏิบัติอย่างมืออาชีพ (Due Professional Care): การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ
- ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ
- ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

ง. การรักษาความลับ (Confidentiality): ความมั่นคงปลอดภัยของข้อมูล

- ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ
- ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ
- จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

จ. ความเป็นอิสระ (Independence): พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรม ของข้อสรุปการตรวจสอบ

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

๑.๒.๒ วัตถุประสงค์ในการตรวจสอบ

๑) เพื่อตรวจสอบการปฏิบัติตามของหน่วยงาน กับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๒) เพื่อประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๑.๒.๓ ขอบเขตการตรวจสอบ

การตรวจสอบจะครอบคลุมตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

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

๑.๒.๔ แนวทางการตรวจสอบ

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

ก. การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

ข. ตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่กรมฯ เผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๑.๒.๕ ข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้

ก. ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

ข. เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงาน ซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

ค. เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำในการตรวจสอบปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม

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
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

๑.๒.๖ สรุปผลการตรวจสอบ

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

ก. ความเหมาะสมของความเห็นของหน่วยงานในการตอบสนองต่อผลการตรวจสอบ

ข. ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคง ปลอดภัยของหน่วยงาน

๑.๒.๗ รูปแบบรายงานการตรวจสอบ 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 ๑.๓ ของเอกสารนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๑.๔ ของเอกสารนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ: ก. มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ข. ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และวิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในส่วน ๑.๖ ของเอกสารนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในส่วน ๑.๗ ของเอกสารนี้

๑.๓ ขั้นตอนการปฏิบัติในการตรวจสอบ

๑. ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๒. ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

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

๓. ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๔. ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้นโดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

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

๕. ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๖. คณะทำงานรับทราบผลการตรวจสอบ

๗. ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษาความลับในการตรวจสอบ

๘. คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๙. คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๑๐. ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

องค์ประกอบที่ ๒ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางปฏิบัติ

เพื่อให้กรมส่งเสริมอุตสาหกรรมสามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง จึงได้กำหนดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง ประกอบด้วยรายละเอียด ดังต่อไปนี้

๒.๑ กำหนดบทบาทและความรับผิดชอบ

เพื่อให้ตระหนักถึงบทบาทและหน้าที่ของผู้มีส่วนเกี่ยวข้องในการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนถึงบทบาทหลักในการประเมินความเสี่ยง ได้แก่

๑. หัวหน้าหน่วยงาน (Head of Organization)

เจ้าหน้าที่ระดับสูงสุด (Highest-level Senior Official) ภายในองค์กรที่มีภาระหน้าที่และความรับผิดชอบโดยรวม (Responsibility and Accountability) ในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ขององค์กร และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

๒. เจ้าของกระบวนหลัก (Business Owner)

เจ้าหน้าที่ระดับสูงสุดของสำนักหรือเทียบเท่า (Business Unit) ที่รับผิดชอบในการตรวจสอบให้แน่ใจว่ากิจกรรมตามภารกิจหรือบริการบรรลุเป้าหมาย/เป้าประสงค์ของสำนัก หรือแบ่งปันข้อกังวลหรือข้อสังเกตเกี่ยวกับผลกระทบที่มีต่อการดำเนินงานตามเป้าหมายในกรณีที่ระบบมีการหยุดชะงัก

๓. ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งองค์กร ควรทำหน้าที่เป็นสะพานเชื่อมระหว่างหน้าที่ทางเทคนิคและเจ้าของกระบวนการหลักในระหว่างกระบวนการประเมินความเสี่ยง และจัดให้มีการกำกับดูแลกิจกรรมการประเมินความเสี่ยงเพื่อให้แน่ใจว่ามีการตัดสินใจตามความเสี่ยงที่สอดคล้องกัน

๔. ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน

บุคคลหรือกลุ่มงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชั่น เพื่อสนับสนุนการทำงานของระบบที่สนับสนุนกิจกรรมตามภารกิจหรือบริการ ควรรู้จักทรัพย์สินของระบบและการดำเนินงานด้านเทคนิคเป็นอย่างดี และสามารถให้คำแนะนำเกี่ยวกับผลกระทบทางเทคนิคสำหรับระบบที่ถูกบุกรุกได้

โดยกรมส่งเสริมอุตสาหกรรม ได้กำหนดบทบาทและหน้าที่ของผู้มีส่วนเกี่ยวข้องในการประเมินความเสี่ยง ตามตารางดังต่อไปนี้

ลำดับ	ตำแหน่ง	หน้าที่	ความรับผิดชอบ
๑	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)	หัวหน้าหน่วยงาน (Head of Organization)	มีภาระหน้าที่และความรับผิดชอบโดยรวม (Responsibility and Accountability) ในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ขององค์กร และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด
๒	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	เจ้าของกระบวนหลัก (Business Owner)	ตรวจสอบให้แน่ใจว่ากิจกรรมตามภารกิจหรือบริการบรรลุเป้าหมาย/เป้าประสงค์ของสำนักหรือแบ่งปันข้อกังวล หรือข้อสังเกตเกี่ยวกับผลกระทบที่มีต่อการดำเนินงานตามเป้าหมายในกรณีที่ระบบมีการหยุดชะงัก
๓	เจ้าหน้าที่กลุ่มแผนงานสารสนเทศและบริหารทั่วไป	ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)	บุคคลหรือกลุ่มภายในหน่วยงานที่รับผิดชอบแนวทางการบริหารความเสี่ยงทั่วทั้งองค์กร
๔	เจ้าหน้าที่กลุ่มระบบคอมพิวเตอร์และเครือข่าย และเจ้าหน้าที่กลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ	ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน	บุคคลหรือกลุ่มงานที่รับผิดชอบในการบำรุงรักษาและการดำเนินงานของโครงสร้างพื้นฐานทางเทคโนโลยี รวมถึงเครือข่ายและแอปพลิเคชั่น

๒.๒ ระบุทรัพย์สิน

เป็นสิ่งแรกที่ควรดำเนินการ โดยระบุและสร้างทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยงดังนี้

- ทรัพย์สินสำคัญ มีความสำคัญต่อการบรรลุวัตถุประสงค์ขององค์กรโดยรวมและมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์ เช่น ในระบบควบคุมแบบกระจายของโรงไฟฟ้า (Distributed Control System (DCS)) โปรแกรมควบคุมลอจิกแบบตั้งโปรแกรมได้ (Programmable Logic Controller (PLC)) ที่ควบคุมระบบไฟฟ้าจะได้รับการพิจารณาว่าเป็นทรัพย์สินสำคัญ เนื่องจากมีผลโดยตรงต่อการผลิตไฟฟ้า ซึ่งเป็นวัตถุประสงค์ทางธุรกิจโดยรวมของโรงไฟฟ้า ผู้โจมตีที่ต้องการขัดขวางการผลิตไฟฟ้า มีแนวโน้มที่จะโจมตีและควบคุมตรรกะภายใน PLC

- ทรัพย์สินที่เกี่ยวข้อง เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ เช่น ในสภาพแวดล้อม Windows ทั่วไป เซิร์ฟเวอร์ Active Directory (AD) ที่เก็บรักษาหรือตรวจสอบข้อมูลรับรองการเข้าสู่ระบบของผู้ใช้ไปยังเซิร์ฟเวอร์หลายเครื่องมักจะได้รับการพิจารณาว่าเป็นทรัพย์สินที่เกี่ยวข้อง เนื่องจากเป็นสะพานเชื่อมการโจมตีเปลี่ยนเข้าสู่เซิร์ฟเวอร์เหล่านี้

โดยกรมส่งเสริมอุตสาหกรรมได้กำหนดทรัพย์สินทะเบียนทรัพย์สินทางกายภาพและทางตรรกะทั้งหมดที่ประกอบกันเป็นระบบที่อยู่ภายในขอบเขตการประเมินความเสี่ยง ดังนี้

ลำดับ	กลุ่มทรัพย์สิน	ประเภททรัพย์สิน
๑	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	ทรัพย์สินที่เกี่ยวข้อง
๒	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	ทรัพย์สินที่เกี่ยวข้อง
๓	ข้อมูลบัญชีผู้ดูแลระบบ	ทรัพย์สินที่เกี่ยวข้อง
๔	Network Diagram	ทรัพย์สินที่เกี่ยวข้อง
๕	รายงานการบำรุงรักษา	ทรัพย์สินที่เกี่ยวข้อง
๖	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	ทรัพย์สินที่เกี่ยวข้อง
๗	พื้นที่ปฏิบัติงานของเจ้าหน้าที่	ทรัพย์สินที่เกี่ยวข้อง
๘	อุปกรณ์จอภาพและแป้นพิมพ์	ทรัพย์สินที่เกี่ยวข้อง
๙	อุปกรณ์ network	ทรัพย์สินสำคัญ
๑๐	เครื่องคอมพิวเตอร์แม่ข่าย	ทรัพย์สินสำคัญ
๑๑	อุปกรณ์จัดเก็บข้อมูล	ทรัพย์สินสำคัญ
๑๒	อุปกรณ์รักษาความปลอดภัยเครือข่าย	ทรัพย์สินสำคัญ
๑๓	อุปกรณ์สำรองไฟฟ้า	ทรัพย์สินสำคัญ
๑๔	ผู้ให้บริการภายนอก	ทรัพย์สินที่เกี่ยวข้อง
๑๕	ระบบปฏิบัติการ	ทรัพย์สินสำคัญ
๑๖	โปรแกรมสนับสนุน	ทรัพย์สินที่เกี่ยวข้อง

๒.๓ ระบุภัยคุกคาม และช่องโหว่

กรมส่งเสริมอุตสาหกรรม ได้กำหนดภัยคุกคาม และช่องโหว่ ที่อาจจะเกิดขึ้นกับระบบคอมพิวเตอร์และเครือข่าย ดังนี้

ลำดับ	ภัยคุกคาม	ช่องโหว่
๑	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง
๒	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูล ระบบมีช่องโหว่
๓	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล

ลำดับ	ภัยคุกคาม	ช่องโหว่
๔	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบุคคลเข้าถึงข้อมูล
๕	ผู้ไม่ได้รับอนุญาตเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการกำหนดสิทธิ และทบทวนสิทธิ
๖	ผู้ไม่ได้รับอนุญาตเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการตรวจสอบช่องโหว่ของระบบหรือระบบล้าสมัย
๗	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน
๘	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน
๙	ข้อมูลติดไวรัสหรือ Ransomware	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ
๑๐	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน
๑๑	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา
๑๒	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้
๑๓	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration
๑๔	เกิดโรคระบาด ไม่สามารถเข้าปฏิบัติงานได้	ขาดการป้องกันและควบคุมการแพร่ระบาดของโรค
๑๕	ระบบกระแสไฟฟ้าขัดข้อง	ภัยธรรมชาติ เช่น ฝนตก พายุหรือฟ้าผ่าทำให้อุปกรณ์ไฟฟ้าทำงานผิดพลาดหรือชำรุด
๑๖	ระบบกระแสไฟฟ้าขัดข้อง ไฟดับ	สัตว์ที่ขึ้นไปอยู่บนเสาไฟฟ้า หรือสายไฟฟ้าทำให้เกิดกระแสไฟฟ้าลัดวงจร
๑๗	ชุมนุมประท้วง ก่อจลาจล ปิดสถานที่	การบริหารงานหรือนโยบายของภาครัฐ
๑๘	ระบบขัดข้องเป็นเวลานาน	ขาดการเฝ้าระวัง แจ้งเตือน และตรวจสอบการทำงานของระบบ
๑๙	ระบบขัดข้องเป็นเวลานาน	ขาดการสำรองข้อมูล

๒.๔ กำหนดความเสี่ยง

การกำหนดคำนิยามทั่วไปของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ในแนวทางประกาศฉบับนี้ ความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ ๑. ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน และ ๒. ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

๒.๔.๑ กำหนดโอกาส (Determine Likelihood)

เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา เพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ซึ่งประเมินจากภัยคุกคาม และช่องโหว่ ซึ่งพิจารณาจากปัจจัยดังนี้

- ความสามารถในการค้นพบ (Discoverability) สามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่
- ความสามารถในการใช้ประโยชน์ (Exploitability) เป็นการใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี
- ความสามารถในการทำซ้ำ (Reproducibility) สามารถกสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ตัวอย่างตารางการประเมินเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำขั้นตอนต่อไปนี้

- ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (ระดับ ๑-๓)
- เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยงโดยระดับ ๓ คือ“มีแนวโน้มสูง”และ ๑ คือ “เป็นไปได้ยาก”

Likelihood Rating	ความสามารถในการค้นพบ (Discoverability)	ความสามารถในการใช้ประโยชน์ (Exploitability)	ความสามารถในการทำซ้ำ (Reproducibility)
High (๓)	**ช่องโหว่ของเป้าหมาย** - สามารถค้นพบได้โดยการค้นพบ/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) - สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	**การโจมตี** - สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย - สามาถทำได้ด้วยเครื่องมือที่หาได้ทั่วไปโดยไม่ต้องมีความรู้ด้านเทคนิค	**การโจมตี** - สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configurator) หรือเงื่อนไขของเหตุการณ์ (Event Condition) - สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	**ช่องโหว่ของเป้าหมาย** - สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรมและการสื่อสารของเป้าหมาย เช่น การฟิช	**การโจมตี** - สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย เช่น Admin/SYSTEM/Root	**การโจมตี** - สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง - สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย

Likelihood Rating	ความสามารถในการค้นพบ (Discoverability)	ความสามารถในการใช้ประโยชน์ (Exploitability)	ความสามารถในการทำซ้ำ (Reproducibility)
	(Fuzzing) กับแพคเกจเครือข่าย การดักเจ็บเครือข่าย (Network Sniffing) - สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายหรือส่วนเครือข่ายเดียวกัน	- สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	
Low (๑)	**ช่องโหว่ของเป้าหมาย** - สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย - สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	**การโจมตี** - สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) เช่น Admin/System/Root - สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคชั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	**การโจมตี** - สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง - สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

๒.๔.๒ กำหนดผลกระทบ (Determine Impact)

สถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้

- ระดับชาติ (National) ผลประทบอาจเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ
- หน่วยงาน (Organizational) ผลกระทบอาจเกิดการหยุดชะงักในการดำเนินงาน ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน
- บุคคล (Individual) ผลกระทบอาจเกิดการสูญเสียชีวิตและการบาดเจ็บ

ตัวอย่างตารางประเมินเพื่อพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” และ ๑ คือ “เล็กน้อย”) คำอธิบายที่ระบุในตารางตัวอย่างด้านล่าง เป็นข้อมูลทั่วไป หน่วยงานควรตรวจสอบและปรับแต่งคำอธิบายสำหรับการจัดอันดับผลกระทบแต่ละรายการ

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)		
	ต่ำ	กลาง	สูง
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาความถูกต้อง ครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบน้อยหรืออย่างจำกัด(Limited) และเกิดผลประโยชน์แห่งชาติ สำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาต อาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิด ผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อย หรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางตัวอย่างเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินสิบล้านบาท	เกินกว่าสิบล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่มีผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบ ต่อชีวิตร่างกายหรืออนามัย	ผู้ใช้บริการ หรือผู้มีส่วนได้เสีย ได้รับผลกระทบต่อร่างกายหรืออนามัยไม่เกินหนึ่งพันคน	ผู้ใช้บริการ หรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคน หรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคน แต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบ หรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
			เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

๒.๔.๓ กำหนดความเสี่ยงที่ยอมรับได้ หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ของหน่วยงานที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้สามารถระบุได้ว่าสามารถยอมรับความเสี่ยงได้มากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตัวอย่างตารางการยอมรับความเสี่ยงและการปรับแต่งตามแต่ละรายการเพื่อให้เหมาะสมกับบริบทขององค์กร

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
Low	ไม่จำเป็นต้องมีมาตรการควบคุมจัดการความเสี่ยงเพิ่มเติมหรืออาจมีได้หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว
Medium	ไม่จำเป็นต้องมีมาตรการควบคุมจัดการความเสี่ยงเพิ่มเติมหรืออาจมีได้หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว
High	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันทีต้องมีมาตรการในการจัดการความเสี่ยง

โดยกรมส่งเสริมอุตสาหกรรมได้กำหนดเกณฑ์ระดับค่าความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ดังนี้

	โอกาสที่จะเกิดขึ้น (Likelihood)			
ผลกระทบ (Impact)	ระดับความเสี่ยง	๑	๒	๓
	๓	M๓๑	H๓๒	H๓๓
	๒	L๒๑	M๒๒	H๒๓
	๑	L๑๑	L๑๒	L๑๓

ระดับความเสี่ยง	เขตสี	สัญลักษณ์ระดับความเสี่ยง	ความหมาย
ระดับความเสี่ยงต่ำ (Low: L)	เขียว	L	ไม่จำเป็นต้องมีมาตรการควบคุมจัดการความเสี่ยงเพิ่มเติมหรืออาจมีได้ หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว
ระดับความเสี่ยงปานกลาง (Medium: M)	เหลือง	M	ไม่จำเป็นต้องมีมาตรการควบคุมจัดการความเสี่ยงเพิ่มเติมหรืออาจมีได้ หากไม่ใช้ทรัพยากรเพิ่มเติมหรือมีแผนงานอื่นรองรับอยู่แล้ว

ระดับความเสี่ยง	เขตสี	สัญลักษณ์ระดับความเสี่ยง	ความหมาย
ระดับความเสี่ยงสูงมาก (High: H)	แดง	H	ความเสี่ยงระดับนี้ไม่สามารถยอมรับได้และจะสร้างผลกระทบรุนแรงจนกิจกรรมที่เกี่ยวข้องจำเป็นต้องยุติลงทันทีต้องมีมาตรการในการจัดการความเสี่ยง

๒.๕ การประเมินความเสี่ยง

การประเมินความเสี่ยงต้องประเมินโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยจะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินงานของกรมส่งเสริมอุตสาหกรรม รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

ดังนั้น กรมส่งเสริมอุตสาหกรรม จึงได้กำหนดสถานการณ์ความเสี่ยง (Construct Risk Scenarios) รายละเอียดตามตารางใน**ภาคผนวก ก แบบประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ**

๒.๖ การจัดการความเสี่ยง

การจัดการความเสี่ยง ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ

นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงานเพื่อใช้ติดตามและทบทวนความเสี่ยง

๒.๗ การติดตามและทบทวนความเสี่ยง

กรมส่งเสริมอุตสาหกรรมได้กำหนดกระบวนการในการติดตามและทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง

๒.๘ การรายงานความเสี่ยง

กรมส่งเสริมอุตสาหกรรมจะรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรม ตามรอบการประชุมของคณะกรรมการฯ

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

องค์ประกอบที่ ๓ แผนการรับมือภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมส่งเสริมอุตสาหกรรมนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแผนการรับมือภัยคุกคามทางไซเบอร์ในประกาศฉบับนี้ ประกอบด้วย

๓.๑ วัตถุประสงค์

๑. เพื่อกำหนดมาตรการ นโยบาย และขั้นตอนในการปฏิบัติตรวจสอบ ควบคุม ป้องกัน ลดความเสียหายและแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์

๒. เพื่อสร้างความเชื่อมั่นให้กับบุคลากรของกรมส่งเสริมอุตสาหกรรมและผู้ประกอบการ ในการได้รับการป้องกันจากภัยคุกคามทางไซเบอร์ทุกรูปแบบ

๓. เพื่อเตรียมความพร้อมด้านบุคลากรของกรมส่งเสริมอุตสาหกรรม ในการป้องกันภัยคุกคามทางไซเบอร์และปฏิบัติตามภารกิจได้อย่างต่อเนื่องมีประสิทธิภาพ

๔. เพื่อเป็นแนวทางการดำเนินงาน ในการพัฒนา เผยแพร่ความรู้ กำกับดูแล ความเข้าใจเกี่ยวกับการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์

๓.๒ ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมส่งเสริมอุตสาหกรรม รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๓.๓ หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมอุตสาหกรรม มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ที่สำคัญ

๓.๔ หน้าที่ในการดำเนินการตามแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมส่งเสริมอุตสาหกรรม มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามขั้นตอนปฏิบัติของแผนรับมือฯ ฉบับนี้ โดยให้ทุกหน่วยงานภายในกรมส่งเสริมอุตสาหกรรม เป็นหน่วยงานสนับสนุนในการดำเนินการตามแผนรับมือฯ

๓.๕ รายละเอียดการบังคับใช้เอกสาร

๑. รายละเอียดเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	กลุ่มระบบคอมพิวเตอร์และเครือข่าย
ผู้ดำเนินการตามเอกสาร (Owner)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
วันที่จัดทำเอกสาร (Date created)	วัน/เดือน/ปี
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	คณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของกรมส่งเสริมอุตสาหกรรม
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) วัน/เดือน/ปี
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	วัน/เดือน/ปี

๒. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	**วันที่อนุมัติ (Date of Approval)**	**ผู้อนุมัติ (Approved by)**	**สถานะ (Description of change)**
๑.๑	วัน/เดือน/ปี	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)	อนุมัติในหลักการ

๓.๖ เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๑. ประกาศกรมส่งเสริมอุตสาหกรรม เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม ประจำปี พ.ศ. ๒๕๖๙

๒. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

๓. ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๓.๗ บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

๓.๗.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย

ลำดับ	ชื่อ นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	๘ ชั่วโมง/ ๕ วัน	๐๒ ๔๓๐ ๖๘๗๙ ต่อ ๑๗๐๐	หัวหน้าทีมฯ (Team manager)	รับแจ้งเหตุการณ์กำกับดูแลและรายงานเหตุการณ์ภัยคุกคามต่อผู้บริหารของหน่วยงาน
๒	ผู้อำนวยการกลุ่มระบบคอมพิวเตอร์และเครือข่าย และผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ	๘ ชั่วโมง/ ๕ วัน	๐๒ ๔๓๐ ๖๘๗๙ ต่อ ๑๗๓๐	รองหัวหน้าทีม (Deputy team manager)	รับแจ้งเหตุการณ์
๓	เจ้าหน้าที่กลุ่มระบบคอมพิวเตอร์และเครือข่าย และเจ้าหน้าที่กลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ	๘ ชั่วโมง/ ๕ วัน	๐๒ ๔๓๐ ๖๘๗๙ ต่อ ๑๗๓๙	ทีมรับแจ้งเหตุฯ	รับแจ้งเหตุการณ์
๔	ผู้รับจ้างพัฒนาและดูแลระบบ	๒๔ ชั่วโมง/ ๗ วัน	๐๒ ๔๓๐ ๖๘๗๙ ต่อ ๑๗๔๐	ทีมรับแจ้งเหตุฯ	รับแจ้งเหตุการณ์

๓.๗.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Repones Team : CIRT) ประกอบด้วย

ลำดับ	ชื่อ-นามสกุล	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	ผู้อำนวยการกลุ่มระบบคอมพิวเตอร์และเครือข่ายและผู้อำนวยการกลุ่ม	รองหัวหน้าทีมรับมือฯ (Deputy team	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้

ลำดับ	ชื่อ-นามสกุล	หน้าที่	ความรับผิดชอบ
	พัฒนาระบบเทคโนโลยีสารสนเทศ		
๓	เจ้าหน้าที่กลุ่มระบบคอมพิวเตอร์และเครือข่าย และเจ้าหน้าที่กลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ หน่วยงานภายใต้กรมส่งเสริมอุตสาหกรรม ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
๔	ผู้รับจ้างพัฒนาและดูแลระบบ	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ประกอบด้วย

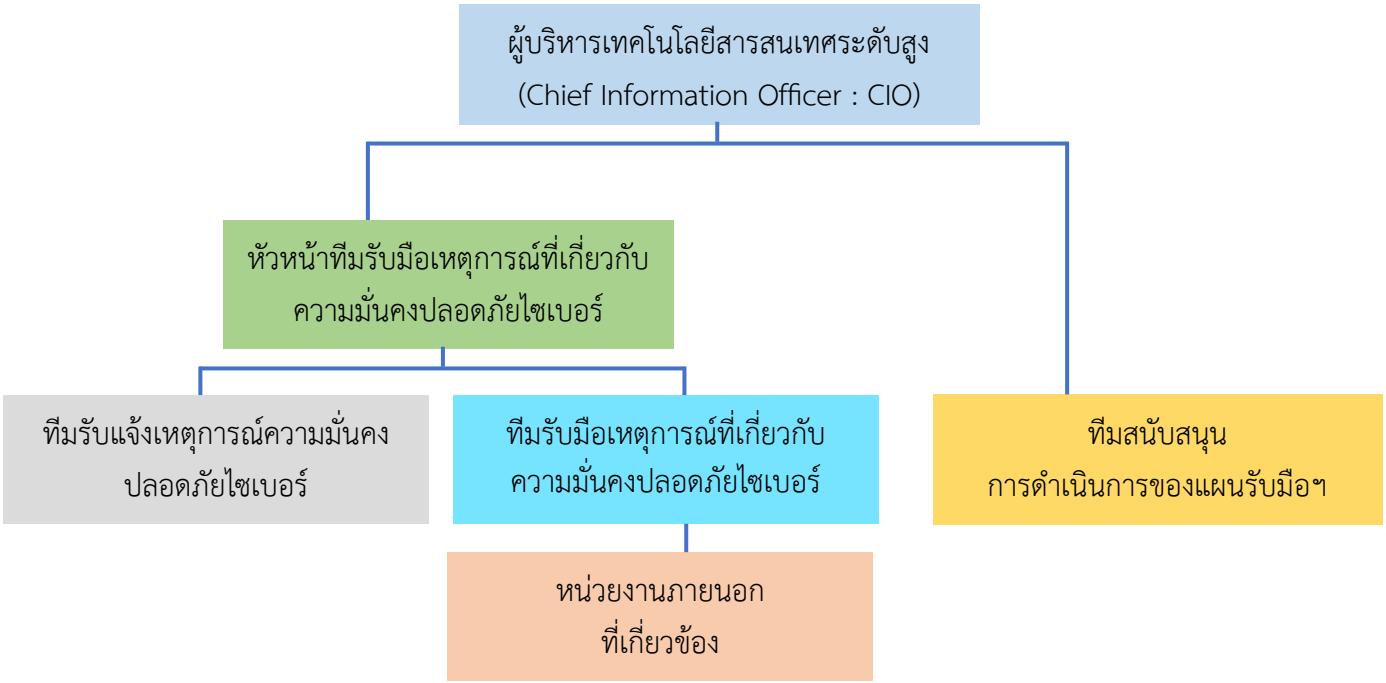
ลำดับ	ตำแหน่ง	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)	๐๒ ๔๓๐ ๖๘๖๓ ต่อ ๑๐๙๒	รับผิดชอบสั่งการและกำกับดูแล ติดตามการดำเนินงานด้านเทคโนโลยีสารสนเทศของกรมส่งเสริมอุตสาหกรรม	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๒	กลุ่มนิติการ	๐๒ ๔๓๐ ๖๘๖๕ ต่อ ๑๐๖๓	ผู้เชี่ยวชาญด้านกฎหมายและเจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย	ที่ปรึกษาด้านกฎหมาย
๓	ผู้ตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์		ตรวจสอบความปลอดภัยของระบบ IT โดยใช้วิธีการประเมินช่องโหว่	ทดสอบความมั่นคงปลอดภัยของระบบเครือข่าย

๓.๗.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

ลำดับ	หน่วยงาน	ช่องทางการติดต่อสื่อสาร	ความเกี่ยวข้อง
๑.	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ โทรศัพท์ : ๐๒ ๑๔๒ ๖๘๘๘ โทรสาร : ๐๒ ๑๔๓ ๗๕๙๓ Email: thaicert@ncsa.or.th	รับผิดชอบงานตามพระราชบัญญัติและประสานการปฏิบัติงานร่วมกันทั้งภาครัฐและเอกชน ไม่ว่าในสถานการณ์ทั่วไปหรือสถานการณ์ที่เป็นภัยต่อความมั่นคงอย่างร้ายแรง อันจะทำให้การป้องกันและการรับมือกับภัยคุกคามทางไซเบอร์เป็นไปอย่างมีประสิทธิภาพ

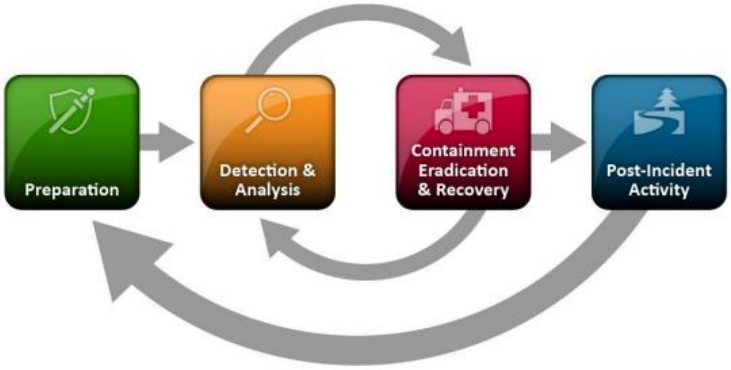
ลำดับ	หน่วยงาน	ช่องทางการติดต่อสื่อสาร	ความเกี่ยวข้อง
๒.	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	๑๒๐ หมู่ ๓ ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐ โทร. ๐๒ ๑๔๒ ๑๐๓๓, ๐๒ ๑๔๑ ๖๙๙๓ Email: saraban@pdpc.or.th	วิเคราะห์และรับรองความสอดคล้องและความถูกต้องตามมาตรฐาน หรือตามมาตรการหรือกลไกการกำกับดูแลที่เกี่ยวข้องกับการคุ้มครองข้อมูลส่วนบุคคล รวมทั้งตรวจสอบและรับรองนโยบายในการคุ้มครองข้อมูลส่วนบุคคล ตามมาตรา ๒๙ แห่งพระราชบัญญัติฯ
๓.	บริษัท โทรคมนาคมแห่งชาติ จำกัด (มหาชน) หรือ NT	Contact Center: ๑๘๘๘	ผู้ให้บริการเครือข่าย

๓.๗.๔ โครงสร้างรายงานเหตุการณ์ (Incident Reporting Structure)



๓.๘ ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ สามารถแบ่งขั้นตอนการดำเนินการออกได้เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติสากลที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ (NIST.SP.๘๐๐-๖๑r๒) โดยมีขั้นตอน ดังนี้



รูปที่ ๓ ขั้นตอนการดำเนินการเพื่อจัดการภัยคุกคามทางไซเบอร์ (NIST Cybersecurity Framework)

๓.๘.๑ ขั้นการเตรียมการ (Preparation)

การดำเนินการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ เพื่อให้กรมส่งเสริมอุตสาหกรรม มีขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้นสำหรับการรับมือกับเหตุการณ์ โดยจะต้องพิจารณาทั้งในด้านบุคลากร ด้านกระบวนการและด้านเทคโนโลยี และเตรียมความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์อย่างทันเหตุการณ์ โดยดำเนินการดังต่อไปนี้

๓.๘.๑.๑ การเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนสำหรับการรับมือภัยคุกคามทางไซเบอร์และการวิเคราะห์ภัยคุกคามทางไซเบอร์ เช่น Firewall ระบบป้องกันการบุกรุก เป็นต้น โดยใช้ระบบจัดเก็บและวิเคราะห์ข้อมูลเครือข่ายทางคอมพิวเตอร์และการรวบรวมข่าวเกี่ยวกับภัยคุกคามทางไซเบอร์

๓.๘.๑.๒ การจัดตั้งบุคลากรหรือทีมงาน เพื่อเตรียมพร้อมรับมือกับเหตุการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

(๑) ทีมผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ข้อ ๓.๗.๑

(๒) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ข้อ ๓.๗.๒

(๓) โครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์ ข้อ ๓.๗.๔

(๔) ช่องทางการรายงานเหตุการณ์และติดตามข้อมูลสถานการณ์

๓.๘.๑.๓ การสร้างความความรู้ ความเข้าใจด้านการรักษาความมั่นคงปลอดภัยให้กับบุคลากร (Security Awareness) เพื่อให้บุคลากรสามารถดูแลรักษาใช้งานทรัพยากรและระบบสารสนเทศได้อย่างปลอดภัย รวมถึงวิธีการตอบสนองภัยคุกคามทางไซเบอร์ในเบื้องต้นและดำเนินการแจ้งให้ทีมที่ทำหน้าที่รับมือภัยคุกคามทางไซเบอร์รับทราบเมื่อมีเหตุการณ์ผิดปกติ

๓.๘.๑.๔ กำหนดให้มีการปิดช่องโหว่ของระบบปฏิบัติการและระบบอื่น ๆ เป็นประจำ

๓.๘.๑.๕ มีการกำหนดสิทธิของผู้ใช้งาน โดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น

๓.๘.๑.๖ การจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของกรมส่งเสริมอุตสาหกรรม

๓.๘.๑.๗. กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์

ระดับความรุนแรง (Severity Level)	คำอธิบาย (Description)	เวลาในการตอบสนอง (Threat Response SLA)
ต่ำ	เหตุการณ์ที่มีผลกระทบน้อยที่สุด โดยไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ เช่น การรับส่งอีเมลที่เกิด SPAM และมีการแทรกแซงเว็บการพนัน หรือไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยที่ไม่ได้รับอนุญาต	ภายใน ๔ ชั่วโมง
ปานกลาง	เหตุการณ์ที่มีผลกระทบปานกลาง โดยมีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์ หรือข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต	ภายใน ๔ ชั่วโมง
สูง	เหตุการณ์ที่เกิดผลกระทบสูง เช่น ระบบของกรมส่งเสริมอุตสาหกรรมบางระบบไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่มทั้งภายในและภายนอกได้ หรือข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้ รับอนุญาต	ภายใน ๑-๒ ชั่วโมง
รุนแรง	เหตุการณ์ที่เกิดผลกระทบรุนแรง เช่น ระบบของกรมส่งเสริมอุตสาหกรรม ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์ หรือข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลายโดยไม่ได้รับอนุญาต	ภายใน ๑ ชั่วโมง

๓.๘.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

กรมส่งเสริมอุตสาหกรรมได้ดำเนินการการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ตามขั้นตอนดังนี้

ระดับ	แนวปฏิบัติพื้นฐาน
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ ในระดับไม่ร้ายแรง	๑. ตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคาม ทางไซเบอร์ โดยอาศัยข้อมูลจากอุปกรณ์ตรวจจับดังต่อไปนี้ ๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท DDos BOTNET Phishing Sniffing Hacker และระบบตรวจสอบและโต้ตอบการบุกรุก (IPS)

ระดับ	แนวปฏิบัติพื้นฐาน
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ในระดับร้ายแรง	๑.๒ IPS ทำหน้าที่ตรวจจับวิเคราะห์ Log file ป้องกันและประเมินความเสี่ยงเหตุการณ์ในระบบเครือข่าย ๑.๓ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว และรักษาความปลอดภัยการปกป้องอุปกรณ์ จากมัลแวร์ต่าง ๆ มีการป้องกันอย่างครอบคลุม ตั้งแต่ภัยคุกคามแบบเก่าไปจนถึงภัยคุกคามแบบใหม่ ๆ ๑.๔ ซอฟต์แวร์ตรวจสอบประสิทธิภาพเครือข่าย (Network Monitoring Software) ตรวจสอบความผิดปกติที่เกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์ส่วนกลางและส่วนภูมิภาค ๑.๕ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) ๒. จัดให้มีทีมงานที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ ๓. จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัย ด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น ๔. วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรม การใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหา ความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) ๕. ทันทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลา ประทับข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ ๖. ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้นและติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่า

ระดับ	แนวปฏิบัติพื้นฐาน
	สถานการณ์ดังกล่าว จะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ๗. จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น ๘. ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี ๙. ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคล ดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	๑. จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น ๒. จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและวิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ ๓. จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้ หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือ เมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น ๔. วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

โดยกรมส่งเสริมอุตสาหกรรมจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องหลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.๒๕๖๖ ดังนี้

๑. การรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบ ภายในระยะเวลาที่หน่วยงาน ควบคุมหรือกำกับดูแลกำหนด อ้างอิงตาม **ภาคผนวก ข บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์**

๒. การบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ด้วย อ้างอิงตาม **ภาคผนวก ค บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)**

๓. กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๔ แห่งประกาศฯ ฉบับดังกล่าวใช้แบบฟอร์มการรายงานตามกฎหมาย อ้างอิงตาม **ภาคผนวก ง ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น**

๔. กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตาม ข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์มแบบรายงานภัยคุกคามทางไซเบอร์ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง อ้างอิงตาม **ภาคผนวก จ แบบฟอร์มแบบรายงานภัยคุกคามทางไซเบอร์**

๕. หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสารแบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี โดยใช้แบบฟอร์มการรายงานตามกฎหมาย อ้างอิงตาม **ภาคผนวก ฉ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี**

๓.๘.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment Eradication & Recovery)

เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์หรือเมื่อกรมส่งเสริมอุตสาหกรรมได้รับแจ้งเตือน จะดำเนินการวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของเหตุการณ์และลดผลกระทบต่อการดำเนินงานให้น้อยที่สุด ซึ่งจะครอบคลุมในด้านการให้บริการ ด้านข้อมูล และความสามารถในการฟื้นฟู

ระดับ	แนวปฏิบัติพื้นฐาน
กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ในระดับไม่ร้ายแรง	๑. ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้แนวทางดังกล่าวรวมถึง ๑.๑ การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น

ระดับ	แนวปฏิบัติพื้นฐาน
	๑.๒ การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของ ฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น ๑.๓ การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด ๒. ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้ เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิคและเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี ๓. ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น ๔. ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจน ผู้ที่อาจได้รับผลกระทบอย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือ หน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ทั้งนี้ ในการแจ้งหรือ รายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับ ดูแล กำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่องลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ระดับ	แนวปฏิบัติพื้นฐาน
	๕. ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น ๖. ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติ ภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบ ให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น ๗. สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคาม ทางไซเบอร์ในระดับร้ายแรง	๑. หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) ๒. ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ ๓. ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับและเนื้อหาที่ต้องรายงาน ลำดับชั้น การรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือ ที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ ๔. ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ ตามกฎหมาย

ระดับ	แนวปฏิบัติพื้นฐาน
	๕. พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุน การรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes)
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็น ภัยคุกคามทาง ไซเบอร์ในระดับวิกฤติ	ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของ หน่วยงานทำได้อย่างรวดเร็ว

๓.๘.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

การดำเนินงานภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ จำเป็นต้องจัดให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูลเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา หาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ในอนาคต นอกจากนี้ต้องมีการเก็บรักษาข้อมูลและพยานหลักฐาน เช่น ไฟล์ที่อยู่ในคอมพิวเตอร์ อุปกรณ์อิเล็กทรอนิกส์ รวมถึงหลักฐานดิจิทัลที่ถูกสร้างจากระบบคอมพิวเตอร์ เพื่อใช้ในกระบวนการทาง Digital Forensics เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่นๆที่เกี่ยวข้อง

ระดับ	แนวปฏิบัติพื้นฐาน
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทาง ไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ ๑. นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคาม ทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจ ดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกัน การเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง ๒. รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และ วัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน ๓. ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสมและเป็นปัจจุบัน

ระดับ	แนวปฏิบัติพื้นฐาน
	๔. เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดีตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

หลักการดูแลรักษาหลักฐานทางดิจิทัล (Digital Forensics) ที่สำคัญมีดังนี้

๑. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
๒. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ ๑) ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker ๒) ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น ๓) ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด ๔) ต้องทำการบันทึกหลักฐาน (Chain of Custody)
๓. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖
๔. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริงหรือเพื่อค้นหาสาเหตุของการเกิด Incident
๕. Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form[๑] ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการจัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้ จึงจะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา

๓.๘.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

กรมส่งเสริมอุตสาหกรรมดำเนินการจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ที่ช่วยให้แนวทางเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ ซึ่งสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ อ้างอิงตาม **ภาคผนวก ช รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist**

การจัดทำรายละเอียดแผนฯ เพื่อเตรียมความพร้อมกับสถานการณ์ที่เกิดขึ้นจริง โดยกำหนดให้มีการซักซ้อม การรับมือ การแลกเปลี่ยนข้อมูล รวมถึงการติดตามข่าวเกี่ยวกับภัยคุกคามทางไซเบอร์ เพื่อเตรียมความพร้อมรับมือในภาวะวิกฤต จึงได้จัดทำเอกสารแผนเผชิญเหตุการณ์ผิดปกติด้านสารสนเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ (Playbook for Security Incident and Cybersecurity Incident) การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) อ้างอิงตาม **ภาคผนวก ซ Play book ransomware**

แหล่งที่มา

- 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

ภาคผนวก ก
แบบประเมินความเสี่ยงความมั่นคงปลอดภัยสารสนเทศ

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๑	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง	๑		๑	๑	๑	๑	๑	๑	๑	๒	Low
๒	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูลระบบมีช่องโหว่	๒			๑	๑	๑	๒	๒	๒	๑	Low
๓	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล		๑	๑	๑	๑	๑	๑	๑	๒	๑	Low
๔	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบบุคคลเข้าถึงข้อมูล	๒	๒	๒	๑	๑	๑	๒	๒	๒	๑	Low
๕	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน			๒	๑	๑	๑	๒	๑	๒	๑	Low
๖	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน			๒	๑	๑	๑	๒	๑	๓	๑	Medium
๗	กระบวนการสำรองข้อมูลและทดสอบข้อมูล	Information	ข้อมูลติดไวรัสหรือ Ransomware	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ		๒	๓	๑	๑	๑	๒	๒	๓	๑	Medium
๘	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง		๒	๓	๒	๑	๒	๒	๒	๓	๑	Medium
๙	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูลระบบมีช่องโหว่		๑	๒	๑	๑	๑	๒	๑	๒	๑	Low
๑๐	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล		๑	๑	๑	๑	๑	๑	๑	๑	๑	Low
๑๑	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบบุคคลเข้าถึงข้อมูล	๑	๑	๑	๑	๑	๑	๑	๑	๒	๑	Low
๑๒	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน			๒	๑	๑	๑	๒	๒	๒	๑	Low
๑๓	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน			๒	๑	๑	๑	๑	๑	๑	๑	Low
๑๔	ข้อมูลทะเบียนทรัพย์สินสารสนเทศ	Information	ข้อมูลติดไวรัส	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ			๒	๑	๑	๑	๒	๒	๒	๒	Medium

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๑๕	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง	๑		๒	๑	๑	๑	๒	๒	๒	๑	Low
๑๖	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูลระบบมีช่องโหว่	๑		๒	๑	๑	๑	๒	๒	๒	๑	Low
๑๗	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล	๑	๑	๒	๑	๑	๑	๒	๒	๒	๒	Medium
๑๘	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบบุคคลเข้าถึงข้อมูล	๑	๑	๑	๑	๑	๑	๒	๒	๒	๑	Low
๑๙	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน	๑		๒	๑	๑	๑	๒	๒	๒	๑	Low
๒๐	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน	๑		๒	๑	๑	๑	๒	๒	๒	๑	Low
๒๑	ข้อมูลบัญชีผู้ดูแลระบบ	Information	ข้อมูลติดไวรัส	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ	๑		๒	๑	๑	๑	๒	๒	๒	๒	Medium
๒๒	Network Diagram	Information	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง			๑	๑	๑	๑	๑	๑	๑	๑	Low
๒๓	Network Diagram	Information	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูลระบบมีช่องโหว่	๑		๒	๑	๑	๑	๑	๑	๑	๑	Low
๒๔	Network Diagram	Information	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล		๑	๑	๑	๑	๑	๑	๑	๑	๑	Low
๒๕	Network Diagram	Information	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบบุคคลเข้าถึงข้อมูล	๑	๑	๑	๑	๑	๑	๒	๒	๒	๑	Low
๒๖	Network Diagram	Information	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน			๑	๑	๑	๑	๑	๑	๑	๑	Low
๒๗	Network Diagram	Information	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน			๑	๑	๑	๑	๑	๑	๑	๒	Low
๒๘	Network Diagram	Information	ข้อมูลติดไวรัสหรือ Ransomware	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ			๑	๑	๑	๑	๑	๑	๑	๑	Low

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๒๙	รายงานการบำรุงรักษา	Information	ข้อมูลสูญหาย ถูกขโมย	ขาดการตรวจสอบความครบถ้วนสมบูรณ์ของข้อมูลสำรอง รวมถึงขาดการทดสอบข้อมูลว่าสามารถนำมากู้คืนระบบได้จริง				๑	๑	๑	๑	๒	๒	๑	Low
๓๐	รายงานการบำรุงรักษา	Information	ข้อมูลถูกเปิดเผยโดยมิได้รับอนุญาตจากการบุกรุก/เจาะระบบ	ขาดการกำหนดสิทธิการเข้าถึงข้อมูลระบบมีช่องโหว่	๑		๒	๑	๑	๑	๒	๒	๒	๑	Low
๓๑	รายงานการบำรุงรักษา	Information	ข้อมูลขาดการปรับปรุงล้าสมัย ไม่ถูกต้อง ไม่พร้อมใช้งาน	ขาดการทบทวนข้อมูล ปรับปรุงข้อมูล		๑	๑	๑	๑	๑	๑	๑	๑	๒	Low
๓๒	รายงานการบำรุงรักษา	Information	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการตรวจสอบบุคคลเข้าถึงข้อมูล	๑	๑	๑	๑	๑	๑	๒	๒	๒	๑	Low
๓๓	รายงานการบำรุงรักษา	Information	ข้อมูลถูกทำลายโดยไฟไหม้ ไม่สามารถนำมาใช้งานได้	อุปกรณ์ไฟฟ้าขั้วต่อหลวมไม่ได้มาตรฐาน			๑	๑	๑	๑	๑	๑	๑	๑	Low
๓๔	รายงานการบำรุงรักษา	Information	ข้อมูลถูกลบโดยไม่ตั้งใจ	ขาดความรอบคอบในการปฏิบัติงาน			๑	๑	๑	๑	๑	๑	๑	๒	Low
๓๕	รายงานการบำรุงรักษา	Information	ข้อมูลติดไวรัสหรือ Ransomware	ดาวน์โหลดไฟล์หรือเปิดไฟล์ที่ไม่น่าเชื่อถือ				๑	๑	๑	๒	๒	๒	๑	Low
๓๖	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๑	๑	๑	๑	๒	๑	๑	๓	Low
๓๗	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๑	๑	๑	๒	๒	๑	๑	๒	Low
๓๘	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้			๑	๑	๑	๒	๒	๑	๑	๑	Low
๓๙	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึง	๑	๑	๑	๑	๑	๒	๒	๑	๑	๑	Low
๔๐	คอมพิวเตอร์ตั้งโต๊ะเจ้าหน้าที่	Hardware	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration			๑	๑	๑	๑	๑	๑	๑	๒	Low
๔๑	พื้นที่ปฏิบัติงานของเจ้าหน้าที่	Locations	เกิดโรคระบาด ไม่สามารถเข้าปฏิบัติงานได้	ขาดการป้องกันและควบคุมการแพร่ระบาดของโรค			๑	๑	๑	๑	๒	๑	๒	๒	Medium
๔๒	พื้นที่ปฏิบัติงานของเจ้าหน้าที่	Locations	ระบบกระแสไฟฟ้าขัดข้อง	ภัยธรรมชาติ เช่น ฝนตก พายุหรือฟ้าผ่า ทำให้อุปกรณ์ไฟฟ้าทำงานผิดพลาดหรือชำรุด			๑	๑	๑	๑	๒	๑	๒	๑	Low
๔๓	พื้นที่ปฏิบัติงานของเจ้าหน้าที่	Locations	ระบบกระแสไฟฟ้าขัดข้อง ไฟดับ	สัตว์ที่ขึ้นไปอยู่บนเสาไฟฟ้า หรือสายไฟฟ้า ทำให้เกิดกระไฟฟ้าลัดวงจร			๑	๑	๑	๑	๒	๑	๒	๑	Low

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๔๔	พื้นที่ปฏิบัติงานของเจ้าหน้าที่	Locations	ชุมนุมประท้วง ก่อจราจลปิดสถานที่	การบริหารงานหรือนโยบายของภาครัฐ			๒	๑	๑	๑	๒	๒	๒	๑	Low
๔๕	อุปกรณ์ network	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๒	๒	๑	๑	๒	๒	๓	๑	Medium
๔๖	อุปกรณ์ network	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๒	๒	๑	๑	๒	๒	๓	๑	Medium
๔๗	อุปกรณ์ network	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้			๒	๒	๑	๑	๒	๒	๓	๑	Medium
๔๘	อุปกรณ์ network	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึงอุปกรณ์	๑	๑	๒	๒	๑	๑	๒	๒	๓	๑	Medium
๔๙	เครื่องคอมพิวเตอร์แม่ข่าย	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๒	๒	๑	๑	๒	๒	๒	๑	Low
๕๐	เครื่องคอมพิวเตอร์แม่ข่าย	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๒	๒	๑	๑	๒	๒	๒	๑	Low
๕๑	เครื่องคอมพิวเตอร์แม่ข่าย	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้			๒	๑	๑	๑	๒	๒	๒	๑	Low
๕๒	เครื่องคอมพิวเตอร์แม่ข่าย	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึง	๑	๑	๒	๑	๑	๑	๒	๒	๒	๑	Low
๕๓	เครื่องคอมพิวเตอร์แม่ข่าย	Hardware	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration			๒	๑	๑	๑	๒	๒	๒	๒	Medium
๕๔	อุปกรณ์จัดเก็บข้อมูล	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๒	๒	๑	๑	๒	๒	๒	๑	Low
๕๕	อุปกรณ์จัดเก็บข้อมูล	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๒	๒	๑	๑	๒	๒	๒	๑	Low
๕๖	อุปกรณ์จัดเก็บข้อมูล	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้			๒	๑	๑	๑	๒	๒	๒	๑	Low
๕๗	อุปกรณ์จัดเก็บข้อมูล	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึง	๑	๑	๑	๑	๑	๑	๒	๒	๑	๑	Low
๕๘	อุปกรณ์จัดเก็บข้อมูล	Hardware	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration			๑	๑	๑	๑	๒	๒	๒	๑	Low
๕๙	ผู้ให้บริการภายนอก	Service	ผู้ให้บริการภายนอกเปิดเผยข้อมูลความลับ	การควบคุมความลับของข้อมูลไม่มีประสิทธิผล	๒	๒	๒	๒	๑	๒	๒	๒	๒	๒	Medium
๖๐	ผู้ให้บริการภายนอก	Service	การทำงานหรือการให้บริการหยุดชะงัก	ไม่ได้กำหนดคุณสมบัติของผู้ให้บริการภายนอก			๒	๑	๑	๒	๒	๒	๒	๑	Low

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๖๑	ผู้ให้บริการภายนอก	Service	การทำงานหรือการให้บริการหยุดชะงัก	บริษัทผู้ให้บริการภายนอกไม่ได้ส่งผู้ปฏิบัติงานแทน			๒	๑	๑	๒	๒	๒	๒	๑	Low
๖๒	ผู้ให้บริการภายนอก	Service	เข้าถึงอุปกรณ์และแก้ไขข้อมูลโดยไม่ได้รับอนุญาติ	ขาดการทบทวนสิทธิการเข้าถึงอุปกรณ์	๒	๒	๒	๒	๑	๒	๒	๒	๒	๑	Low
๖๓	อุปกรณ์รักษาความปลอดภัยเครือข่าย	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๒	๑	๑	๑	๒	๒	๓	๑	Medium
๖๔	อุปกรณ์รักษาความปลอดภัยเครือข่าย	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๒	๑	๑	๑	๒	๒	๓	๑	Medium
๖๕	อุปกรณ์รักษาความปลอดภัยเครือข่าย	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้	๑	๑	๒	๑	๑	๑	๒	๒	๓	๑	Medium
๖๖	อุปกรณ์รักษาความปลอดภัยเครือข่าย	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงข้อมูลเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึง	๑	๑	๒	๑	๑	๑	๒	๒	๒	๑	Low
๖๗	อุปกรณ์รักษาความปลอดภัยเครือข่าย	Hardware	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration			๒	๑	๑	๑	๒	๒	๓	๑	Medium
๖๘	อุปกรณ์สำรองไฟฟ้า	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดอุปกรณ์ทดแทน			๑	๒	๑	๑	๒	๒	๒	๑	Low
๖๙	อุปกรณ์สำรองไฟฟ้า	Hardware	อุปกรณ์เสียไม่สามารถทำงานได้	ขาดการทำสัญญาบำรุงรักษา			๑	๒	๑	๑	๒	๒	๒	๑	Low
๗๐	อุปกรณ์สำรองไฟฟ้า	Hardware	อุปกรณ์ถูกทำลาย	ผู้ไม่มีสิทธิ์บุกรุกสามารถเข้าถึงอุปกรณ์ได้			๒	๑	๑	๑	๒	๒	๑	๑	Low
๗๑	อุปกรณ์สำรองไฟฟ้า	Hardware	ผู้ไม่ได้รับอนุญาตสามารถเข้าถึงเปลี่ยนแปลงหรือแก้ไขข้อมูล	ขาดการกำหนดสิทธิหรือทบทวนสิทธิการเข้าถึง		๑	๒	๑	๑	๑	๑	๑	๑	๑	Low
๗๒	อุปกรณ์สำรองไฟฟ้า	Hardware	ระบบหยุดทำงานไม่สามารถทำงานได้เป็นระยะเวลานาน	ขาดการ Backup ค่า Configuration			๑	๑	๑	๑	๑	๑	๒	๑	Low
๗๓	ระบบปฏิบัติการ	Software	ผู้ไม่ได้รับอนุญาติเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการกำหนดสิทธิ และทบทวนสิทธิ	๑	๑	๑	๑	๑	๑	๑	๑	๑	๑	Low
๗๔	ระบบปฏิบัติการ	Software	ผู้ไม่ได้รับอนุญาติเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการตรวจสอบช่องโหว่ของระบบหรือระบบล้าสมัย	๑	๑	๑	๑	๑	๑	๒	๒	๒	๑	Low
๗๕	ระบบปฏิบัติการ	Software	ระบบขัดข้องเป็นเวลานาน	ขาดการเฝ้าระวัง แจ้งเตือน และตรวจสอบการทำงานของระบบ			๑	๑	๑	๑	๑	๑	๑	๑	Low
๗๖	ระบบปฏิบัติการ	Software	ระบบขัดข้องเป็นเวลานาน	ขาดการสำรองข้อมูล			๑	๑	๑	๑	๒	๑	๒	๑	Low

ลำดับที่ (No.)	กลุ่มทรัพย์สิน (Groups of Asset)	ประเภททรัพย์สิน (Types of Asset)	ภัยคุกคาม (Threat)	ช่องโหว่ (Vulnerability)	กระทบด้าน			ระดับผลกระทบในแต่ละด้าน					ผลกระทบ (Impact)	โอกาสที่จะเกิด (Likelihood)	ระดับความเสี่ยงโดยรวม (Risk Exposure)
					ความลับ (C)	ความถูกต้อง (I)	ความพร้อมใช้ (A)	ด้านการเงิน	อันตรายต่อชีวิต	ผู้ใช้บริการได้รับความเสียหาย	ด้านการดำเนินงาน	ด้านความมั่นคง			
๗๗	โปรแกรมสนับสนุน	Software	ผู้ไม่ได้รับอนุญาติเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการกำหนดสิทธิ และทบทวนสิทธิ	๑	๑	๑	๑	๑	๑	๑	๑	๑	๑	Low
๗๘	โปรแกรมสนับสนุน	Software	ผู้ไม่ได้รับอนุญาติเข้าถึงระบบเปลี่ยนแปลงและแก้ไขทำให้ระบบเกิดเหตุขัดข้อง	ขาดการตรวจสอบช่องโหว่ของระบบหรือระบบล้าสมัย	๑	๑	๑	๑	๑	๑	๒	๒	๒	๑	Low
๗๙	โปรแกรมสนับสนุน	Software	ระบบขัดข้องเป็นเวลานาน	ขาดการเฝ้าระวัง แจ้งเตือน และตรวจสอบการทำงานของระบบ			๑	๑	๑	๑	๑	๑	๒	๑	Low
๘๐	โปรแกรมสนับสนุน	Software	ระบบขัดข้องเป็นเวลานาน	ขาดการสำรองข้อมูล			๑	๑	๑	๑	๒	๑	๒	๑	Low

ภาคผนวก ข
บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

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

ภาคผนวก ค
บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง ๓๐/๑/๖๘ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก ง
ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

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)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง 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

ภาคผนวก จ
แบบฟอร์มแบบรายงานภัยคุกคามทางไซเบอร์

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

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)

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

☐ 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

ภาคผนวก ฉ
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)	
สวิตช์ (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 ช
รายการตรวจสอบการจัดการเหตุการณ์

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (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	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ภาคผนวก ซ

Play book ransomware

การเตรียมการ (Preparation)	
วัตถุประสงค์	๑.มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ ๒.มีกระบวนการ และกลไกในการป้องกันที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นการตรวจจับความพยายามในการบุกรุกได้อีกด้วย
การดำเนินการ	คำอธิบาย
จัดเตรียมทรัพยากร	อ้างถึงข้อ ๓.๙.๑ ขั้นการเตรียมการ (Preparation)
ดำเนินการป้องกันก่อนเกิดเหตุ	การรับมือ Ransomware ในปัจจุบันให้มุ่งเน้นไปที่เรื่องของการ Backup ระบบและข้อมูลการจัดการเรื่องของข้อมูลที่รั่วไหลโดยเฉพาะเรื่องของการ Take Down แหล่งที่รั่วไหลของข้อมูล การมีมาตรการในการเยี่ยวยาผู้ที่ได้รับผลกระทบจากการรั่วไหลของข้อมูล รวมทั้งควรมีความพร้อมในการดำเนินการ Personal information usage Monitoring สำหรับบุคคลที่ข้อมูลรั่วไหลว่าจะมีข้อมูลถูกนำไปใช้ที่ใดได้บ้าง
การตรวจจับและวิเคราะห์ (Detection and Analysis)	
วัตถุประสงค์	๑.รับแจ้งเหตุการณ์โจมตี ๒.การระบุความเสียหายเบื้องต้น ๓.การระบุสาเหตุที่การโจมตีสำเร็จ ๔.การระบุความสามารถของผู้บุกรุกและเครื่องมือที่ใช้รวมถึง Malware
การดำเนินการ	**คำอธิบาย**
รับแจ้งเหตุ	ส่วนใหญ่เมื่อการโจมตีประเภท Ransomware เกิดขึ้นจะรับทราบได้จากการที่ผู้ใช้งานระบบเป็นผู้แจ้ง
วิเคราะห์การโจมตีและขอบเขตเสียหาย	ผลกระทบเบื้องต้นสามารถสอบถามได้จากผู้ใช้งานระบบ รวมถึงการดำเนินการก และเป็นผลให้การโจมตีสำเร็จ รวมทั้งใช้ข้อมูลจากการสอบถามเป็นข้อมูลเบื้องต้นในการจัดการภัยคุกคามและค้นหาระบบอื่นๆที่อาจจะได้รับผลกระทบในลักษณะเดียวกัน
จัดเก็บหลักฐานทางดิจิทัลที่จำเป็นรวมถึงตัวอย่าง Malware	การโจมตีที่สำเร็จ หมายถึง การโจมตีที่สามารถผ่านกลไกการป้องกันมาได้ ซึ่งเป็นการโจมตีที่มีความซับซ้อน ซึ่งการจะทราบถึงเทคนิควิธิการโจมตี ลักษณะที่ใช้ และผลกระทบที่เป็นไปได้ทั้งหมด ต้องอาศัยการเก็บข้อมูลและการวิเคราะห์ขั้นสูง การเก็บข้อมูลจากจุดต่างๆของเครื่องคอมพิวเตอร์ที่โดนโจมตีและอุปกรณ์เครือข่ายที่ทำงานร่วมกันจึงเป็นสิ่งจำเป็น โดยที่ต้องคำนึงถึงความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้า ประกอบด้วย - RAM - Network Connection - Running Process - Opened Files - Swap Memory - Hard Disk image

	- System Log - Network Log - External Media ข้อมูลที่อ่อนไหวต่อการสูญเสียกระแสไฟฟ้า คือ ข้อมูลที่จะหายไปหากไม่มีกระแสไฟฟ้าค่อยเลี้ยง เช่น RAM เป็นต้น ดังนั้น เพื่อให้หลักฐานยังคงอยู่ครบถ้วน ในบางกรณี การเก็บข้อมูลจึงต้องกระทำอย่างรวดเร็ว โดยผู้เชี่ยวชาญ และก่อนที่จะมีการปิดเครื่องคอมพิวเตอร์ และหากการตอบสนองเกิดขึ้นเร็วพอ โอกาสที่จะได้ตัวอย่างของ Malware ที่เป็น Ransomware มาวิเคราะห์จะมีโอกาสสูงขึ้น การดำเนินการทั้งหมดจะต้องถูกบังคับอย่างละเอียดเพื่อการอ้างอิงถึงในภายหลังโดยเฉพาะการขึ้นสู่ศาล (หากจำเป็น)
วิเคราะห์ข้อมูลหลักฐานดิจิทัลเพื่อหาข้อสรุปจากการโจมตีและความเสียหายที่เกิดจาก Malware	ข้อมูลจากขั้นตอนการดำเนินการ จะสรุปได้ ๓ เรื่องดังต่อไปนี้ ๑.สาเหตุที่การโจมตีประสบความสำเร็จ เพื่อการแก้ไขข้อมูลที่ตรงจุด ซึ่งต้องวิเคราะห์จากข้อมูลการสัมภาษณ์ และข้อมูลที่จัดเก็บได้ในขั้นตอนก่อนหน้า โดยเฉพาะการทำ Data Correlation และ Timeline Analysis ๒.โอกาสและรูปแบบของผลกระทบที่อาจจะขยายวงกว้างออกไปได้ โดยเฉพาะความสามารถของภัยคุกคามและ Malware ที่ใช้งาน เพื่อที่จะได้ค้นหาและหยุดการแพร่กระจายของภัยคุกคาม ซึ่งต้องพิจารณาจากข้อมูลที่จัดเก็บได้ในขั้นตอนการดำเนินการ ที่ได้จากการทำ Malware Analysis ๓.การจัดทำ Indicator of Compromise (IoC) จากผลการวิเคราะห์ที่ได้ เพื่อใช้ในการ Scan ระบบอื่นๆ ในเครือข่ายเดียวกัน หรือเครือข่ายใกล้เคียง เพื่อระบุขอบเขตของการแพร่กระจายของ Malware และภัยคุกคาม
ขยายผลการวิเคราะห์ความเสียหายที่เกิดจากข้อมูลรั่วไหล	เมื่อทราบว่ามีข้อมูลรั่วไหล ต้องทำการเตรียมความพร้อมและตรวจสอบความเป็นไปได้ของข้อมูลที่รั่วไหลว่าสามารถไปปรากฏอยู่ในแหล่งใดบ้าง โดยสามารถพิจารณาจากระบบที่ได้รับผลกระทบ
ติดต่อประสานงานกับหน่วยงานภายในและภายนอก	ข้อมูลที่ได้จากการวิเคราะห์จำเป็นที่จะต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้อง โดยขึ้นอยู่กับเหตุการณ์และความจำเป็น โดยในกรณีของ Ransomware และ Data Lekage จากภายในองค์กร ควรมีหน่วยงานที่ต้องติดต่อสื่อสารอย่างน้อยดังนี้ ๑.การแจ้งผลการวิเคราะห์ให้กับทีมผู้ดูแลระบบ เพื่อทำการแก้ไขจุดอ่อนและความเสียหายที่เกิดขึ้นกับระบบ ๒.กรณีระบบไม่สามารถให้บริการตามปกติได้ ต้องติดต่อประสานงานให้กับทีมรับแจ้งเหตุการณ์ ๓.การแจ้งหน่วยงานกำกับดูแลตามเกณฑ์ที่กำหนด ๔.การแจ้งเจ้าของข้อมูลที่รั่วไหล ตามเงื่อนไขกฎหมายที่เกี่ยวข้อง หรือตามความเหมาะสมและความจำเป็น

การระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ	
วัตถุประสงค์	๑.การค้นหา กำจัด และควบคุมการแพร่กระจายของ Malware ๒.การค้นหาและควบคุมการรั่วไหลของข้อมูล ๓.การกู้คืนระบบให้กลับมาทำงานปกติ
การดำเนินการ	คำอธิบาย
นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบเพื่อกำจัดภัยคุกคามออกจากระบบ	ขั้นตอนที่สามารถดำเนินการควบคู่กับการวิเคราะห์ข้อมูล คือ การจำกัดความเสียหายเบื้องต้น ซึ่งปกติจะดำเนินการตัดการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่โดนโจมตีออกจากเครือข่าย หรือทำการปิดการทำงานของอุปกรณ์ลงโดยวิธี Shutdown หรือถอดสายไฟทันที ทั้งนี้ วิธีที่เลือกใช้ควรคำนึงถึงความเสียหายที่จะเกิดกับข้อมูลหลักฐานทางดิจิทัลเสมอ และควรมีการเก็บข้อมูลออกจากอุปกรณ์นั้นๆ ด้วยวิธีที่ถูกต้องก่อนที่จะมีการปิดการทำงาน ผลการวิเคราะห์ข้อมูลหลักฐานทางดิจิทัลจะทำให้ได้ข้อสรุปของการโจมตี ตั้งแต่ช่องโหว่ที่ใช้ ความเสียหายที่เกิดขึ้น และร่องรอยที่เกี่ยวข้อง เช่น การเข้าถึง/เปลี่ยนแปลง File, Registry, Networking Resource, Network Storage เป็นต้น ซึ่งทั้งหมดนี้สามารถใช้ในการแก้ไข incident ได้นอกจากนี้ การ Scan เพื่อค้นหา Indicator of Compromise (IoC) เป็นอีกหนึ่งวิธีที่ช่วยให้การค้นหา และกำจัดภัยคุกคามสามารถดำเนินการได้เร็วขึ้น
ควบคุมและเยียวยา ความเสียหายจากการรั่วไหลของข้อมูล	การรั่วไหลของข้อมูลถึงแม้จะไม่สามารถถูกแก้ไขได้อย่างสิ้นเชิง แต่ควรมีการตอบสนองที่สำคัญเพื่อช่วยบรรเทาความเสียหาย และลดหรือกำจัดผลกระทบจากการรั่วไหลนั้นได้ คือ การระบุจุดที่ข้อมูลรั่วไหลถูกเปิดเผย เช่น เว็บไซต์ที่ถูกแฮ็กหรือถูกขโมย เป็นต้น และควรมีขั้นตอนหรือแนวทางในการดำเนินการ Take Down แหล่งข้อมูลเหล่านั้นเท่าที่ทำได้ และควรมีมาตรการเยียวยาเจ้าของข้อมูลและผู้ที่ได้รับผลกระทบตามที่กฎหมายกำหนด
กู้คืนระบบและข้อมูลหากมีความเสียหาย	เมื่อแก้ไขและกำจัดภัยคุกคามออกจากระบบได้แล้ว หากจำเป็นต้องมีการกู้คืนระบบหรือข้อมูลที่ได้รับความเสียหายกลับมาจาก Backup System Image ซึ่งหากตรวจพบ ควรดำเนินการแก้ไขก่อนนำมาใช้งาน
การดูแลความผิดปกติอย่างต่อเนื่อง	การดูแลความผิดปกติ ต้องเริ่มต้นตั้งแต่เมื่อมีการนำอุปกรณ์ที่โดนโจมตีออกจากเครือข่าย จนถึงการกู้คืนระบบเรียบร้อยแล้ว รวมทั้งหลังจากกลับมาปฏิบัติงานตามปกติอีกสักระยะหนึ่ง โดยการกำหนดระยะเวลาจะขึ้นอยู่กับแต่ละองค์กรซึ่งอย่างน้อยไม่ควรต่ำกว่า ๔๘ ชั่วโมง ทั้งนี้ หากพบเจอความผิดปกติให้กลับไปดำเนินการในขั้นตอนการตรวจจับและวิเคราะห์ อีกครั้ง

การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์	
วัตถุประสงค์	ปรับปรุงพัฒนาแผนการรับมือหรือความพร้อมด้านอื่นๆ จากข้อมูลที่ได้จากการรับมือ
การดำเนินการ	คำอธิบาย
การเรียนรู้เพื่อปรับปรุง	อ้างอิงข้อ ๓.๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity) และดำเนินการ ๑. การตรวจสอบและวิเคราะห์เหตุการณ์ - ระบุจุดเริ่มต้นของการโจมตี (เช่น ช่องโหว่หรือพฤติกรรมที่ทำให้ระบบถูกโจมตี) - ผลกระทบที่เกิดขึ้นต่อระบบ ข้อมูล หรือผู้ใช้งาน - วิธีการที่ใช้ในการแก้ไขและระยะเวลาที่ใช้ในการจัดการปัญหา ๒. การปรับปรุงมาตรการรักษาความปลอดภัย - การอัปเดตและแก้ไขช่องโหว่ของซอฟต์แวร์และระบบปฏิบัติการ - การปรับปรุงการตั้งค่าความปลอดภัยของเครือข่าย และการกำหนดสิทธิ์การเข้าถึงใหม่ ๓. การฝึกอบรมและให้ความรู้แก่บุคลากร - จัดอบรมเกี่ยวกับวิธีระบุและรับมือกับภัยคุกคามไซเบอร์ - สร้างแนวทางการรายงานเหตุการณ์ผิดปกติในระบบ - ให้ความรู้เกี่ยวกับหลักการรักษาความปลอดภัยข้อมูลและการใช้งานเครือข่ายอย่างถูกต้อง ๔. การจัดทำรายงานและเอกสาร - จัดทำรายงานสรุปเหตุการณ์ รวมถึงรายละเอียดของการตอบสนองและการแก้ไข ๕. การทดสอบระบบและการตรวจสอบความปลอดภัย - ดำเนินการประเมินช่องโหว่เพื่อตรวจสอบความแข็งแกร่งของระบบ - วิเคราะห์หาช่องโหว่ใหม่ที่อาจถูกโจมตี