แผนรับมือเหตุภัยคุกคามทางไซเบอร์
กรมโรงงานอุตสาหกรรม
(Cyber Incident Response Procedure)

จัดทำโดย
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมโรงงานอุตสาหกรรม

พฤศจิกายน ๒๕๖๗

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมโรงงานอุตสาหกรรม

1.หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมโรงงานอุตสาหกรรม ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (1) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมินผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้งและ (2) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตาม นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมโรงงานอุตสาหกรรม ประจำปี 2566 ด้วย

2.วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นใน กรมโรงงานอุตสาหกรรม โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้ กรมโรงงานอุตสาหกรรม การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมโรงงานอุตสาหกรรม

3. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของกรมโรงงานอุตสาหกรรม รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

4. หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงภาครัฐระดับกรม (DCIO) อย่างน้อยปีละ 1 ครั้ง

5**. หน้าที่ในการดำเนินการตามแผน**

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการ ตามแผนรับมือฯ โดยมีหน่วยงานสนับสนุนประกอบด้วย กองกฎหมาย สำนักงานเลขานุการกรม และกลุ่มตรวจสอบภายใน

6. รายละเอียดการบังคับใช้เอกสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้ระบุรายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

6.1. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	ศูนย์เทคโนโลยีสารสนเทศ และการสื่อสาร
ผู้ดำเนินการตามเอกสาร (Owner)	
วันที่จัดทำเอกสาร (Date created)	มกราคม 2567
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	DCIO กรมโรงงานอุตสาหกรรม
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	มกราคม 2568

ตารางที่ 1 รายละเอียดของเอกสาร (Document control)

6.2. **การเปลี่ยนแปลงเอกสาร (Version control)**

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
1.0	8 กุมภาพันธ์ 2567		
2.0	27 พฤศจิกายน 2567	รองอธิบดีกรมโรงงานอุตสาหกรรม รักษาราชการแทน อธิบดีกรมโรงงานอุตสาหกรรม	การวิเคราะห์ระบบที่ให้บริการของ กรอ. ที่มีความสำคัญ

ตารางที่ 2 การเปลี่ยนแปลงเอกสาร (Version control)

7. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

7.1 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมโรงงานอุตสาหกรรม ประจำปี 2566

7.2 นโยบายการคุ้มครองข้อมูลส่วนบุคคล (Privacy Policy) กรมโรงงานอุตสาหกรรม พ.ศ. 2565

7.3 ประมวลแนวปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมโรงงานอุตสาหกรรม พ.ศ. 2567

7.4 NIST SP 800-61r2 Computer Security Incident Handling Guide

8. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (Observable Occurrence) ในระบบ เครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลในเชิงลบ

เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

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

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ[1] หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา 49 ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

9. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

9.1. ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้ระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ โดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง/ 7 วัน ดังนี้

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	นายโยธิน คำนนท์	06.00 – 18.00 น.	080-450-5266	ผู้รับแจ้งเหตุหลัก	รับแจ้งเหตุเมื่อมีการตรวจพบ/ได้รับรายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
2	นายภาณุพงศ์ สงวนประเสริฐ	18.00 – 06.00 น.	086-048-2883	ผู้รับแจ้งเหตุรอง	รับแจ้งเหตุเมื่อมีการตรวจพบ/ได้รับรายงานเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

ตารางที่ 3 ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

9.2. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team: CIRT)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบใด เช่น แบบรวมศูนย์ (Centralize), แบบกระจาย (Distributed), แบบให้คำปรึกษา (Coordinating) หรือ แบบอื่นๆ ตามบริบทของหน่วยงาน

โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	ธีรทัศน์ อิศรางกูร ณ อยุธยา (ผอ.ศส.)	เบอร์ภายใน : 2500 เบอร์มือถือ : 061-397-7932 Email: teeratas.i@diw.mail.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
2	นางสาวประนมพร โลกคำลือ	เบอร์ภายใน : 2517 เบอร์มือถือ : 094-650-0440 Email: pranomporn.l@diw.mail.go.th	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
3	นายโยธิน คำนนท์	เบอร์ภายใน : 2508 เบอร์มือถือ : 080-450-5266 Email: yotin.k@diw.mail.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ (ชื่อหน่วยงานเจ้าของระบบภายใต้หน่วยงานของท่าน) ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
4	นายภาณุพงศ์ สงวนประเสริฐ / นายวชิรพงษ์ แน่นหนา	เบอร์ภายใน : 2508 เบอร์มือถือ : 086-048-2883 Email: panupong.s@diw.mail.go.th เบอร์ภายใน : 2508 เบอร์มือถือ : 096-946-4941 Email: wachirapong.n@diw.mail.go.th	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

ตารางที่ 4 โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
1	พรยศ กลั่นกรอง (DCIO)	เบอร์ภายใน : 1002 เบอร์โทรศัพท์ : 081-648-9500 Email: pornyod.k@diw.mail.go.th	ผู้บริหารจัดการความเสี่ยง	รับผิดด้านบริหารความเสี่ยง
2	ธีรทัศน์ อิศรางกูร ณ อยุธยา (ผอ.ศส.)	เบอร์ภายใน : 2500 เบอร์มือถือ : 061-397-7932 Email: teeratas.i@diw.mail.go.th	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
3	พวงผกา ภูตลาดขาม	เบอร์ภายใน : 1100 เบอร์มือถือ : 092-924-5928 Email: pungpaka.p@diw.mail.go.th	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ดูแลให้คำแนะนำควบคุมกฎหมาย
4	ภาณุพงศ์ สงวนประเสริฐ	เบอร์ภายใน : 2508 เบอร์มือถือ : 086-048-2883 Email: panupong.s@diw.mail.go.th	ผู้ทดสอบเจาะระบบ	เจาะระบบและป้องกันระบบเครือข่าย
5	วริศรา ทะนันไชย	เบอร์ภายใน : 1301 เบอร์มือถือ : 081-626-3759 Email: -	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่ด้านร่างกฎหมาย (คล้ายทนายความ)
6	ภาวิดา อมรประเวศ	เบอร์ภายใน : 1208 เบอร์มือถือ : 063-265-5424 Email: phawida.a@diw.mail.go.th	ผู้รับผิดชอบด้านสื่อสารองค์กร	เป็นผู้ประชาสัมพันธ์ขององค์กร

ตารางที่ 5 โครงสร้างทีมสนับสนุนการดำเนินการรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

9.3. หน่วยงานภายนอกที่เกี่ยวข้อง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีข้อมูลติดต่อสื่อสารกับผู้แทนจากแต่ละหน่วยงานภายนอกที่เกี่ยวข้องอย่าง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT, กรมศุลกากร และกรมพัฒนาธุรกิจการค้า โดยมีรายละเอียดดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	02-142-6888 Email: thaicert@ncsa.or.th	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	
2	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	02-142-6885 (ติดต่อเวลาทำการ), 02-114-3531 (24 ชั่วโมง) Email: thaicert@ncsa.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	
3	วรสันติ์ เหล่าชัย	เบอร์ภายใน : 1208 เบอร์มือถือ : 081-116-4234 Email: worasan.l@diw.mail.go.th	ศูนย์เฝ้าระวังสิ่งแวดล้อมอุตสาหกรรม	หน่วยงานกำกับดูแล
4	ผู้แทนจากกรมศุลกากร	02-109-3000 Email: callcenter@thainsw.net	กรมศุลกากร	
5	สิริมนต์ คงรื่น คณาพัฒน์ ปลั่งศรีสกุล	02-253-0561 ต่อ 4417 02-253-0561 ต่อ 4447	การนิคมอุตสาหกรรมแห่งประเทศไทย	
6	ฐิรศ อธิกุลวริน	02-547-5048	กรมพัฒนาธุรกิจการค้า	

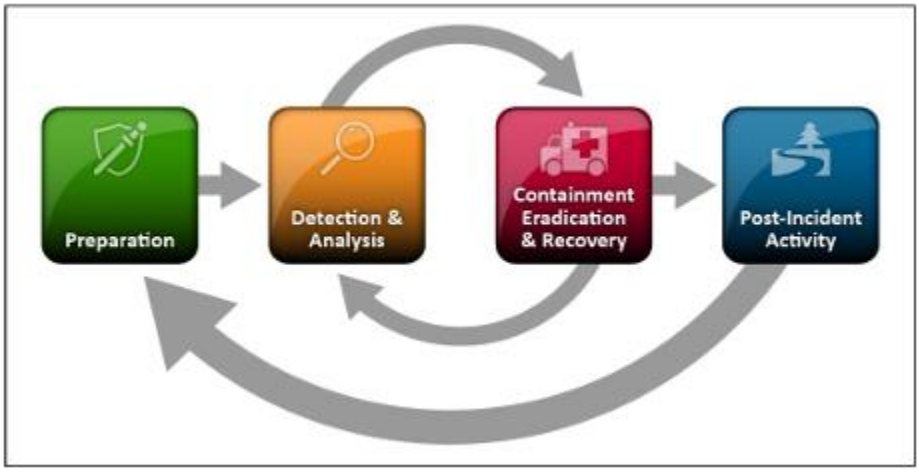
ตารางที่ 6 หน่วยงานภายนอกที่เกี่ยวข้อง

9.4. โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก โดยกำหนดให้ปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (ดังภาคผนวกที่ 1)

10. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ 19.1 ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564, ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564 และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566 รวมถึง (นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน) ดังนี้



รูปที่ 1 ภาพวงจรชีวิตการตอบสนองเหตุการณ์ (Incident Response Life Cycle)

10.1 ขั้นการเตรียมการ (Preparation)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือ โดยดำเนินการดังต่อไปนี้

1) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ 9.2

2) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ 9.4

3) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

4) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร, กลไกรายงานเหตุการณ์, ห้องประชุม War room เป็นต้น

5) จัดเตรียมอุปกรณ์, ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

6) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

7) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน (รายละเอียดปรากฏตามภาคผนวก 1)

ทั้งนี้ ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.1 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.2 ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม มีการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

หมวดหมู่เหตุการณ์

หมวดหมู่เหตุการณ์จะถูกจัดประเภทเป็นหนึ่งในสี่ระดับความรุนแรง ระดับความรุนแรงเหล่านี้ขึ้นอยู่กับผลกระทบต่อกรมโรงงานอุตสาหกรรม และสามารถแสดงได้ในแง่ของผลกระทบทางการเงิน ผลกระทบต่อบริการและ/หรือการปฏิบัติงานของภารกิจภารกิจของเรา ผลกระทบต่อภาพลักษณ์ของประเทศไทย หรือผล กระทบต่อความไว้วางใจจากลูกค้าและพลเมืองของประเทศไทย ฯลฯ ตารางด้านล่างนี้แสดงรายการระดับความรุนแรงและคำจำกัดความของระดับความรุนแรงแต่ละระดับ

ระดับความรุนแรง (Severity Level)	อธิบาย (Description)	เวลาตอบสนอง
0. ระดับต่ำ (Low)	เหตุการณ์ที่มีผลกระทบน้อยที่สุด ตัวอย่างอาจเป็นอีเมลขยะ การติดไวรัสที่แยกได้ เป็นต้น	24-48 ชั่วโมง
1. ธรรมดา (Medium)	เหตุการณ์ที่มีผลกระทบอย่างมีนัยสำคัญ ตัวอย่างอาจเป็นความล่าช้าหรือความสามารถที่จำกัดในการให้บริการ บรรลุภารกิจของ ประเทศไทย การส่งจดหมายอิเล็กทรอนิกส์หรือการถ่ายโอนข้อมูลที่สำคัญล่าช้า เป็นต้น	6-8 ชั่วโมง
2. สูง (High)	เหตุการณ์ที่เกิดผลกระทบรุนแรง ตัวอย่างอาจเป็นการหยุดชะงักในการให้บริการและ/หรือการปฏิบัติหน้าที่ภารกิจของเรา ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับของ ถูกบุกรุก ไวรัสหรือเวิร์มแพร่กระจายอย่างกว้างขวางและส่งผลกระทบต่อพนักงานมากกว่า 1 เปอร์เซ็นต์ ระบบความปลอดภัยสาธารณะไม่พร้อมใช้งาน หรือผู้บริหารระดับสูงของประเทศไทย ได้รับแจ้งแล้ว	2-3 ชั่วโมง
3. สูงมาก (Extreme)	เหตุการณ์ที่ส่งผลกระทบเป็นหายนะ ตัวอย่างอาจเป็นการปิดบริการเครือข่ายของประเทศไทยทั้งหมด ข้อมูลที่เป็นกรรมสิทธิ์หรือเป็นความลับของ ประเทศไทยถูกบุกรุกและเผยแพร่ใน/บนสถานที่หรือไซต์สาธารณะ ระบบความปลอดภัยสาธารณะใช้งานไม่ได้ ฝ่ายบริหารจะต้องแถลงต่อสาธารณะ	30 นาที

ตารางที่ 7 ระดับความรุนแรง

วงจรชีวิตการตอบสนองเหตุการณ์ (Incident Response Life Cycle) หมายถึงชุดของขั้นตอนหรือช่วงเวลาที่องค์กรปฏิบัติตามเมื่อต้องการตอบสนองและจัดการกับเหตุการณ์ด้านความปลอดภัย ขั้นตอนเหล่านี้มักประกอบด้วย:

1) หน่วยงานจะต้องดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/ Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่าง ดังนี้

ประเภท	อธิบาย	วิธีการรับมือ
อุปกรณ์บันทึกข้อมูลแบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงาน และตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด
การลดระดับความร้ายแรง (Attrition)	การโจมตีที่ใช้วิธีการบังคับดุร้ายเพื่อประนีประนอม ลดระดับ หรือทำลายระบบเครือข่าย หรือบริการ (เช่น DDoS ที่มีจุดประสงค์เพื่อทำให้เสียหรือปฏิเสธการเข้าถึงบริการหรือแอปพลิเคชัน การโจมตีแบบดุร้ายต่อกลไกการตรวจสอบสิทธิ์ เช่น รหัสผ่าน CAPTCHAS หรือลายเซ็นดิจิทัล)	
Website (เว็บไซต์)	การโจมตีที่ดำเนินการจากเว็บไซต์หรือแอปพลิเคชันบนเว็บ ตัวอย่างเช่น การโจมตีด้วยสคริปต์ข้ามไซต์ที่ใช้ในการขโมยข้อมูลประจำตัว หรือการเปลี่ยนเส้นทางไปยังไซต์ที่ใช้ประโยชน์จากช่องโหว่ของเบราว์เซอร์และติดตั้งมัลแวร์	ใช้ข้อมูลที่สำรองไว้ทั้งระบบและฐานข้อมูลนำมาทำใหม่
การแอบอ้างบุคคลอื่น: (Impersonation)	การโจมตีที่เกี่ยวข้องกับการแทนที่สิ่งที่ไม่เป็นพิษเป็นภัยด้วยสิ่งที่เป็นอันตราย เช่น การปลอมแปลง การโจมตีโดยคนตรงกลาง จุดเชื่อมต่อไร้สายอันธพาล และการโจมตีแบบฉีด SQL ล้วนเกี่ยวข้องกับการแอบอ้างบุคคลอื่น	
การใช้งานที่ไม่เหมาะสม:	เหตุการณ์ใดๆ ที่เกิดจากการละเมิดนโยบายการใช้งานที่ยอมรับได้ของ	

(Improper Usage)	องค์กรโดยผู้ใช้ที่ได้รับอนุญาต ยกเว้นหมวดหมู่ข้างต้น ตัวอย่างเช่น ผู้ใช้ติดตั้งซอฟต์แวร์แชร์ไฟล์ ส่งผลให้ข้อมูลที่ละเอียดอ่อนสูญหาย หรือผู้ใช้ทำกิจกรรมที่ผิดกฎหมายบนระบบ	
การสูญหายหรือถูกขโมยอุปกรณ์ (Loss or Theft of Equipment)	การสูญหายหรือถูกขโมยอุปกรณ์คอมพิวเตอร์หรือสื่อที่องค์กรใช้ เช่น แล็ปท็อป สมาร์ทโฟน หรือโทเค็นการตรวจสอบสิทธิ์	การดำเนินคดีความกับผู้ขโมยอย่างเด็ดขาด
อื่นๆ	การโจมตีที่ไม่เข้าข่ายประเภทอื่นๆ	

ตารางที่ 8 แนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ให้ความสำคัญกับแนวทางปฏิบัติที่แนะนำสำหรับการจัดการเหตุการณ์ทุกประเภท การให้คำแนะนำเฉพาะเจาะจงตามเวกเตอร์การโจมตีอยู่นอกเหนือขอบเขตของเอกสารเผยแพร่นี้ แนวทางดังกล่าวจะมีระบุไว้ในเอกสารเผยแพร่แยกต่างหากซึ่งกล่าวถึงหัวข้อการจัดการเหตุการณ์อื่นๆ เช่น NIST SP 800-83 เกี่ยวกับการป้องกันและการจัดการเหตุการณ์มัลแวร์

2) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ

3) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้องเช่น ผลกระทบต่อการทำงานของระบบ (Functional Impact) ผลกระทบต่อข้อมูล (Transformation Impact) และความสามารถในการกู้คืน (Recoverability Effort) เป็นต้น

4) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 2)

5) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย และข้อมูลดังกล่าว

ได้ระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้งาน บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสมโดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก 3)

6) ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้จัดให้มีการทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปีภายในวันที่ 31 มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก3 โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก 4)

ทั้งนี้ ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.2 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.3 ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication and Recovery)

การดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

1) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

2) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

3) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

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

5) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

ทั้งนี้ ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.3 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.4. ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

กำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม จะต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2560 และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง คือ ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

นอกจากนี้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้พิจารณาดำเนินการตามเอกสารแนบท้าย 2 ตารางที่ 2.4 ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 เพิ่มเติม

10.5. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมโรงงานอุตสาหกรรม ได้เตรียมการสำหรับจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก 5)

11. แผนเผชิญเหตุการณ์ผิดปกติด้านสารสนเทศที่เกี่ยวข้องกับความมั่นคงปลอดภัยสารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์

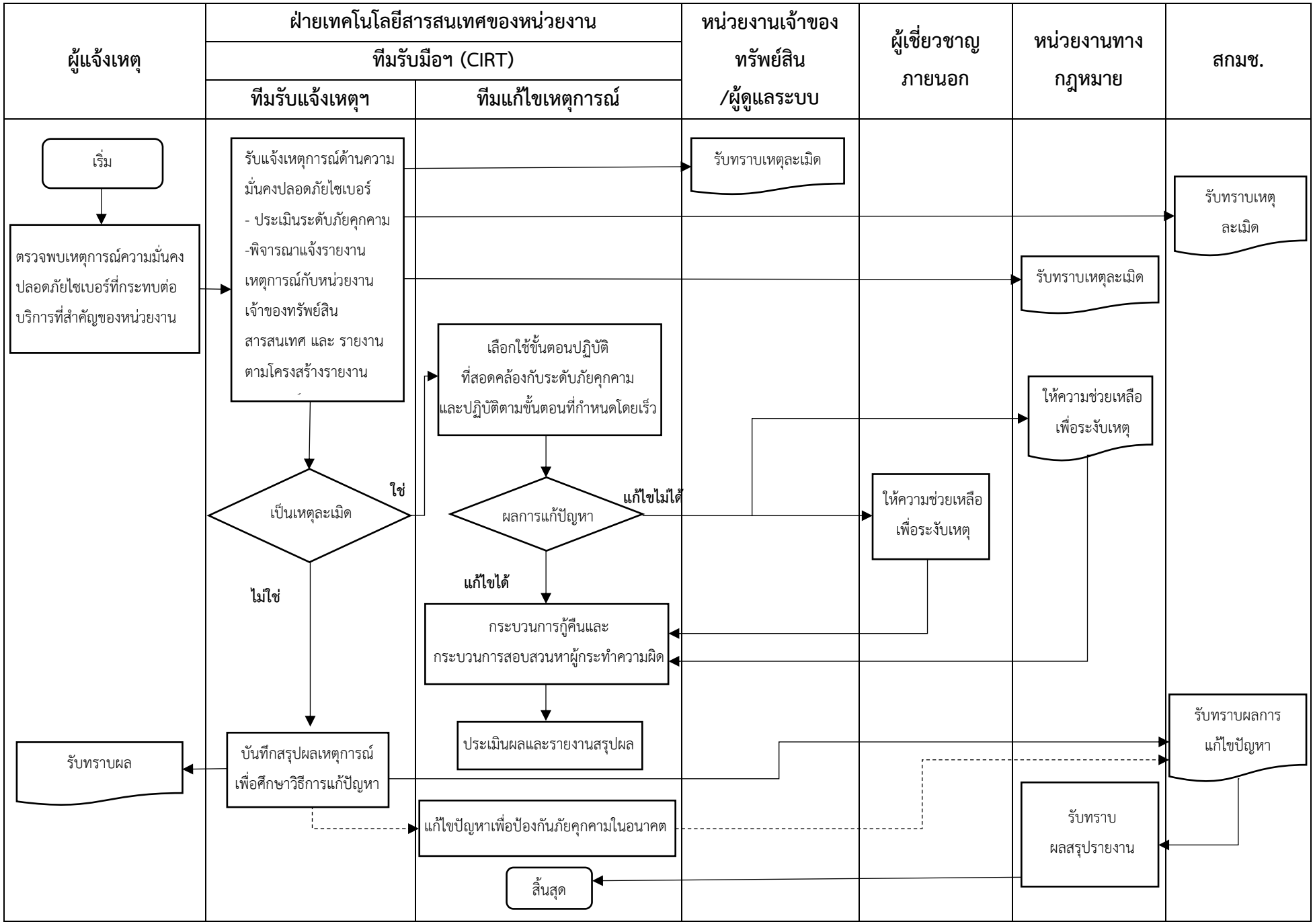
การจัดทำรายละเอียดแผนฯ เพื่อเตรียมความพร้อมกับสถานการณ์ที่เกิดขึ้นจริง โดยกำหนดให้มีการซักซ้อมการรับมือ การแลกเปลี่ยนข้อมูล รวมถึงการติดตามข่าวเกี่ยวกับภัยคุกคามทางไซเบอร์เพื่อเตรียมความพร้อมรับมือในภาวะวิกฤต จึงได้จัดทำเอกสารแผนเผชิญเหตุการณ์ผิดปกติด้านสารสนเทศที่เกี่ยวข้องกับความมั่นคง ปลอดภัย

สารสนเทศและความมั่นคงปลอดภัยทางไซเบอร์ (Playbook for Security Incident and Cybersecurity Incident) แบ่งตามหมวดหมู่ภัยคุกคาม ดังนี้

1. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt) ประกอบด้วย
   - การพยายามโจมตีแบบ SQL Injection
2. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance) ประกอบด้วย
   - การสแกนระบบเครือข่าย (Network Scanning)
3. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity) ประกอบด้วย
   - การละเมิดข้อมูล (Data Breach)
4. การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) ประกอบด้วย
   - กรณีระบบคอมพิวเตอร์ของ กรมโรงงานอุตสาหกรรม ถูกโจมตีโดย Ransomware
5. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion) ประกอบด้วย
   - การพยายามโจมตีแบบ Brute Force
6. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion) ประกอบด้วย
   - การถูกขโมยบัญชีผู้ใช้งานสื่อสังคมออนไลน์ของหน่วยงาน
7. การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)

ภาคผนวก 1

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



ภาคผนวก 2

ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

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

ภาคผนวก 3

ตัวอย่าง : บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น **(**ข้อเท็จจริง**,** สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ**)**
ตัวอย่าง 12/1/66 – 09.00 น.	ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน

ภาคผนวก 4

เอกสาร ก1 ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
1. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
2. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
3. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)
4. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
5. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[2] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

6. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ 0 หมวดหมู่ที่ 1 และหมวดหมู่ที่ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

เอกสาร ก2 แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ 1
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** โปรดระบุ **วันที่:** เลือกวันที่ **เวลา:** โปรดระบุ
ก1. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ
ก2. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก3. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก4. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์[3] ในระดับใด (มาตรา 60) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข1. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข2. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข3. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ 2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ 3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ 4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ 5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ 6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ 7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ 8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. 2564 (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ 0 1 และ 9 ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ข4. 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

ค1. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า 1 รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค2. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

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

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค3. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ 2

หมวด ง : รายละเอียดภัยคุกคาม

ง1. ข้อมูลการตรวจจับและการวิเคราะห์

ง1.1 <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (System Access)

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

ง1.2 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

ง1.3 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

ง1.4 <u>รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</u>

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 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

ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ) โปรดระบุ

ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

ง2. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

ง2.2 การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

เอกสาร ก3 แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกจู่โจมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[4]

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

ภาคผนวก 5

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
1	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
1.1	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
1.2	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
1.3	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
1.4	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
3	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
4	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ภาคผนวก 6

การวิเคราะห์ระบบที่ให้บริการของกรมโรงงานอุตสาหกรรมที่มีความสำคัญ

1. ระบบงานที่ให้บริการของกรมโรงงานอุตสาหกรรม

รายชื่อ	RTO	RPO	MTPD
ระบบบริการอินเทอร์เน็ตและเครือข่ายของกรมโรงงานอุตสาหกรรม	12 ชม.	24 ชม.	24 ชม.
ระบบทะเบียนโรงงาน	12 ชม.	24 ชม.	24 ชม.
ระบบงานทะเบียนเครื่องจักร	12 ชม.	24 ชม.	24 ชม.
ระบบจดทะเบียนเครื่องจักรออนไลน์	12 ชม.	24 ชม.	24 ชม.
ระบบการจัดการวัสดุที่ไม่ใช้แล้วทางอิเล็กทรอนิกส์	12 ชม.	24 ชม.	24 ชม.
ระบบงานวัตถุอันตราย	12 ชม.	24 ชม.	24 ชม.
เว็บไซต์กรมโรงงานอุตสาหกรรม	12 ชม.	24 ชม.	24 ชม.
ระบบโทรศัพท์บนเครือข่ายอินเทอร์เน็ต (IP Phone)	12 ชม.	24 ชม.	24 ชม.
ระบบขอรับบริการด้านอุปกรณ์และระบบเครือข่าย	24 ชม.	24 ชม.	24 ชม.
ระบบสารบรรณอิเล็กทรอนิกส์	24 ชม.	24 ชม.	24 ชม.
ระบบจองห้องประชุมของกรมโรงงานอุตสาหกรรม	24 ชม.	24 ชม.	24 ชม.

* หมายเหตุ

ระยะเวลาสูงสุดที่ยอมรับได้ให้ระบบหยุดทำงาน (Recovery Time Objective : RTO)

ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหายได้ (Recovery Point Objective : RPO)

ระยะเวลาที่ระบบหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD)

2. ผู้ดูแลระบบงานที่ให้บริการของกรมโรงงานอุตสาหกรรม และข้อมูลการติดต่อ

รายชื่อระบบงาน	เบอร์โทรติดต่อกรณีพบ Incident	
	กลุ่ม	เบอร์โทร
ระบบบริการอินเทอร์เน็ตและเครือข่ายของกรมโรงงานอุตสาหกรรม	กลุ่มบริการอุปกรณ์และระบบเครือข่าย	02-430-6316 ต่อ 2508
ระบบทะเบียนโรงงาน	กลุ่มบริการระบบสารสนเทศ 3	02-430-6316 ต่อ 2504
ระบบงานทะเบียนเครื่องจักร	กลุ่มบริการระบบสารสนเทศ 1	02-430-6316 ต่อ 2502
ระบบจดทะเบียนเครื่องจักรออนไลน์	กลุ่มบริการระบบสารสนเทศ 1	02-430-6316 ต่อ 2502
ระบบการจัดการวัสดุที่ไม่ใช้แล้วทางอิเล็กทรอนิกส์	กลุ่มบริการระบบสารสนเทศ 2	02-430-6316 ต่อ 2503
ระบบงานวัตถุอันตราย	กลุ่มบริการระบบสารสนเทศ 4	02-430-6316 ต่อ 2505

เว็บไซต์กรมโรงงานอุตสาหกรรม	กลุ่มบริการระบบสารสนเทศกลาง	02-430-6316 ต่อ 2507
ระบบโทรศัพท์บนเครือข่ายอินเทอร์เน็ต (IP Phone)	กลุ่มบริการอุปกรณ์และระบบเครือข่าย	02-430-6316 ต่อ 2508
ระบบขอรับบริการด้านอุปกรณ์และระบบเครือข่าย	กลุ่มบริการอุปกรณ์และระบบเครือข่าย	02-430-6316 ต่อ 2508
ระบบสารบรรณอิเล็กทรอนิกส์	กลุ่มบริการระบบสารสนเทศ 1	02-430-6316 ต่อ 2504
ระบบจองห้องประชุมของกรมโรงงานอุตสาหกรรม	กลุ่มบริการระบบสารสนเทศกลาง	02-430-6316 ต่อ 2507

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ.2564
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566
- NIST SP 800-61r2 Computer Security Incident Handling Guide
- ACSC Cyber Incident Response Plan Guidance

****

.....	.....
(นางสาวประนมพร โลกคำลือ)	(นายพรยศ กลั่นกรอง)
ผู้อำนวยการกลุ่มบริการอุปกรณ์และระบบเครือข่าย	รองอธิบดีกรมโรงงานอุตสาหกรรม
ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	รักษาราชการแทน อธิบดีกรมโรงงานอุตสาหกรรม
ผู้จัดทำ	ผู้อนุมัติ