



แผนการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ของ สำนักงานนโยบายและแผนการขนส่งและจราจร
กระทรวงคมนาคม

ประจำปีงบประมาณ พ.ศ. 2569



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



www.otp.go.th



แผนการรับมือเหตุภัยคุกคามทางไซเบอร์
(Cybersecurity Incident Response Plan)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. ขอบเขต	๑
๔. หน้าที่การทบทวนแผน	๑
๕. หน้าที่ในการดำเนินการตามแผน	๑
๖. รายละเอียดการบังคับใช้เอกสาร	๒
๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง	๒
๘. นิยาม	๒
๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์	๓
๑๐. ขั้นตอนการรับมือ	๘
ภาคผนวก ๑ แผนผังการรับมือเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท	๑๔
ภาคผนวก ๒ ตัวอย่าง : บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์	๒๒
ภาคผนวก ๓ บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)	๒๓
ภาคผนวก ๔	
เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง	๒๔
เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์	๒๕
เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี	๒๘
ภาคผนวก ๕ ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)	๓๑
ภาคผนวก ๖ กระบวนการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ สำหรับหน่วยงานของรัฐ	๓๒

๑. หลักการและเหตุผล

แผนการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง ดังนี้

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายในหรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. ด้วย

ทั้งนี้ เพื่อดำเนินการด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เป็นไปตาม มาตรา ๔๔ แห่ง พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สนข. จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้น เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคต และเป็นไปตามกรอบมาตรฐานด้านความมั่นคงปลอดภัยทางไซเบอร์ (NIST Cybersecurity Framework) ซึ่งประกอบด้วย ๕ ขั้นตอนหลัก ได้แก่ Identify (ระบุ), Protect (ป้องกัน), Detect (ตรวจจับ), Respond (ตอบสนอง) และ Recover (กู้คืน)

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุการณ์คุกคามทางไซเบอร์ที่เกิดขึ้นใน สนข. โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่าง ๆ ภายใน สนข. การกำหนดประเภทของเหตุการณ์คุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุการณ์คุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุการณ์คุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของ สนข.

๓. ขอบเขต

แผนการรับมือฯ ฉบับนี้ ใช้อยู่รับมือเหตุการณ์คุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ และข้อมูลดิจิทัลของ สนข. รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ที่เข้าถึงระบบงานสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

ศทท. มีหน้าที่จัดทำ ทบทวน และขออนุมัติแผนการรับมือฯ ฉบับนี้ถึงผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร ผ่านผู้ที่ได้รับมอบอำนาจให้ดูแลงานด้านความมั่นคงปลอดภัยไซเบอร์ ได้แก่ ผู้บริหารจัดการความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ประจำ สนข.

๕. หน้าที่ในการดำเนินการตามแผน

ศทท. มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนการรับมือเหตุการณ์คุกคามทางไซเบอร์ ฉบับนี้ โดยมีกลุ่มงานสนับสนุนภายในได้ ศทท. ประกอบด้วย กลุ่มพัฒนาระบบคอมพิวเตอร์เครือข่าย (กพค.) กลุ่มพัฒนาระบบข้อมูลสารสนเทศ (กขส.) และกลุ่มนโยบายและบริหารสารสนเทศ (กนส.) รวมถึงหน่วยงานหรือกลุ่มงานที่มีส่วนเกี่ยวข้องกับระบบสารสนเทศหรือภัยคุกคามทางไซเบอร์

๖. รายละเอียดการบังคับใช้เอกสาร

รายละเอียดที่เกี่ยวข้องกับเอกสาร ดังต่อไปนี้

๖.๑ รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	นายทรงเกียรติ ตะเภาทอง
ผู้ดำเนินการตามเอกสาร (Owner)	ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
วันที่จัดทำเอกสาร (Date created)	๑๕ พฤษภาคม ๒๕๖๙
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข.
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	๒๕ มิถุนายน ๒๕๖๙
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

๖.๒. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๒	๒๘ สิงหาคม ๒๕๖๙	ผู้อำนวยการสำนักงานนโยบายและแผนการขนส่งและจราจร	ฉบับล่าสุด

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๗.๑ แผนนโยบายและแนวปฏิบัติแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข.

๗.๒ นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลของ สนข.

๗.๓ ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๘. นิยาม

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

เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber Threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมีมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ^๑ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๙. บทบาทหน้าที่และโครงสร้างที่รับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงานกรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อ และมอบหมายให้มีผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ ครอบคลุมตลอดระยะเวลา ๒๔ ชั่วโมง / ๗ วัน

ลำดับ	ชื่อ - นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายณฤทธิ มัยรัตน์ นวช.คอมฯ ขฟ. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๙ ๔๙๑๕ ๑๕๓๖	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๒	นายพิสิฐ ป้อมทอง นวช.คอมฯ ชก. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๘ ๔๓๑๐ ๐๒๐๘	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๓	นายชัยวัฒน์ ธรรมาสถิตนุกุล นวช.คอมฯ ชก. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๘ ๑๒๐๖ ๕๒๕๔	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๔	นายทรงเกียรติ ตะเภาทอง นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๙ ๗๒๔๕ ๕๓๔๒	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๕	นางสาวรุ่งทิพย์ ศรีบุญชู นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๘ ๗๔๗๒ ๕๖๒๕	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๖	นางสาวชนันดา ดวงพรหม นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง / ๗ วัน	โทร. ๐๙ ๓๕๓๖ ๖๓๖๔	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

^๑ เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ มีนิยามตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ.2566

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team : CIRT)

สนข. ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (Centralize) ตามบริบทของหน่วยงาน^๒ โดย สนข. ระบุรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นางสาวจิรกร ห้วยหงษ์ทอง ผอ.ศทท. ในฐานะผู้บริหารจัดการ ความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ประจำ สนข.	ภายใน : ๔๐๐๘ มือถือ : ๐๘ ๑๑๓๘ ๓๘๔๐ email : Jirungruk.hua@otp.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหาร เทคโนโลยีสารสนเทศ ของหน่วยงาน
๒	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. หน.กพค. ศทท.	ภายใน : ๔๕๑๕ มือถือ : ๐๙ ๔๙๑๕ ๑๕๓๖ email : narit.mai@otp.go.th	รองหัวหน้าทีม รับมือฯ (Deputy Team Manager)	ทำหน้าที่แทน กรณี หัวหน้าทีมรับมือฯ ไม่อยู่/ ไม่สามารถปฏิบัติงานได้
๓	นายพิสิฐ ป้อมทอง นวช.คอมฯ ขก. ศทท.	ภายใน : ๔๕๑๐ มือถือ : ๐๘ ๔๓๑๐ ๐๒๐๘ email : pisit.pom@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๔	นายชัยวัฒน์ ธรรมาสถิตินุกูล นวช.คอมฯ ขก. ศทท.	ภายใน : ๔๐๑๔ มือถือ : ๐๘ ๑๒๐๖ ๕๒๕๔ email : chaiwat.tha@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๕	นายทรงเกียรติ ตะเภาทอง นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๔๕ มือถือ : ๐๙ ๗๒๔๕ ๕๓๔๒ email : srongkiat.tap@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๖	นางสาวรุ่งทิพย์ ศรีบุญชู นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๘๑ มือถือ : ๐๘ ๗๔๗๒ ๕๖๒๕ email : roongthip.sri@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๗	นางสาวชนันดา ดวงพรหม นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๘๑ มือถือ : ๐๙ ๓๕๓๖ ๖๓๖๔ email : chananda.dua@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๘	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. หน.กพค. ศทท.	ภายใน : ๔๕๑๕ มือถือ : ๐๙ ๔๙๑๕ ๑๕๓๖ email : narit.mai@otp.go.th	เจ้าหน้าที่เทคนิคฯ (Technical leader)	ทำหน้าที่ให้ความเห็น เกี่ยวกับแนวทางที่เหมาะสม ในการควบคุมผลกระทบ จากภัยคุกคามทางไซเบอร์

^๒ หน่วยงานอาจเลือกใช้โมเดลโครงสร้างทีมรับมือฯ แบบรวมศูนย์ (Centralize) แบบกระจาย (Distributed) แบบให้คำปรึกษา (Coordinating) หรือแบบอื่นๆ ตามบริบทของหน่วยงานที่อาจแตกต่างกัน ทั้งนี้ ท่านสามารถศึกษาเพิ่มเติมได้ที่ NIST SP 800-61r2 ข้อที่ ๒.๔ หน้า ๑๓

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ได้กำหนดบุคคลดังต่อไปนี้เพื่อทำหน้าที่สนับสนุนการดำเนินการของแผนการรับมือฯ ฉบับนี้ ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสุรพงษ์ เมียนมิตร รองผู้อำนวยการ สนช.	ภายใน : ๐ ๒๒๑๖ ๙๘๘๙ มือถือ : email : surapong.mea@otp.go.th	ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง ระดับกรม (DCIO) ประจำ สนช.	ทำหน้าที่ผู้บริหารจัดการ ควบคุมสถานการณ์ และผลกระทบจาก ภัยคุกคามทางไซเบอร์
๒	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. หน.กพค. ศทท.	ภายใน : ๔๕๑๕ มือถือ : ๐๙ ๔๙๑๕ ๑๕๓๖ email : narit.mai@otp.go.th	เจ้าหน้าที่ด้านการปฏิบัติ ตามกฎหมาย (Compliance)	ผู้ควบคุมการจัดการ กับภัยความเสี่ยง ที่เกิดขึ้นให้สอดคล้อง และเป็นไปตามกฎหมาย
๓	นายทรงเกียรติ ตะเกาทอง นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๔๕ มือถือ : ๐๙ ๗๒๔๕ ๕๓๔๒ email : srongkiat.tap@otp.go.th	ผู้ทดสอบเจาะระบบ	ดำเนินการตรวจหา ช่องโหว่ของระบบ
๔	นายณัฐกรฤศ พุฒแก้ว ฝ่ายนิติการ สนช.	ภายใน : ๑๐๒๕ มือถือ : ๐๖ ๓๒๐๓ ๔๓๒๘ email : nutthakrit.put@otp.go.th	ผู้เชี่ยวชาญด้านกฎหมาย	ดำเนินการด้านกฎหมาย ที่เกี่ยวข้อง
๕	นางสาวจิรังกร ห้วยหงษ์ทอง ผอ.ศทท.	ภายใน : ๔๐๐๘ มือถือ : ๐๘ ๑๑๓๘ ๓๘๔๐ email : jirungruk.hua@otp.go.th	ผู้บริหารจัดการความเสี่ยง	บริหารจัดการกับภัย ความเสี่ยงที่เกิดขึ้น ให้เป็นไปตามแนวทาง และแผนการรับมือ
๖	นางสาวจิรังกร ห้วยหงษ์ทอง ผอ.ศทท.	ภายใน : ๔๐๐๘ มือถือ : ๐๘ ๑๑๓๘ ๓๘๔๐ email : jirungruk.hua@otp.go.th	ผู้รับผิดชอบด้านสื่อสารองค์กร	ดำเนินการประสาน ผู้ที่เกี่ยวข้องทั้งภายใน และภายนอก

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

สนช. จัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยไซเบอร์ เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานกำกับดูแล (Regulator) ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) และผู้ให้บริการภายนอกของหน่วยงาน ดังนี้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการ การรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เบอร์โทรศัพท์ : ๐ ๒๑๔๒ ๖๘๘๘ email : thaicert@ncsa.or.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารซี) ชั้น ๑๐ ศูนย์ราชการ เฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	สำนักงานคณะกรรมการ การรักษาความมั่นคง ปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	หน่วยงานกำหนดนโยบาย มาตรการ แนวทางการรักษา ความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานภาครัฐ และภาคเอกชน ในการป้องกัน รับมือ และลดความเสี่ยงจาก ภัยคุกคามทางไซเบอร์ ภายในประเทศ
๒	นายจิระพงศ์ เทพพิทักษ์ รองปลัดกระทรวง คมนาคม	เบอร์โทรศัพท์ : ๐ ๒๒๘๓ ๓๑๓๐ email : saraban@mot.go.th ที่อยู่สำนักงาน : ๓๘ ถนนราชดำเนินนอก แขวงวัดโสมนัส เขตป้อมปราบศัตรูพ่าย กรุงเทพฯ ๑๐๑๐๐	กระทรวงคมนาคม	ผู้บริหารเทคโนโลยี สารสนเทศระดับสูงระดับ กระทรวง (MCIO) ประจำ กระทรวงคมนาคม และหน่วยงานกำกับดูแล
๓	ศูนย์ประสานการรักษา ความมั่นคงปลอดภัย ระบบคอมพิวเตอร์ แห่งชาติ (ThaiCERT)	เบอร์โทรศัพท์ : ๐ ๒๑๔๒ ๓๕๓๑ email : info@turnonsolution.co.th ที่อยู่สำนักงาน : ๑๒๐ หมู่ ๓ อาคารรัฐประศาสนภักดี (อาคารซี) ชั้น ๑๐ ศูนย์ราชการ เฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	ThaiCERT	หน่วยงานเฝ้าระวังความเสี่ยง ในการเกิดภัยคุกคาม ทางไซเบอร์ ติดตาม วิเคราะห์ และประมวลผลข้อมูลเกี่ยวกับ ภัยคุกคามทางไซเบอร์ และ การแจ้งเตือนเกี่ยวกับภัย คุกคามทางไซเบอร์
๔	นายประติมากร ทองเพชร เจ้าหน้าที่โครงการ	เบอร์โทรศัพท์ : ๐๙ ๔๒๕๑ ๒๙๒๒ email : info@turnonsolution.co.th ที่อยู่สำนักงาน : บริษัท เทิร์นออนโซลูชั่น จำกัด เลขที่ ๑๙๘/๙๓ หมู่บ้านวิลล่า โนวา วัชรพล สายไหม ถนนสายไหม แขวงสายไหม เขตสายไหม กรุงเทพมหานคร	บริษัท เทิร์นออนโซลูชั่น จำกัด	ผู้รับจ้างบำรุงรักษาระบบ คอมพิวเตอร์

๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

สนช. จัดทำแนวทางการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ (Incident Reporting Structure) เพื่อเป็นแนวทางในการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์สำหรับ สนช. ซึ่งเป็นหน่วยงานของรัฐ ที่มีได้เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยสอดคล้องกับขั้นตอนการดำเนินการมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังนี้ (รายละเอียดปรากฏตามภาคผนวก ๖)

๙.๔.๑ การแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์ระหว่างขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ให้ดำเนินการ ดังนี้

(๑) การแจ้งเหตุภัยคุกคามทางไซเบอร์ ให้ดำเนินการดังนี้

(๑.๑) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ สนช. ที่ทำให้บริการของหน่วยงานด้อยประสิทธิภาพลง หรือเสียหายจนไม่สามารถทำงานหรือให้บริการได้ หรือทำให้การทำงานของหน่วยงานล้มเหลว หรือมีเหตุอันสมควรเชื่อได้ว่าการก่อภัยคุกคามทางไซเบอร์นั้นกระทบหรืออาจกระทบต่อความสงบเรียบร้อยของประชาชน หรือเป็นภัยต่อความมั่นคงของรัฐ หรืออาจทำให้ประเทศหรือส่วนใดส่วนหนึ่งของประเทศตกอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา การรบหรือการสงคราม ให้หน่วยงานแจ้งไปยัง สกมช. ภายใน ๒๔ ชั่วโมง นับแต่ทราบถึงเหตุภัยคุกคามทางไซเบอร์นั้น และแจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยการนำส่งเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง หรือนำส่งเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ ที่มีข้อมูลครบถ้วนตามที่กำหนดไว้ในเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง ทั้งนี้ ให้เพิ่มเติมข้อมูลอื่นใดตามที่ระบุในเอกสาร ก๒ เท่าที่สามารถกระทำได้ และจัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย และให้ดำเนินการรายงานภัยคุกคามทางไซเบอร์ ตามความในข้อ ๙.๔.๑ (๒.๑)

(๑.๒) ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ต่อระบบสารสนเทศของ สนช. แต่ไม่ส่งผลกระทบในทำนองเดียวกันกับกรณีในข้อ ๙.๔.๑ (๑) ให้หน่วยงานดังกล่าวแจ้งไปยัง สกมช. โดยเร็ว และแจ้งไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด โดยการนำส่งเอกสาร ก๑ ข้อมูลที่ต้องแจ้ง หรือนำส่งเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ ที่มีข้อมูลครบถ้วนตามที่สามารถกระทำได้ และจัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย และอาจดำเนินการรายงานภัยคุกคามทางไซเบอร์ ตามความในข้อ ๙.๔.๒ (๒.๒)

(๒) การรายงานภัยคุกคามทางไซเบอร์ ให้ดำเนินการ ดังนี้

(๒.๑) ในกรณีที่เหตุภัยคุกคามทางไซเบอร์นั้น เป็นเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบสารสนเทศของของ สนช. ให้รายงานไปยัง สกมช. ภายใน ๒๔ ชั่วโมง และรายงานไปยังหน่วยงานควบคุมหรือกำกับดูแลของตนภายในเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนดโดยการนำส่งเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ หน่วยงานอาจจะระบุข้อมูลเฉพาะเท่าที่ทราบหรือสามารถระบุได้ในขณะนั้น ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย ทั้งนี้หากมิได้มีการแจ้งภัยคุกคามฯ ตามข้อ ๙.๔.๑ (๑) ให้ทำการรายงานตามข้อนี้เป็นการแจ้งเหตุภัยคุกคามไปในคราวเดียวกัน

หากไม่อาจหรือไม่สามารถดำเนินการจัดเตรียมข้อมูลและจัดส่งรายงานได้ภายใน ๒๔ ชั่วโมง ให้แจ้งเหตุขัดข้องดังกล่าวแก่ สกมช. ทราบโดยเร็ว แต่ต้องไม่เกินระยะเวลา ๒๔ ชั่วโมง นับแต่ทราบถึงเหตุภัยคุกคามทางไซเบอร์นั้น

(๒.๒) ในกรณีที่เกิดภัยคุกคามที่มีลักษณะตามข้อ ๔.๑.๑ (๒) สนข. อาจแบ่งปันข้อมูลเกี่ยวกับภัยคุกคามทางไซเบอร์โดยรายงานข้อมูลตามที่กำหนดไว้ในเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย ทั้งนี้ หากมิได้มีการแจ้งภัยคุกคามฯ ตามข้อ ๔.๔.๑ (๒) ให้นำการรายงานตามข้อนี้เป็นการแจ้งเหตุภัยคุกคามไปในคราวเดียวกัน

๔.๔.๒ การรายงานเหตุภัยคุกคามทางไซเบอร์เพิ่มเติม ระหว่างขั้นตอนที่ ๓ : การระงับภัยคุกคามทางไซเบอร์ ปรียบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ

กรณี สนข. มีความคืบหน้าหรือมีข้อมูลเพิ่มเติมในระหว่างการระงับภัยคุกคามทางไซเบอร์ ปรียบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ อันนอกเหนือจากการรายงานภัยคุกคามทางไซเบอร์ตามกรณี ข้อ ๔.๔.๒ ให้หน่วยงานปรับปรุงเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ฉบับที่ได้จัดส่งต่อ สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ตามข้อ ๔.๑.๒ ให้สอดคล้องกับข้อมูลที่หน่วยงานได้สืบทราบเพิ่มมากขึ้นในระหว่างการดำเนินการรับมือและแก้ไขภัยคุกคามทางไซเบอร์และจัดส่งรายงานที่ได้ปรับปรุงเพิ่มเติมไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย

๔.๔.๓ การรายงานปิดเหตุภัยคุกคามทางไซเบอร์ ระหว่างขั้นตอนที่ ๔ : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

เมื่อเหตุภัยคุกคามทางไซเบอร์ตามกรณีข้อ ๔.๔.๒ สิ้นสุดลง ให้ สนข. เพิ่มเติมข้อมูลลงในเอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์ฉบับที่ได้จัดส่งไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตนตามข้อ ๔.๔.๒ ให้ครบถ้วน และจัดส่งรายงานที่ปรับปรุงสมบูรณ์แล้วไปยัง สกมช. และหน่วยงานควบคุมหรือกำกับดูแลของตน ผ่านช่องทางอิเล็กทรอนิกส์ที่มีความปลอดภัย

๑๐. ขั้นตอนการรับมือ

แผนการรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๔.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรียบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ รวมถึงแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ สนข. ดังนี้

๑๐.๑ ขั้นตอนการเตรียมการ (Preparation)

สนข. มีมาตรการเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) ซึ่งเป็นสิ่งที่ต้องดำเนินการในระยะเริ่มต้นเพื่อให้มีความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อมการจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือโดยดำเนินการ ดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๙.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๙.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และการติดต่อไปยังหน่วยงาน CIRT ต่างๆ

(๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสารของบุคลากร กลไกรายงานเหตุการณ์ ห้องประชุม War Room เป็นต้น

(๕) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน โดยหน่วยงานอาจดูตัวอย่างการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ได้ (รายละเอียดปรากฏตามภาคผนวก ๑)

ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมินปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๒ ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยดำเนินการดังต่อไปนี้

(๑) สนข. ได้ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิดขึ้นกับหน่วยงาน โดยรูปแบบการโจมตีที่ควรจัดเตรียมแนวทางรับมือไว้นั้น อาจพิจารณาได้จาก Attack Vector ที่หน่วยงานมี เช่น มีการอนุญาตให้ใช้งานอุปกรณ์แบบถอดได้ (External/Removable Media) ซึ่งมีความเสี่ยงต่อการเผยแพร่มัลแวร์ หรือมีการให้บริการเว็บไซต์ที่เสี่ยงต่อการโจมตีแบบ Cross-site Scripting เป็นต้น

(๒) สนข. ดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น

(๓) สนข. จัดทำแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (Functional impact) ผลกระทบต่อข้อมูล (Information impact) และความสามารถในการกู้คืน (Recoverability effort)^๓ เป็นต้น

^๓ หน่วยงานอาจพิจารณากำหนดระดับความรุนแรงภัยคุกคามออกเป็น ๓ ประเภท โดยศึกษาเพิ่มเติมได้ที่ NIST SP 800-61r2 ข้อที่ ๓.๒.๖ หน้าที่ ๓๒

ตารางที่ ๑ ตัวอย่างเกณฑ์การประเมินระดับของภัยคุกคาม

ความรุนแรง	คำอธิบาย	การตอบสนองต่อเหตุการณ์
ต่ำ (Low)	ส่งผลกระทบต่อหน่วยงานในวงจำกัด เช่น เกิดการหยุดชะงักของการให้บริการเล็กน้อย หรือกระทบแค่หน่วยงานเดียว สามารถกู้คืนโดยใช้ทรัพยากรที่มีได้ความเสียหายทางการเงินต่ำ ไม่ส่งผลกระทบต่อชื่อเสียงหรือความเชื่อมั่นของสาธารณะ หรือไม่เกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแล	แก้ไขภายใน ๗๒ ชั่วโมง
ปานกลาง (Medium)	ส่งผลกระทบต่อหน่วยงานในระดับปานกลาง เช่น เกิดการหยุดชะงักของการให้บริการที่ยาวนานขึ้น กระทบหลายหน่วยงาน สามารถกู้คืนได้แต่ต้องมีการจัดหาทรัพยากรเพิ่ม มีความเสียหายทางการเงินมากขึ้น เริ่มส่งผลกระทบต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมาย หรือหน่วยงานกำกับดูแลในระดับไม่ร้ายแรง	แก้ไขภายใน ๔๘ ชั่วโมง
สูง (High)	ส่งผลกระทบอย่างมากต่อหน่วยงาน เช่น ระบบสารสนเทศบางส่วนถูกทำลาย การดำเนินงานหยุดชะงักอย่างมากในช่วงเวลาหนึ่ง เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก ข้อมูลสำคัญจำนวนมากสูญหาย ความเสียหายทางการเงินสูง ส่งผลกระทบอย่างมากต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับร้ายแรง	แก้ไขภายใน ๒๔ ชั่วโมง
สูงมาก (Extreme)	ส่งผลกระทบอย่างร้ายแรงต่อหน่วยงาน เช่น มีภัยคุกคามต่อชีวิต ระบบสารสนเทศหลักถูกทำลาย การดำเนินงานทั้งหมดหยุดชะงักจนต้องปิดการให้บริการ ไม่สามารถทำการกู้คืนได้ ข้อมูลสำคัญจำนวนมากสูญหายและถูกนำไปเผยแพร่ต่อสาธารณะ ความเสียหายทางการเงินสูงมาก ส่งผลกระทบอย่างรุนแรงต่อชื่อเสียงและความเชื่อมั่นของสาธารณะ หรือเกี่ยวข้องกับการรายงานต่อหน่วยงานด้านกฎหมายหรือหน่วยงานกำกับดูแลในระดับวิกฤติ	แก้ไขภายใน ๔ ชั่วโมง

(๔) สนช. จัดทำบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๒)

(๕) มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) ที่บันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอน ตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย โดยระบุรายละเอียด เวลาที่เกิดเหตุตลอดถึงระยะเวลาที่ใช้ระงับเหตุด้วย ทั้งนี้ ควรบันทึกข้อมูลดังกล่าว โดยระบบวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๓)

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

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

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามข้อ ๕ แห่งประกาศฯ ฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยัง สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมหรือกำกับดูแล จะต้องจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๔) การส่งข้อมูลจะต้องส่งผ่านช่องทางที่มีความมั่นคงปลอดภัย มีการเข้ารหัสของข้อมูลที่เหมาะสม และส่งผ่านช่องทางที่สำนักงานกำหนด

นอกจากนี้ หน่วยงานจะพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery)

เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปรามปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์

ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปราม ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปราม ภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

- (๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- (๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
- (๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์
- (๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึง การได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน
- (๕) ดำเนินการตามระเบียบวิธีการทำงานมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการ ด้านนิติวิทยาศาสตร์/การกู้คืน และการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้ หน่วยงานจะพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๑๐.๔ ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)

เป็นการดำเนินการที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity) นั้น หน่วยงานควรกำหนดขั้นตอนวิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทาง ที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการ ทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุง การดำเนินการเพื่อป้องกันการเกิดซ้ำ

นอกจากนี้ หน่วยงานจะพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๔ ในประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการ ป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

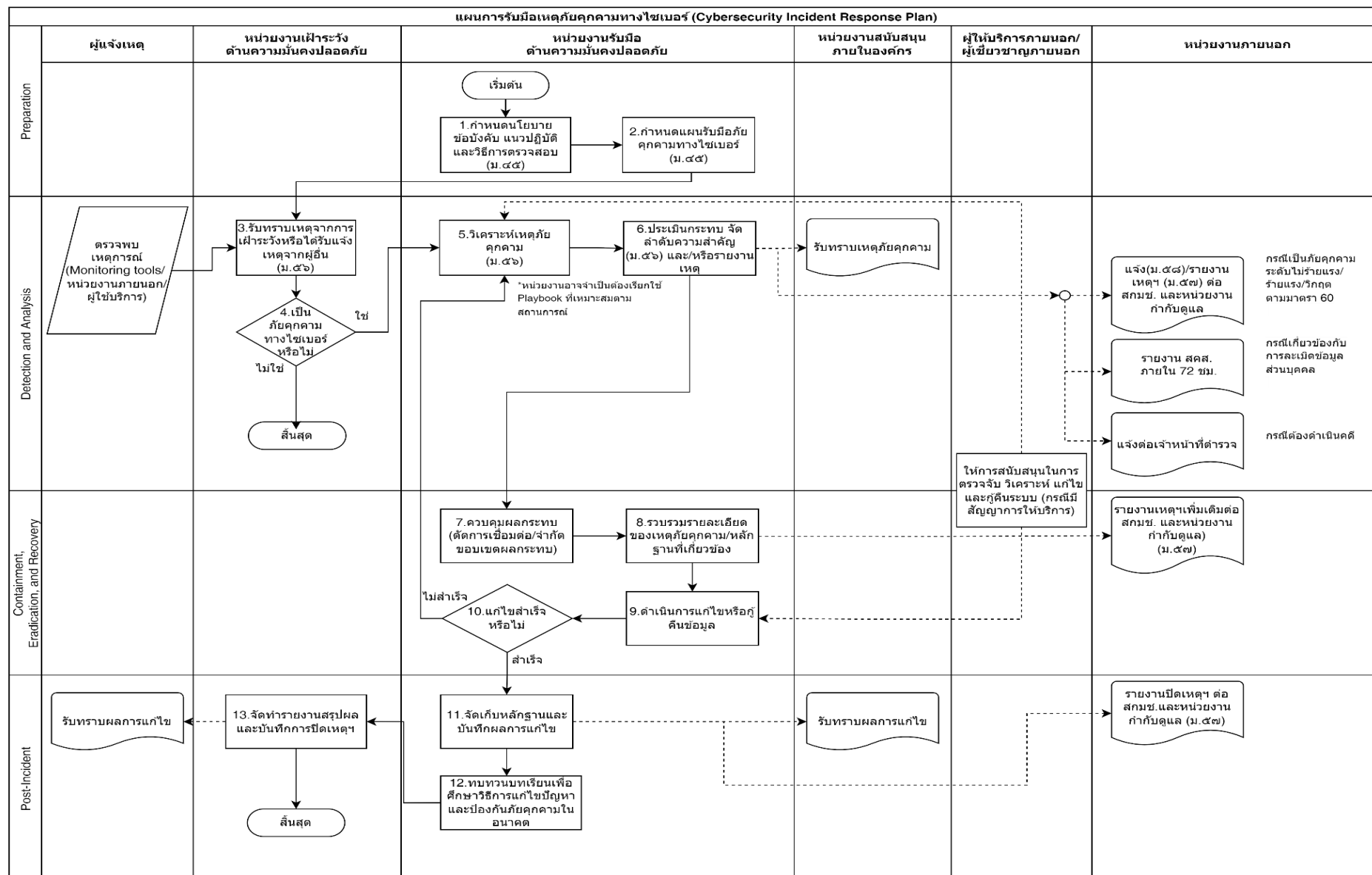
๑๐.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้งานหน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียด ปรากฏตามภาคผนวก ๕)

ภาคผนวก

ภาคผนวก ๑ แผนผังการรับมือเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท

๑. แผนผังการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)



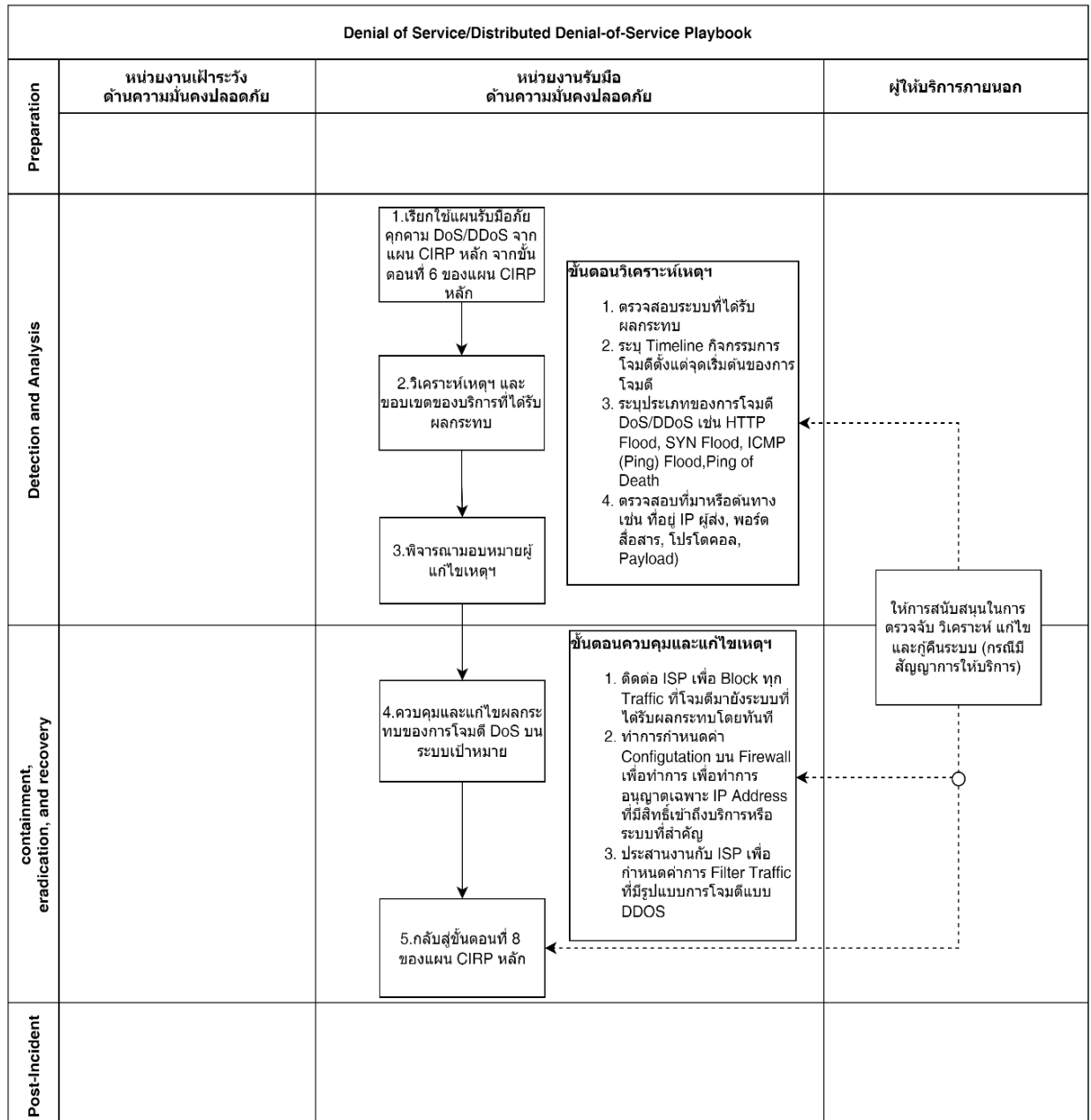
คำอธิบายแผนการรับมือเหตุการณ์คุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการเตรียมการ (Preparation)		
๑	กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหาร ของหน่วยงานกำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้อง ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา ๑๓ วรรคหนึ่ง (๔))
๒	กำหนดแผนการรับมือภัยคุกคาม ทางไซเบอร์ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผน การรับมือภัยคุกคามทางไซเบอร์ โดยระบุภัยคุกคาม ทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอน และวิธีการในการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ กำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มี การทดสอบแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)		
๓	รับทราบเหตุจากการเฝ้าระวังหรือได้รับ แจ้งเหตุจากผู้อื่น (ม.๕๖)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ได้รับทราบเหตุ จากการเฝ้าระวัง (Monitoring tools) หรือได้รับแจ้งเหตุ จากผู้อื่นที่ตรวจพบเหตุการณ์ เช่น หน่วยงานภายนอก หรือผู้ใช้บริการ
๔	เป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณา เหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
๕	วิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณา ประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียด แหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม ข้อมูล จำนวนระบบ บริการ หรือสินทรัพย์ที่ได้รับผลกระทบ
๖	ประเมินกระทบ และจัดลำดับ ความสำคัญ (ม.๕๖)	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการ ประเมินกระทบ และจัดลำดับความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคาม ทางไซเบอร์ หมายเหตุ: หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์ ๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุ ภัยคุกคามทางไซเบอร์ต่อหน่วยงานต่าง ๆ <ul style="list-style-type: none">กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤต ตามมาตรา ๖๐ หน่วยงานต้องแจ้งเหตุภัยคุกคาม (มาตรา ๕๘) (แบบฟอร์ม ก.๑ หรือมีข้อมูลเทียบเท่า) และ/หรือรายงาน

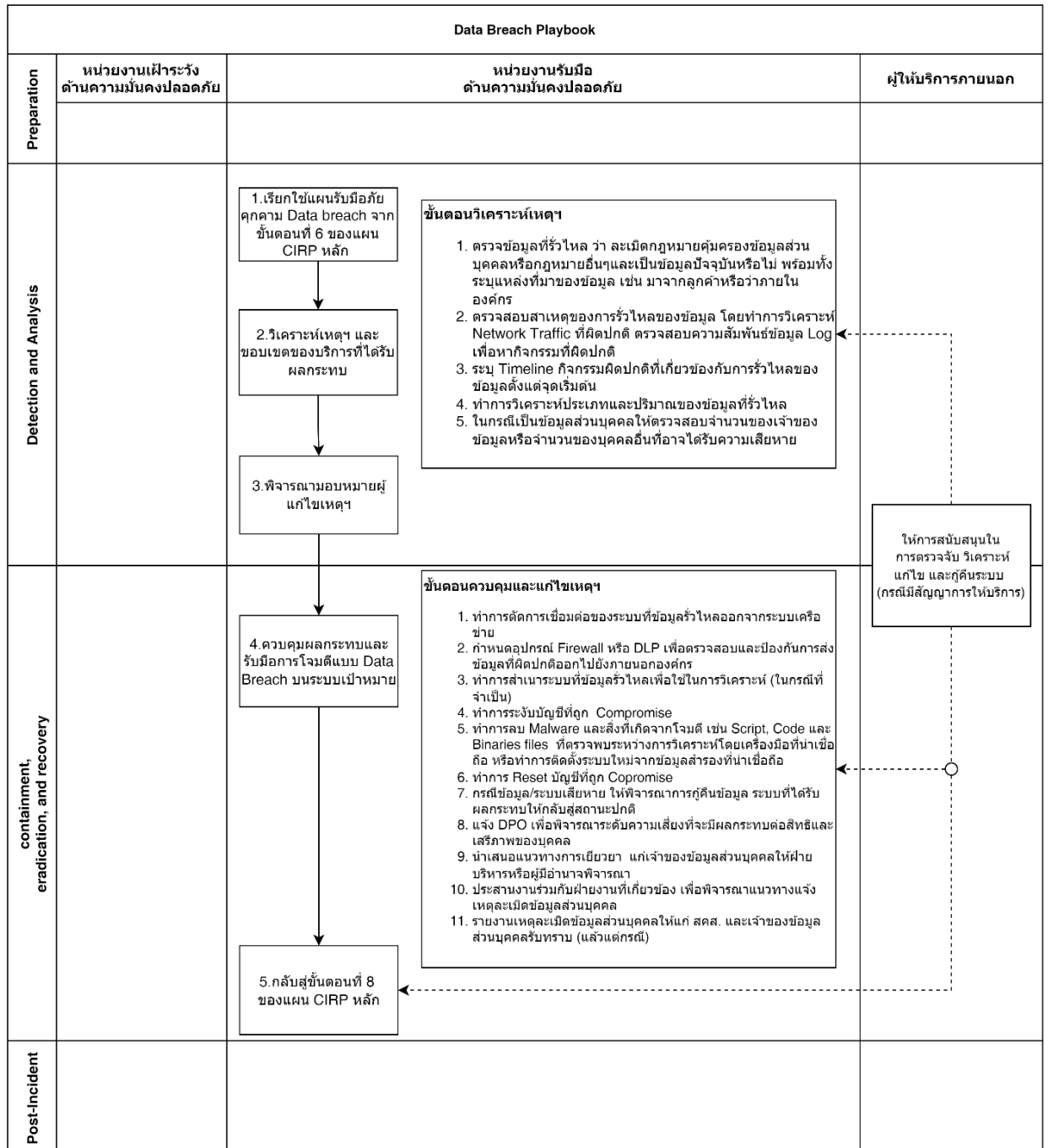
ลำดับ	หัวข้อ	คำอธิบาย
		<p>เหตุภัยคุกคาม (มาตรา ๕๗) (แบบฟอร์ม ก.๒) ต่อ สกมช. และหน่วยงานกำกับดูแล</p> <ul style="list-style-type: none"> ■ กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. ■ กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้น เหตุนั้นเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้องแจ้งไปยัง เจ้าหน้าที่ตำรวจเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปรามปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery)		
๗	ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/ จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัด ขอบเขต (Containment) ผลกระทบของเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำการกำจัดสาเหตุ (Eradicate the incident) กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคาม อื่น ๆ
๘	รวบรวมรายละเอียดของเหตุภัย คุกคาม/หลักฐานที่เกี่ยวข้อง	<p>๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึก เหตุการณ์ และดำเนินการจัดเก็บรักษาหลักฐานเกี่ยวกับ เหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึง การได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน</p> <p>๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงาน เหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)</p>
๙	ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งาน กระบวนการกู้คืน (Recovery Process)
๑๐	แก้ไขสำเร็จหรือไม่	<p>หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาว่า ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะ พร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบ กลับมาทำงานได้ตามปกติ ให้ดำเนินการต่อที่ขั้นตอนที่ ๑๑ หากยังไม่สามารถแก้ไขได้ ให้ดำเนินการขั้นตอนที่ ๕ ซ้ำ เพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง</p>
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๑๑	จัดเก็บหลักฐานและบันทึกผลการแก้ไข	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษา ข้อมูล และพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการ ทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์ หรือดำเนินคดี

ลำดับ	หัวข้อ	คำอธิบาย
		๒. บันทึกผลการแก้ไขเหตุการณ์ภัยคุกคามและวิธีการแก้ไข เพื่อจัดเก็บเป็นบทเรียน ๓. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๑๒	ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไข ปัญหา และป้องกันภัยคุกคามใน อนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุม ทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนด แนวทางในการป้องกันการเกิดเหตุซ้ำ หรือป้องกันภัยคุกคาม อื่น ๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
๑๓	จัดทำรายงานสรุปผลและบันทึก การปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงาน สรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไข ไปยังผู้เกี่ยวข้องให้รับทราบ

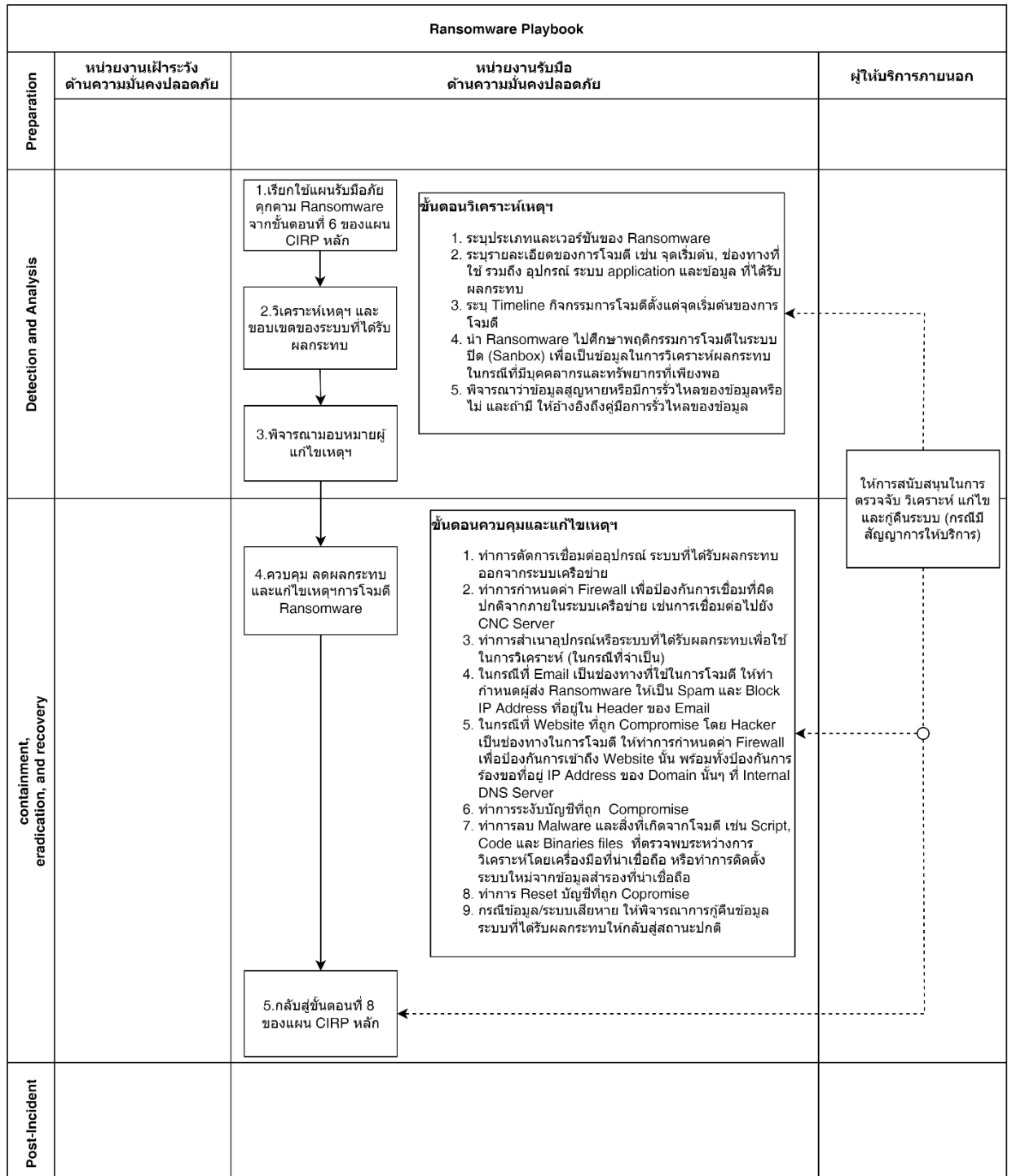
๒. ขั้นตอนการรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook)



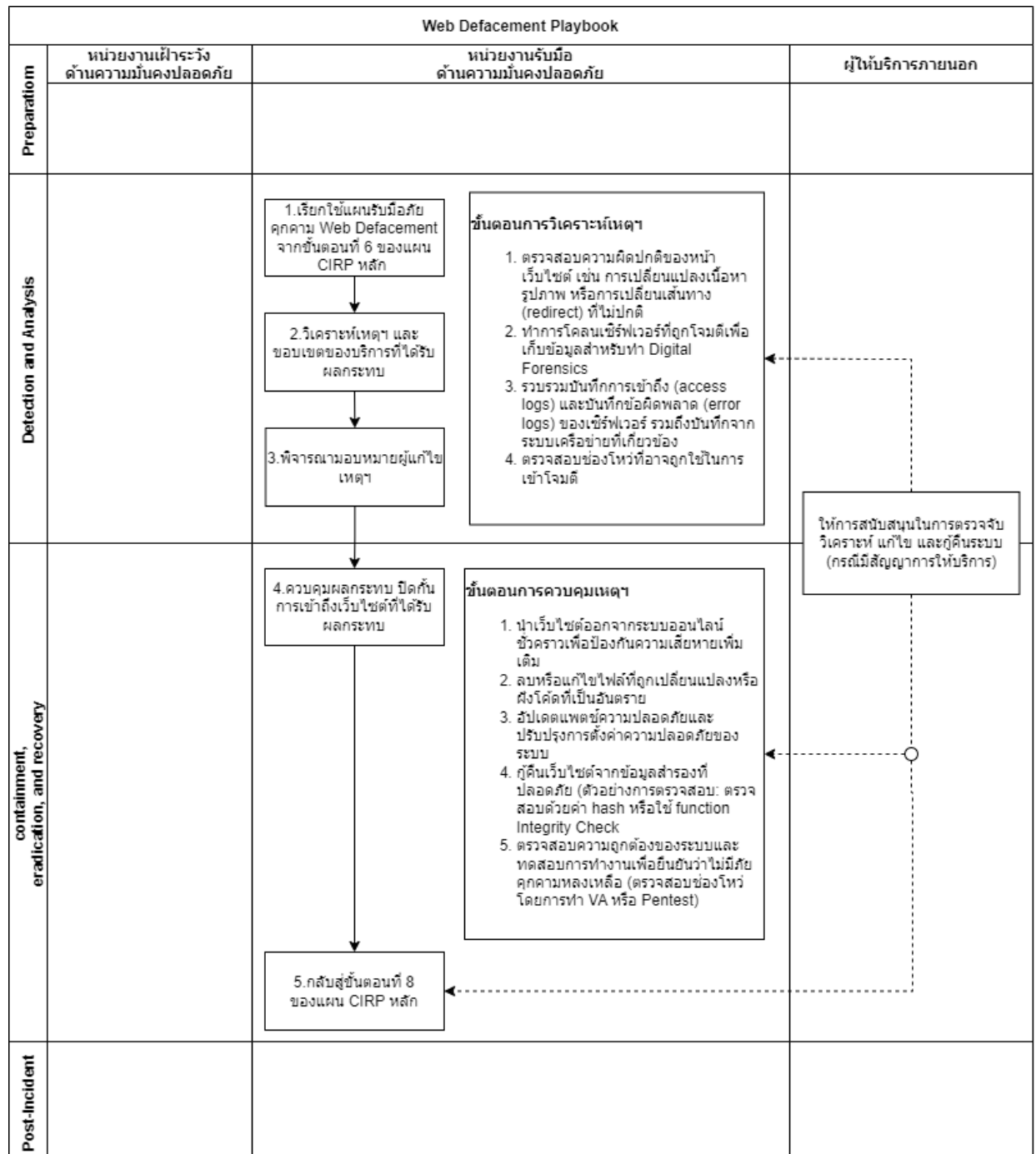
๓. ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)



๔. ขั้นตอนการรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook)



๕. ขั้นตอนการรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook)



ภาคผนวก ๒

บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนอง ต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงาน ความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๓

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

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

ภาคผนวก ๔

เอกสาร ก๑ ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น																	
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง																	
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม																	
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)																	
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม																	
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ^๔ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิฤต (ก) ☐ วิฤต (ข) ☐ ยังไม่สามารถระบุได้																	
๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ) <table border="1"><thead><tr><th>หมวดหมู่*</th><th>คำอธิบาย</th></tr></thead><tbody><tr><td>หมวดหมู่ที่ ๒</td><td>การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)</td></tr><tr><td>หมวดหมู่ที่ ๓</td><td>การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)</td></tr><tr><td>หมวดหมู่ที่ ๔</td><td>การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)</td></tr><tr><td>หมวดหมู่ที่ ๕</td><td>การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)</td></tr><tr><td>หมวดหมู่ที่ ๖</td><td>การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)</td></tr><tr><td>หมวดหมู่ที่ ๗</td><td>การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)</td></tr><tr><td>หมวดหมู่ที่ ๘</td><td>เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)</td></tr></tbody></table> <p>* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)</p>		หมวดหมู่*	คำอธิบาย	หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)	หมวดหมู่ที่ ๔	การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)	หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
หมวดหมู่*	คำอธิบาย																
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)																
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)																
หมวดหมู่ที่ ๔	การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)																
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)																
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)																
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)																
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)																

⁴ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.) : โปรดระบุ หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี) : โปรดระบุ วันที่ : เลือกวันที่ เวลา : โปรดระบุ
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม : โปรดระบุ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม : โปรดระบุ
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล : โปรดระบุ ตำแหน่งงาน : โปรดระบุ ชื่อหน่วยงาน : โปรดระบุ อีเมล : โปรดระบุ โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ^๕ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

⁵ พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำ หรือการดำเนินการใด ๆ โดยมีขอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์	
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม วันที่ : เลือกวันที่ เวลา : โปรดระบุ	
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ ☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____	
ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)	
หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ
<p>* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)</p>	
ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ: สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง) : โปรดระบุ ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : โปรดระบุ บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการเงิน) : 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 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access) วันที่ : เลือกวันที่ เวลา : โปรดระบุ ไม่ทราบ : ☐										
ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์ รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การโจรกรรม, 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 ในกรณีที่มีข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย) : โปรดระบุ จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ ชนิดของข้อมูล (เลือกทุกข้อที่ใช้) : <table border="0"><tr><td>☐ ข้อมูลไบโอเมตริกซ์</td><td>☐ ข้อมูลการติดต่อ</td></tr><tr><td>☐ ข้อมูลการเงิน</td><td>☐ ข้อมูลบุคลากรของรัฐ</td></tr><tr><td>☐ หมายเลขบัตรประชาชน</td><td>☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ</td></tr><tr><td>☐ ข้อมูลทางการแพทย์</td><td></td></tr><tr><td>☐ อื่น ๆ : โปรดระบุ</td><td></td></tr></table> จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ : โปรดระบุ ผลกระทบอื่น ๆ ที่เกิดขึ้น : โปรดระบุ	☐ ข้อมูลไบโอเมตริกซ์	☐ ข้อมูลการติดต่อ	☐ ข้อมูลการเงิน	☐ ข้อมูลบุคลากรของรัฐ	☐ หมายเลขบัตรประชาชน	☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ	☐ ข้อมูลทางการแพทย์		☐ อื่น ๆ : โปรดระบุ	
☐ ข้อมูลไบโอเมตริกซ์	☐ ข้อมูลการติดต่อ									
☐ ข้อมูลการเงิน	☐ ข้อมูลบุคลากรของรัฐ									
☐ หมายเลขบัตรประชาชน	☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ									
☐ ข้อมูลทางการแพทย์										
☐ อื่น ๆ : โปรดระบุ										

<p>๑๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</p> <p>หมายเลข CVE : โปรดระบุ</p> <p>ช่องโหว่ที่ถูกใช้โจมตี : โปรดระบุ</p> <p>การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น : โปรดระบุ</p> <p>อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)</p> <div>☐ ระบบล่ม</div> <div>☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ</div> <div>☐ บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ</div> <div>☐ การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ</div> <div>☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)</div> <div>☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ</div> <div>☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ</div> <div>☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย</div> <div>☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง</div> <div>☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก</div> <div>☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย</div> <div>☐ รูปแบบการใช้งานที่ผิดปกติ</div> <div>☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ</div> <div>☐ ความพยายามที่จะเขียนไฟล์ของระบบ</div> <div>☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ</div> <div>☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ</div> <div>☐ การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)</div> <div>☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ</div> <div>☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ</div> <div>☐ การแก้ไขหน้าเว็บ</div> <div>☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น</div> <div>☐ การเปลี่ยนแปลงในไคเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ</div> <div>☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)</div> <div>☐ สิ่งผิดปกติไปจากเดิมอื่น ๆ : โปรดระบุ</div>
<p>๑๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน</p> <p>(เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ) : โปรดระบุ</p>
<p>๑๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม : โปรดระบุ</p>
<p>๑๒. ข้อมูลการระงับ ปรามปราม และฟื้นฟู</p>
<p>๑๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม : โปรดระบุ</p>
<p>๑๒.๒ การคาดการณ์ความสามารถฟื้นฟู</p> <p>โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ตรงการเพิ่ม และประมาณระยะเวลาการฟื้นฟู</p>
<p>๑๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)</p>
<p>๑๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่ : เลือกวันที่ เวลา : โปรดระบุ</p>
<p>๑๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน : โปรดระบุ</p>
<p>๑๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม : โปรดระบุ</p>

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์^๖

หมวดหมู่	คำอธิบาย	จำนวน
๐	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (Training and Exercises)	
๑	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
๔	การบุกรุกโดยใช้มัลแวร์ (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
เครื่องคอมพิวเตอร์แม่ข่าย / แอคทีฟ ไดเรกทอรี (Active Directory)	
เครื่องเวิร์กสเตชัน (Workstation)	
สวิตช์ (Switch) / เราเตอร์ (Router)	
เว็บไซต์ (Website)	
อื่น ๆ	

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์^๗

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

^๖ หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.๒๕๖๔

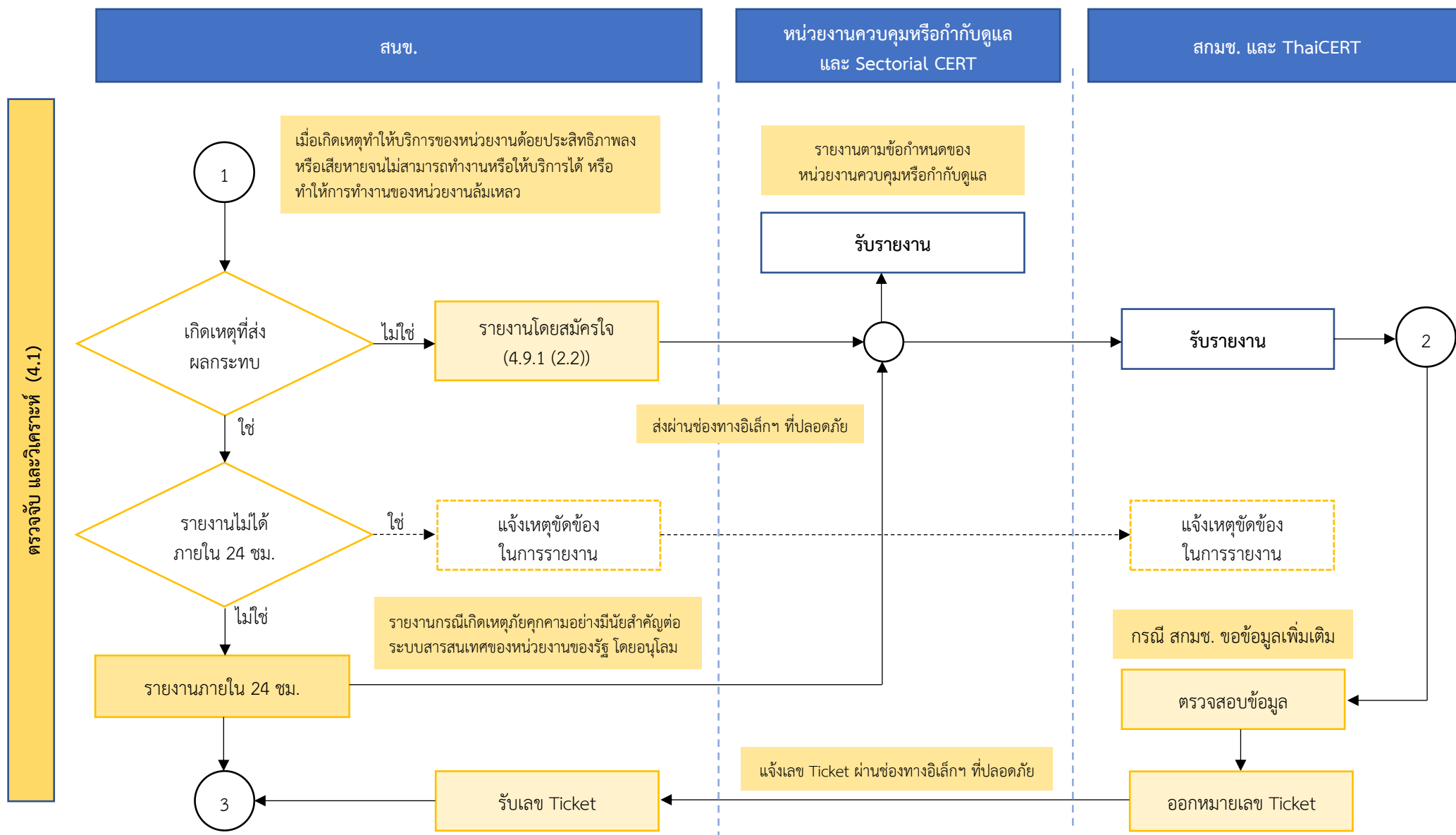
^๗ ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒

ภาคผนวก ๕

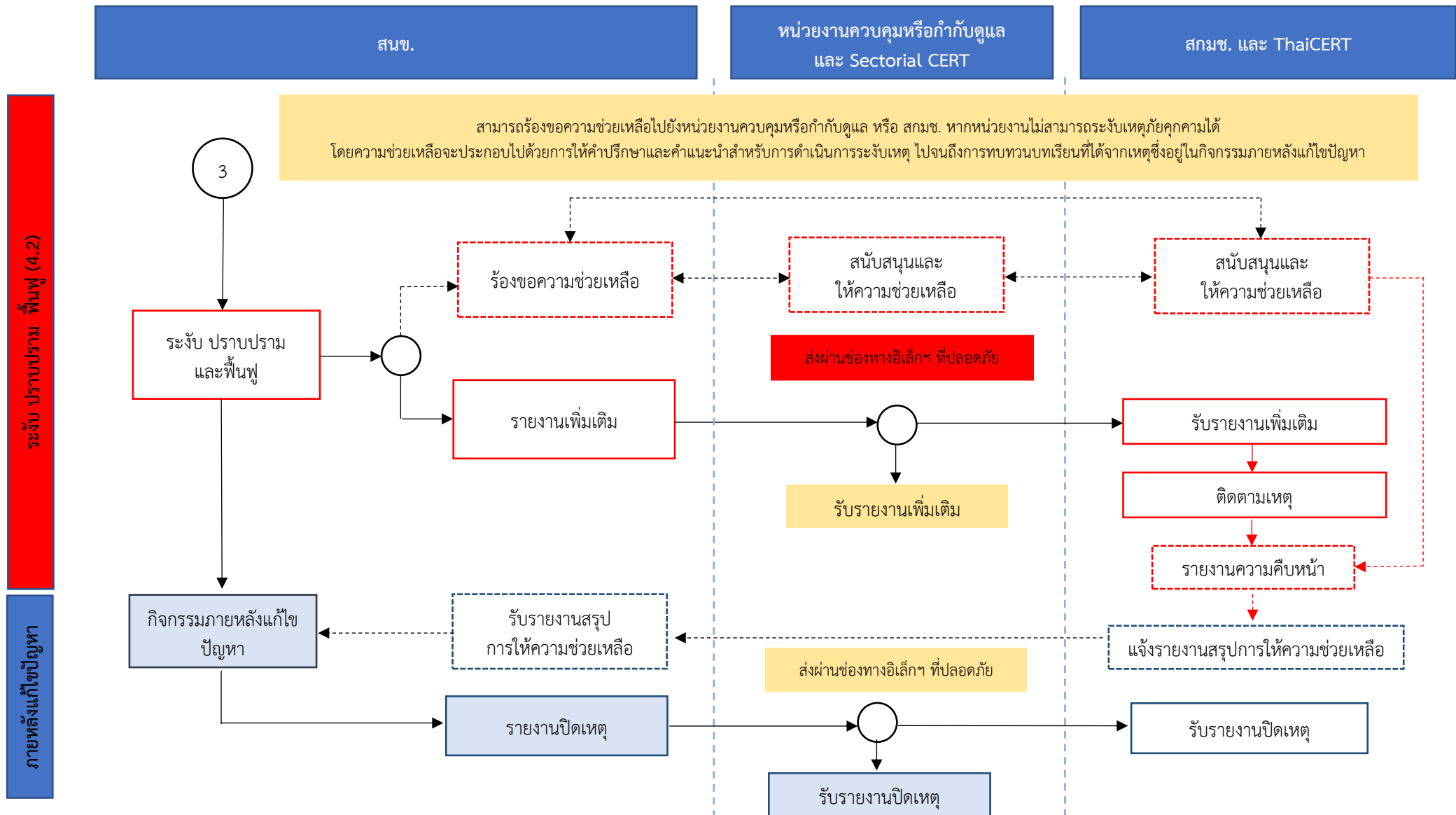
ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นตอนการระงับภัยคุกคาม ปรามปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์	
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 ๖ กระบวนการแจ้งหรือรายงานเหตุการณ์คุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ



ภาคผนวก ๖ กระบวนการแจ้งหรือรายงานเหตุภัยคุกคามทางไซเบอร์สำหรับหน่วยงานของรัฐ (ต่อ)



แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ประเมิน ประเมิน และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทาง ไซเบอร์ พ.ศ. ๒๕๖๖
- NIST SP 800-61r2 Computer Security Incident Handling Guide
- ACSC Cyber Incident Response Plan Guidance

ผู้จัดทำร่าง

๑. นายพิสิษฐ์ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรังกร ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายนฤทีร์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร