

แผนรับมือเหตุภัยคุกคามทางไซเบอร์
ของสำนักงานเศรษฐกิจการคลัง

ศูนย์เทคโนโลยีสารสนเทศ
สำนักงานเศรษฐกิจการคลัง

รายละเอียดการบังคับใช้เอกสาร

รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	ส่วนนโยบายโครงสร้างพื้นฐานและความมั่นคงปลอดภัย
ผู้ดำเนินการตามเอกสาร (Owner)	หน่วยงานภายในสำนักงานเศรษฐกิจการคลังและหน่วยงานภายนอกที่เกี่ยวข้อง
วันที่จัดทำเอกสาร (Date created)	วันที่ ๒๕๖๘
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	วันที่ ๒๕๖๘
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	ผู้อำนวยการสำนักงานเศรษฐกิจการคลัง
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑	วันที่ ๒๕๖๘		

สารบัญ

	หน้า
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. ขอบเขต	๑
๔. หน้าที่การทบทวนแผน	๑
๕. หน้าที่ในการดำเนินการตามแผน	๒
๖. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง	๒
๗. นิยาม	๓
๘. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์	๔
๙. รูปแบบภัยคุกคามไซเบอร์	๘
๑๐. ขั้นตอนการรับมือกับภัยคุกคามทางไซเบอร์	๙
๑๑. ภาคผนวก ๑	๒๓
๑๒. ภาคผนวก ๒	๒๕
๑๓. ภาคผนวก ๓	๒๘
๑๔. ภาคผนวก ๔	๓๐
๑๕. ภาคผนวก ๕	๓๒
๑๖. ภาคผนวก ๕.๑	๓๓
๑๗. ภาคผนวก ๕.๒	๓๕
๑๘. ภาคผนวก ๕.๓	๔๑
๑๙. ภาคผนวก ๖	๔๓
๒๐. ภาคผนวก ๗	๔๖
๒๑. ภาคผนวก ๘	๔๙
๒๒. ภาคผนวก ๙	๕๑

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วย (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานเศรษฐกิจการคลังด้วย

๒. วัตถุประสงค์

เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นในสำนักงานเศรษฐกิจการคลัง โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับกอง/ศูนย์/กลุ่ม ต่าง ๆ ภายใต้สำนักงานเศรษฐกิจการคลัง การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของสำนักงานเศรษฐกิจการคลัง

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังจะเป็นการกำหนดโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ บทบาทหน้าที่ความรับผิดชอบ และโครงสร้างการรายงานเหตุการณ์ รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ รวมถึงข้อมูลดิจิทัลของสำนักงานเศรษฐกิจการคลัง ตลอดจนบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศ สำนักงานเศรษฐกิจการคลัง มีหน้าที่จัดทำและทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง โดยจัดให้มีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์สำคัญ

/๕. หน้าที่ ...

๕. หน้าที่ในการดำเนินการตามแผน

ส่วนนโยบายโครงสร้างพื้นฐานและความมั่นคงปลอดภัย ศูนย์เทคโนโลยีสารสนเทศ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง โดยมีหน่วยงานสนับสนุนประกอบด้วย ศูนย์เทคโนโลยีสารสนเทศ และ กอง/ศูนย์/กลุ่ม ที่เป็นเจ้าของกระบวนการที่เกี่ยวข้องหรือเจ้าของข้อมูลภายในสำนักงานเศรษฐกิจการคลัง

๖. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๖.๑ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้อง

- นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๑
- แผนบริหารความเสี่ยงต่อทรัพยากรเทคโนโลยีสารสนเทศและเครือข่ายของสำนักงานเศรษฐกิจการคลัง เพื่อบริหารจัดการกระบวนการบริหารความเสี่ยงตามมาตรฐาน COSO
- แผนบริหารความต่อเนื่องในสภาวะวิกฤตของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๕
- แผนบริหารจัดการความเสี่ยงของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๖

๖.๒ นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้อง

นโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคลของสำนักงานเศรษฐกิจการคลัง พ.ศ. ๒๕๖๗

๖.๓ กฎหมายที่เกี่ยวข้อง

ที่	กฎหมายที่เกี่ยวข้อง
๑	**พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม**
	ประกาศกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เรื่อง หลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๖๔
๒	**พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒**
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการจัดทำและเก็บรักษาบันทึกรายการของกิจกรรมการประมวลผลข้อมูลส่วนบุคคลสำหรับผู้ประมวลผลข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง มาตรการรักษาความมั่นคงปลอดภัยของผู้ควบคุมข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง หลักเกณฑ์และวิธีการในการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๕
	ประกาศคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล เรื่อง การจัดให้มีเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลตามมาตรา ๔๑ (๒) แห่งพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ พ.ศ. ๒๕๖๖

/กฎหมายที่เกี่ยวข้อง ...

ที่	กฎหมายที่เกี่ยวข้อง
๓	**พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒**
	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔
	ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖
	ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. ๒๕๖๖

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า เหตุการณ์ที่เกิดขึ้นจากการเฝ้าระวังสังเกตการณ์ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้

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

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

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

/๘. บทบาท ...

๘. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๘.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสุขุมภัทร จุฬุวรรณ	เวลาทำการ จ. - ศ. เวลา ๘.๓๐ น. – ๑๖.๓๐ น. และกรณีฉุกเฉินนอกเวลาทำการ	๐๘๕-๔๕๐-๒๓๓๐	รับแจ้งเหตุ	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และบันทึกเหตุการณ์ พร้อมทั้งรายงานให้หัวหน้าทีมรับมือทราบ รวมถึงตรวจสอบ ติดตามเจ้าหน้าที่บริษัทคู่สัญญา
๒	นายปิยวรรษ เกียรติกูล	เวลาทำการ จ. - ศ. เวลา ๘.๓๐ น. – ๑๖.๓๐ น. และกรณีฉุกเฉินนอกเวลาทำการ	๐๖๑-๔๔๖-๒๖๔๔	รับแจ้งเหตุ	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ และบันทึกเหตุการณ์ พร้อมทั้งรายงานให้หัวหน้าทีมรับมือทราบ รวมถึงตรวจสอบ ติดตามเจ้าหน้าที่บริษัทคู่สัญญา
๓	เจ้าหน้าที่บริษัทคู่สัญญา	ตลอดระยะเวลา ๒๔ ชั่วโมง / ๗ วัน	มือถือ	เจ้าหน้าที่บริษัทคู่สัญญา	ตรวจสอบแก้ไขและรายงานผลการดำเนินงาน

๘.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

สำนักงานเศรษฐกิจการคลัง ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (ทีมรับมือ) ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อ - นามสกุล รายละเอียดการติดต่อ	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสุภชัย ภูริเกษม ผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศ	๐๘๖-๙๙๙-๙๙๖๖	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

/ลำดับ ...

ลำดับ	ชื่อ - นามสกุล รายละเอียดการติดต่อ	ช่องทางการ ติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๒	นายนิติสิริ ประสาทกุล ผู้อำนวยการส่วนระบบข้อมูลและนวัตกรรมเทคโนโลยีสารสนเทศ	๐๘๑-๖๒๖-๓๐๔๖	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่ หรือไม่สามารถปฏิบัติงานได้
๓	นายสุขุมภัทร จุฬุวรรณ	๐๘๕-๔๕๐-๒๓๓๐	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความช่วยเหลือ ติดตาม ตรวจสอบระบบสารสนเทศและระบบเครือข่าย พร้อมทั้งให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๔	นายปิยวรรษ เกียรติกูล	๐๖๑-๔๔๖-๒๖๔๔	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ให้ความช่วยเหลือ ติดตาม ตรวจสอบระบบสารสนเทศและระบบเครือข่าย พร้อมทั้งให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลการโจมตีทางไซเบอร์		เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลการโจมตีทางไซเบอร์	ดำเนินการแก้ไขเหตุขัดข้องตามสัญญาที่ตกลงกันไว้ร่วมกัน
๖	เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลระบบสารสนเทศ		เจ้าหน้าที่บริษัท คู่สัญญาที่ดูแลระบบสารสนเทศที่เกี่ยวข้อง	ดำเนินการแก้ไข/กู้คืนระบบสารสนเทศตามสัญญาที่ตกลงกันไว้ร่วมกัน

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลัง (สศค.) (แผนรับมือฯ) ดังนี้

ลำดับ	บุคลากรที่เกี่ยวข้อง	หน้าที่	ความรับผิดชอบ
๑	ผอ. กอง/สำนัก	เจ้าหน้าที่บริหารจัดการผลกระทบจากภัยคุกคามทางไซเบอร์	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๒	นิติกร สศค.	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตรวจสอบแผนรับมือฯ ให้สอดคล้องกับกฎหมายที่เกี่ยวข้อง

/ลำดับ ...

ลำดับ	บุคลากรที่เกี่ยวข้อง	หน้าที่	ความรับผิดชอบ
๓	เจ้าหน้าที่บริษัทคู่สัญญา	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตาม [นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของ]
๔	ผู้เชี่ยวชาญด้านกฎหมาย	ผู้เชี่ยวชาญด้านกฎหมาย	ทำหน้าที่เป็นที่ปรึกษาด้านกฎหมายที่เกี่ยวข้อง
๕	เจ้าหน้าที่ ศทส. ที่ได้รับมอบหมาย	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้องของหน่วยงาน]
๖	เจ้าหน้าที่ ศทส. ที่ได้รับมอบหมาย	ผู้รับผิดชอบด้านสื่อสารองค์กร	ทำหน้าที่ตาม [นโยบาย หรือคำสั่งที่เกี่ยวข้อง]

๘.๓ <u>หน่วยงานภายนอกที่เกี่ยวข้อง</u>

ข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.), หน่วยงานกำกับดูแล (Regulator), THAI – CERT และผู้ให้บริการภายนอกของ สศค. เป็นต้น

ลำดับที่	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	โทร ๐๒-๑๔๒-๖๘๘๘	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	แจ้งเหตุภัยคุกคามทางไซเบอร์ และให้คำแนะนำ/แนวทางการรับมือภัยคุกคามทางไซเบอร์
๒	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	โทร ๐๒-๑๔๒-๖๘๘๘ Email: thaicert@ncsa.or.th	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	แจ้งเหตุภัยคุกคามทางไซเบอร์
๓	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	โทร ๐๒-๑๔๒-๑๐๓๓ โทร ๐๒-๑๔๑-๖๙๙๓	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	แจ้งเหตุละเมิดข้อมูลส่วนบุคคล

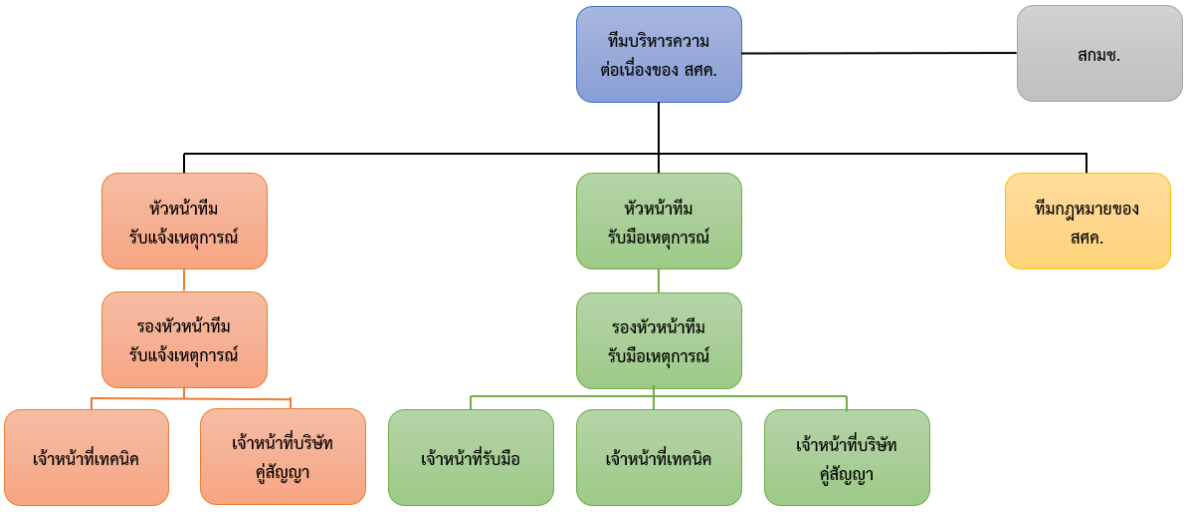
/ลำดับที่ ...

ลำดับที่	ชื่อ - นามสกุล	ช่อง ทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๔	บริษัทคู่สัญญา ดูแลระบบ Network		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Network
๕	บริษัทคู่สัญญา ดูแลระบบ VM		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ VM
๖	บริษัทคู่สัญญา ดูแลระบบ Backup		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Backup
๗	บริษัทคู่สัญญา ดูแลระบบ Data Center		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Data Center
๘	บริษัทคู่สัญญา ดูแลระบบ Storage		บริษัทผู้ให้บริการภายนอก	ดูแลระบบ Storage
๙	บริษัทคู่สัญญา ดูแลระบบตรวจจับและป้องกันมัลแวร์		บริษัทผู้ให้บริการภายนอก	ดูแลระบบตรวจจับและป้องกันมัลแวร์k

๘.๔ <u>โครงสร้างการรายงานเหตุการณ์</u> (Incident Reporting Structure)

สำนักงานเศรษฐกิจการคลังได้จัดให้มีแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่า หน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ดังรูป

/รูปที่ ๑ โครงสร้าง ...



รูปที่ ๑ โครงสร้างการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
(Incident Reporting Structure)

๙. รูปแบบภัยคุกคามไซเบอร์

๙.๑ Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้ โดยมีพฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)

๙.๒ Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไขเว็บไซต์โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้วจะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็นเว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

๙.๓ Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือช่องทาง Social โดยใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

๙.๔ Web application attacks คือ วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์และ Web Server หรือ Database Server

๙.๕ Spam คือ วิธีการที่ผู้ส่งหรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล ข้อความหรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์หรือช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับเพื่อสร้างความรำคาญหรือก่อกวน

/๙.๖ DDoS ...

๙.๖ DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการให้บริการหรือระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียวภายในเวลาเดียวกัน จุดประสงค์ที่ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้หรือระบบล่ม

๙.๗ Data breach คือ เกิดการรั่วไหลของข้อมูลที่อาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของเว็บไซต์ ข้อมูลของแอปพลิเคชันหรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชันหรือผู้ให้บริการระบบไม่ทราบซึ่งผู้โจมตีต้องการนำข้อมูลไปขายหรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ

๙.๘ Insider threat คือ ภัยที่เกิดจากบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจหรือไม่ตั้งใจผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ขององค์กร หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กรอาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่ายและเสี่ยงต่อข้อมูลสำคัญที่อาจจะถูกขโมย ซึ่งผลลัพธ์ของภัยนี้มีความรุนแรงต่อภาพลักษณ์องค์กรและการขาดความน่าเชื่อถือ

๙.๙ Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่ถูกโปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

๙.๑๐ Ransomware คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่องคอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

๙.๑๑ Cryptojacking คือ วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการติดตั้งโปรแกรมที่ใช้เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

๙.๑๒ ผู้บุกรุก (Hacker) ผู้ที่ไม่ได้รับอนุญาตให้เข้าใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๑๐. ขั้นตอนการรับมือกับภัยคุกคามทางไซเบอร์

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของสำนักงานเศรษฐกิจการคลังฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ

/และหน่วยงาน ...

และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ โดยมีขั้นตอนการดำเนินการ เป็น ๔ ขั้นตอนหลัก เพื่อให้สอดคล้องกับมาตรฐานหรือแนวทางปฏิบัติที่เกี่ยวข้องกับการจัดการภัยคุกคามทางไซเบอร์ ดังนี้



รูปที่ ๒ ภาพแสดงขั้นตอนการดำเนินมาตรการที่เกี่ยวข้องเพื่อจัดการภัยคุกคามทางไซเบอร์ (Incident Handling Cycle)

๑๐.๑ ขั้นการเตรียมการ (preparation)

การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งจำเป็นที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน การจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือ ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดตามข้อ ๘.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดตามข้อ ๘.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

- การจัดเตรียมข้อมูลและอุปกรณ์ให้พร้อมต้องจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์
- การตั้งค่าอุปกรณ์และระบบต่าง ๆ ให้มีความปลอดภัยและเหมาะสม
- การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึงการสร้างเครือข่ายความร่วมมือแนวทางป้องกันและการเตรียมการเบื้องต้น

/(๔) จัดเตรียม ...

(๔) จัดเตรียมข้อมูลและอุปกรณ์ในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ ได้แก่

- รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รายละเอียดตามข้อ ๘.๒
- ช่องทางการรายงานเหตุการณ์ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์แจ้งศูนย์เทคโนโลยีสารสนเทศตรวจสอบ
- ช่องทางรายงานและติดตามข้อมูล สถานการณ์การดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(๕) จัดเตรียมอุปกรณ์ ซอฟต์แวร์ และแหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ ได้แก่

- จัดเตรียมสถานที่จัดเก็บที่มีความมั่นคงปลอดภัย เพื่อใช้ในการจัดเก็บหลักฐาน ข้อมูล และพยานวัตถุอื่น ๆ ที่สำคัญ
- ดำเนินการตั้งค่าระบบต่าง ๆ ให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Firewall IPS เป็นต้น การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องปฏิบัติการศูนย์ข้อมูล มีการปิดช่องโหว่และการกำหนดสิทธิ์ของผู้ใช้โดยการให้สิทธิ์เท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ Update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือฯ ของหน่วยงาน (รายละเอียดปรากฏตามภาคผนวก ๑)

นอกจากนี้ สำนักงานเศรษฐกิจการคลังยังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๒)

/๑๐.๒ ขั้นการตรวจจับ ...

๑๐.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น มีมาตรการและแนวปฏิบัติตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ) โดยดำเนินการดังต่อไปนี้

(๑) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้นหรืออาจเกิด (Common Attack Vectors/Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น ดังนี้

ประเภทภัยคุกคามของหน่วยงาน	คำอธิบาย	วิธีการรับมือ
อุปกรณ์แบบถอดได้ (External/Removable Media)	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง เช่น โค้ดที่เป็นอันตรายแพร่กระจายไปยังระบบจากแฟลชไดรฟ์ที่ติดไวรัส	ดำเนินการถอนการติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายและตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด
Website Defacement	การโจมตีเว็บไซต์เพื่อเปลี่ยนแปลงข้อมูลที่เผยแพร่หน้าเว็บ ซึ่งผู้โจมตีมีวัตถุประสงค์เพื่อปรับเปลี่ยนหน้าเว็บไซต์แรกของเว็บไซต์เป้าหมาย หรือทั้งเว็บไซต์ จากเดิมไปเป็นหน้าเว็บไซต์ใหม่	ดำเนินการปิด DNS ขานอกที่เป็นสาเหตุของภัยคุกคาม จากนั้นผู้ดูแลระบบเว็บไซต์ดำเนินการลบไฟล์ที่น่าสงสัย
DDos	การโจมตี DDos เกิดขึ้นเมื่อ Hacker ส่งปริมาณการเข้าชมจำนวนมากไปยังเครือข่ายหรือเซิร์ฟเวอร์ เพื่อทำลายระบบและขัดขวางความสามารถในการให้บริการ การโจมตีเหล่านี้มักถูกนำมาใช้เพื่อโจมตีเว็บไซต์หรือแอปพลิเคชันให้ออฟไลน์ชั่วคราวและการโจมตีแต่ละครั้งอาจเกิดขึ้นเป็นระยะเวลาหลายวันหรือนานกว่านั้น	- ปิดกัน IP ต้องสงสัย - กำหนด Rate Limit ของ Connection
SQL Injection	การโจมตีที่ระบบฐานข้อมูลของเว็บไซต์ ผลคือระบบฐานข้อมูลจะถูกขโมยออกไป หรืออาจจะถูกลบ หรือแก้ไขให้เกิดความเสียหายได้ ช่องโหว่ของ SQL เป็นรูปแบบที่มีมานาน และถูกใช้เป็นจุดอ่อนที่ถูกโจมตีมากที่สุด ซึ่งจุดอ่อนนี้สามารถเกิดขึ้นได้กับระบบฐานข้อมูล เช่น Oracle, Microsoft, MySQL หรืออื่น ๆ	- ทำ Penetration Testing ทุกเว็บไซต์ - Monitor Traffic ต้องสงสัยผ่านระบบ SIEM และแจ้งผู้ดูแลเว็บไซต์เมื่อตรวจสอบพบการโจมตี

ประเภทภัยคุกคามของหน่วยงาน	คำอธิบาย	วิธีการรับมือ
การโจมตีในรูปแบบ Network Scanning	กระบวนการที่ผู้ไม่ประสงค์ดีพยายามทำลายหรือเข้าถึงข้อมูลในระบบเครือข่ายของบุคคลหรือองค์กรอย่างไม่ถูกต้องหรือไม่ได้รับอนุญาต โดยเครื่องมือที่ออกแบบมาเพื่อสแกนหรือสำรวจเครือข่าย	ตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point
Malicious Code (โปรแกรมไม่พึงประสงค์)	มัลแวร์ (Malware), Virus, Worm, Trojan, Ransomware, และ Spyware ต่าง ๆ ซึ่งเป็นโปรแกรมที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ เช่น การโจมตีในรูปแบบ Ransomware โดยการเข้ารหัสไฟล์ของเหยื่อแล้วขโมยข้อมูลของเหยื่อไป จากนั้นผู้โจมตีก็จะเรียกค่าไถ่จากเหยื่อ เพื่อให้เหยื่อยอมจ่ายเงินแลกกับการได้ข้อมูลคืน ช่องทางการโจมตีมาจาก File Attachment ที่แนบ e-Mail เช่น ไฟล์ PDF ที่แนบ Script Ransomware ทำให้เครื่องคอมพิวเตอร์ภายในถูก Ransomware โจมตีและแพร่กระจายไปยังเครื่องคอมพิวเตอร์ ภายในเครือข่ายเดียวกัน	- ทำการรวบรวม Log ทั้งหมดที่เกี่ยวข้องเพื่อทำการวินิจฉัยว่ามีเหตุการณ์ Scan ระบบเครือข่าย - ดำเนินการปิดการเชื่อมต่อ Port SMB* ของเครื่องคอมพิวเตอร์ที่เชื่อมโยงภายในเครือข่ายคอมพิวเตอร์เดียวกัน - ติดตั้งอุปกรณ์ป้องกันการถูกโจมตีจากภัยทางไซเบอร์บนเครือข่ายคอมพิวเตอร์ *Port SMB (Server Message Block) เป็นพอร์ตเครือข่ายที่ใช้สำหรับการแบ่งปันไฟล์และทรัพยากรบนเครือข่ายคคอมพิวเตอร์เป็นหลัก SMB ทำงานบนพอร์ต TCP ๔๔๕ และเปิดใช้งานการเข้าถึงไฟล์ เครื่องพิมพ์ และพอร์ตซีเรียลร่วมกันระหว่างอุปกรณ์บนเครือข่าย
หมวดหมู่ของภัยคุกคามทางไซเบอร์ (ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ)	**คำอธิบาย**	**วิธีการรับมือ**
หมวดหมู่ : ๑ การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	การพยายามทำกิจกรรมที่ไม่สำเร็จ (เหตุการณ์) ความพยายามโดยเจตนาเพื่อเข้าถึงระบบโดยไม่ได้รับอนุญาต ซึ่งพ่ายแพ้โดยกลไกการป้องกันตามปกติ ผู้โจมตีไม่สามารถเข้าถึงระบบ (เช่น ผู้โจมตีพยายามใช้ชื่อผู้ใช้และรหัสผ่านที่ถูกต้องหรืออาจถูกต้อง) และกิจกรรมนี้ไม่สามารถจัดประเภทเป็นการสแกนเชิงสำรวจได้	ดำเนินการตรวจสอบจากการแจ้งเตือนจากอุปกรณ์ที่ตรวจจับสิ่งผิดปกติและทางเจ้าหน้าที่วิเคราะห์ภัยคุกคามจะต้องตรวจสอบ เพื่อให้แน่ใจว่าสิ่งที่แจ้งเตือนมานั้นเป็นเหตุการณ์ที่ต้องระงับและดำเนินการขั้นตอนให้ภัยคุกคามนั้นลดลงหรือหมดไป
หมวดหมู่ : ๒ การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	กิจกรรมที่พยายามรวบรวมข้อมูลที่ใช้เพื่อระบุลักษณะของระบบ แอปพลิเคชัน เครือข่าย ข้อมูล และผู้ใช้งานในระบบที่อาจมีประโยชน์ในการกำหนดการโจมตี	ดำเนินการบล็อก IP ต้นทาง และสร้าง Rule เพื่อบล็อกการ Scan ระบบเครือข่าย หลังจากนั้นให้ทำการรวบรวมหลักฐานของเหตุการณ์ Scan ระบบเครือข่ายเพื่อนำไปสร้างรายงานและองค์ความรู้

/หมวดหมู่ ...

หมวดหมู่ของภัยคุกคามทางไซเบอร์ (ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามฯ)	คำอธิบาย	วิธีการรับมือ
หมวดหมู่ : ๓ การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	ความเสี่ยงที่เกิดขึ้นกับระบบอาจมาจากการกระทำหรือการละเลยของผู้ใช้งานระบบ เช่น การละเลยการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด การไม่ติดตั้งซอฟต์แวร์ป้องกันไวรัส เป็นต้น ซึ่งพฤติกรรมดังกล่าวส่งผลให้เกิดช่องโหว่ที่อาจนำไปสู่การโจมตีทางไซเบอร์ และเป็นต้นเหตุของความเสียหายต่อระบบและข้อมูลสำคัญ	สร้างความตระหนักรู้ให้กับผู้ใช้งานอย่างสม่ำเสมอ แสดงให้เห็นถึงความเสี่ยงของการไม่ดำเนินการตามมาตรฐานที่กำหนด
หมวดหมู่ : ๔ การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	เป็นเหตุการณ์ที่เครื่องคอมพิวเตอร์ลูกข่ายหรือเครื่องคอมพิวเตอร์แม่ข่ายถูกบุกรุกโดยการใช้มัลแวร์ (Malicious Logic) หรือชุดคำสั่งไม่พึงประสงค์ที่มีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่ง	ดำเนินการตัดการเชื่อมต่อทางเครือข่ายและตรวจสอบ Log และใช้เครื่องมือกำจัดมัลแวร์
หมวดหมู่ : ๕ การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	การเข้าถึงระบบโดยไม่ได้รับอนุญาต หรือข้อมูล/บัญชีที่ไม่ได้รับอนุญาต หรือมีสิทธิ์การเข้าถึงระบบที่เกินกว่าสิทธิ์การใช้งานที่ได้รับจากผู้ดูแลระบบ	ดำเนินการตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point ว่าเป็นไปตามเกณฑ์ ต่อไปนี้ ๑. พยายาม Log-in นอกเวลางาน ๒. Log-in ภายใต้ IP ที่กำหนด
หมวดหมู่ : ๖ การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	การเข้าถึงระบบงานด้วยสิทธิพิเศษโดยไม่ได้รับอนุญาต การเข้าถึงแบบมีสิทธิพิเศษในระดับผู้ดูแลระบบหรือระดับ Root ช่วยให้เข้าถึงระบบงานได้ไม่จำกัด	ดำเนินการตรวจสอบ Log ที่มาจาก Firewall, IPS, End Point ว่าเป็นไปตามเกณฑ์ ต่อไปนี้ ๑. พยายาม Log-in นอกเวลางาน ๒. Log-in ภายใต้ IP ที่กำหนด

/(๒) การตรวจจับ ...

(๒) การตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลความรู้จากแหล่งข้อมูลข่าวสารภัยคุกคามจากภายนอกต่าง ๆ (Threat Intelligence) เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น จากหลากหลายช่องทางดังนี้

Channel Types	URL
Cybersecurity news sites	
	https://webboard-nsoc.ncsa.or.th/category/12/cyber-security -news
	https://www.thaicert.or.th/category/cybernews/
	https://www.blognone.com/
	https://www.techtalkthai.com/category/security/
	https://thehackernews.com
Community Facebook Pages	
	https://www.facebook.com/NCSA.Thailand/
	https://www.facebook.com/thaicert/
	https://www.facebook.com/pdpc.th/
	https://www.facebook.com/TBCERT.Official/
	https://www.facebook.com/2600Thailand/
	https://www.facebook.com/owaspbangkok/
	https://www.facebook.com/InfoSecThaiGirl/
	https://www.facebook.com/thaicysec/
	https://www.facebook.com/hackandsecbook/
	https://www.facebook.com/isecure.mssp/
Cyber Threat intelligence Tools	
	https://attack.mitre.org/
	https://www.talosintelligence.com/
	https://www.virustotal.com/gui/
	https://otx.alienvault.com/browse/
	https://urlscan.io
	https://www.opencve.io/cve
	https://www.cvedetails.com/
	https://www.filescan.io/scan
	https://dnsdumpster.com

/(๓) ทีมรับมือ ...

(๓) ทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ดำเนินการวิเคราะห์ผลกระทบ พร้อมทั้งระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

➢ **ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Incident Prioritizaton) ดังนี้**

ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Security Level)	คำอธิบาย	ประเภท/รูปแบบของภัยคุกคาม
๐ ระดับต่ำ (Low)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้างเครือข่าย หรือระบบงานเพียงเล็กน้อย หรืออาจทำให้ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่กระทบกับระบบโดยรวม	- ไวรัสคอมพิวเตอร์ (Computer Virus) - หนอนคอมพิวเตอร์ (Computer worm) - Spam Mail หรืออีเมล์ขยะ - Botnet - สปายแวร์ (Spyware)
๑ ระดับกลาง (Medium)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้าง เครือข่าย หรือระบบงานเพียงเล็กน้อย หรืออาจทำให้ด้อยประสิทธิภาพลงไปบ้าง แต่ไม่ถึงกับทำให้ระบบหรือบริการต้องหยุดชะงัก หรือไม่สามารถใช้งานได้	- ม้าโทรจัน (Trojan horse) - Backdoor - Rootkit - การโจมตีแบบ DoS/DDoS - Phishing
๒ ระดับสูง (High)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบคอมพิวเตอร์ อุปกรณ์ โครงสร้างเครือข่าย หรือระบบงานโดยรวมอย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตี มีความมุ่งหมายที่จะทำให้ระบบและข้อมูลของหน่วยงานเสียหายจนไม่สามารถทำงานหรือให้บริการได้	- ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) - Sniffing - Social Engineering - Password Attack - Insider Treats - SQL Injection - Form Jacking

'ระดับความรุนแรง ...

ระดับความรุนแรงของภัยคุกคามทางไซเบอร์ (Security Level)	คำอธิบาย	ประเภท/รูปแบบของภัยคุกคาม
๓ ระดับร้ายแรง (Extreme)	ภัยคุกคามทางไซเบอร์ที่ส่งผลต่อระบบ คอมพิวเตอร์ อุปกรณ์ โครงสร้าง เครือข่าย หรือระบบงาน อย่างรุนแรง หรือมีเหตุอันควรเชื่อได้ว่า ผู้โจมตีจะทำให้ระบบและข้อมูลของหน่วยงานเสียหาย จนไม่สามารถทำงานหรือให้บริการได้ ส่งผลเสียหายเป็นวงกว้างซึ่งอาจทำให้หน่วยงานอยู่ในภาวะคับขัน หรือมีการกระทำความผิดเกี่ยวกับการก่ออาชญกรรมตามประมวลกฎหมายอาญา	- ผู้บุกรุก (Hacker)

➢ **ผลกระทบต่อการทำงานของระบบ (functional impact)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
ไม่มีผลกระทบ (None)	ไม่มีผลกระทบต่อการดำเนินงาน
ระดับต่ำ (Low)	ส่งผลให้การปฏิบัติงานตามภารกิจหลักมีความล่าช้า แต่ยังสามารถดำเนินงานต่อไปได้
ระดับกลาง (Medium)	ส่งผลให้งานตามภารกิจหลักไม่สามารถดำเนินการได้บางส่วน
ระดับสูง (High)	ส่งผลให้งานตามภารกิจหลักหยุดชะงัก

➢ **ผลกระทบต่อข้อมูล (information impact)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
ไม่มีข้อมูลรั่วไหล (None)	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
ละเมิดความลับของข้อมูลส่วนบุคคล (Confidentiality Breach)	มีการละเมิดความลับของข้อมูลส่วนบุคคลซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล
ละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคล (Integrity Breach)	มีการละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลงแก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
ละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล (Availability Breach)	มีการละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคลซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

/ระดับ ...

➢ **ระดับความสามารถในการกู้คืน (recoverability effort)**

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถารการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๓.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ Incident ซึ่งขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติ และมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๓.๑.๑ <u>ประเภท Alert</u>

(๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

(๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM สามารถทำงานร่วมกับ EDR โดยตรวจจับภัยคุกคามจากการวิเคราะห์ EDR สามารถระบุภัยคุกคามที่อาจเกิดขึ้น เช่น มัลแวร์ แรนซัมแวร์ ความพยายามฟิชชิ่ง และช่องโหว่แบบ zero-day (ช่องโหว่ที่ไม่รู้จักก่อนหน้านี้)

(๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่ายและ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

/(๔) Third-Party ...

(๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงานถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๓.๑.๒ ประเภท Log

(๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

(๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๓.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้

๓.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๓.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งดังนี้

๓.๒.๑ log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๓.๒.๒ Clock Synchronization อุปกรณ์ ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๓.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

๓.๒.๔ Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

(๔) ดำเนินการจัดให้มีบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ (รายละเอียดปรากฏตามภาคผนวก ๓)

/(๕) จัดทำบันทึก ...

(๕) จัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย พร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ ลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ (รายละเอียดปรากฏตามภาคผนวก ๔)

(๖) กรณีจะต้องจัดให้มีการรายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ที่เกี่ยวข้องทราบ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ (ประกาศฯ) ดังนี้

(ก) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นตาม ข้อ ๔ แห่งประกาศฯ ให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ข) กรณีมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบตาม ข้อ ๕ แห่งประกาศฯ ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ค) จัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของสำนักงานเศรษฐกิจการคลัง <u>ภายในวันที่ ๓๑ มกราคม ของปีถัดไป</u> ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

นอกจากนี้ สำนักงานเศรษฐกิจการคลังได้ดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๖)

๑๐.๓ <u>ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)</u>

การดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

/(๑) จำกัดขอบเขต ...

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

(๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

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

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

นอกจากนี้ สำนักงานเศรษฐกิจการคลังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๗)

๑๐.๔ <u>ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์</u> (Post-Incident activity)

การกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้จะต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

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

นอกจากนี้ สำนักงานเศรษฐกิจการคลังดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) ของกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity) ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๘)

/๑๐.๕ <u>การจัดทำ</u> ...

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

ต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งเป็นแนวทางเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๙)

แหล่งที่มา

- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

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

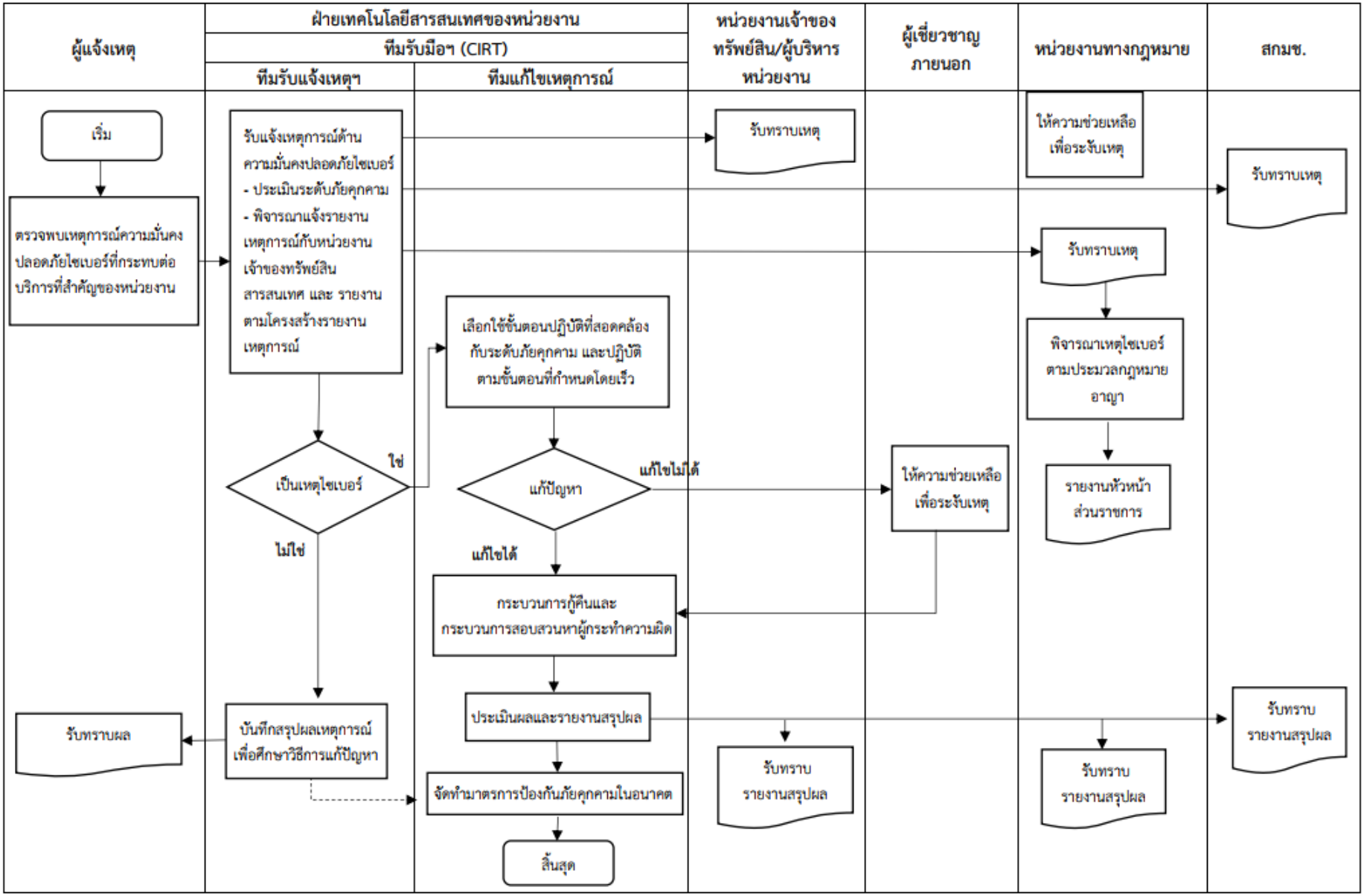
- ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖

- NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide

- ACSC Cyber Incident Response Plan Guidance

ภาคผนวก ๑

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)ของ สศค.



ภาคผนวก ๒

ตารางที่ ๒.๑ การดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับไม่ร้ายแรง** กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับร้ายแรง** กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับวิกฤต**	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคล หรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทางของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น (๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของ อุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography / key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับมอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติเพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่หรือจุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม) (๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลงค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไกที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มีกลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการภัยคุกคามทางไซเบอร์

ภาคผนวก ๓

บันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยทางไซเบอร์

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

ภาคผนวก ๔

บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)

ภาคผนวก ๕

ภาคผนวก ๕.๑

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[๓] ในระดับใด (มาตรา ๖๐)
☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)
☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

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

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

[๓] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภาคผนวก ๕.๒

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[๔] ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

[๔] พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดความหมายของ “ภัยคุกคามทางไซเบอร์” ดังนี้ การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหาย หรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

-๒-

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

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

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ภัยคุกคามหมวดหมู่ที่ ๐ ๑ และ ๙ ไม่เข้าข่ายเป็นภัยคุกคามที่ต้องรายงาน)

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

-๓-

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

-๔-

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

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

วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐

ง๑.๒ ข้อมูลการพบเห็นเหตภัยคุกคามทางไซเบอร์

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

โปรดระบุ

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

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อระบบ 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

-๕-

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

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ
☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ
☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ
☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)
☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ
☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ
☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย
☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง
☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก
☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย
☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ
☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ
☐ การแก้ไขหรือลบข้อมูลฐานผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)
☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ
☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น
☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ
☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)
☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

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

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู
โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

ภาคผนวก ๕.๓

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์[๕]

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

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์[๖]

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

[๕] หมวดหมู่ตามข้อ ๑ ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔

[๖] ระดับภัยคุกคามทางไซเบอร์ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ภาคผนวก ๖

ตารางที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ **ในระดับไม่ร้ายแรง** กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับร้ายแรง**	(1) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคามทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัยด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรมการใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหาความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามี หรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหาและรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี (อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และข้อมูลจราจรทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguardincident data) ให้มีความปลอดภัยเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้นและติดตามเพื่อระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวกแนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงานของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์ รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูลเพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๑) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้แล้วแต่กรณี
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับวิกฤต**	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์และสามารถจัดเก็บและวิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่ายหรือระบบงานหลักที่สูงผิดปกติ หรือ เมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจากข้อมูลในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ภาคผนวก ๗

ตารางที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับไม่ร้ายแรง**	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์ โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจนเพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้ แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่าย ภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่น การจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหาและวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบอย่างทันท่วงทีโดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ ทั้งนี้ ในการแจ้งหรือรายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสมและปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับ ดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวก แนบท้ายนี้ แล้วแต่กรณี (๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์ และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่น การปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐานและดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
	(๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์ (install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณ เตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับร้ายแรง**	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้องกับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายในหน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้น การรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ หน่วยงานควบคุมหรือกำกับดูแล พนักงาน เจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุนการรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident Handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับวิกฤต**	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดยอาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบและเครือข่ายของหน่วยงานทำได้อย่างรวดเร็ว

หมายเหตุ: ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว แต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์โดยใช้ปัจจัยที่ใช้ในการประเมินตามที่ระบุในตามตารางที่ ๑ ของเอกสารแนบ ๑ ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตามให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้นโดยพิจารณาจากตัวอย่างตามที่ระบุในข้อ ๑ ของภาคผนวกแนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์เพื่อระบุระดับของภัยคุกคามทางไซเบอร์

ภาคผนวก ๘

ตารางที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับ **ไม่ร้ายแรง** กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับร้ายแรง** กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ใน**ระดับวิกฤต**	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคามทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบายและกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการและป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสมและเป็นปัจจุบัน (๔) เก็บรักษาข้อมูลและหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือ ใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดีตามแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ภาคผนวก ๙

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

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