แผนรับมือเหตุภัยคุกคามทางไซเบอร์ การฝึกซ้อม
และทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ (INCIDENT RESPONSE PLAN)
โรงพยาบาลสันกำแพง ปีงบประมาณ 2569

สารบัญ

บทนำ

๑. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จัดทำประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของแต่ละหน่วยงานให้สอดคล้องกับนโยบาย และแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง

(๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง

(๒) แผนการรับมือภัยคุกคามทางไซเบอร์ รวมทั้งเพื่อให้เป็นไปตามแผนการตรวจสอบและการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อดำเนินการ ตามพรบการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ โรงพยาบาลสันกำแพง จึงได้จัดทำแผนรับมือภัยคุกคามทางไซเบอร์ขึ้นเพื่อรับมือกับภัยคุกคามทางไซเบอร์ในปัจจุบันและอนาคตโดยให้ครอบคลุมถึงการดำเนินการมาตรการป้องกัน (Protect) การตรวจจับ (Detect) การตอบสนอง (Respond) และการคืนสภาพ (Recover)

๒. วัตถุประสงค์

(๑) เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของโรงพยาบาล

(๒) เพื่อกำหนดกระบวนการในการเฝ้าระวัง ตรวจสอบ ติดตาม และแก้ไขปัญหาที่เกิดขึ้นจากภัยคุกคามทางไซเบอร์

(๓) เพื่อกำหนดขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ และการรายงานเหตุภัยคุกคามทางไซเบอร์ ไปยังหน่วยงานที่เกี่ยวข้อง

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของโรงพยาบาลสันกำแพง รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ที่เข้าถึงระบบสารสนเทศ และข้อมูลดิจิตอลดังกล่าว

๔. หน้าที่การทบทวนแผน

กลุ่มงานสารสนเทศ โรงพยาบาลสันกำแพง มีหน้าที่ทบทวน และขออนุมัติแผนรับมือฉบับ นี้ถึงผู้บริหารสูงสุดของหน่วยงาน หรือผู้บริหารเทคโนโลยีระดับสูงของโรงพยาบาล หรือผู้บริหารความมั่นคงปลอดภัยสารสนเทศระดับสูงของโรงพยาบาล

๕. หน้าที่ในการดำเนินงานตามแผน

ทุกหน่วยงานภายในโรงพยาบาลสันกำแพง มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฉบับนี้ โดยมีงานสารสนเทศ รวมถึงคณะกรรมการที่ทำหน้าที่กำกับดูแลระบบเทคโนโลยี สารสนเทศมีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฉบับนี้

๖. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๖.๑ นโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้อง

- แนวปฏิบัติเรื่องความมั่นคงปลอดภัยสารสนเทศโรงพยาบาลสันกำแพง
- แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลสันกำแพง
- การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลสันกำแพง

๖.๒ นโยบายและแนวปฏิบัติด้านการปกป้องข้อมูลส่วนบุคคลที่เกี่ยวข้อง

- ประกาศนโยบายการคุ้มครองข้อมูลส่วนบุคคล โรงพยาบาลสันกำแพง

๖.๓ กฎหมายที่เกี่ยวข้อง

- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม
- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒
- พระราชบัญญัติการรักษาความมั่งคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
- ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช)

๗. คำนิยาม

เหตุการณ์ (event)	หมายถึง	การเกิดขึ้นที่สังเกตได้ใด ๆ (Observable occurrence) ในระบบเครือข่ายสภาพแวดล้อม กระบวนการลำดับการดำเนินการหรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้
เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident)	หมายถึง	เหตุการณ์ที่มีผลเชิงลบ ที่เกิดจากการกระทำ หรือการดำเนินการใดใดโดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือโปรแกรมที่ไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้าย ต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็น ภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง
ภัยคุกคามทางไซเบอร์ (Cyber threat)	หมายถึง	การกระทำ หรือการดำเนินการใดใดโดยมิชอบ โดยใช้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง
เหตุภัยคุกคามไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ	หมายถึง	เหตุภัยคุกคามไซเบอร์ ที่ปรากฏต่อระบบสาระสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

ได้กำหนดลักษณะ ของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

ลักษณะของภัยคุกคามทางไซเบอร์และปัจจัยที่ใช้ในการประเมินภัยคุกคามทางไซเบอร์แต่ละระดับ

ในการพิจารณาระบุระดับของภัยคุกคามทางไซเบอร์ หน่วยงานโครงสร้างสำคัญทางสารสนเทศ ควรพิจารณาจากเหตุต่าง ๆ ที่เป็นพฤติกรรมแวดล้อม ผลกระทบที่เกิดขึ้น ความเสี่ยงหรือแนวโน้มที่อาจเกิดขึ้นจากภัยคุกคามทางไซเบอร์ในกรณีต่าง ๆ เพื่อพิจารณาว่าลักษณะของภัยคุกคามทางไซเบอร์นั้นอยู่ในระดับใด โดยให้พิจารณาจากปัจจัยที่ใช้การประเมินทั้ง ๔ ปัจจัย ดังนี้

(๑) ลักษณะผลกระทบที่เกิดขึ้นต่ออุปกรณ์หรือระบบงาน

(๒) ลักษณะผลกระทบต่อข้อมูลในระบบ

(๓) แนวโน้มในการกู้คืนระบบ

(๔) ลักษณะผลกระทบต่อผู้รับบริการ

การพิจารณาเพื่อระบุระดับของภัยคุกคามทางไซเบอร์แต่ละระดับนั้น หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ควรพิจารณาให้ครบทั้ง ๔ ปัจจัย ตามที่ได้ระบุไว้ข้างต้น โดยหากปรากฏข้อเท็จจริงว่าลักษณะภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น เข้าลักษณะ หรือมีแนวโน้มเป็นภัยคุกคามทางไซเบอร์ ในระดับใดให้ถือเอาระดับสูงสุดที่ประเมินได้เป็นเกณฑ์ในการระบุระดับของภัยคุกคามไซเบอร์ในครั้งนั้น ๆ นอกจากนี้ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ อาจพิจารณากำหนดปัจจัยที่ใช้ในการประเมิน และลักษณะภัยคุกคามทางไซเบอร์เพิ่มเติมร่วมกับหน่วยงานควบคุมกำกับหรือดูแล เพื่อให้มีแนวทางในการจำแนกระดับของภัยคุกคามทางไซเบอร์ที่เหมาะสม โดยจะต้องมีรายละเอียดไม่น้อยกว่าหรือเทียบเท่ากับแนวทางการพิจารณาที่กำหนดไว้ตามเอกสารแนบท้ายตารางที่ ๑

อย่างไรก็ดีเพื่อให้การดำเนินการรับมือปราบปราม และระงับภัยคุกคามด้านไซเบอร์แต่ละระดับมีความเหมาะสม และสอดคล้องกับสถานการณ์โดยรวมที่เกิดขึ้น คณะกรรมการอาจพิจารณาปรับเปลี่ยน หรือยกระดับของภัยคุกคามไซเบอร์ที่ได้รับรายงานเป็นอย่างอื่นได้ หากปรากฏข้อเท็จจริงเพิ่มเติมหรือพบว่าภัยคุกคาม และไซเบอร์ที่เกิดขึ้นนั้น มีแนวโน้มที่จะลุกลามหรือก่อให้เกิดความเสียหายมากขึ้น

อนึ่ง เพื่อให้สอดคล้องกับสภาวการณ์ที่เปลี่ยนแปลงไป คณะกรรมการ หรือผู้ที่ได้รับมอบหมายจากคณะกรรมการ อาจพิจารณาทบทวนลักษณะภัยคุกคามทางไซเบอร์ ปรับปรุงปัจจัยที่ใช้ในการประเมินหรือนำเงื่อนไขอื่น ๆ มาประกอบการพิจารณาเพิ่มเติมที่เห็นสมควร

๘. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์

๘.๑ ผู้รับเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในโรงพยาบาลสันกำแพง

กลุ่มงานสารสนเทศ ระบุข้อมูลการติดต่อของผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในโรงพยาบาล กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์ที่เกี่ยวข้องกับ ความมั่นคงปลอดภัยไซเบอร์ โดยมีผู้รับแจ้งเหตุหลักรวมถึงช่องทางหลักในการติดต่อ และเตรียมผู้รับแจ้งเหตุคนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้โดย งานสารสนเทศ กำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุ รายละเอียดดังตาราง

ลำดับ	ชื่อ-นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	งานสารสนเทศ	ในเวลาราชการ เวลา ๐๘.๓๐ – ๑๖.๓๐ น.	โทร. ภายใน Back Office	ผู้ประสานงานหลัก/รับแจ้งเหตุ	ผู้ประสานด้านความมั่งคงปลอดภัยไซเบอร์ของโรงพยาบาล
๒		นอกเวลาราชการ	โทร. เจ้าหน้าที่	ผู้ประสานงานหลัก/รับแจ้งเหตุ	ผู้ประสานด้านความมั่งคงปลอดภัยไซเบอร์ของโรงพยาบาล

๘.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์
(Cyber Incident Response Team: CIRT)

งานสารสนเทศ ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ ที่เกี่ยวข้องกับความมั่นคงปลอดภัย ไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อนามสกุล	หน้าที่	ความรับผิดชอบ
๑	หัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์ฯ	หัวหน้าทีมรับมือ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของโรงพยาบาล และเจ้าหน้าที่ทุกระดับ
๒	หัวหน้างานสารสนเทศ	รองหัวหน้าทีมรับมือ (Deputy Team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	เจ้าหน้าที่งานสารสนเทศ	เจ้าหน้าที่รับมือ (Incident Lead)	ทำหน้าที่ช่วยเหลือหน่วยงาน ให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้ ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์

๘.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

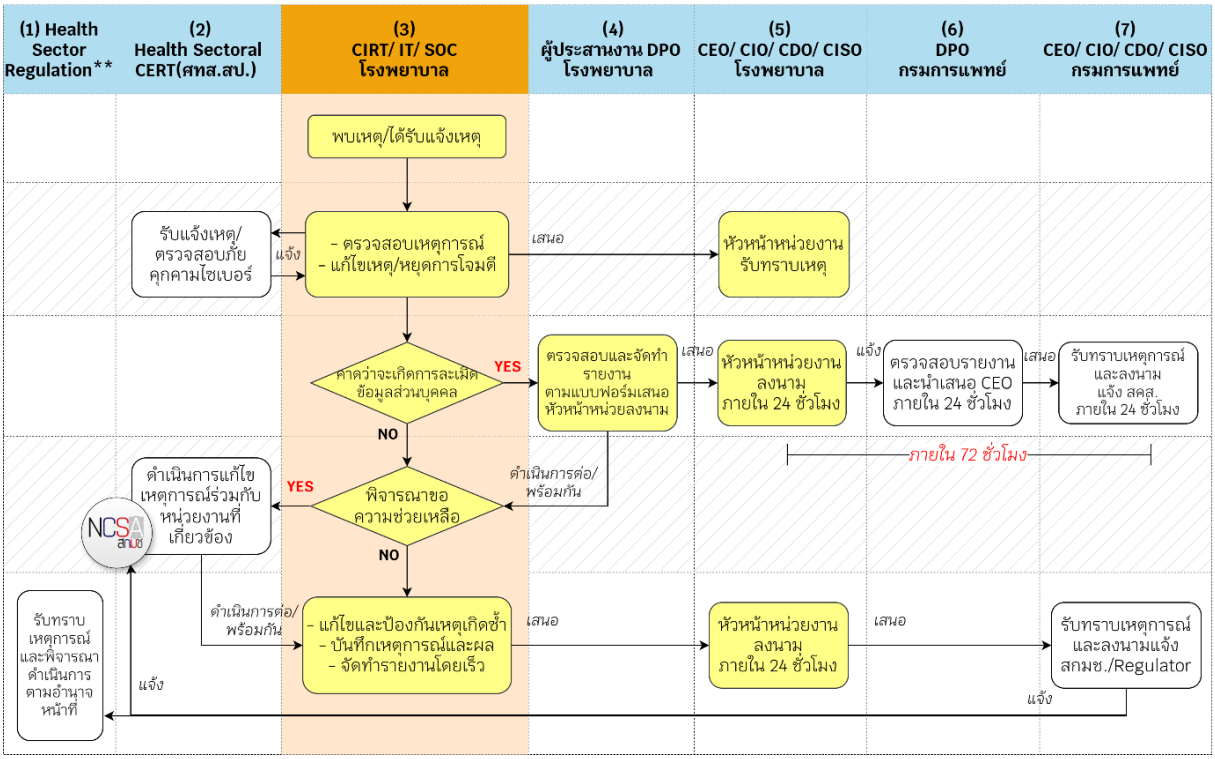
งานสารสนเทศ ได้จัดให้มีข้อมูลติดต่อสื่อสารของหน่วยงานภายนอกที่เกี่ยวข้อง เช่น สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) หน่วยงานกำกับดูแล (Regulator) Health-CERT THAI-CERT และผู้ให้บริการภายนอกของหน่วยงานเช่น หน่วยงานผู้ให้บริการด้านการตรวจสอบพิสูจน์หลักฐานทางดิจิตอล (Digital Forensic Investigator) เป็นต้น

ลำดับ	ชื่อนามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	National Cyber Security Agency	โทร. ๐๒-๑๔๒-๖๘๘๘ Email: saraban@ncsa.or.th ที่อยู่สำนักงาน ๑๒๐ หมู่ ๓	สำนักงานคณะกรรมการการรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	หน่วยงานหลัก

ลำดับ	ชื่อนามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
		อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น ๗ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐		
๒	Health Sectoral CERT	โทร. ๐๒-๕๙๐-๑๑๖๙, ๐๒-๕๙๐-๑๒๐๐, ๐๘๓-๐๖๔-๙๘๖๗ Email health-cirt@moph.go.th Line: @health-cirt https://health-cirt.moph.go.th	ศทส.สป.	แจ้งเหตุภัย คุกคามไซเบอร์ Health Sectoral CERT
๓	สำนักงาน คณะกรรมการ คุ้มครองข้อมูล ส่วนบุคคล	โทร. ๐๒-๑๔๒-๑๐๓๓, ๐๒-๑๔๑-๖๙๙๓ Email: saraban@pdpc.or.th ที่อยู่สำนักงาน ๑๒๐ หมู่ ๓ ชั้น ๖-๙ อาคารรัฐประศาสนภักดี ศูนย์ราชการเฉลิมพระเกียรติ ๘๐ พรรษา ๕ ธันวาคม ๒๕๕๐ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ ๑๐๒๑๐	กระทรวงดิจิทัล เพื่อเศรษฐกิจและ สังคม	แจ้งเหตุการ ละเมิดข้อมูลส่วน บุคคล
๔	กรมการแพทย์	โทร. ๐-๒๕๙๐-๖๐๐๐ Email: saraban@dms.mail.go.th ที่อยู่สำนักงาน ๘๘/๒๓ ถนนติวานนท์ ต.ตลาดขวัญ อ.เมือง จ.นนทบุรี ๑๑๐๐๐	กระทรวง สาธารณสุข	หน่วยงานกำกับ ดูแล

๘.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

งานสารสนเทศ ได้จัดทำแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงานหน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก เป็นต้น รวมถึงกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติและกฎหมายย่อยใด ๆ ที่จะทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมายและข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)
อ้างอิงจาก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

๙. ขั้นตอนการรับมือ

แผนรับมือฉบับนี้ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการ กำกับ ดูแล ด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วย โครงสร้างพื้นฐาน

สำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์ และวิธีการรายงานภัยคุกคามทางไซเบอร์ พ.ศ. ๒๕๖๖ รวมถึงนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของโรงพยาบาลสันกำแพง ดังนี้

วัฏจักรของการตอบสนองต่อเหตุการณ์

๙.๑ ขั้นการเตรียมการ (Preparation)

โรงพยาบาลสันกำแพง จะต้องดำเนินการมาตรการเพื่อเตรียมการ และป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่ การจัดเตรียมข้อมูลให้พร้อม การจัดตั้ง และฝึกอบรมบุคลากรหรือทีมงานการจัดหาเครื่องมือและทรัพยากรต่าง ๆ ที่จำเป็น การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้องรวมถึงการสร้างเครือข่ายความร่วมมือโดยดำเนินการดังต่อไปนี้

(๑) กำหนดโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รายละเอียดปรากฏตามข้อ ๘.๒

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) รายละเอียดปรากฏตามข้อ ๘.๔

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์ และ CIRT

(๔) จัดเตรียมข้อมูลและอุปกรณ์ รวมถึงช่องทางในการติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อและอุปกรณ์ติดต่อสื่อสาร ของบุคลากร กลไกรายงานเหตุการณ์ห้องประชุม (War room) เป็นต้น

(๕) จัดเตรียมอุปกรณ์ซอฟต์แวร์แหล่งข้อมูลสำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๖) จัดให้มีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน (Risk Assessment)

(๗) จัดทำแผนผังโครงสร้างขั้นตอนการรับมือของโรงพยาบาลสันกำแพง โดยทำการจัดทำแผนผังโครงสร้างขั้นตอนการรับมือไว้ (รายละเอียดปรากฏตามภาคผนวก ๒)

นอกจากนี้โรงพยาบาลสันกำแพง จะพิจารณาดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

โรงพยาบาลสันกำแพง จะต้องดำเนินการในการตรวจจับ และวิเคราะห์ภัยคุกคามทางไซเบอร์ ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้โรงพยาบาลสันกำแพง สามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงที เมื่อมีภัยคุกคามไซเบอร์เกิดขึ้นโดยดำเนินการ ดังต่อไปนี้

๙.๒.๑ ดำเนินการจัดเตรียมแนวทางรับมือเมื่อเกิดการโจมตีรูปแบบทั่วไปที่เคยเกิดขึ้น หรืออาจเกิดขึ้นกับหน่วยงาน (Common Attack Vectors/Common Threat Vectors) โดยการโจมตีรูปแบบทั่วไปที่อาจเกิดขึ้น มีตัวอย่างดังนี้

ประเภท	External/Flash Drive
อธิบาย	การโจมตีที่ดำเนินการจากอุปกรณ์แบบถอดได้หรืออุปกรณ์ต่อพ่วง ตัวอย่างเช่น Code ที่เป็นอันตราย แพร่กระจายไปยังระบบปฏิบัติการจากแฟลชไดรฟ์ที่ติดไวรัส
วิธีการรับมือ	ดำเนินการถอนติดตั้งอุปกรณ์แบบถอดได้ที่เป็นสาเหตุของภัยคุกคามออกจากอุปกรณ์และระบบเครือข่ายของหน่วยงาน และตรวจสอบสาเหตุและประเภทของภัยคุกคามว่าเป็นภัยคุกคามประเภทใด

๙.๒.๒ ดำเนินการจัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้น ของการเกิดภัยคุกคามในไซเบอร์ ได้ในระยะเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยดำเนินการดังต่อไปนี้

ก. วิธีที่ใช้ในการตรวจจับภัยคุกคาม

- เตรียมและใช้เครื่องมือ และอุปกรณ์เฝ้าระวังเหตุการณ์ด้านความมั่งคงปลอดภัย

- Firewall ระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์ ที่สามารถควบคุม คัดกรอง ข้อมูลที่รับและส่งผ่านเครือข่ายได้
- IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีโดยเฉพาะที่เกิดขึ้นในระบบเครือข่าย โดยระบบประเภทนี้จะตรวจจับได้เฉพาะสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก
- Endpoint Security ซอฟต์แวร์ตรวจจับโปรแกรมประสงค์ร้ายที่พยายามโจมตีต่อระบบคอมพิวเตอร์และเครือข่าย
- Centralized Log Management ระบบจัดเก็บและบริหารจัดการข้อมูล
- Log File แบบศูนย์กลาง

- ติดตามแหล่งข่าวสารภัยคุกคามจากภายนอก (Threat Intelligence)

Channel Types	URL
Cybersecurity News Sites	
	https://www.thaicert.or.th/category/cybernews/
	https://health-cirt.moph.go.th/pages/dashboard/
	https://www.blognone.com/topics/security
	https://www.techtalkthai.com/category/security/
	https://thehackernews.com/

	https://www.bleepingcomputer.com/news/security/a
Community Facebook Pages	
	https://www.facebook.com/NCSA.Thailand/
	https://www.facebook.com/thaicert/
	https://www.facebook.com/thaicysec/
threat intelligence resources:	
	https://otx.alienvault.com
	https://www.virustotal.com
	https://bazaar.abuse.ch
	https://talosintelligence.com
	https://www.spamhaus.org
	https://www.threatminer.org
	https://attack.mitre.org
	https://www.team-cymru.com
	https://exchange.xforce.ibmcloud.com
	https://www.threatconnect.com/open

ข. จัดประเภทภัยคุกคามไซเบอร์

ประเภท	ความหมาย
Malware/ Malicious Code	ซอฟต์แวร์ หรือ ชุดคำสั่ง (Code) ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่ง ผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบ คอมพิวเตอร์และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ ได้โดยมี พฤติกรรมแตกต่างกันตามที่ผู้ไม่ประสงค์ดีที่ทำการผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึง ไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)
Web-based attacks	วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยหาเว็บไซต์ที่มีช่องโหว่เพื่อแก้ไข เว็บไซต์โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมาย ปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware
Phishing	วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดย ใช้วิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Username, Password หรือ ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

ประเภท	ความหมาย
Web application attacks	วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์และ Web Server หรือ Database Server
Spam	วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail, SMS, เว็บไซต์หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาต ไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน
DDoS (Distributed Denial of Service)	วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์ ระบบการให้บริการ หรือ ระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์ที่ ทำเพื่อให้เว็บไซต์ ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้ หรือระบบล่ม
Data breach	การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต หรือการเข้าถึงข้อมูลโดยอาจเกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูล ของเว็บไซต์ ข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน หรือ ผู้ให้บริการระบบไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูลนั้น ๆ
Insider threat	ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือ ไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิด การโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง
Botnets หรือ Robot Network	โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดีที่ทำการติดตั้งโปรแกรมแบบแฝงตัว อยู่ในเครื่องคอมพิวเตอร์หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่าง ซึ่งแฝงตัวบนเครื่องของเหยื่อและโดยส่วนมากจะไม่ทราบว่ามีการติด Botnets เนื่องจาก Botnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)
Ransomware	คือ Malware ประเภทหนึ่งที่เมื่อถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะทำการล็อคไฟล์ โดยวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่อง ทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ซึ่งจุดประสงค์ของ Ransomware ทำการล็อคไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อคไฟล์เพื่อให้ไฟล์ที่อยู่ภายในเครื่อง คอมพิวเตอร์นั้นสามารถกลับมาใช้งานได้อีกครั้ง
Crypto jacking	วิธีการที่ Hacker เข้าเครื่องคอมพิวเตอร์ของเหยื่อโดยวิธีการต่าง ๆ และแอบทำการ ติดตั้งโปรแกรมที่ใช้ เพื่อการขุดเหรียญ Cryptocurrency โดยอาศัย CPU หรือ GPU บนเครื่องคอมพิวเตอร์ของเหยื่อ ประมวลผลเพื่อสร้างรายได้กลับไปที่ Hacker

ประเภท	ความหมาย
ผู้บุกรุก (Hacker)	ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกคามที่หนัก

นอกจากนี้ยังมีการจำแนกประเภทภัยคุกคามตามประกาศ คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (รายละเอียดปรากฏตามภาคผนวก ๑)

๙.๒.๓ ดำเนินการจัดให้มีแนวทางในการวิเคราะห์ผลกระทบและระดับของภัยคุกคามทางไซเบอร์ (Incident Prioritization) เพื่อรับมือกับภัยคุกคามทางไซเบอร์ให้ทันท่วงที โดยพิจารณาปัจจัยต่างๆที่เกี่ยวข้อง เช่น ผลกระทบต่อการดำเนินงานของระบบ (Functional Impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น

ระดับผลกระทบต่อการดำเนินงาน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่มีผลกระทบต่อการดำเนินงาน
Low	ส่งผลให้การปฏิบัติงานตามภารกิจมีความล่าช้า แต่ยังสามารถดำเนินงานต่อได้
Medium	ส่งผลให้งานตามภารกิจหลัก ไม่สามารถดำเนินการได้บางส่วน หรืออาจกระทบต่อคุณภาพการวินิจฉัยโรคและการรักษาผู้ป่วย
High	ส่งผลให้งานตามภารกิจหลักหยุดชะงัก/ระบบงานตรวจรักษาผู้ป่วยนอกหยุดชะงัก การให้บริการผู้ป่วยที่มาตรวจชาลงอย่างมาก กระทบต่อชีวิตและสุขภาพประชาชน

ระดับผลกระทบต่อข้อมูล

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
None	ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึงโดยที่ไม่ได้รับอนุญาต
Low	การละเมิดความลับของข้อมูลส่วนบุคคล ซึ่งมีการเข้าถึง หรือเปิดเผยข้อมูลส่วนบุคคล
Medium	การละเมิดความถูกต้องครบถ้วนของข้อมูลส่วนบุคคลซึ่งมีการเปลี่ยนแปลง แก้ไขข้อมูลส่วนบุคคลให้ไม่ถูกต้อง ไม่สมบูรณ์ หรือไม่ครบถ้วน
High	การละเมิดความพร้อมใช้งานของข้อมูลส่วนบุคคล ซึ่งทำให้ไม่สามารถเข้าถึงข้อมูลส่วนบุคคลได้ หรือมีการทำลายข้อมูลส่วนบุคคล ทำให้ข้อมูลส่วนบุคคลไม่อยู่ในสภาพที่พร้อมใช้งานได้ตามปกติ

ระดับความสามารถในการกู้คืน

ระดับผลกระทบ	หลักเกณฑ์การพิจารณาระดับของผลกระทบ
Regular	เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
Supplemented	เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
Extended	เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากหน่วยงานภายนอก

Not Recoverable	การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๙.๒.๔ ดำเนินการจัดให้มีการบันทึกรายงานสถานการณ์ เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์มตัวอย่าง (รายละเอียดปรากฏตามภาคผนวก ๓)

๙.๒.๕ โรงพยาบาลสันกำแพง ต้องจัดให้มีการ ทำบันทึกข้อมูลกิจกรรมเหตุการรักษาความมั่นคงปลอดภัยไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับ เหตุการณ์ ความปลอดภัยทางไซเบอร์ทุกขั้นตอน ตั้งแต่ตรวจพบเหตุการณ์ จนถึงกระบวนการสุดท้ายแ ละข้อมูลดังกล่าวควรระบุรายละเอียดพร้อมเวลาที่เกิดเหตุ และระยะเวลาที่ใช้ด้วย บันทึกข้อมูลดังกล่าวที่เกี่ยวข้องกับเหตุการณ์ควรลงวันที่ และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้น ๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม โดยอาจกำหนดให้มีรายละเอียดตามแบบฟอร์ม (รายละเอียดปรากฏตามภาคผนวก ๔)

๙.๒.๖ เนื่องจากโรงพยาบาลสันกำแพง ถือเป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทาง สารสนเทศ (Critical Information Infrastructure: CII) ตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง การกำหนดหลักเกณฑ์ ลักษณะหน่วยงานที่มีภารกิจหรือให้บริการ เป็นหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการมอบหมายการควบคุมและกำกับดูแล พ.ศ. ๒๕๖๔ หมวด ๗ ด้านสาธารณสุข จึงจัดให้มีการรายงานภัยคุกคามไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ผู้ ที่เกี่ยวข้องทราบตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง หลักเกณฑ์และวิธีการรายงานภัยคุกคามไซเบอร์ พ.ศ. ๒๕๖๖ ดังนี้

(ก) กรณีมีเหตุภัยคุกคามไซเบอร์ที่เกิดขึ้นกับหน่วยงานรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามข้อ ๔ แห่งประกาศฉบับดังกล่าวให้ใช้แบบฟอร์ม ก๑ โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ข) กรณีมีเหตุภัยคุกคามไซเบอร์ที่เกิดขึ้นอย่างมีนัยยะสำคัญต่อระบบของหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศกับหน่วยงานรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ตามข้อ ๕ แห่งประกาศฉบับดังกล่าว ให้ใช้แบบฟอร์ม ก๒ รายงานไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติภายในระยะเวลา ๒๔ ชั่วโมง โดยใช้แบบฟอร์มการรายงานตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕)

(ค) หน่วยงานของรัฐหรือหน่วยงานควบคุมกำกับดูแล จะต้องจัดทำ และส่งรายงานสรุปจำนวนเหตุภัยคุกคามไซเบอร์ทั้งหมดที่เกิดขึ้น กับข้อมูลหรือระบบสารสนเทศของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ภายใต้การควบคุมหรือกำกับดูแลของตนในแต่ละปี ภายในวันที่ ๓๑ มกราคมของปีถัดไป ให้แก่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามที่กำหนดในเอกสาร ก๓ โดยใช้แบบฟอร์มแรงงาน ตามกฎหมาย (รายละเอียดปรากฏตามภาคผนวก ๕) นอกจากนี้โรงพยาบาลสันกำแพง พิจารณาดำเนินการตามเอกสารแนบท้ายตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๙.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, eradication and recovery)

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น หรือหน่วยงานได้รับแจ้งเตือน การเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินการ เพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ โดยควรกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพย์สินสำคัญทางสารสนเทศ ให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นตอนนี้ อาจจะต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลาม หรือทวีความรุนแรงมากขึ้น เพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดภัยคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป โดยดำเนินการดังต่อไปนี้

(๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์ โดยเลือกตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut down)
- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network Disconnection) ทั้งนี้ อาจมีการยกเว้นการเชื่อมต่อสำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ที่น่าสงสัยใด ๆ ที่เกิดขึ้นปลายทางแบบเรียวไทม์)
- หยุดการทำงานของฟังก์ชั่นการให้บริการที่เกี่ยวข้องทั้งหมด (Disabling Certain Function)
- เปลี่ยนแปลงเส้นทางจราจรเครือข่าย (Redirect Network Traffic) หรือความสนใจของผู้บุกรุกไปยังระบบ Blackhole/Sandbox/Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญตามประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

(๒) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึก การยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน เพื่อให้การแก้ไข Incident ส่งผลกระทบต่อการให้บริการให้น้อยที่สุด (Minimizing Impact to the business)

นอกจากนี้หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ได้ในชั้นศาล เช่น
    - การจัดการข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (Volatile data)
    - การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานของระบบ (System snapshot) หรือข้อมูลอื่นๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์เชิงเทคนิคตามกฎหมายกำหนด
- หลักฐานมีบันทึกการเข้าถึงและกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลดังต่อไปนี้
    - ข้อมูลเฉพาะตัว เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
    - ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บ และรักษาหลักฐานระหว่างการรับมือ Incident
    - สถานที่จัดเก็บหลักฐาน

(๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์ ตามรายละเอียดข้อ ๙.๒

(๔) การจำกัดสาเหตุ (Eliminate) เมื่อดำเนินการสอบสวนสาเหตุที่มา ผลกระทบที่เกิดขึ้น รวมถึงทราบช่องทางที่ผู้บุกรุกได้สร้างขึ้นไว้เพื่อเข้ามาในระบบทั้งหมดได้เรียบร้อย การกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบได้แก่

- การปิดช่องโหว่ของระบบ
- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ
- การแจ้งให้ System Administrator ที่เกี่ยวข้องเปลี่ยนรหัสผ่าน
- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน
- การลบโปรแกรมประเภท Backdoor ออกจากระบบ
- การใช้ข้อมูล Indicator of Compromise (IOC) ในกาสแกนหามัลแวร์ หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุก เพื่อดำเนนิการกำจัดให้ออกจากระบบทั้งหมด

(๕) การเรียกการใช้งานกระบวนการกู้คืนและฟื้นฟูระบบ (Recovery Process) หลังจากการดำเนินการจำกัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยในขั้นตอนนี้สิ่งที่มีความสำคัญ และควรมีการเตรียมความพร้อม ได้แก่

- การเตรียมการทำ Master Image ที่มีความปลอดภัย สำหรับ Restore Operation System หรือ Application Software ต่าง ๆ
- การ Restore ข้อมุลกลับเข้าระบบจาก Backup Storage/Backup Tape

(๖) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์ การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

นอกจากนี้โรงพยาบาลสันกำแพง พิจารณาดำเนินการตามเอกสารแนบท้ายตารางที่ ๒. ๓ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์นั้น ให้จัดทำข้อกำหนด ขั้นตอน วิธีปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้อง เพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าวจะช่วยให้หน่วยงาน สามารถเรียนรู้จากเหตุภัยคุกคามไซเบอร์ ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามไซเบอร์ต่อไปในอนาคต นอกจากนี้โรงพยาบาลสันกำแพง ต้องเก็บรักษาข้อมูล และพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องร้องทุกข์ หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม (ถ้ามี) หรือกฎหมายอื่นที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) การทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุ และแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

(๒) ดำเนินการตามเอกสารแนบท้ายตารางที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔ เพิ่มเติม

๙.๕ การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงาน เกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยสามารถใช้ข้อมูลเพื่อประกอบพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๖)

เอกสารอ้างอิง

แผนการรับมือภัยคุกคามทางไซเบอร์ โรงพยาบาลประสาท เชียงใหม่

แผนการรับมือภัยคุกคามทางไซเบอร์ กรมการขนส่งทางราง

แผนรับมือภัยคุกคามทางไซเบอร์ Cybersecurity Incident Response Plan จุฬาลงกรณ์มหาวิทยาลัย

แผนรับมือภัยคุกคามทางไซเบอร์กรมกิจการเด็กและเยาวชน

แนวทางการดำเนินงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร สำหรับโรงพยาบาลของรัฐ พ.ศ. ๒๕๖๗ สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอรแหงขาติ (สกมช.) และ สมาคมเวชสารสนเทศไทย (Thai Medical Informatics Association – TMI)

เอกสารแนบท้าย

ตารางที่ ๒.๑ การดำเนินการมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (Preparation)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
กรณีบริการ ระบบ หรืออุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ <u>ระดับไม่ร้ายแรง</u> กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคาม ทางไซเบอร์ <u>ในระดับร้ายแรง</u> กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคาม ทางไซเบอร์ <u>ในระดับวิกฤต</u>	(๑) จัดเตรียมข้อมูลและอุปกรณ์การติดต่อสื่อสารที่จำเป็น เช่น ข้อมูลการติดต่อของบุคคลหรือองค์กรต่าง ๆ คู่มือการปฏิบัติงานเพื่อรับมือกับภัยคุกคามทางไซเบอร์ และกลไกอื่นใด ที่ช่วยสนับสนุนการรายงานเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น เป็นต้น (๒) จัดเตรียมอุปกรณ์หรือทรัพยากรสนับสนุนที่จำเป็นสำหรับการรับมือกับภัยคุกคามทางไซเบอร์ (๓) ดำเนินการให้มีการจัดหมวดหมู่ข้อมูลและระบบสารสนเทศให้สอดคล้องกับแนวทาง ของกฎหมาย กฎเกณฑ์ หรือนโยบายต่าง ๆ ที่เกี่ยวข้อง เพื่อธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) ตลอดจนสภาพพร้อมใช้งาน (availability) ของข้อมูลและระบบสารสนเทศดังกล่าว (๔) จัดเตรียมข้อมูลสนับสนุนที่จำเป็นสำหรับการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ เช่น รายการทรัพย์สินสำคัญทางสารสนเทศ และแผนผังโครงสร้างเครือข่าย (Network diagrams) เป็นต้น (๕) พิจารณาซ่อนบริการหรือระบบที่ผู้โจมตีสามารถค้นพบในเครือข่ายได้ง่าย โดยไม่ต้องใช้ ความพยายามเจาะระบบ เช่น การค้นหาผ่านกลไกการสืบค้น (discovery protocol) เป็นต้น (๖) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) (๗) กำหนดตัวบุคคลหรือมอบหมายให้เจ้าหน้าที่ที่มีความชำนาญเป็นผู้ดำเนินการที่เกี่ยวข้องกับการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ รวมถึงการทำหน้าที่ ในการประสานงานหรือหารือกับผู้ที่เกี่ยวข้อง (๘) จัดให้มีกระบวนการในการพิสูจน์ตัวตนผู้ใช้งานก่อนทำการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ใด ๆ เช่น การเข้ารหัสข้อมูลและการบริหารจัดการคีย์สำหรับการเข้าถึงระบบต่าง ๆ (cryptography/key managements) เป็นต้น (๙) ตรวจสอบแอปพลิเคชันที่ให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความปลอดภัยเพียงพอ โดยมีการคัดกรองนักพัฒนา (developer screening) ที่ได้รับ มอบหมายให้ดำเนินการใด ๆ กับเครือข่าย แอปพลิเคชัน หรือระบบงานต่าง ๆ (๑๐) ดำเนินการให้มีการทดสอบความสามารถในการตอบสนองต่อภัยคุกคามทางไซเบอร์ (incident respond capability testing) (๑๑) รวบรวมข่าวกรองเกี่ยวกับภัยคุกคามทางไซเบอร์ (threat Intelligence) (๑๒) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติ เพื่อดำเนินการทดสอบการเจาะระบบเป็นประจำ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อพบช่องโหว่ หรือ จุดอ่อนต่าง ๆ (ถ้าหน่วยงานมีความพร้อม)

	(๑๓) กำหนดแนวทางและระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ (๑๔) ดำเนินการควบคุมการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ต่าง ๆ (configuration change control) และจัดทำแผนการบริหารจัดการการตั้งค่าหรือการเปลี่ยนแปลง ค่าของอุปกรณ์ (configuration management plan) โดยจะต้องจัดให้มีกลไก ที่สามารถบันทึกประวัติการเปลี่ยนแปลงการตั้งค่าของอุปกรณ์ที่เป็นลายลักษณ์อักษร การแจ้งเตือนเมื่อมีการเปลี่ยนแปลงค่าของอุปกรณ์ที่ตั้งไว้ และให้พิจารณาจัดให้มี กลไกที่สามารถป้องกันการเปลี่ยนแปลงค่าของอุปกรณ์ต่าง ๆ โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๑๕) จัดให้มีการฝึกอบรมเพื่อเตรียมพร้อมรับมือกับสถานการณ์ฉุกเฉินเมื่อมีภัยคุกคาม ทางไซเบอร์เกิดขึ้น (simulated events) เพื่อให้ผู้ปฏิบัติรับทราบบทบาทและ ความรับผิดชอบของตนเมื่อต้องรับมือกับสถานการณ์ดังกล่าว (๑๖) สร้างเครือข่ายความร่วมมือเพื่อแบ่งปันข้อมูลและประสานงานเกี่ยวกับการจัดการ ภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๒ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
กรณีบริการ ระบบหรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็น ภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบหรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	(๑) จัดให้มีกลไกที่สามารถตรวจจับสิ่งบ่งชี้หรือลักษณะเบื้องต้นของการเกิดภัยคุกคาม ทางไซเบอร์ได้ในเวลาอันเหมาะสม โดยอาจอาศัยข้อมูลจากแหล่งข้อมูลต่าง ๆ เช่น ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์สำหรับหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ เป็นต้น (๒) จัดให้มีกลไกที่สามารถรับการแจ้งเตือนเกี่ยวกับภัยคุกคามทางไซเบอร์ (๓) จัดให้มีข้อพึงปฏิบัติพื้นฐานเกี่ยวกับการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อความการแจ้งข้อผิดพลาด หรือข้อความเตือนภัยจากเครื่องมือรักษาความปลอดภัย ด้านไซเบอร์ และการตรวจสอบระบบงานที่มีความสำคัญ (critical systems) โดยจะต้องจัดให้มีข้อพึงปฏิบัติที่สูงขึ้นสำหรับทุกระบบงานที่มีความสำคัญมากขึ้น (๔) วิเคราะห์ข้อมูลและประวัติการใช้งานต่าง ๆ เช่น ลักษณะการใช้งานเครือข่ายและ ระบบงาน (profile networks and systems) เป็นต้น เพื่อทำความเข้าใจพฤติกรรม การใช้งานในช่วงเวลาปกติ (normal behaviors) ทำการศึกษาวิจัยและค้นหา ความสัมพันธ์ของข้อมูลในระบบกับสถานการณ์ต่าง ๆ (event correlation) (๕) ทันทีที่พบว่ามีหรืออาจมีภัยคุกคามทางไซเบอร์เกิดขึ้น ให้ดำเนินการสืบหา และรวบรวมข้อมูลทั้งหมด เช่น ลักษณะภัยคุกคามทางไซเบอร์, ช่องโหว่ที่อาจถูกใช้ในการโจมตี, สถานการณ์ของการโจมตี(อาทิ กำลังเกิดเหตุหรือสถานการณ์ได้สิ้นสุดแล้ว การโจมตีเป็นผลสำเร็จหรือไม่สำเร็จ ฯลฯ) จำนวนระบบหรือบริการที่ได้รับผลกระทบ, โฮสต์เนม ตำแหน่งหรือสถานที่ของระบบหรือบริการที่ได้รับผลกระทบ ข้อมูลผู้ใช้ เวลาประทับ ข้อมูล payload ข้อมูลแจ้งเตือนจาก IDS (ถ้ามี) และ ข้อมูลจราจร

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
	ทางคอมพิวเตอร์ (log) เป็นต้น โดยหน่วยงานจะต้องเก็บรักษาข้อมูลดังกล่าว (safeguard incident data) ให้มีความปลอดภัย เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์และใช้เป็นพยานหลักฐานในการดำเนินคดี รวมถึงการจัดทำรายงานที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ (๖) ระบุหมวดหมู่ของภัยคุกคามทางไซเบอร์ตามสถานการณ์ที่เกิดขึ้น และติดตามเพื่อระบุ หมวดหมู่ของภัยคุกคามทางไซเบอร์ที่เปลี่ยนแปลงไปจนกว่าสถานการณ์ดังกล่าวจะสิ้นสุด โดยอาจพิจารณาจากข้อมูลตามที่ระบุในข้อ ๒ ของภาคผนวก ๑ แนบท้ายนี้ (๗) จัดลำดับความสำคัญของการดำเนินการเพื่อรับมือกับภัยคุกคามทางไซเบอร์ ให้ทันท่วงที โดยพิจารณาปัจจัยต่าง ๆ ที่เกี่ยวข้อง เช่น ผลกระทบต่อการทำงาน ของระบบ (functional impact) ผลกระทบต่อข้อมูล (information impact) และความสามารถในการกู้คืน (recoverability effort) เป็นต้น (๘) ศึกษาวิธีและลักษณะการโจมตี พร้อมทั้งระบุสาเหตุที่แท้จริงของภัยคุกคามทางไซเบอร์รวมถึงจุดอ่อนของระบบที่ถูกโจมตี (๙) ดำเนินการแจ้งไปยังผู้ที่รับผิดชอบในการเผชิญเหตุหรือผู้ที่เกี่ยวข้องผ่านช่องทางที่มีความปลอดภัย โดยคำนึงถึงระดับชั้นความลับและความสำคัญของข้อมูล เพื่อให้บุคคลดังกล่าวสามารถปฏิบัติหน้าที่ในการรับมือกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้น (๑๐) รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศอย่างมีนัยสำคัญให้ผู้ที่เกี่ยวข้องทราบ ภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด (โดยหน่วยงานควบคุมหรือกำกับดูแลอาจกำหนดให้นำข้อปฏิบัติตามแผนการกู้คืนของหน่วยงานมาประกอบการพิจารณาด้วยก็ได้) หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวกแนบท้ายนี้ แล้วแต่กรณี
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) จัดให้มีกลไกที่สามารถแจ้งเตือนได้ทันที (real-time alerts) เมื่อพบว่ามีภัยคุกคาม ทางไซเบอร์เกิดขึ้น (๒) จัดให้มีกลไกหรือระบบงานที่สามารถติดตามเหตุการณ์ และสามารถจัดเก็บและ วิเคราะห์ข้อมูลต่าง ๆ เพื่อตรวจจับการเกิดภัยคุกคามทางไซเบอร์ได้โดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม) (๓) จัดให้มีการแจ้งเตือนเกี่ยวกับความผิดปกติของการใช้ทรัพยากรของระบบงาน เช่น แจ้งเตือนเมื่อหน่วยความจำที่ใช้ในการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์เหลือน้อย (storage capacity warning) เมื่อมีการใช้หน่วยประมวลผลกลาง (CPU) หรือมีการใช้ หน่วยความจำหลัก (RAM) ของอุปกรณ์เครือข่าย หรือระบบงานหลักที่สูงผิดปกติ หรือ เมื่อมีการส่งข้อมูลออกนอกเครือข่ายมากผิดปกติ เป็นต้น (๔) วิเคราะห์ข้อมูลและค้นหาความสัมพันธ์ของข้อมูลกับเหตุการณ์ต่าง ๆ (information correlation) โดยอาจรับข้อมูลจากแหล่งข้อมูลอื่น ๆ นอกเหนือจาก

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
	ข้อมูลในระบบ เพื่อเพิ่มความสามารถในการรับรู้และดำเนินการตรวจจับ และวิเคราะห์ภัยคุกคามทางไซเบอร์ได้อย่างมีประสิทธิภาพ

ตารางที่ ๒.๓ การดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ กำรปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง	(๑) ดำเนินการตามแนวทางหรือวิธีการในการจำกัดขอบเขตและระงับภัยคุกคามทางไซเบอร์โดยที่แนวทางหรือวิธีการดังกล่าวจะต้องมีหลักเกณฑ์ที่ชัดเจน เพื่อใช้ประกอบการตัดสินใจในการดำเนินการ ทั้งนี้แนวทางดังกล่าวรวมถึง (๑.๑) การดำเนินการเชิงเทคนิค เช่น การลบมัลแวร์ การปิดการใช้งานบัญชีของผู้ใช้งานที่ถูกละเมิด การปิดระบบหรือตัดการเชื่อมต่อของระบบจากเครือข่ายภายหลังการเก็บหลักฐานหรือข้อมูลที่จำเป็นเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ และใช้เป็นพยานหลักฐานในการดำเนินคดีแล้ว เป็นต้น (๑.๒) การดำเนินการเชิงบริหาร เช่น กำหนดแนวทางดำเนินการหรือการตัดสินใจของ ฝ่ายบริหารของหน่วยงาน การสื่อสารทั้งภายในและภายนอกหน่วยงาน เป็นต้น (๑.๓) การเตรียมการเพื่อดำเนินการทางกฎหมายกับผู้กระทำความผิด (๒) ดำเนินการตามแนวปฏิบัติที่เกี่ยวข้องเพื่อเก็บรวบรวมและจัดการหลักฐานต่าง ๆ ที่เกี่ยวข้องกับการก่อภัยคุกคามทางไซเบอร์โดยทันทีหลังจากที่ตรวจพบ เช่นการจัดการกับข้อมูลที่บันทึกอยู่ในหน่วยความจำประเภทที่สามารถสูญหายได้เมื่อปิดอุปกรณ์ (volatile data) การเก็บข้อมูลจราจรทางคอมพิวเตอร์ (logs) ข้อมูลเกี่ยวกับมัลแวร์ ข้อมูลสถานะของระบบ (system snapshot) หรือข้อมูลอื่น ๆ ที่จำเป็นให้เพียงพอสำหรับใช้วิเคราะห์ในเชิงเทคนิค และเพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ และใช้เป็นพยานหลักฐานในการดำเนินคดี (๓) ดำเนินการเพื่อให้มีการระบุแหล่งที่มาของการโจมตี (attacking host) เช่น การระบุหมายเลขประจำเครื่อง (IP address) การระบุช่องทางที่ผู้โจมตีใช้ การค้นหา และวิจัยที่มาของการโจมตีจากแหล่งข้อมูลต่าง ๆ เช่น ฐานข้อมูลภัยคุกคามทางไซเบอร์ที่รวบรวมข้อมูลจากหลายแหล่ง เป็นต้น (๔) ประสานงานเพื่อแจ้งหรือรายงานสถานการณ์การรับมือภัยคุกคามทางไซเบอร์และความคืบหน้าในการตอบสนองไปยังบุคคลหรือหน่วยงานที่เกี่ยวข้อง ตลอดจนผู้ที่อาจได้รับผลกระทบ อย่างทันท่วงที โดยอาจขอความช่วยเหลือไปยังบุคคลหรือหน่วยงานต่าง ๆ โดยเฉพาะการเกิดภัยคุกคามทางไซเบอร์ที่จัดอยู่ในหมวดหมู่ที่ ๑, ๒, ๔, ๕ และ ๗ ตามที่ระบุในข้อ ๑ ของภาคผนวก ๑ แนบท้ายนี้ทั้งนี้ ในการแจ้งหรือ รายงานสถานการณ์นั้น หน่วยงานควรเลือกใช้ช่องทางที่มีความเหมาะสม และปลอดภัย และดำเนินการแจ้งหรือรายงานเหตุภายในระยะเวลาที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด หรืออาจเทียบเคียงจากตัวอย่างตามที่ระบุในข้อ ๓ ของภาคผนวก ๑ แนบท้ายนี้ แล้วแต่กรณี

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
	(๕) ดำเนินการจัดการกับช่องโหว่ทั้งหมดที่ได้รับผลกระทบจากภัยคุกคามทางไซเบอร์และดำเนินการตามวิธีการป้องกันระบบจากความเสียหายที่อาจเกิดขึ้นเพิ่มเติม เช่นการปรับเปลี่ยนการควบคุมการเข้าถึงเครือข่าย (อาทิ ไฟร์วอลล์) การติดตั้งลายเซ็นของ Anti-Virus หรือ IDS / IPS ใหม่ หรือการเปลี่ยนแปลงทางกายภาพในโครงสร้างพื้นฐาน และดำเนินการระงับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยทันทีหลังจากที่ตรวจพบ เป็นต้น (๖) ดำเนินการที่เกี่ยวข้องเพื่อให้มั่นใจว่าระบบงานต่าง ๆ ยังคงสามารถใช้งานได้ตามปกติ ภายในกรอบระยะเวลาที่กำหนด (restore within time period) เช่น การกู้คืนระบบ ให้กลับมาดำเนินการได้ตามปกติ (integrity restoration) การสร้างระบบงานขึ้นใหม่ (rebuild) การแทนที่ไฟล์ที่ได้รับผลกระทบ (replace) การติดตั้งโปรแกรมคอมพิวเตอร์(install) การเปลี่ยนแปลงรหัสผ่าน และการรักษาความปลอดภัยทางเครือข่าย (securing network) เป็นต้น (๗) สร้างมาตรการป้องกันทั้งเชิงรุกและเชิงรับเพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะคล้ายคลึงกันเกิดขึ้นอีกในอนาคต เช่น การเพิ่มมาตรการเฝ้าระวังสัญญาณเตือนและเหตุการณ์ต่าง ๆ ที่มีความเกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นแล้ว เป็นต้น
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง	ให้หน่วยงานดำเนินการตามข้อ ๑ และดำเนินมาตรการเพิ่มเติม ดังนี้ (๑) หากมีความจำเป็น ให้หน่วยงานดำเนินการใช้ระบบงานสำรองสำหรับการประมวลผล (alternate processing) การจัดเก็บข้อมูล (storage site) และกู้คืนข้อมูลที่เกี่ยวข้อง กับการทำรายการหรือการดำเนินธุรกรรมต่าง ๆ (transaction recovery) (๒) ส่งคำแจ้งเตือนเพื่อขอรับการสนับสนุน ความช่วยเหลือ หรือประสานความร่วมมือไปยังหน่วยงานที่เกี่ยวข้อง (supply chain coordination) รวมถึงแจ้งไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (๓) ดำเนินการตามนโยบายการรายงานเกี่ยวกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นภายใน หน่วยงานซึ่งครอบคลุมถึงรูปแบบ ระดับความลับ และเนื้อหาที่ต้องรายงาน ลำดับชั้น การรายงาน กำหนดเวลา เครื่องมือที่ใช้รายงาน (โดยอาจพิจารณาใช้เครื่องมือ ที่สามารถช่วยรายงานภัยคุกคามโดยอัตโนมัติ (ถ้าหน่วยงานมีความพร้อม)) (๔) ให้การช่วยเหลือ สนับสนุน หรือปฏิบัติงานร่วมกับสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติหน่วยงานควบคุมหรือกำกับดูแล พนักงานเจ้าหน้าที่ หรือบุคคลอื่นใดที่ปฏิบัติหน้าที่หรือได้รับมอบหมายให้ปฏิบัติหน้าที่ตามกฎหมาย (๕) พิจารณาจัดให้มีกลไกที่สามารถทำงานได้โดยอัตโนมัติในการรับมือหรือสนับสนุน การรับมือเมื่อเกิดภัยคุกคามทางไซเบอร์ (automated incident handling processes) (ถ้าหน่วยงานมีความพร้อม)
กรณีบริการ ระบบ หรือ อุปกรณ์มี	ให้หน่วยงานดำเนินการตามข้อ ๑ ถึงข้อ ๒ และดำเนินมาตรการเพิ่มเติม ดังนี้

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baseline)
แนวโน้มที่จะเกิดผลกระทบเป็น ภัยคุกคามทาง ไซเบอร์ในระดับวิกฤติ	(๑) ดำเนินการตามแผนการทำงานในการกู้คืนระบบงานต่าง ๆ เพื่อให้ระบบสามารถ ให้บริการได้ภายในกรอบระยะเวลาที่กำหนด (restore within time period) โดย อาศัยความรู้จากทีมผู้เชี่ยวชาญด้านต่าง ๆ เพื่อให้การกู้คืนระบบ และเครือข่ายของ หน่วยงานทำได้อย่างรวดเร็ว

หมายเหตุ: ในกรณีที่มีภัยคุกคามทางไซเบอร์เกิดขึ้นแล้ว แต่หน่วยงานยังไม่สามารถระบุระดับของภัยคุกคามทางไซเบอร์โดยใช้ปัจจัยที่ใช้ใน การประเมินตามที่ระบุในตามตารางที่ ๑ ของเอกสารแนบ ๑ ได้ ซึ่งอาจเกิดจากการที่หน่วยงานยังไม่สามารถรวบรวมรายละเอียดหรือ ข้อมูลที่จำเป็นเพื่อใช้ในการวิเคราะห์ได้ในช่วงแรก หรือไม่ว่าด้วยเหตุอื่นใดก็ตาม ให้หน่วยงานดำเนินการประเมินผลกระทบเบื้องต้น โดย พิจารณาจากตัวอย่างตามที่ระบุในข้อ ๑ ของภาคผนวก ๑ แนบท้ายนี้ จนกว่าจะมีข้อมูลหรือปรากฏหลักฐานที่เพียงพอต่อการวิเคราะห์เพื่อระบุ ระดับของภัยคุกคามทางไซเบอร์

ตารางที่ ๒.๔ การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (post-incident activity)

ระดับ	แนวปฏิบัติพื้นฐาน (Security Control Baselines)
กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับไม่ร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กรณีบริการ ระบบ หรืออุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ในระดับวิกฤต	ภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ ให้หน่วยงานพิจารณาดำเนินการดังนี้ (๑) นำเหตุการณ์ที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์ที่เกิดขึ้นและมีลักษณะเป็นภัยคุกคาม ทางไซเบอร์ที่มีนัยสำคัญมาเป็นกรณีศึกษา เช่น การพิจารณาถึงจุดอ่อนของโครงสร้างพื้นฐานของบริการ นโยบาย และกระบวนการ การฝึกบุคลากร การระบุผู้มีอำนาจดำเนินงาน และเครื่องมือที่ใช้ เป็นต้น และหาแนวทางเพื่อเตรียมการรับมือและป้องกันการเกิดภัยคุกคามทางไซเบอร์ที่มีลักษณะดังกล่าวร่วมกับบุคคลหรือหน่วยงานที่เกี่ยวข้อง (๒) รวบรวมข้อมูลการดำเนินงานที่เกี่ยวข้องกับการรับมือภัยคุกคามทางไซเบอร์ (โดยอาจดำเนินการเป็นรายสัปดาห์หรือรายเดือน) เช่น จำนวนของภัยคุกคามทางไซเบอร์ที่เกิดขึ้น เวลาที่ใช้ในการจัดการกับภัยคุกคามทางไซเบอร์ประเภทต่าง ๆ และวัตถุประสงค์ของการโจมตี เป็นต้น เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายในหน่วยงาน (๓) ปรับปรุงมาตรการเตรียมการ และป้องกัน รับมือ ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับให้มีความเหมาะสม และเป็นปัจจุบัน (๔) เก็บรักษาข้อมูล และหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดีตามแนวทาง และระยะเวลาการเก็บรักษาหลักฐานเกี่ยวกับการก่อภัยคุกคามทางไซเบอร์ที่หน่วยงานได้กำหนด

ภาคผนวก

ภาคผนวก ๑

ข้อ ๑ การจำแนกหมวดหมู่ของภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย
๐	เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (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)

* การแจ้งหรือรายงานภัยคุกคามตามหมวดนี้เกิดขึ้นเมื่อผู้เผชิญเหตุยังไม่ทราบรายละเอียดภัยคุกคาม และกำลังดำเนินการวิเคราะห์เหตุการณ์ (เช่น อาจอยู่ในช่วงแรก ๆ ที่พบการกระทำผิด) โดยหากทราบผลของการสอบสวนแล้ว ผู้รายงานควรเปลี่ยนเป็นหมวดอื่นให้ถูกต้อง และในรายงาน สรุปปิดเหตุการณ์ ไม่ควรมีภัยคุกคามที่อยู่ในหมวดนี้ เนื่องจากการวิเคราะห์สอบสวนเสร็จสิ้นแล้ว)

ข้อ ๒ ลักษณะภัยคุกคามทางไซเบอร์แยกตามระดับต่าง ๆ

ประเภทอุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	๑ Unsuccessful Activity Attempt	๒ Reconnaissance	๓ Non-Compliance Activity	๔ Malicious Logic	๕ User Level Intrusion	๖ Root Level Intrusion	๗ Denial of Service
Backbone	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เราเตอร์	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายสำหรับการจัดการเครือข่ายหรือดูแลความปลอดภัย	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	วิกฤต	วิกฤต	วิกฤต
เครื่องแม่ข่ายที่ไม่ได้ให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง	ร้ายแรง

ประเภทอุปกรณ์เครือข่าย	หมวดหมู่ภัยคุกคาม						
	๑ Unsuccessful Activity Attempt	๒ Reconnaissance	๓ Non-Compliance Activity	๔ Malicious Logic	๕ User Level Intrusion	๖ Root Level Intrusion	๗ Denial of Service
เครื่องแม่ข่ายที่เปิดให้บริการกับสาธารณะ	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง
เครื่อง Workstation	ไม่ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง	ไม่ร้ายแรง	ไม่ร้ายแรง	ร้ายแรง

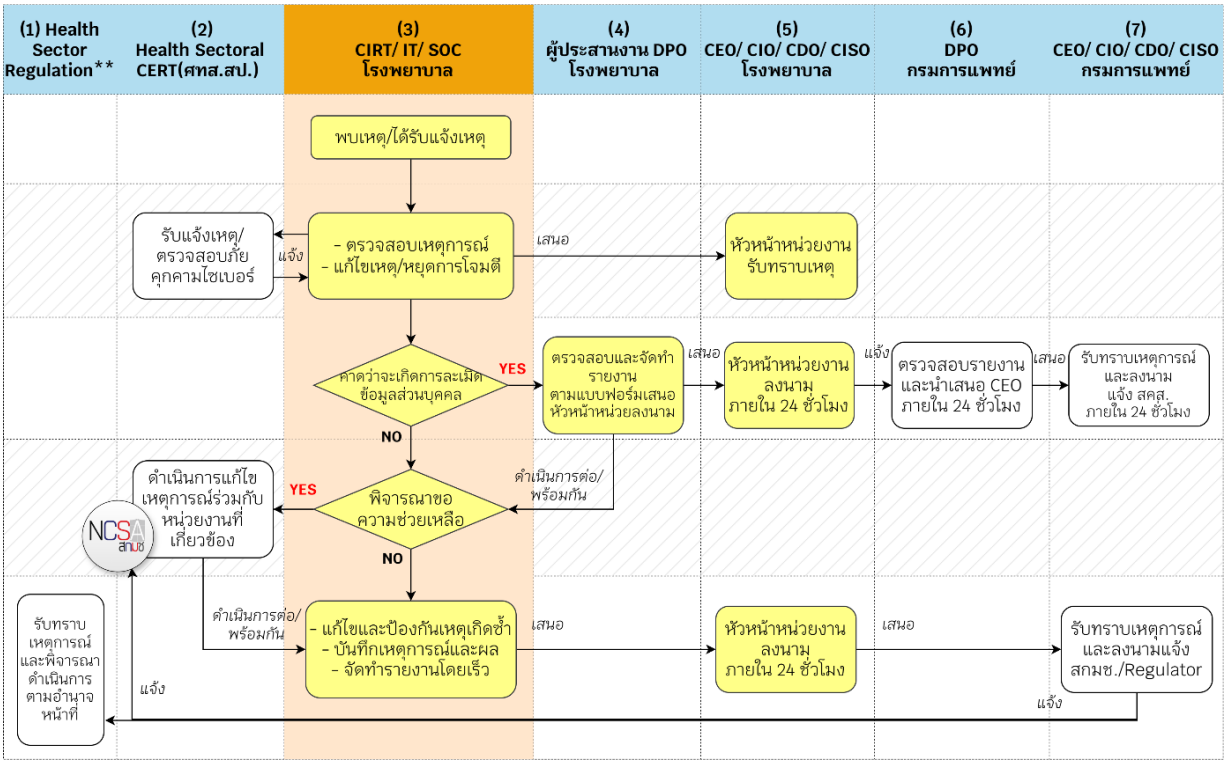
ข้อ ๓ ตัวอย่างกำหนดระยะเวลาในการแจ้งและรายงานภัยคุกคามทางไซเบอร์

หมวดหมู่	คำอธิบาย	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุม หรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๑	Unsuccessful Activity Attempt	ทุกเหตุการณ์	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๒	Reconnaissance	ทุกเหตุการณ์	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด
๓	Non-Compliance Activity	ทุกเหตุการณ์	**๓๐ นาที**	**๒ ชั่วโมง**	**๘ ชั่วโมง**
๔	Malicious Logic	วิกฤติ	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
		ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
		ไม่ร้ายแรง	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด
๕	User Level Intrusion	วิกฤติ	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
		ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
		ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๖	Root Level Intrusion	วิกฤติ	**๑๐ นาที**	**๓๐ นาที**	**๑ ชั่วโมง**
		ร้ายแรง	**๒๐ นาที**	**๑ ชั่วโมง**	**๒ ชั่วโมง**
		ไม่ร้ายแรง	**๓๐ นาที**	**๒ ชั่วโมง**	**๔ ชั่วโมง**
๗	Denial of Service	วิกฤติ	**๑๐ นาที**	**๓๐**	**๑ ชั่วโมง**
		ร้ายแรง	**๑๐ นาที**	**๑ ชั่วโมง**	**๑ ชั่วโมง**
		ไม่ร้ายแรง	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด	ตามที่รพ.กำหนด
๘	Investigating	-	**๒๐ นาที**	ตามเวลาที่ต้องใช้สืบสวน	**๔ ชั่วโมง**

หมวดหมู่	คำอธิบาย	ระดับภัยคุกคามทางไซเบอร์	การแจ้งเบื้องต้นตามช่องทางที่กำหนด (ภายในเวลา)	การส่งรายงานให้หน่วยงานควบคุม หรือกำกับดูแล (ภายในเวลา)	การส่งรายงานให้สำนักงาน (ภายในเวลา)
๙	Explained Anomaly	-	-	**๔ ชั่วโมง**	**๑๒ ชั่วโมง**

ภาคผนวก ๒

แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response)



โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)
อ้างอิงจาก ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

ภาคผนวก ๓

ตัวอย่าง : แบบบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่	**เวลา**	**ผู้บันทึกรายงาน :** **ติดต่อ :**
วัน และเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้า ครั้งถัดไป :		

ภาคผนวก ๔

ตัวอย่าง : บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง สถานการณ์ที่เกิดขึ้น การตัดสินใจ ผลกระทบ)

ภาคผนวก ๕

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	☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ในระดับใด (มาตรา ๖๐)	☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	**คำอธิบาย**
☐	หมวดหมู่ที่ ๐ เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
☐	หมวดหมู่ที่ ๑ การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
☐	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)
☐	หมวดหมู่ที่ ๙ เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)
~~ทั้งนี้ ภัยคุกคามหมวดหมู่ที่ ๐, ๑ และ ๙ ไม่เข่าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน~~	

เอกสาร ก๒ แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑
หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.):
หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):
วันที่: เวลา:
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม
ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม:
ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม:
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม
ชื่อ-นามสกุล: ตำแหน่งงาน:
ชื่อหน่วยงาน: อีเมล:
โทรศัพท์ (ที่ทำงาน / มือถือ) :
ก๓. ความต่อเนื่องของเหตุภัยคุกคาม
☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
ก๔. ลักษณะภัยคุกคามทางไซเบอร์
ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน ☐ ใช่ ☐ ไม่ใช่
เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้
หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์
ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม วันที่ : _____ เวลา: _____ **วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม** วันที่ : เวลา:
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ ☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว เมื่อวันที่: เวลา:
ข๓. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	**คำอธิบาย**
☐	หมวดหมู่ที่ ๐ เหตุการณ์จำลอง และ การฝึกจู่โจม ของหน่วยงานเอง (Training and Exercises)
☐	หมวดหมู่ที่ ๑ การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
☐	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)
☐	หมวดหมู่ที่ ๙ เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)
☐	อื่นๆ โปรดระบุ

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

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง): *โปรดระบุ*

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ : *โปรดระบุ*

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน): *โปรดระบุ*

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): *โปรดระบุ*

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 : _____เวลา:_____ไม่ทราบ: ☐

๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

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

โปรดระบุ

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

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): *โปรดระบุ*

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: *โปรดระบุ*

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): *โปรดระบุ*

มูลค่าความเสียหาย (โดยประมาณ): *โปรดระบุ*

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : *โปรดระบุ*

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : *โปรดระบุ*

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: *โปรดระบุ*

ผลกระทบอื่น ๆ ที่เกิดขึ้น: *โปรดระบุ*

๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: *โปรดระบุ*

ช่องโหว่ที่ถูกใช้จู่โจม: *โปรดระบุ*

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น: *โปรดระบุ*

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม

☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ

☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ

☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ

☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ

☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ

☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: *โปรดระบุ*

ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน
(เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)
โปรดระบุ

ง๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม:
โปรดระบุ

ง๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม:
โปรดระบุ

ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู
โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด
วันที่: *โปรดระบุ* เวลา: *โปรดระบุ*

ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน:
โปรดระบุ

๑๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: *โปรดระบุ*

เอกสาร ก๓ แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

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

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

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

ภาคผนวก ๖

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 ให้เริ่มบันทึกการสอบสวน และรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น 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) ให้ทำซ้ำขั้นตอนการตรวจจับ และการวิเคราะห์ภัยคุกคามทางไซเบอร์ (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	