ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี
Medical Education Center Udonthani Hospital

MEC UDON HOSPITAL EDUCATION CENTER

แผนบริหารความต่อเนื่องและแผนกู้คืนระบบสารสนเทศ

(Business Continuity Plan: BCP and Disaster Recovery Plan: DRP)

ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี

พ.ศ. 2567

แผนบริหารความต่อเนื่องและแผนกู้คืนระบบสารสนเทศ
ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี 2567

๑. บทนำ

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ โดยจะระบุขั้นตอนที่จำเป็น ผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่ การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery) และการดำเนินการภายหลังการรับมือและตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ต่อหน่วยงานในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมี ประสิทธิภาพ เหมาะสมกับขนาด ความซับซ้อน ความเสี่ยง และรูปแบบในการ ดำเนินงานของหน่วยงาน

๒. ปัญหา

ปัญหาที่เกิดขึ้นจากเหตุการณ์ Ransomware Attack ทำให้ระบบเครือข่ายในโรงพยาบาลหยุดชะงักทั้งหมดและส่งผลต่อศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานีในด้าน Network และ Data AD (Active Directory) ฐานข้อมูล User กลางการเข้าใช้งานระบบเน็ตเวิร์คต่างๆ ทั้งหมด จึงทำให้ไม่สามารถเข้าถึงข้อมูลได้เลย ทั้ง Web site บริหารงานบุคคล สป. กรมบัญชีกลาง หรือโปรแกรมบริหารงาน บุคคลของกลุ่มงานทรัพยากรบุคคล โปรแกรมวันลา ส่งผลทำงานเกิดความล่าช้าและไม่ต่อเนื่อง เนื่องจากไม่สามารถ บันทึกข้อมูลบุคลากร ตรวจสอบข้อมูลจำนวนบุคลากร การเข้าถึงข้อมูลต่างและรายงานต่างๆ รวมถึงหน่วยงานไม่ สามารถบันทึกข้อมูลวันลาผ่านระบบไม่ได้

๓.วิเคราะห์สาเหตุของปัญหา

ระบบรักษาความปลอดภัยและระบบป้องกันของ IT โรงพยาบาลมีช่องโหว่ การเข้าถึง Web site ที่นอกเหนือจากการปฏิบัติงาน รวมทั้งระบบปฏิบัติการของคอมพิวเตอร์ในหน่วยงานล้าสมัย ทำให้อาชญากรทางไซต์เบอร์สามารถเข้าถึง ระบบการทำงานและเข้าถึงข้อมูลอิเล็กทรอนิกส์ของโรงพยาบาลอุดรธานี และทำให้ระบบเครือข่ายของโรงพยาบาลหยุดชะงัก

แนวทางการแก้ไขปัญหา

ผู้บริหารศูนย์แพทย์ ร่วมกับ หน่วยงาน และฝ่าย IT ปรับปรุง แก้ไข และพัฒนาระบบรักษาความปลอดภัยทาง IT และหาวิธีป้องกันของโรงพยาบาลอย่าง สม่ำเสมอ พัฒนาการจัดทำระบบสำรองข้อมูลที่ปลอดภัยอย่างเข้มแข็ง และมีการสำรองข้อมูลอย่างสม่ำเสมอและ จัดเก็บไว้ในที่ที่จะถูกโจมตีได้ยาก ควรแยกระบบการ สำรองข้อมูลหน่วยงานสนับสนุ และหน่วยงานทางด้านการรักษา อย่างชัดเจน หากถูก อาชญากรทางไซต์เบอร์โจมตี ข้อมูลฝ่ายนึงฝ่ายใดยังคงอยู่ และอาจไม่ได้รับผลกระทบจากการถูกโจมตี พัฒนาบุคลากรในการเข้าใช้งานระบบและให้ตระหนักกับปัญหาที่เกิดขึ้น มีการจำกัดสิทธิการเข้าถึงข้อมูลการใช้ระบบตามระดับความจำเป็น มีการแยกระบบที่ให้บริการทางการรักษา ระบบข้อมูลต่าง ๆ ในการใช้ Internet ตามความจำเป็นและ เหมาะสมกับงาน และแยก สัญญาณ WiFi SSID ของผู้ใช้งานกับระบบงานหลัก ออกจากกันเมื่อเวลาเกิดเหตุการณ์

อุปสรรค

ระบบปฏิบัติการคอมพิวเตอร์ในหน่วยงานมีความล้าสมัย ทำให้ไม่รองรับกับระบบปฏิบัติการที่ไม่ปลอดภัย ทำ

๔. หน้าที่การทบทวนแผน

ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี มีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้

๕. หน้าที่ในการดำเนินการตามแผน

หน่วยงานที่ดูแลด้านระบบสารสนเทศของศูนย์แพทยฯ ประกอบด้วย ศูนย์คอมพิวเตอร์ โรงพยาบาลอุดรธานี บริษัท บิช โนเทค จำกัด , บริษัท แปซิฟิก จำกัด ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือ

๖. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (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. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกบความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

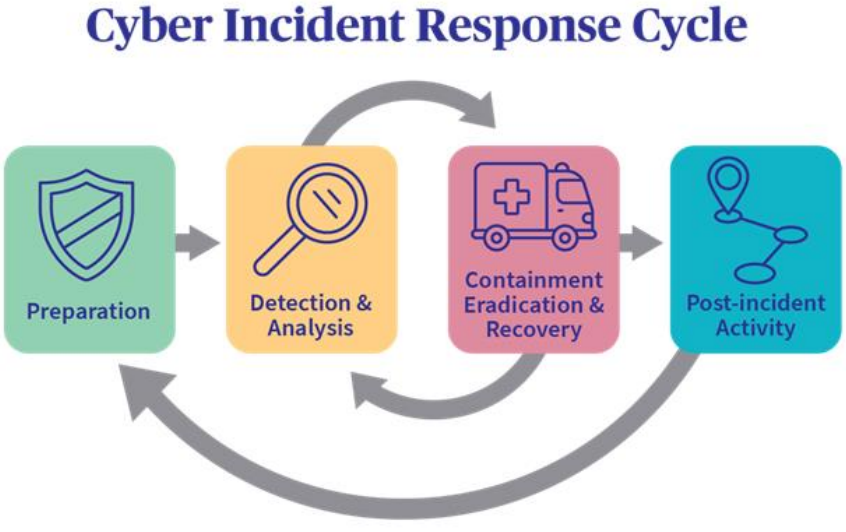
ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	หัวหน้าฝ่ายโครงสร้างพื้นฐาน	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน

ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
	และบริการคอมพิวเตอร์(ศูนย์คอม)		
๒	นายสุนทร พรหมวงศา	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้ -ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๓	นายคณวัฒน์ ผุยมาตย์	เจ้าหน้าที่รับมือฯ (Incident lead)	-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๔	ผู้แทนจากหน่วยบริษัท ที่ดูแลด้านเน็ตเวิร์ค (ทีมกู้คืนระบบแม่ข่าย , และเน็ตเวิร์คทั้งหมด)	เจ้าหน้าที่รับมือฯ (Incident lead)	-ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ -ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๕	ผู้แทนส่วนแผนงาน	ผู้บริหารจัดการความเสี่ยง	ทำหน้าที่ประเมินผลกระทบ-ความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
๖	ผู้แทนส่วนประชาสัมพันธ์	ผู้รับผิดชอบด้านสื่อสารองค์กร	ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๙. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์

มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงประกาศศูนย์แพทยศาสตรศึกษาชั้นคลินิก เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้



๙.๑ <u>ขั้นการเตรียมการ</u> เป็นการดำเนินมาตรการเพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น 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) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๑ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

๙.๒ <u>ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์</u> เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่

ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจ หลีกเลี่ยงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำปนที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทัน ทวงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๙.๒.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกใน การปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติ และมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๙.๒.๒.๑ ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM (จะจัดหา ในปีงบประมาณ ๒๕๖๗)

๓) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๙.๒.๑.๒ ประเภท Log

๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์

๙.๒.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้

๙.๒.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๙.๒.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ ความผิดปกติเมื่อได้รับแจ้งดังนี้

๙.๒.๒.๑ log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐาน ทางกฎหมายหรือเรียกดูในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๙.๒.๒.๒ Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๙.๒.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ ข้อมูล

๙.๒.๒.๔ Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุ ที่แท้จริงได้เพื่อกำจัดผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

๙.๒.๓ การบันทึกภัยคุกคาม

ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม

๙.๒.๔ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่ อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๙.๒.๔.๑ ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการ ดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาส เกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์
- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายใน และภายนอก
- High ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

๙.๒.๔.๒ ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อม ใช้

(Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูล สำคัญ (Sensitive Information)อย่างไร เช่น ข้อมูลถูกทำลาย หรือสูญหาย หรือรั่วไหล หรือการแก้ไขโดยไม่ได้รับ อนุญาตเป็นต้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีข้อมูลรั่วไหล ถูกเปลี่ยนแปลง ทำลาย หรือเข้าถึง โดยที่ไม่ได้รับอนุญาต
- Privacy Breach ข้อมูลที่ใช้ระบุตัวบุคคล (Personal Identifiable Information; PII) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้ รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้ รับอนุญาต

๙.๒.๔.๓ ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุ ภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญ ในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือ จากภายนอก ๙
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะ แล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๙.๒.๕ การติดต่อประสานงานและแจ้งข้อมูล

ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้อง โครงสร้างการรับมือ ภัยคุกคามทางไซเบอร์(ตามภาคผนวก) รายละเอียดมีดังนี้

ลำดับ	ผู้เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้รับผลกระทบจาก incident	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบ หรือ สงสัยว่ามีภัยคุกคามเกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือและตอบสนองต่อ incident	๑.รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน ๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident	๑.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ ตรวจจับ ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน

ลำดับ	ผู้เกี่ยวข้อง	หน้าที่
		๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตามกำกับ ดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยไซเบอร์

หมายเหตุ ทีมรับมือและตอบสนองต่อ incident และทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident ควรเป็นบุคลากรที่มีความรู้ ความสามารถ มีประสบการณ์ ผ่านการอบรมด้าน Cybersecurity ที่มีการรับรอง Certification และความเชี่ยวชาญเฉพาะด้าน เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์

๙.๒.๖ การฝึกฝนและการทดสอบ

ผู้ทำหน้าที่รับมือและตอบสนองต่อ incident ควรได้รับการอบรมฝึกฝนและทดสอบการรับมือ และตอบสนองต่อ incident เพื่อให้ทุกคนตระหนักและเข้าใจถึงหน้าที่ความรับผิดชอบ และเป้าหมายตามแผนที่ กำหนด รวมทั้งเพื่อเป็นการพัฒนาทักษะเพื่อให้สามารถดำเนินงานตามแผนได้อย่างมีประสิทธิภาพ และควรจัดให้มี การทดสอบแผนเป็นประจำ เพื่อประเมินและทราบถึงประเด็นหรือช่องโหว่ (Gap) ที่ควรพัฒนา และเพิ่มความ ชำนาญให้กับบุคลากรของทีมรับมือและตอบสนองฯ โดยการทดสอบแผนควรดำเนินการทดสอบอย่างสม่ำเสมอ

๙.๓ <u>ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ</u>

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกู้คืนทรัพยสินสำคัญทางสารสนเทศให้กลับมา ดำเนินงานหรือให้บริการได้ตามปกติ

๙.๓.๑ วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- ปิดระบบ (Shut Down)

- ตัดการเชื่อมต่อทางเครือข่ายทั้งหมด (Network disconnection) ทั้งนี้ อาจมียกเว้นการเชื่อมต่อ สำหรับ Endpoint Detection & Response Agent (กระบวนการตรวจสอบและตรวจจับกิจกรรมหรือเหตุการณ์ ที่น่าสงสัยใด ๆ ที่เกิดขึ้นที่ปลายทางแบบเรียลไทม์)

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)

- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/ Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย

๙.๓.๒ การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อย ที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการ ตาม

ขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้ ได้ในชั้นศาล

- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

- การเปลี่ยนตัวผู้ดูแลจำเป็นต้องมีการจัดทำบันทึกห่วงโซ่หลักฐาน (Chain of Custody) (ภาคผนวก) รายละเอียดเกี่ยวกับหลักฐาน ควรประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

๑) ข้อมูลเฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น

๒) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident

๓) สถานที่จัดเก็บหลักฐาน

๙.๓.๓ การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ ๒ เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อย ซึ่งการกำจัดสาเหตุที่ทำให้เกิด Incident และผลกระทบ ได้แก่

- การปิดช่องโหว่ของระบบ- การยกเลิก User Account ที่ผู้บุกรุกใช้เข้าสู่ระบบ

- การแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน

- การลบโปรแกรมประเภท Backdoor ออกจากระบบ

- การใช้ข้อมูล Indicator of Compromise (Ioc) ในการสแกนหา Malware หรือร่องรอยอื่น ๆ ในระบบที่ยังหลงเหลือของผู้บุกรุกเพื่อดำเนินการกำจัดให้ออกจากระบบทั้งหมด

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควรเตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย

- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

๙.๔ <u>ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์</u>

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ตองเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์หรือใช้ในกรณีที่ต้องการร้องทุกขหรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น ๑๒ ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภท

นั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปใน ระหว่างที่ตองระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน และกำนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะ ดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

๑. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลัง รับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
๒. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ ๑. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker ๒. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น ๓. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด ๔. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
๓. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับ ต้นฉบับด้วยวิธีCryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖
๔. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือ เพื่อค้นหาสาเหตุของการเกิด Incident
๕. Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการ เคลื่อนย้าย

Chain of custody หรือ “ห่วงโซ่การคุ้มครองพยานหลักฐาน” คือ เอกสารแสดงลำดับการเกิดเหตุการณ์ หรือเอกสารแสดงทุกขั้นตอน ตั้งแต่การยึดเครื่องคอมพิวเตอร์ การดูแลรักษา การควบคุม การวิเคราะห์ และการ จัดเก็บหลักฐานทางอิเล็กทรอนิกส์ เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในยืนยันได้ในชั้นศาล หลักฐานเหล่านี้จึง จะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำ ขึ้นมา

15. ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูลที่หน่วยเทคโนโลยีสารสนเทศ ต้องใช้ด าเนินการ เนื่องจากระบบบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยเทคโนโลยีสารสนเทศ รองรับระบบและ ข้อมูลของหน่วยงานภายในสถาบันในลักษณะแบบรวมศูนย์ ดังนั้น หน่วยงานจึงใช้ข้อมูลสารสนเทศโดยการเชื่อมโยง ระบบของหน่วยงานเข้ากับหน่วยหน่วยเทคโนโลยีสารสนเทศ ผ่านเครือข่ายอินเทอร์เน็ตและ

เครือข่ายภายในสถาบัน ดังนั้นหากระบบมีปัญหา ต้องรอให้หน่วยเทคโนโลยีสารสนเทศกู้คืนระบบก่อน หน่วยงานภายในต่างๆ จึงจะสามารถ ใช้งานระบบได้ต่อไป หน่วยเทคโนโลยีสารสนเทศจึงมีความจำเป็นสำคัญที่จะต้องดูแลระบบสารสนเทศ ระบบคอมพิวเตอร์และระบบ เครือข่ายให้พร้อมรองรับความต่อเนื่องในการใช้งานของหน่วยงานต่างๆ ตามตารางดังต่อไปนี้ ประเภททรัพยากร แหล่งข้อมูล ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ 1 ชั่วโมง 4 ชั่วโมง 8 ชั่วโมง 1 วัน 3 วัน 7 วัน 15 วัน Internet Link 2 Link และ Backup

ประเภททรัพยากร	**แหล่งข้อมูล**	**ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ**						
		1 ชั่วโมง	4 ชั่วโมง	8 ชั่วโมง	1 วัน	3 วัน	7 วัน	15 วัน
Internet Link 2 Link และ Backup Link	AIS internet / TOT			✓				
DNS /DHCP Server	Data Center			✓				
Firewall	Data Center			✓				
Core Switch	Data Center/ DR Site			✓				
ระบบ AD (Active Directory)	Data Center			✓				
E-Mail/ Intranet	Google Drive Cloud			✓				
Physical Server	Data Center			✓				
ระบบ VPN Virtual Private Network	Data Center/ DR			✓				

ข้อมูลสำหรับการติดต่อหน่วยงานภายใน

ชื่อหน่วยงาน	รายชื่อผู้ติดต่อ	โทรศัพท์	ระบบ
1. บริษัท บิ อินโน เทค จำกัด	1.บัญชา โพธิ์ทัย	096-247-9926	MA server & network
	2.อติกันต์ ปาขำ	083-939-2841	Access point (wifi)
	3.อภิเชษฐ์ บุญคง	080-727-5097	
	4.อัครพงษ์ ปัญญาวงศ์	086-441-2136	
2.บริษัท แปซิฟิก จำกัด	คุณไบรท์		Access point Printer
3. บริษัท แอดวานซ์ อินโฟร์ เซอร์วิส จำกัด	Call center (Ais)	1149,1175	internet
4. บริษัท ทีโอที จำกัด มหาชน	Call center (NT)	1100	internet
5. บริษัท SP Auto	คุณตั้ม	097-312-5599	แอร์ห้อง DC DR

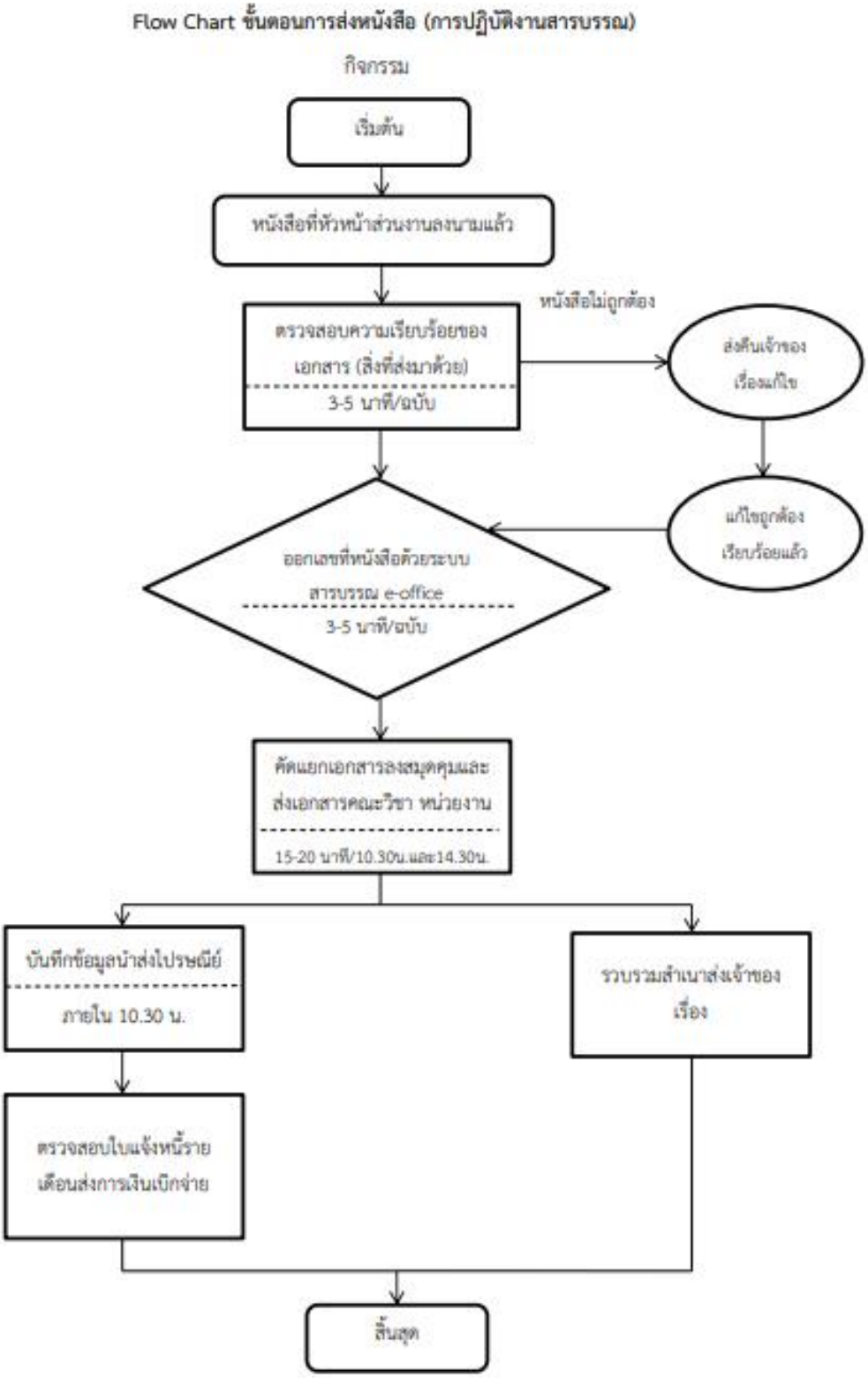
แผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับ	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		2566	2567	2568	2569	2570	
1.	ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบภายในหรือภายนอก				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
2.	ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย cyber ด้านระบบเครือข่าย /ระบบสารสนเทศ/ ระบบดิจิทัล					✓	สุนทร พรหมวงศา คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
3.	จัดทำและทบทวนแผนรับมือภัยคุกคามทางไซเบอร์ของระบบเครือข่าย/ระบบสารสนเทศ/ระบบดิจิทัล				✓		สุนทร พรหมวงศา คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
4.	จัดทำและปรับปรุงคู่มือ/แผนงาน/กระบวนการที่เกี่ยวข้องในการป้องกันภัยคุกคามทาง cyber แต่ละระบบสำรสนเทศหรือฐานข้อมูล				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
5.	ขั้นตอนที่๑ : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
6.	จัดทำรายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสอบต่อภัยคุกคามทางไซเบอร์				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
7.	จัดทำรูปแบบ/แบบฟอร์มการรายงานเหตุการณ์ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
8.	จัดทำแบบฟอร์มการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตการณ์ที่ได้รับแจ้ง				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
9.	จัดเตรียมสถานที่จัดเก็บ ที่มีความมั่นคงปลอดภัย เพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูล และพยานวัตถุอื่น ๆ ที่สำคัญ (ใช้ห้อง data center)				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล

ลำดับ	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		2566	2567	2568	2569	2570	
10.	จัดหาอุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
11.	จัดหาระบบตรวจจับและป้องกันภัยคุกคามไซเบอร์ ของเครื่องคอมพิวเตอร์แม่ข่าย (Server EndPoint Detection & Response) ทำการตดิดตั้งและทำการปรับ Fine Tune				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
12.	จัดตั้งทีมรับมือภัยคุกคามทาง cyber					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
13.	ส่งบุคลากรเพื่อเข้ารับการฝึกอบรมด้าน cyber security					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
14.	ตั้งค่าระบบต่าง ๆ ที่ใช้งานอยู่ในปัจจุบันให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS และระบบสารสนเทศที่พัฒนาขึ้น การ MA ระบบอย่างต่อเนื่อง)				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
15.	ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
16.	ขั้นตอนที่๓: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
17.	จัดทำคู่มือหรือวิธิการควบคุมความเสียหาย การจัดเก็บและดูแลหลักฐานทางดิจิทัล ของระบบสารสนเทศในแต่ละระบบ				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
18.	จัดทำแนวทางการจำกัดสาเหตุและการกู้คืน ระบบสารสนเทศในแต่ละระบบ หรือแต่ละ เหตการณ์ที่สามารถเกิดขึ้นได้				✓		คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
19.	ขั้นตอนที่๔ : การดำเนินการภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล

ลำดับ	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		2566	2567	2568	2569	2570	
20.	จัดทำบันทึกข้อมูลสถติ ภัยคุกคามทางไซเบอร์เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล
21.	จัดทำแนวทางปฏิบัติในการดูแลรักษาหลักฐานทางดิจิทัลของระบบสารสนเทศแต่ละระบบ					✓	คณวัฒน์ ผุยมาตย์ และบริษัทที่ดูแล

Flow Chart BCP ระบบงานสารบรรณ ศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี



Flow Chart ระบบจองรถยนต์ศูนย์แพทย์

Flow Chart BCP ระบบหอพักศูนย์แพทยศาสตรศึกษาชั้นคลินิก โรงพยาบาลอุดรธานี

Flowchart การเข้าพักหอพัก

1. เริ่มจากผู้ใช้ค้นหาข้อมูลห้องว่าง ตรวจสอบสถานะของห้องว่าว่างหรือไม่ จากแฟ้มข้อมูลห้องพัก
2. ถ้ามีห้องว่างก็จะทำสัญญา ถ้าไม่มีห้องว่างก็ทำการจอง
3. รับชำระเงินค่าประกัน
4. ทำการบันทึกและออกใบเสร็จ
5.จบการทำงาน
6. เจ้าของห้องพักจะได้รับรายงานข้อมูลห้องพัก และข้อมูลการเข้า