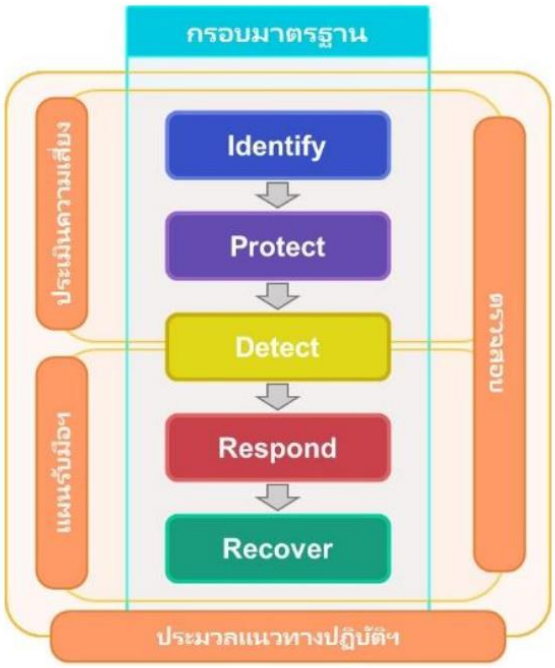
แผนรับมือเหตุภัยคุกคามทางไซเบอร์ โรงพยาบาลไชยปราการ
(Cyber Incident Response Plan)

๑. หลักการและเหตุผล

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์โดยจะระบุขั้นตอนที่จำเป็นผลลัพธ์ที่ได้จากแผนการตอบสนองต่อภัยคุกคามทางไซเบอร์ และข้อควรระวังในแต่ละ ขั้นตอน ซึ่งครอบคลุมตั้งแต่การเตรียมความพร้อม (Preparation) การตรวจจับ และวิเคราะห์ (Detection & Analysis) การควบคุมความเสียหายการกำจัดสาเหตุของภัยคุกคามและการกู้คืน (Containment ,Eradication & Recovery) และการดำเนินการภายหลังการรับมือ และตอบสนองเสร็จสิ้น (Post Incident Activity) มุ่งหวังให้เป็นประโยชน์ต่อหน่วยงานในการนำไปประยุกต์ใช้ให้สามารถดำเนินการได้อย่างมีประสิทธิภาพ เหมาะสมกับขนาดความซับซ้อน ความเสี่ยงและรูปแบบในการดำเนินงานของหน่วยงาน

แผนรับมือภัยคุกคามทางไซเบอร์ใช้เป็นแนวทางในการเตรียมความพร้อมเพื่อรับมือและตอบสนองต่อภัยคุกคาม การจัดทำแผนนี้เป็นส่วนหนึ่งของแผนรักษาความมั่นคงปลอดภัยไซเบอร์ซึ่งประกอบด้วย

แผนดำเนินการอย่างต่อเนื่อง Business Continuity Plan (BCP)
แผนการรับมือภัยคุกคามทางไซเบอร์ (Cyber Incident Response Plan : CIRP)
แผนฟื้นฟูระบบ (Business Recovery Plan : BRP)
แผนป้องกันและเผชิญเหตุภัยพิบัติ (Disaster Recovery Plan (DRP)
แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)



รูปที่ ๑ แสดงประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒. วัตถุประสงค์

๒.๑. เพื่อสร้างความเชื่อมั่นให้ผู้ใช้งานระบบเครือข่ายโรงพยาบาลไชยปราการได้รับการปกป้องต่อภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ

๒.๒. เพื่อกำหนดมาตรการ นโยบาย และกลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการรับมือในภาวะฉุกเฉินเพื่อแก้ไขปัญหาอย่างทันท่วงที

๒.๓. เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงานภายในโรงพยาบาลให้สามารถป้องกันตนเองจากภัยคุกคามต่างๆ สามารถรายงานเหตุภัยคุกคามทางไซเบอร์และทราบขั้นตอนการรับมือเหตุภัยคุกคาม ทางไซเบอร์ตามขอบเขตที่กำหนดไว้

๒.๔. เพื่อสื่อสารไปยังผู้มีส่วนได้ส่วนเสียเพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของโรงพยาบาลไชยปราการ

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศและข้อมูลดิจิทัลของโรงพยาบาลไชยปราการ รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

คณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของโรงพยาบาลไชยปราการมีหน้าที่ทบทวนและขออนุมัติแผนฉบับนี้ต่อคณะกรรมการบริหารความเสี่ยงโรงพยาบาลและคณะกรรมการบริหารโรงพยาบาล

๕. หน้าที่ในการดำเนินการตามแผน

หน่วยงานที่ดูแลด้านระบบสารสนเทศของโรงพยาบาล ประกอบด้วย กลุ่มงานเทคโนโลยีสารสนเทศ กลุ่มงานสุขภาพดิจิทัลกลุ่มงานเวชระเบียนและข้อมูลทางการแพทย์คณะกรรการคณะกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์คณะกรรมการสุขภาพดิจิทัลเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลและคณะกรรมการสารสนเทศโรงพยาบาลไชยปราการ มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนฉบับนี้

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ ประกาศโรงพยาบาลไชยปราการ เรื่อง นโยบายเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๕

๖.๒ ประกาศโรงพยาบาลไชยปราการ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

๖.๓ ประกาศโรงพยาบาลไชยปราการ เรื่อง นโยบายการคุ้มครองข้อมูลส่วนบุคคล พ.ศ.๒๕๖๕

๖.๔ ระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับผู้ใช้งานทั่วไป) พ.ศ. ๒๕๖๗

๗. นิยาม

เหตุการณ์ (Event) หมายความว่า การเกิดขึ้นที่สังเกตได้ใด ๆ (observable occurrence) ในระบบเครือข่าย สภาพแวดล้อม กระบวนการ ลำดับการดำเนินการ หรือบุคลากร เหตุการณ์อาจมีหรือไม่มีลักษณะที่ส่งผลเชิงลบก็ได้ เหตุภัยคุกคามทางไซเบอร์ (Cyberincident) หมายความว่าเหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใดโดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

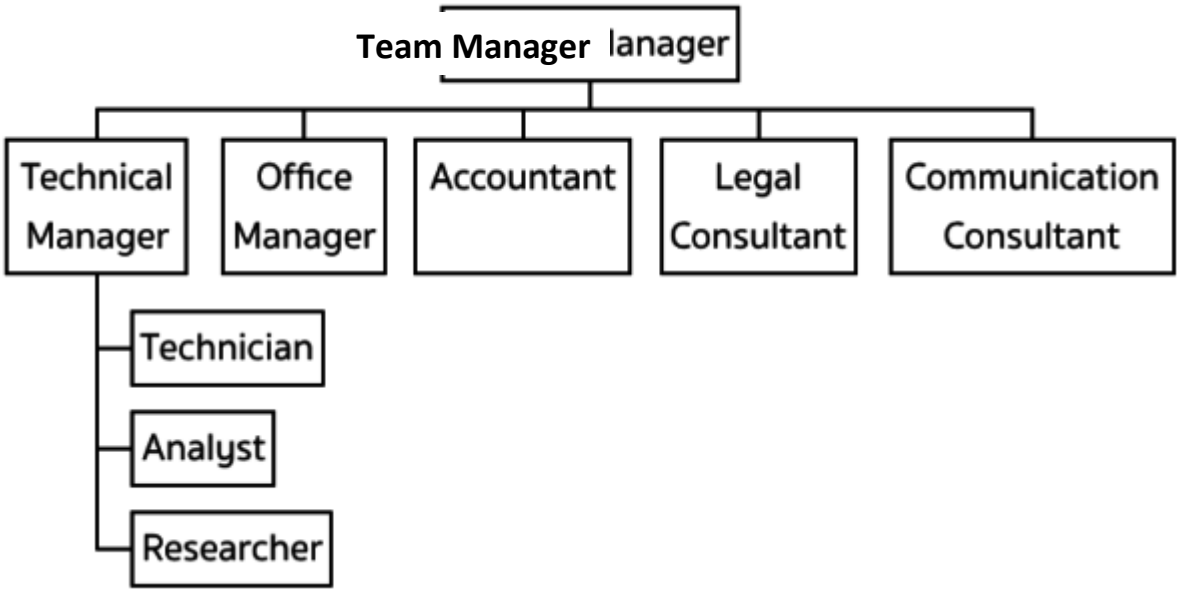
ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้องและเป็นภยันตรายที่ใกล้จะถึงที่จะก่อ ให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ระบบคอมพิวเตอร์หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญหมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศและเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่ง คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทาง ไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

โรงพยาบาลไชยปราการ ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ (รายละเอียดโครงสร้างเพิ่มเติมทีมดังภาคผนวก ๑) ประกอบด้วย

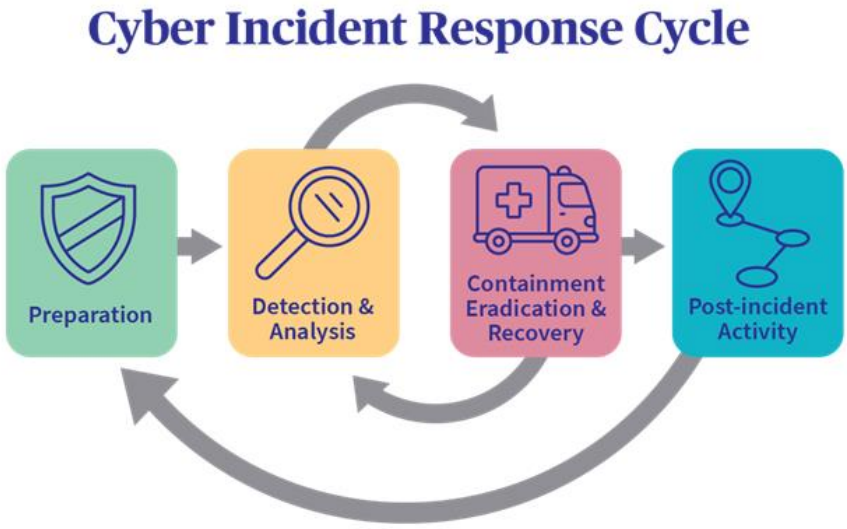
ทีมตอบสนองต่อเหตุการณ์อาจเป็นชุดย่อยของศูนย์การดำเนินการรักษาความปลอดภัย (SOC) ซึ่งจัดการการดำเนินการรักษาความปลอดภัยนอกเหนือจากการตอบสนองต่อเหตุการณ์



ลำดับที่	ชื่อ นามสกุล รายละเอียดการติดต่อ	หน้าที่	ความรับผิดชอบ
๑	นพ.กิตติพันธุ์ ฉลอม (CIO)	หัวหน้าทีม (Team manager)	ทำหน้าที่บริหารจัดการทีมเพื่อ ควบคุม ระงับเหตุจำกัดความเสียหายและสื่อสารกับผู้บริหารของโรงพยาบาล
๒	นาง ดรุณี อินต๊ะ	รองหัวหน้าทีม (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีม ไม่อยู่/ไม่สามารถปฏิบัติงานได้
๓	นาย ไชยกาญจน์ วิเชียรธนเมธา	เจ้าหน้าที่เทคนิค (Technical lead)	ทำหน้าที่ประเมินความเสียหายกำจัดและควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ (Control and Respond)
๔	นายนิรุตติ์ เพียกุณา	เจ้าหน้าที่วิเคราะห์และสืบเหตุ (Investigate lead)	ทำหน้าที่ค้นหาสาเหตุ แหล่งที่มาของภัยคุกคามทางไซเบอร์ (Investigate)
๕	ผู้แทนจาก สกมช.	เจ้าหน้าที่ (Incident lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
๖	ผู้แทนจากบริษัทเอกชนดูแลด้าน Cybersecurity Vender ของโรงพยาบาล	เจ้าหน้าที่ (Incident lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการจัดการและควบคุมภัยคุกคามทางไซเบอร์
๗	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคลประจำโรงพยาบาลไชยปราการ	เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคล (DPO)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการคุ้มครองข้อมูลส่วนบุคคลของรับบริการและประสานงานกับสำนักงานคุ้มครองข้อมูลส่วนบุคคล (สคส)
๙	ผู้แทนส่วนสารบรรณนิติการ	ผู้เชี่ยวชาญด้านกฎหมาย (Legal Consultant)	ทำหน้าที่ประเมินผลกระทบและ ความเสี่ยงที่เกี่ยวกับกฎหมายความมั่นคงปลอดภัยทางไซเบอร์ กฎหมาย PDPA
๙	นพ.ศุภชัย ลวณะสกล นายแพทย์ชำนาญการ	ประธานกรรมการบริหารความเสี่ยง (Risk Management)	ทำหน้าที่ประเมินผลกระทบความเสี่ยงในภาพรวมของทั้งโรงพยาบาล
๑๐	ผู้แทนส่วน ประชาสัมพันธ์	ผู้รับผิดชอบด้านสื่อสารองค์กร (Communication Consult)	ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วน เสียเกี่ยวกับความมั่นคงปลอดภัย ไซเบอร์

๙. ขั้นตอนการรับมือ

แผนฉบับนี้ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของ รัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงประกาศโรงพยาบาลไชยปราการ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลไชยปราการ พ.ศ. ๒๕๖๕ ดังนี้



๙.๑ ขั้นการเตรียมการ 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 [รายละเอียดตามผนวก ๒]

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

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

๙.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆเพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตามแต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันทวงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๙.๒.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกใน การปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์หาความผิดปกติและมีการปรับ Finetune เพื่อให้มีความเหมาะสมกับสภาพการใช้งาน ของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

ประเภท Alert

๑) Firewall ปัจจุบันโรงพยาบาลไชยปราการ Forti Gate 61E มีแผนปรับเปลี่ยน เป็น 61F ในปีงบประมาณ ๖๘

๒) Anti-Virusปัจจุบันโรงพยาบาลใช้ Kaspersky สำหรับเครื่องลูกข่าย และ Kaspersky สำหรับเครื่องแม่ข่ายระบบ E-office windows server ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย

ประเภท Log

๑) Operating System and Application Log โดยอุปกรณ์ FortiGate ข้อมูลจาก Log ของ Hosxp และ Application ที่ประกอบไปด้วยการบันทึกเหตุการณ์หลายประเภท สามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์ โดยสามารถเก็บข้อมูลได้สูงสุด ๗ วัน

๒) Network Access Control (NAC) อุปกรณ์เครือข่ายที่มีควบคุมและการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์ ปัจจุบันโรงพยาบาลใช้ระบบ Fortinet

ประเภทข้อมูลอื่นๆ

ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้ เช่น เว็ปไซด์ สกมช. Thai Health CERT ข่าวสารทางโทรทัศน์

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 จึงต้องมีการเก็บรักษาไว้เป็นอย่างดีและตามระยะเวลาตามกฎหมายกำหนด

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 สกมช. CERT ต่าง ๆ

๙.๒.๓ การบันทึกภัยคุกคาม

กรณีปฏิบัติงานปกติประจำวันจะต้องมีเจ้าหน้าที่สารสนเทศเข้ามาดู Alert และ Log ตามข้อ ๙.๒.๑ ทุกครั้งที่ขึ้นเวรเช้าและเวรบ่าย และเขียนรายงานสรุป ตามแบบฟอร์ม (รายละเอียดดังภาคผนวก ๓) และ CISO นำเหตุการณ์ที่สำคัญรายงานที่ประชุมกรรมการรักษาความมั่นคงปลอดภัยทางไซเบอร์ทุกเดือน

หากมีเหตุการณ์ความเสี่ยงที่รุนแรงระดับกลางขึ้นไปต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพและเป็นระบบโดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม (รายละเอียดดังภาคผนวก ๓)

๙.๒.๔ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident

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

๙.๒.๔.๑ ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการและการ ดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาส เกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบ

ทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังครบถ้วนสมบูรณ์
- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายในและภายนอก
- 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 หรือทำลายโดยไม่ได้ รับอนุญาต

๙.๒.๔.๓ ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุ ภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญ ในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบรวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

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

๙.๒.๕ การติดต่อประสานงานและแจ้งข้อมูล

ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้ ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้องโครงสร้างการรับมือ ภัยคุกคามทางไซเบอร์(ตามภาคผนวก) รายละเอียดมีดังนี้

ลำดับที่	ผู้เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้รับผลกระทบจาก incident	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือ สงสัยว่ามีภัยคุกคามเกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือและตอบสนองต่อ incident	๑.รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน ๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมเฝ้าระวังและวิเคราะห์การแจ้ง เตือน incident	๑.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ ตรวจจับ ทุกวันและทำบันทึกประจำวัน ๒.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดใหม่ให้เจ้าหน้าที่ ในหน่วยงาน ๓.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับ ดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคง ปลอดภัยไซเบอร์

หมายเหตุ : ทีมรับมือและตอบสนองต่อ incident และทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident ควรเป็น บุคลากรที่มีความรู้ 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 ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกูคืนทรัพยสินสำคัญทางสารสนเทศให้กลับมา 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 โดย CIO เป็นผู้ตัดสินใจเลือกแนวที่รวดเร็วและจำกัดความเสียหายให้ได้วงจำกัดมากที่สุด

๙.๓.๒ การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

วัตถุประสงค์หลักของการจัดเก็บหลักฐาน คือเพื่อให้การแก้ไข Incident ส่งผลกระทบต่อธุรกิจให้น้อย ที่สุด (Minimizing impact to the business) นอกจากนี้ หลักฐานอาจมีความจำเป็นที่จะต้องใช้ในการดำเนินการ ตามขั้นตอนทางกฎหมาย ดังนี้ การดำเนินการจัดเก็บหลักฐานทางดิจิทัลสามารถดำเนินการโดยพิจารณา ตามหลักการดังต่อไปนี้

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวกับหลักฐานดิจิทัลเพื่อให้สามารถนำไปใช้ 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 และ

ช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา 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 จะเข้าสู่ กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติโดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควร เตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

- การ Restore Operating System หรือ Application Software ต่าง ๆ จาก Master Image ที่ปลอดภัย
- การ Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

๙.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวของเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามให้ใช้ แผนดังภาคผนวก และแผนฟื้นฟูระบบ (Business Recovery Plan : BRP) และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ตอไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกขหรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น ๑๒ ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติวาด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไปใน ระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตีเมื่อมีการเก็บรวบรวข้อมูล และหลักฐานที่จำเป็นแล้ว โดยการดูแลรักษาหลักฐานทางดิจิทัลที่ต้องดำเนินมีดังนี้

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 และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำขึ้นมา

แหล่งที่มา

ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

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

NIST SP ๘๐๐-๖๑r๒ Computer Security Incident Handling Guide

แนวทางการดำเนินงาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอรสำหรับโรงพยาบาลของรัฐ พ.ศ. ๒๕๖๗ (HAIT plus)

ตารางแสดงความสอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่องประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนฉบับนี้
๑๙.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	ข้อที่ ๘
(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	ข้อที่ ๙.๑ (๒) ผนวก ๑
(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	ข้อที่ ๙.๑ (๓)
(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	ข้อที่ ๙.๓ (๑)
(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	ข้อที่ ๙.๓ (๒)
(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	ข้อที่ ๙.๓ (๓)
(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	ข้อที่ ๙.๓ (๔)
(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	ข้อที่ ๙.๓ (๕)

ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ พ.ศ. ๒๕๖๔	แผนฉบับนี้
(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ (ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	ข้อที่ ๙.๔

ภาคผนวก ๑

โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)

ทีมตอบสนองต่อเหตุการณ์ซึ่งเรียกอีกอย่างว่าทีมตอบสนองต่อเหตุการณ์ด้านความปลอดภัยของคอมพิวเตอร์ (CSIRT), ทีมตอบสนองต่อเหตุการณ์ไซเบอร์ (CIRT), หรือทีมตอบสนองต่อเหตุฉุกเฉินเกี่ยวกับคอมพิวเตอร์ (CERT) ประกอบด้วยกลุ่มบุคลากรข้ามสายงานในองค์กรที่มีหน้าที่รับผิดชอบในการดำเนินการตามแผนตอบสนองต่อเหตุการณ์ ซึ่งไม่เพียงรวมถึงบุคคลที่กำจัดภัยคุกคามเท่านั้น แต่ยังรวมถึงบุคคลที่ตัดสินใจทางธุรกิจหรือทางกฎหมายที่เกี่ยวข้องกับเหตุการณ์ด้วย ทีมโดยประกอบด้วยสมาชิกดังต่อไปนี้

ผู้จัดการการตอบสนองต่อเหตุการณ์ จะกำกับดูแลการตอบสนองทุกขั้นและแจ้งให้ผู้เกี่ยวข้องภายในรับทราบ ตำแหน่งคือรองผู้อำนวยการด้านสุขภาพดิจิทัล

นักวิเคราะห์ด้านการรักษาความปลอดภัยจะศึกษาเหตุการณ์ดังกล่าวเพื่อพยายามทำความเข้าใจถึงสิ่งที่เกิดขึ้น พร้อมทั้งบันทึกการค้นพบและรวบรวมหลักฐานการพิสูจน์อีกด้วย ตำแหน่งคือหัวหน้ากลุ่มงานเทคโนโลยีสารสนเทศ

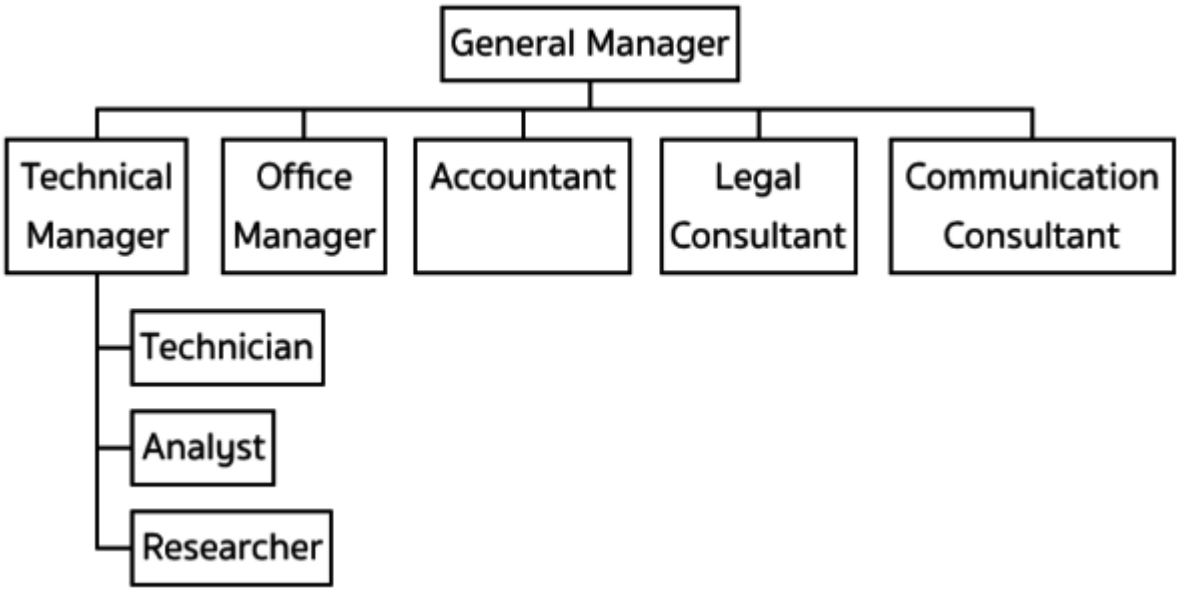
นักวิจัยด้านภัยคุกคามจะศึกษาข้อมูลภายนอกองค์กรเพื่อรวบรวมข่าวกรองที่ให้บริบทเพิ่มเติม ตำแหน่งคือหัวหน้างาน Infrastructure - Cybersecurity

บุคคลจากคณะผู้บริหาร ได้แก่ คณะกรรมการความมั่นคงปลอดภัยทางไซเบอร์ระดับโรงพยาบาล

ผู้เชี่ยวชาญด้านทรัพยากรบุคคลจะช่วยจัดการภัยคุกคามจากภายใน

ที่ปรึกษาภายนอกที่จะช่วยทีมสำรวจปัญหาด้านการรับผิดและตรวจสอบให้แน่ใจว่ามีการรวบรวมหลักฐานการพิสูจน์ ได้แก่ สกมช. สคส.

ทีมประชาสัมพันธ์จะประสานงานในการสื่อสารภายนอกที่ถูกต้องกับสื่อ ลูกค้า และผู้เกี่ยวข้องรายอื่นๆ



คุณสมบัติและทักษะ Technician ที่พึงมี ประกอบด้วย

- ศักยภาพด้านบุคคล

- ยืดหยุ่น มีความคิดสร้างสรรค์ และทำงานเป็นทีม
- มีทักษะการวิเคราะห์ที่ดีเยี่ยม
- สามารถอธิบายข้อมูลเชิงเทคนิคให้ผู้อื่นเข้าใจได้ง่าย
- มีความมั่นใจสูงและทำงานอย่างเป็นระบบ
- อดทนต่อความกดดัน
- มีทักษะด้านการติดต่อสื่อสารและการเขียนดีเยี่ยม
- เปิดใจและพร้อมที่เรียนรู้สิ่งใหม่
- ศักยภาพด้านเทคนิค
- มีความรู้ทางด้านเทคโนโลยีอินเทอร์เน็ตและโปรโตคอลอย่างกว้างขวาง
- มีความรู้ทางด้านระบบ Linux, Unix และ Windows
- มีความรู้ทางด้านอุปกรณ์โครงสร้างเครือข่าย
- มีความรู้ทางด้านแอพพลิเคชันและบริการบนอินเทอร์เน็ต เช่น SMTP, HTTP(s), Social Media และอื่นๆ
- มีความรู้ทางด้านภัยคุกคาม เช่น DDoS, Phishing, Defacing, Malware และอื่นๆ
- มีความรู้ทางด้านการประเมินความเสี่ยงและการวางระบบ
- มีความรู้ทางด้านการวิเคราะห์ข้อมูลแบบ Big Data และ Malware
- ศักยภาพด้านอื่นๆ
- พร้อมทำงานแบบ ๗/๒๔ หรือพร้อมรับการติดต่อตลอดเวลา
- สามารถทำงานต่างจังหวัดหรือระยะไกลได้
- มีประสบการณ์การทำงานในสาย IT Security

ภาคผนวก ๒

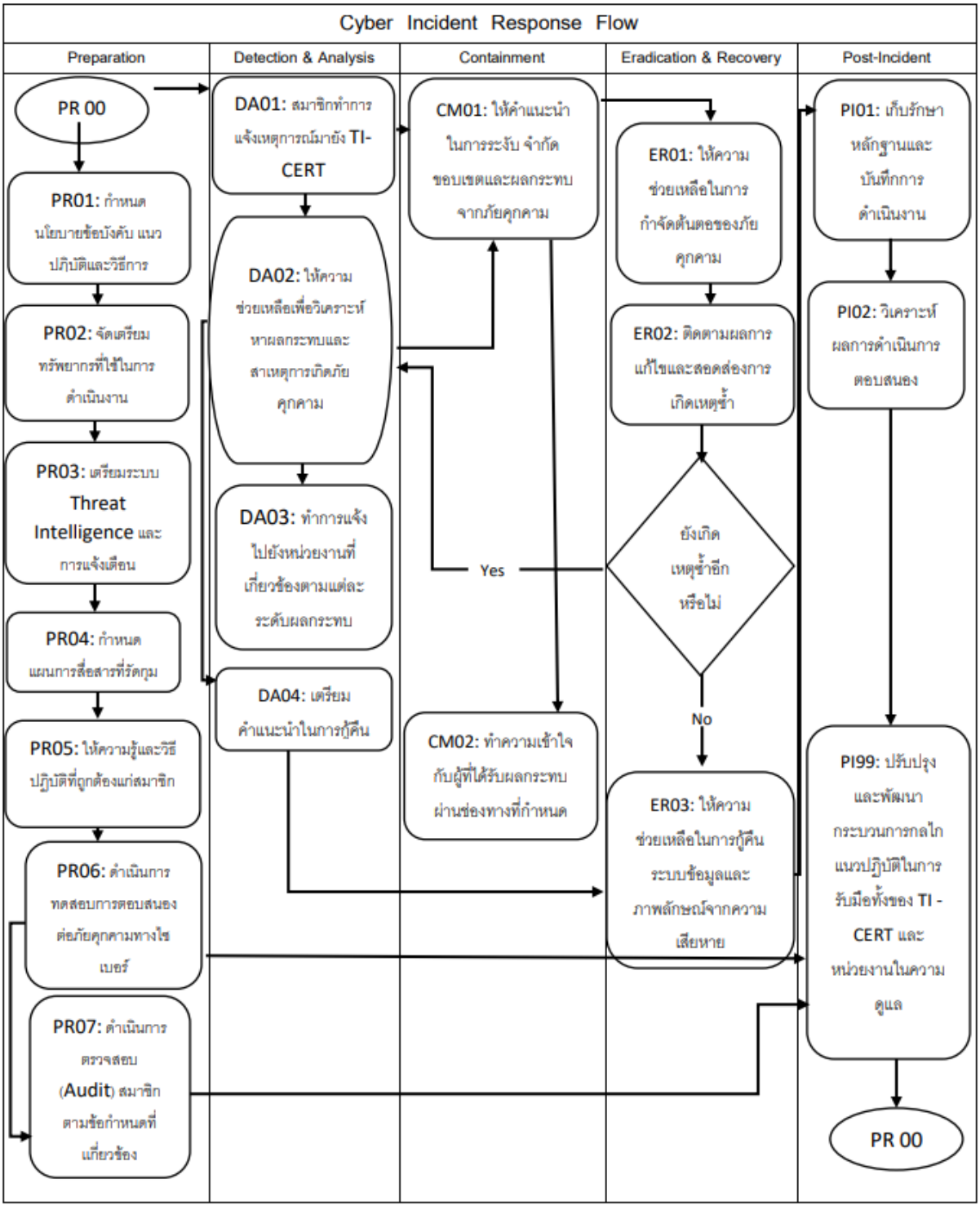
โครงสร้างการรับมือภัยคุกคามทางไซเบอร์ และ Call Tree เมื่อเกิดเหตุการณ์คุกคามทางไซเบอรโรงพยาบาลไชยปราการ ๒๕๖๗ ประเภทรุนแรง

รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์มีดังนี้

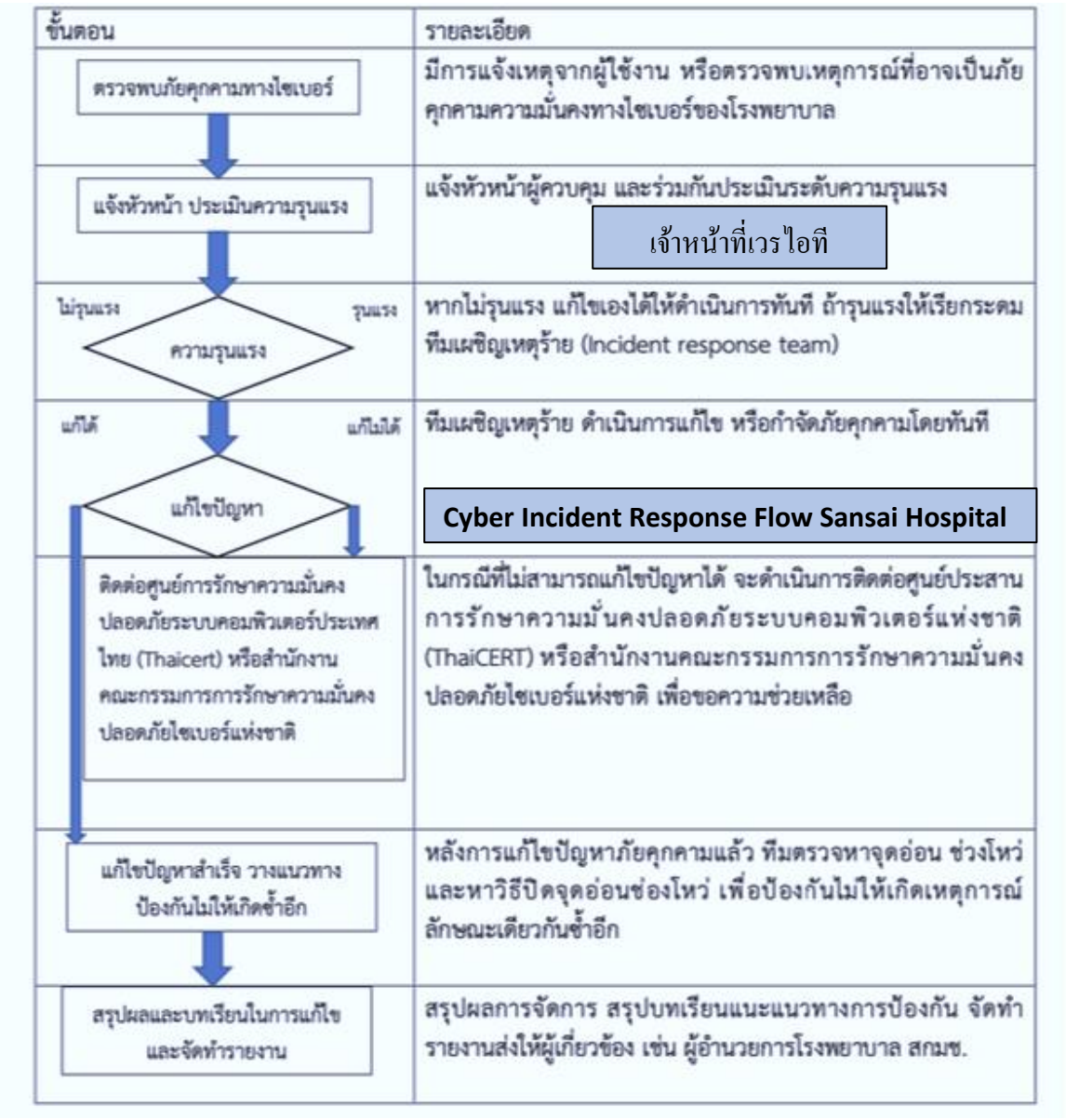
ขั้นตอน	ผู้รับผิดชอบ/ผู้ประสานงาน
๑.การแจ้งเหตุ	ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก incident เจ้าหน้าที่เวรไอที (๐๕๓-๘๗๐๔๔๔-๕๐๑)
๒. ขั้นการเตรียมการ (Preparation) ๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน ๒.๓ เตรียมการป้องกันและแจ้งเตือน ๒.๔ เตรียมรายละเอียดช่องทางการ ติดต่อสื่อสาร ๒.๕ การให้ความรู้ และวิธีปฏิบัติ ๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทาง ไซเบอร์	นายไชยกาญจน์ วิเชียรธนเมธา (PR ๐๑-๐๗) โทร ๐๘๖-๖๕๖๘๐๗๒ ⬇ แจ้งผู้อำนวยการโรงพยาบาลไชยปราการ โทร ๐๙๓๖๓๕๖๙๙๘
๓.ขั้นการตรวจจับและวิเคราะห์ภัยคุกคาม (Detection & Analysis) ๓.๑ รับแจ้งเหตุ ๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง ๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม ๓.๔ จัดลำดับความสำคัญของ incident	นางดรุณี อินต๊ะ (DA ๐๑-๐๔) โทร ๐๘๒-๓๙๒๗๐๙๕

ขั้นตอน	ผู้รับผิดชอบ/ผู้ประสานงาน
๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และภายนอก	
๔. การระงับภัยคุกคามทางไซเบอร์ (Containment) ๔.๑ ควบคุมความเสียหาย ๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล	นายไชยกาญจน์ วิเชียรธนเมธา (CM-๐๑)
๕.การปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟู (Eradication & Recovery) ๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี ๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จาก ความเสียหาย	นายนิรุตติ์ เพียกุณา (ER-๐๑)
๖.การดำเนินการภายหลังการแก้ปัญหาภัยคุกคาม (Post-incident) ๖.๑ เก็บรักษาหลักฐานและบันทึกการ ดำเนินงาน ๖.๒ ปรับปรุงและพัฒนากระบวนการ กลไก แนวปฏิบัติในการรับมือ	นายไชยกาญจน์ วิเชียรธนเมธา (PI ๐๑-๐๒) นายนิรุตติ์ เพียกุณา (PI ๙๙)

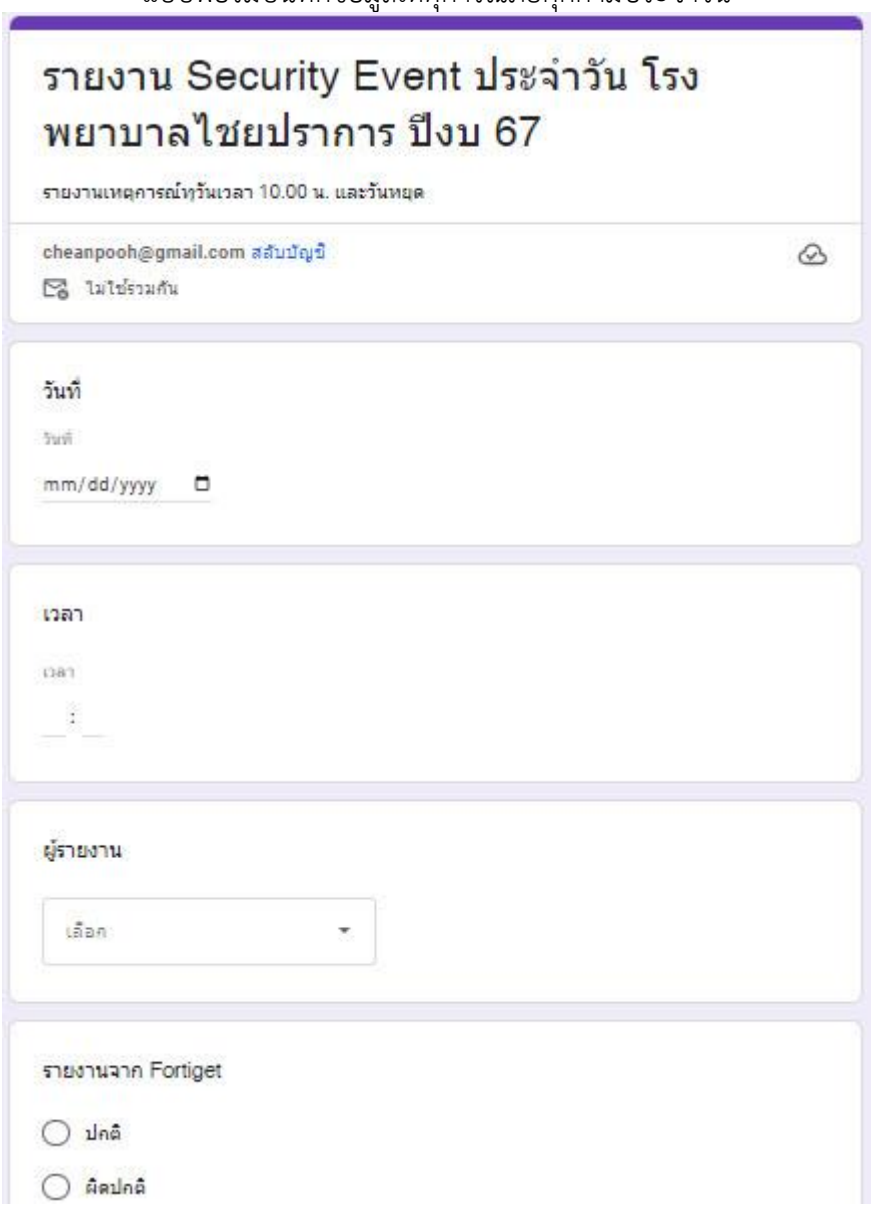
Cyber Incident Response Flow Sansai Hospital



สรุปขั้นตอนการเผชิญเหตุ และแกไข เมื่อเกิดภัยคุกคามทางไซเบอรโรงพยาบาลไชยปราการ ๒๕๖๗


ขั้นตอน
รายละเอียด
ตรวจพบภัยคุกคามทางไซเบอร์
มีการแจ้งเหตุจากผู้ใช้งาน หรือตรวจพบเหตุการณ์ที่อาจเป็นภัยคุกคามความมั่นคงทางไซเบอร์ของโรงพยาบาล
แจ้งหัวหน้า ประเมินความรุนแรง
แจ้งหัวหน้าผู้ควบคุม และร่วมกันประเมินระดับความรุนแรง
เจ้าหน้าที่เวรไอที
ไม่รุนแรง
รุนแรง
ความรุนแรง
หากไม่รุนแรง แก้ไขเองได้ให้ดำเนินการทันที ถ้ารุนแรงให้เรียกระดมทีมเผชิญเหตุร้าย (Incident response team)
แก้ได้
แก้ไม่ได้
แก้ไขปัญหา
ทีมเผชิญเหตุร้าย ดำเนินการแก้ไข หรือกำจัดภัยคุกคามโดยทันที
Cyber Incident Response Flow Sansai Hospital
ติดต่อศูนย์การรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (Thaicert) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
ในกรณีที่ไม่สามารถแก้ไขปัญหาได้ จะดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT) หรือสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เพื่อขอความช่วยเหลือ
แก้ไขปัญหาสำเร็จ วางแนวทางป้องกันไม่ให้เกิดซ้ำอีก
หลังการแก้ไขปัญหาภัยคุกคามแล้ว ทีมตรวจหาจุดอ่อน ช่วงโหว่ และหาวิธีปิดจุดอ่อนช่องโหว่ เพื่อป้องกันไม่ให้เกิดเหตุการณ์ลักษณะเดียวกันซ้ำอีก
สรุปผลและบทเรียนในการแก้ไขและจัดทำรายงาน
สรุปผลการจัดการ สรุปบทเรียนแนะแนวทางการป้องกัน จัดทำรายงานส่งให้ผู้เกี่ยวข้อง เช่น ผู้อำนวยการโรงพยาบาล สกมช.

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคามประจำวัน



รายงาน Security Event ประจำวัน โรงพยาบาลไชยปราการ ปีงบ 67

รายงานเหตุการณ์ทุกวันเวลา 10.00 น. และวันหยุด

cheanpooh@gmail.com สลับบัญชี

ไม่ใช่ร่วมกัน

วันที่

วันที่

mm/dd/yyyy

เวลา

เวลา

:

ผู้รายงาน

เลือก

รายงานจาก Fortiget

ปกติ

ผิดปกติ

รายการตรวจสอบ เหตุการณ์ที่อาจเป็นร่องรอยของการละเมิดความมั่นคงปลอดภัยไซเบอร์ในโรงพยาบาล

เหตุการณ์		วันเวลาที่รายงานขึ้นไป
1. การจราจรใน network ของโรงพยาบาลหนาแน่นผิดปกติ	☐ ไม่พบ ☐ พบ	
2. พื้นที่ว่างใน hard disk ของเครื่องแม่ข่าย หายไปผิดปกติ	☐ ไม่พบ ☐ พบ	
3. CPU Usage สูงผิดปกติ	☐ ไม่พบ ☐ พบ	
4. พบการสร้างบัญชี user ใหม่ โดยผู้ดูแลระบบไม่ได้ดำเนินการ	☐ ไม่พบ ☐ พบ	
5. พบการใช้บัญชีผู้ดูแลระบบ โดยผู้ดูแลระบบไม่ได้ดำเนินการ	☐ ไม่พบ ☐ พบ	
6. พบการปิดบัญชีผู้ใช้งาน โดยผู้ดูแลระบบไม่ได้ดำเนินการ	☐ ไม่พบ ☐ พบ	
7. พบการใช้บัญชีผู้ใช้งานโดยเจ้าของบัญชีลาพักผ่อน ลาศึกษาต่อ ไม่อยู่	☐ ไม่พบ ☐ พบ	
8. log files ถูกลบทิ้งไป	☐ ไม่พบ ☐ พบ	
9. log files เต็ม มีเหตุการณ์ไม่ธรรมดาบันทึกไว้ใน log file จำนวนมาก	☐ ไม่พบ ☐ พบ	
10. การแจ้งเตือนจาก antivirus หรือระบบตรวจจับการบุกรุก	☐ ไม่พบ ☐ พบ	
11. ระบบ antivirus หรือระบบป้องกันอื่น ๆ ถูกปิดไป	☐ ไม่พบ ☐ พบ	
12. มีการเปลี่ยนแปลงใน patch โดยผู้ดูแลระบบไม่ได้ดำเนินการ	☐ ไม่พบ ☐ พบ	
13. พบการเชื่อมโยงเครื่องมือแพทย์ใน network ของโรงพยาบาลไปยัง IP ภายนอก ☐ ไม่พบ ☐ พบ		
14. พบคำสั่งขอรายละเอียดเครื่องแม่ข่ายเข้ามาในระบบ	☐ ไม่พบ ☐ พบ	
15. ความเร็วของการส่งข้อมูลในระบบเครือข่ายลดลงมากเห็นได้ชัด	☐ ไม่พบ ☐ พบ	
16. เกิดหน้าจอแสดงผล error ในหน้า web, เครื่องแม่ข่าย หรือ ฐานข้อมูล	☐ ไม่พบ ☐ พบ	
17. ชื่อไฟล์หรือไดเร็กทอรีถูกเปลี่ยน แทรกด้วยอักขระผิดปกติ	☐ ไม่พบ ☐ พบ	
18. ค่าของระบบที่ตั้งไว้ (system configuration) เปลี่ยนแปลงไป	☐ ไม่พบ ☐ พบ	
19. มี email จำนวนมากส่งเข้ามา มีลักษณะเนื้อหาไม่ปกติ	☐ ไม่พบ ☐ พบ	
20. พบการส่งข้อมูลในเส้นทางที่ไม่เคยใช้	☐ ไม่พบ ☐ พบ	
21. เครื่องคอมพิวเตอร์หรืออุปกรณ์เกิดอาการผิดปกติพร้อมกันจำนวนมาก	☐ ไม่พบ ☐ พบ	
22. พบการข้ามขั้นตอนการมาตรฐานการทำงานที่ตั้งไว้ ด้านการสำรองข้อมูล หรือ การ fail over ☐ ไม่พบ ☐ พบ		
23. มีเครื่องที่ส่งข้อมูลจำนวนมากผ่านเครือข่าย โดยผู้ใช้ไม่ได้ทำงานที่แปลกไป	☐ ไม่พบ ☐ พบ	
24. พบการใช้พลังงานจาก data center มากกว่าปกติ	☐ ไม่พบ ☐ พบ	
25. พบการแจ้งปัญหาขัดข้องในระบบจากผู้ใช้งานจำนวนมากพร้อม ๆ กัน	☐ ไม่พบ ☐ พบ	

ภาคผนวก ๓

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคามกรณีมีความเสี่ยงระดับปานกลางขึ้นไป

๑. ชื่อเหตุการณ์ ..... ๒. หมายเลขของเหตุการณ์.....

๓. วันที่บันทึกเหตุการณ์ .....

๔. หมายเลขของเหตุการณ์อื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้.....

๕. ข้อมูลของผู้แจ้งเหตุการณ์ ๖. ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์

ชื่อ-นามสกุล	ชื่อ-นามสกุล .....
หน่วยงาน	หน่วยงาน .....
โทรศัพท์	โทรศัพท์ .....
อีเมล	อีเมล .....

๗. วันที่และเวลาเกิดเหตุการณ์ .....

๘. วันที่และเวลาพบเหตุการณ์ .....

๙. วันที่และเวลารายงานเหตุการณ์ .....

๑๐. รายละเอียดหตุการณ์ .....

.....

.....

๑๑. การดำเนินการทั้งหมดของทีมรับมือและตอบสนอง .....

.....

.....

๑๒.การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนอง.....

.....

.....

๑๓.ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ.....

.....

.....

๑๔.รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์.....

.....

.....

๑๕.สรุปสาระสำคัญของเหตุการณ์.....

.....

.....

แผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์

ลำดับที่	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐	
๑	ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบภายในหรือภายนอก						
๒	ประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย cyber ด้านระบบเครือข่าย /ระบบสารสนเทศ/ ระบบดิจิทัล						
๓	จัดทำและปรับปรุงคู่มือ/แผนงาน/กระบวนการที่เกี่ยวข้องในการป้องกันภัยคุกคามทาง cyber แต่ละระบบสำรสนเทศหรือฐานข้อมูล						
๔	จัดทำและปรับปรุงคู่มือ/แผนงาน/กระบวนการที่เกี่ยวข้องในการป้องกันภัยคุกคามทาง cyber แต่ละระบบสำรสนเทศหรือฐานข้อมูล						
๕	ขั้นตอนที่๑ : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ จัดทำรายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสอบต่อภัยคุกคามทางไซเบอร์						
๖	จัดทำรูปแบบ/แบบฟอร์มการรายงานเหตุการณ์ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์						
๗	จัดทำแบบฟอร์มการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตุการณ์ที่ได้รับแจ้ง						
๘	จัดเตรียมสถานที่จัดเก็บ ที่มีความมั่นคงปลอดภัย เพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility) ข้อมูล และพยานวัตถุอื่น ๆ ที่สำคัญ (ใช้ห้อง data center)						
๙	จัดหาอุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์						
๑๐	จัดหาระบบตรวจจับและป้องกันภัยคุกคามไซเบอร์ ของเครื่องคอมพิวเตอร์แม่ข่าย (Server EndPoint Detection & Response) ทำการตดิดตั้งและทำการปรับ Fine Tune						

ลำดับที่	กิจกรรม	ปีงบประมาณ					ผู้รับผิดชอบ
		๒๕๖๖	๒๕๖๗	๒๕๖๘	๒๕๖๙	๒๕๗๐	
๑๑	จัดตั้งทีมรับมือภัยคุกคามทาง cyber						
๑๒	ส่งบุคลากรเพื่อเข้ารับการฝึกอบรมด้าน cyber security						
๑๓	ตั้งค่าระบบต่าง ๆ ที่ใช้งานอยู่ในปัจจุบันให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS และระบบสารสนเทศที่พัฒนาขึ้น การ MA ระบบอย่างต่อเนื่อง)						
๑๔	ขั้นตอนที่ ๒: การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์						
๑๕	ขั้นตอนที่๓: การระงับภัยคุกคามทางไซเบอร์ ปราบปรามภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบงานที่ได้รับผลกระทบ						
๑๖	จัดทำคู่มือหรือวิธิการควบคุมความเสียหาย การจัดเก็บและดูแลหลักฐานทางดิจิทัลของระบบสารสนเทศในแต่ละระบบ						
๑๗	จัดทำแนวทางการจำกัดสาเหตุและการกู้คืน ระบบสารสนเทศในแต่ละระบบ หรือแต่ละ เหตการณ์ที่สามารถเกิดขึ้นได้						
๑๘	ขั้นตอนที่๔ : การดำเนินการภายหลังการแก้ไขปัญหาภัยคุกคามทางไซเบอร์						
๑๙	จัดทำบันทึกข้อมูลสถติ ภัยคุกคามทางไซเบอร์เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน						
๒๐	จัดทำแนวทางปฏิบัติในการดูแลรักษาหลักฐานทางดิจิทัลของระบบสารสนเทศแต่ละระบบ						