



แผนการรับมือภัยคุกคามทางไซเบอร์ (๒๕๖๘ - ๒๕๗๑)

Digitally signed by ศาสตราจารย์ ดร. ชัยวัฒน์ วัฒนศิริ
DN: c=TH, o=มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา, ou=มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา, email=chawalit@bsru.ac.th, cn=ศาสตราจารย์ ดร. ชัยวัฒน์ วัฒนศิริ
Reason: I am the author of this document.
Date: 2025.09.15 14:29:30
+07'00'
Foxit PDF Editor Version: 12.1.1

มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา



BANSOMDEJCHAOPRAYA
RAJABHAT UNIVERSITY

สารบัญ

หัวข้อ	หน้า
แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์	๑
๑. หลักการและเหตุผล	๑
๒. วัตถุประสงค์	๑
๓. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑
๔. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์	๑
๕. แผนรับมือภัยคุกคามทางไซเบอร์	๒
แผนรับมือภัยคุกคามทางไซเบอร์	๔
๑. หลักการและเหตุผล	๔
๒. วัตถุประสงค์	๔
๓. แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์	๕
๔. ขั้นตอนที่ ๑ : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์	๕
๕. ขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์	๖
๖. ขั้นตอนที่ ๓ : การระงับภัยคุกคามทางไซเบอร์และการฟื้นฟูระบบที่ได้รับผลกระทบ	๑๐
๗. ขั้นตอนที่ ๔ : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์	๑๑
ภาคผนวก	๑๓

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์

๑. หลักการและเหตุผล

เนื่องด้วยพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วยแผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถใช้งานได้

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานมีการปฏิบัติได้อย่างรวดเร็ว ถูกต้อง และมี ประสิทธิภาพ

๓. แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ในกระบวนการจัดทำและผลกระทบของบริการที่สำคัญของหน่วยงานอย่างน้อยปีละ ๑ ครั้ง โดยผู้ตรวจสอบภายในหรือภายนอก

๔. การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง ดังต่อไปนี้

- ๑) การประเมินความเสี่ยง (Risk Assessment)
- (ก) การระบุความเสี่ยง (Risk Identification)

ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคาม ทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก

(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis)

ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

(ค) การประเมินค่าความเสี่ยง (Risk Evaluation)

ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการทำงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคง ปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๒) การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับนอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๓) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๔) การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น

๕. แผนรับมือภัยคุกคามทางไซเบอร์

๕.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน

๕.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิภาพไปยัง บุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐ

๕.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๕.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อม การปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

แผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ปรากฏตามภาคผนวก

แผนรับมือภัยคุกคามทางไซเบอร์

หลักการและเหตุผล

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

วัตถุประสงค์

เพื่อป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน ให้มีการดำเนินการตรวจสอบข้อมูลที่เกี่ยวข้อง ข้อมูลคอมพิวเตอร์ และระบบคอมพิวเตอร์ของหน่วยงาน รวมถึงพฤติกรรมแวดล้อม เพื่อประเมินว่ามีภัยคุกคามทางไซเบอร์ แนวทางปฏิบัติในการรับมือเหตุภัยคุกคามทางไซเบอร์

ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นต่อหน่วยงานจนส่งผลกระทบต่อการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงทางเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ สามารถจำแนกหมวดหมู่ตามประกาศของคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.) เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ. ๒๕๖๔ ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

๑. เหตุการณ์จำลอง และการฝึกซ้อมของหน่วยงานเอง (Training and Exercises)
๒. การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)
๓. การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
๔. การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)
๕. การบุกรุกโดยใช้มัลแวร์ (Malicious Logic)
๖. การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
๗. การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
๘. การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
๙. เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
๑๐. เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่ เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)

แนวทางการปฏิบัติ

แนวทางการปฏิบัติ เพื่อให้มีความเข้าใจขั้นตอนการปฏิบัติต่าง ๆ และมีความพร้อมในการปฏิบัติงานในหน้าที่ความรับผิดชอบจึงแบ่งขั้นตอนการปฏิบัติออกเป็น ๔ ขั้นตอน ตามประกาศ กมช. เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ สรุปได้ดังนี้

ขั้นตอนที่ ๑ : การเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์

การจัดเตรียมข้อมูลให้พร้อม ต้องจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือภัยคุกคามทางไซเบอร์ได้แก่

๑.๑ การจัดเตรียมเครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ ได้แก่

- รายชื่อและช่องทางการติดต่อของผู้ที่เกี่ยวข้องและประสานงานในการรับมือและตอบสนองต่อภัย คุกคามทางไซเบอร์ (ภาคผนวก)

- ช่องทางการรายงานเหตุการณ์ ให้ผู้ได้รับผลกระทบหรือพบเห็นเหตุการณ์ แจ้งมายังมหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา

- ช่องทางการรายงานและติดตามข้อมูลสถานการณ์ดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

- ห้องประชุม (war room)

- สถานที่จัดเก็บจัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการเก็บหลักฐาน (Secure Storage Facility)

ข้อมูลและพยานวัตถุอื่น ๆ ที่สำคัญ ใช้ห้อง Data center

๑.๒ อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์ภัยคุกคามทางไซเบอร์ใช้อุปกรณ์ SIEM (ปีงบประมาณ พ.ศ. ๒๕๖๗)

๑.๓ ให้มีการจัดตั้งและฝึกอบรมบุคลากรหรือทีมงาน

- โครงสร้างทีมรับมือภัยคุกคามทางไซเบอร์

ทีมงานที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ประกอบด้วยทีมรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ ได้แก่

๑) บุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงทางไซเบอร์ จากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้นในหน่วยงาน

๒) บุคลากรที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ หน้าที่ คือ เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ

๓) user Awareness training การจัดฝึกอบรมเพื่อให้บุคลากรในหน่วยงานมีความรู้ความเข้าใจ มีความระมัดระวังและเข้าใจถึงความผิดปกติที่เกิดจากการโจมตีทางไซเบอร์รวมทั้งเข้าใจวิธีการตอบสนองในเบื้องต้นและดำเนินการแจ้งให้หน่วยงานที่ทำหน้าที่รับมือและตอบสนองรับทราบเมื่อมีเหตุการณ์ผิดปกติ

๑.๔ การตั้งค่าระบบต่าง ๆ ให้ปลอดภัย เป็นการตั้งค่าอุปกรณ์เครือข่ายที่จำเป็น เช่น Router, Firewall, IPS การกำหนดแนวทางการรักษาความมั่นคงปลอดภัยของห้องแม่ข่าย มีการปิดช่องโหว่และทำการ Patch ระบบ มีการกำหนดสิทธิ์ของผู้ใช้งานโดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น การ update Security Patch เป็นประจำ การมี Software ในการป้องกันและตรวจจับความผิดปกติในระบบ เช่น Malware Prevention

๑.๕ การจัดทำนโยบาย แผนงาน และกระบวนการที่เกี่ยวข้อง รวมถึง การสร้างเครือข่ายความร่วมมือแนวทางป้องกัน และการเตรียมการเบื้องต้น

ขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้ว ก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจ หลีกเลียงได้ การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทัน ท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๒.๑ การกำหนดวิธีการที่จะใช้ในการตรวจจับ incident

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

ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต
- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่อุปกรณ์ที่ใช้เพื่อการป้องกัน และตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกัน และต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์ และเครือข่ายมีดังนี้

๒.๑.๑ ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) SIEM ระบบตรวจจับความผิดปกติโดยใช้ข้อมูล Log จากระบบอื่น ๆ เพื่อนำมาวิเคราะห์ โดยต้องตั้งค่า Rule set โดยผู้เชี่ยวชาญ และเหมาะสมกับสภาพแวดล้อมที่เชื่อมต่ออยู่กับ SIEM (จะจัดหา ในปีงบประมาณ 2567)

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

๔) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๒.๑.๒ ประเภท Log

๑) Operating System and Application Log ข้อมูลจาก Log ของ OS และ Application ที่ประกอบไปด้วย การบันทึกเหตุการณ์ หลายประเภทสามารถถูกใช้ในการตรวจจับภัยคุกคามบางอย่างได้ขึ้นอยู่กับ ประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านมาเข้าออกเครือข่ายสามารถถูกใช้ในการ ตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการ วิเคราะห์

๒.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้

๒.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๒.๒ การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง

การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ ความผิดปกติเมื่อได้รับแจ้งดังนี้

๒.๒.๑ log Retention Policy คือ การใช้ Log จากอุปกรณ์ต่าง ๆ เช่น IPS, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และบันทึกเหตุการณ์เก็บไว้เพื่อหลักฐาน ทางกฎหมายหรือเรียกดู ในอนาคต จึงต้องมีการเก็บรักษาไว้เป็นอย่างดี และตามระยะเวลาตามกฎหมายกำหนด

๒.๒.๒ Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ ตรงกันอยู่เสมอเพื่อให้การ Correlate Event ทำได้ง่าย

๒.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

๒.๒.๔ Seek Assistance เมื่อทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ incident เพื่อหาสาเหตุที่แท้จริงได้เพื่อ กำจัด ผู้บุกรุกออกจากระบบ จะใช้บริการให้คำแนะนำปรึกษาจากภายนอก เช่น CERT ต่าง ๆ

๒.๓ การบันทึกภัยคุกคาม ต้องทำการบันทึกข้อมูลเหตุการณ์ภัยคุกคามเพื่อช่วยในการรับมือและตอบสนองภัยคุกคามอย่างมีประสิทธิภาพ และเป็นระบบ โดยทำการบันทึกตั้งแต่การตรวจพบจนถึงสิ้นสุดของเหตุการณ์ภัยคุกคาม แบบฟอร์มการบันทึก ข้อมูลเหตุการณ์ภัยคุกคาม (ภาคผนวก)

๒.๔ การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับ ความสำคัญของ Incident และช่วยในการตัดสินใจ เชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้ อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่ อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการ วิเคราะห์ผลกระทบและการ

จัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๒.๔.๑ ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาส เกิดขึ้นหากเหตุการณ์ภัยคุกคาม ยังไม่ถูกควบคุมโดยทันทีซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบ การให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการ ดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมี ผลเสียมากยิ่งขึ้น โดยระดับของ Functional Impact มีดังนี้

- None ไม่มีผลกระทบในการให้บริการหรือดำเนินงานตามปกติ
- Low มีผลน้อยมากต่อกระบวนการทำงานหลัก ทำให้ช้าลงบ้างแต่ผลที่ได้ยังคงครบถ้วนสมบูรณ์
- Medium ไม่สามารถให้บริการที่ครบถ้วนสมบูรณ์กับผู้ใช้งานบางกลุ่ม ทั้งภายในและภายนอก
- High ไม่สามารถให้บริการกับผู้ใดได้อีกต่อไป เป็นการหยุดชะงักโดยสมบูรณ์

๒.๔.๒ ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล ควรพิจารณา 3 ด้าน ได้แก่ ด้านการรักษา ความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อม ใช้ (Availability) รวมทั้ง ควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมที่จะส่งผลต่อข้อมูล 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) รั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับ อนุญาต
- Proprietary Breach ข้อมูลความลับที่ใช้ในการดำเนินธุรกิจ รั่วไหล หรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
- Integrity Loss ข้อมูลที่เป็น Privacy และ Propriety ถูกเปลี่ยนแปลง หรือทำลาย โดยไม่ได้รับอนุญาต

๒.๔.๓ ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลา และทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของ เหตุ ภัยคุกคามและประเภทของทรัพย์สิน สารสนเทศ เช่น ระบบ และข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่าย ในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้ โดยระดับของ Recoverability Effort มีดังนี้

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

วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๒.๕ การติดต่อประสานงานและแจ้งข้อมูล ทีมรับมือและตอบสนองภัยคุกคามต้องแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้องเพื่อให้

ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ โดยมีบุคลากรที่เกี่ยวข้อง โครงสร้างการรับมือ ภัยคุกคาม ทางไซเบอร์ (ตามภาคผนวก) รายละเอียดมีดังนี้

ลำดับ	ผู้เกี่ยวข้อง	หน้าที่
๑	ผู้ที่ได้รับผลกระทบจาก incident	แจ้งเหตุหรือรายงานด้านความมั่นคงปลอดภัยไซเบอร์ที่พบหรือสงสัยว่ามีภัยคุกคามเกิดขึ้น
๒	ผู้รับแจ้งเหตุ	รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยไซเบอร์
๓	ทีมรับมือ และตอบสนองต่อ incident	รับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดขึ้นใหม่ให้เจ้าหน้าที่ในหน่วยงาน มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๔	ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือน incident	1.เฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจากอุปกรณ์ตรวจจับ 2.ให้คำแนะนำปรึกษาบุคลากรที่เกี่ยวข้องกับจุดอ่อน การป้องกัน ข้อควรระมัดระวัง และแจ้งเตือนภัยคุกคามที่เกิดขึ้นใหม่ให้เจ้าหน้าที่ในหน่วยงาน 3.มีส่วนร่วมกับหน่วยงานภายนอกองค์กร เช่น Thai CERT เพื่อแบ่งปันข้อมูลข่าวสารด้านภัยคุกคามทางไซเบอร์เพื่อป้องกัน และตอบสนองภัยคุกคามได้เร็วขึ้น
๕	ผู้บริหาร	รับผิดชอบกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหา และสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจนติดตาม กำกับดูแล ควบคุมเจ้าหน้าที่ เกี่ยวกับการป้องกันความมั่นคงปลอดภัยไซเบอร์

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

๒.๖ การฝึกฝนและการทดสอบ

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

ขั้นตอนที่ ๓ : การระงับภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบที่ได้รับผลกระทบ

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ เมื่อหน่วยงานได้รับแจ้งเตือนการเกิดภัยคุกคามทางไซเบอร์ หน่วยงานต้องมีการกำหนดแนวทางการดำเนินมาตรการเพื่อระงับภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบ ที่ได้รับผลกระทบ (Containment, Eradication, and Recovery) โดยกำหนดให้ สอดคล้องกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์ แต่ละระดับ จนกระทั่งสามารถกู้คืนข้อมูลทางสารสนเทศให้กลับมา ดำเนินงานหรือให้บริการได้ตามปกติ

๓.๑ วิธีการควบคุมความเสียหาย คือการตัดสินใจเลือกใช้วิธีการที่เหมาะสม ดังนี้

- หยุดการเชื่อมต่อจากภายนอก (Public Network disconnection)
- ตัดการเชื่อมต่อภายในเครือข่ายทั้งหมด (Local Network disconnection) ทั้งนี้ อาจมีกเว้นการการเชื่อมต่อกับ

ระบบตรวจสอบเพื่อเข้าตรวจสอบหาสาเหตุและจุดมุ่งหมายในการดักโจมตี

- หยุดการทำงานของฟังก์ชันที่เกี่ยวข้อง (Disabling Certain Functions)
- Redirect Network Traffic และ/หรือความสนใจของผู้บุกรุกไปยัง Blackhole/ Sandbox/Honeypot

ทั้งนี้ การตัดสินใจเลือกใช้วิธีการควบคุมความเสียหายจะขึ้นอยู่กับลักษณะสถานการณ์ที่กำลังเผชิญ

ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุม ความเสียหาย

๓.๒ การจัดเก็บและดูแลรักษาหลักฐานทางดิจิทัล

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

- เป็นไปตามขั้นตอนที่กำหนดไว้ในกฎหมายข้อบังคับที่เกี่ยวข้องกับหลักฐานดิจิทัล เพื่อให้สามารถนำไปใช้

ได้ในชั้นศาล

- หลักฐานมีบันทึกการเข้าถึงและการกระทำการใด ๆ ต่อหลักฐานตลอดเวลาอย่างรัดกุม

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

- ๑) ข้อมูล เฉพาะ เช่น Location, Serial Number, Model Number, Hostname, Media Access Control (MAC) และ Address เป็นต้น
- ๒) ชื่อ ตำแหน่ง และช่องทางการติดต่อผู้จัดเก็บและรักษาหลักฐานระหว่างการรับมือ Incident
- ๓) สถานที่จัดเก็บหลักฐาน

๓.๓ การกำจัดสาเหตุและการกู้คืนระบบให้กลับมาทำงานปกติ

เมื่อมีการควบคุมความเสียหาย และมีการเก็บหลักฐานข้อมูลเพิ่มเติมเรียบร้อยแล้วข้อมูลทั้งหมด จะต้องนำกลับมาวิเคราะห์ตามหลักการที่ได้กล่าวไว้ใน “ขั้นตอนที่ 2 เรื่องการตรวจจับและวิเคราะห์ (Detection & Analysis)” จนกว่าจะสามารถกำจัดสาเหตุที่ทำให้เกิด Incident และช่องทางที่ผู้บุกรุกได้สร้างไว้เพื่อเข้ามา ในระบบทั้งหมดได้เรียบร้อยแล้ว 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 กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยในขั้นตอนนี้สิ่งที่มีความสำคัญเป็นอย่างยิ่ง และควร เตรียมการล่วงหน้าในเรื่องดังต่อไปนี้

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

ขั้นตอนที่ ๔ : การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องของภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-incident Activity) นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็นในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการ ใช้ข้อมูลเพื่อประกอบการพิจารณาปรับปรุง

นอกจากนี้ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็น

ความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบางประเภทนั้นอาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่ามีภัยคุกคามทางไซเบอร์เกิดขึ้น เนื่องจากข้อมูลดังกล่าวอาจสูญหายไป ในระหว่างที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี เมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำบันทึกข้อมูลสถิติภัยคุกคาม ทางไซเบอร์ โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแลและรับผิดชอบภายใน หน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยคุกคามทางไซเบอร์ในลักษณะ ดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมีดังนี้

1. Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น
2. Acquisition	ดำเนินการจัดเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้ 1. ต้องป้องกันการเปลี่ยนแปลงของหลักฐานด้วยการใช้งาน Hardware Write Blocker 2. ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น 3. ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด 4. ต้องทำการบันทึกหลักฐาน (Chain of Custody)
3. Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD5, SHA1, SHA256
4. Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident
5. 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 เนื่องจากหลักฐานที่พบสามารถนำไปใช้ในชั้นศาล หลักฐานเหล่านี้จึง จะต้องได้รับการจัดการอย่างระมัดระวัง และรอบคอบเพื่อหลีกเลี่ยงข้อกล่าวหาว่าเป็นหลักฐานที่ปลอมหรือทำ ขึ้นมา

ภาคผนวก

แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

1. ชื่อเหตุการณ์ 2. หมายเลขของเหตุการณ์.....

วันที่บันทึกเหตุการณ์

หมายเลขของเหตุการณ์อื่นๆที่เกี่ยวข้องกับเหตุการณ์นี้

ข้อมูลของผู้แจ้งเหตุการณ์ 6.ข้อมูลของเจ้าหน้าที่ที่รับมือเหตุการณ์

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

วันที่และเวลาเกิดเหตุการณ์

.....

วันที่และเวลาพบเหตุการณ์

.....

วันที่และเวลารายงานเหตุการณ์

.....

รายละเอียดเหตุการณ์

.....

.....

.....

การดำเนินการทั้งหมดของทีมรับมือและตอบสนอง

.....

.....

การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนอง

.....

.....

ค่าใช้จ่ายในการฟื้นฟูสภาพปกติ

.....

รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์

.....

.....

สรุปสาระ

.....

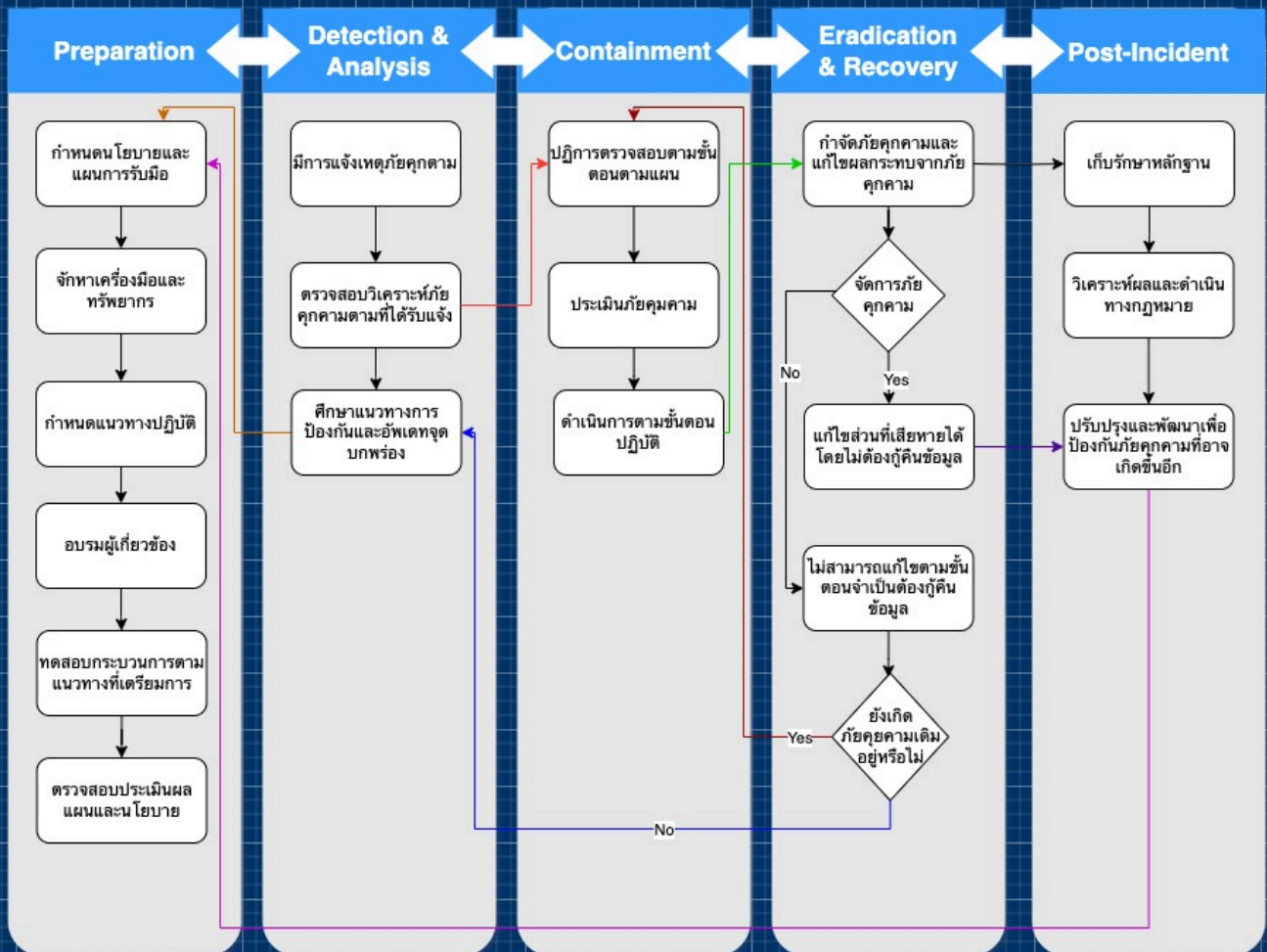
เอกสาร chain of custody

ชื่อเหตุการณ์

หมายเลขของเหตุการณ์.....

รายการ	รายละเอียด
๑. วันและเวลาของการเก็บหลักฐาน	
๒. สถานที่ที่เก็บหลักฐาน	
๓. รายชื่อผู้เชี่ยวชาญ	
๔. รายชื่อเจ้าของเครื่องคอมพิวเตอร์	
๕. เหตุผลในการเก็บรวบรวมหลักฐาน	
๖. หมายเลขของคดี	
๗. ชนิดของอุปกรณ์	
๘. หมายเลข Serial Number ของอุปกรณ์ (ถ้ามี)	
๙. รุ่นของอุปกรณ์	
๑๐. ความจุของอุปกรณ์ หรือ Hard disk	
๑๑. คำอธิบาย ทางกายภาพของคอมพิวเตอร์ เช่น กำลังเปิดใช้งาน หรือปิดอยู่	
๑๒. ชื่อของไฟล์ทั้งหมดที่ถูกเก็บรวบรวม	
๑๓. ความคิดเห็น ข้อเสนอแนะ และปัญหาที่พบ	
๑๔. ลายเซ็นของบุคคลที่ดำเนินการกับหลักฐาน	
๑๕. รายละเอียดอื่น ๆ ที่พบขณะเก็บหลักฐาน (หากเป็นไปได้ให้บันทึกให้มากที่สุด)	

Cyber Security Incident Response Process Flowchart [BSRU]



โครงสร้างการรับมือภัยคุกคามทางไซเบอร์

รายละเอียดของขั้นตอนการปฏิบัติเพื่อรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์มีดังนี้

ขั้นตอน	ผู้รับผิดชอบ
๑. การแจ้งเหตุ	ผู้พบเห็น/ผู้ที่ได้รับผลกระทบจาก incident
๒. Preparation ๒.๑ นโยบายหรือแนวปฏิบัติที่เกี่ยวข้อง ๒.๒ จัดเตรียมทรัพยากรที่ใช้ในการดำเนินงาน ๒.๓ เตรียมการป้องกันและแจ้งเตือน ๒.๔ เตรียมรายละเอียดช่องทางการติดต่อสื่อสาร ๒.๕ การให้ความรู้ และวิธีปฏิบัติ ๒.๖ ทดสอบการตอบสนองต่อภัยคุกคามทาง ไซเบอร์	ทีมรับมือและตอบสนองต่อ incident และหน่วยงานที่ใช้งานระบบ
๓. Detection & Analysis ๓.๑ รับแจ้งเหตุ ๓.๒ วิเคราะห์ความผิดปกติเมื่อได้รับแจ้ง ๓.๓ บันทึกข้อมูลเหตุการณ์ภัยคุกคาม ๓.๔ จัดลำดับความสำคัญของ incident ๓.๕ ติดต่อประสานงานกับหน่วยงานภายใน และภายนอก	ผู้รับแจ้งเหตุ ทีมเฝ้าระวังและวิเคราะห์การแจ้งเตือนภัยคุกคามจาก อุปกรณ์ตรวจจับ ผู้รับแจ้งเหตุ ทีมรับมือและตอบสนองต่อ incident ทีมรับมือและตอบสนองต่อ incident
๔. Containment ๔.๑ ควบคุมความเสียหาย ๔.๒ จัดเก็บและดูแลหลักฐานทางดิจิทัล	ทีมรับมือและตอบสนองต่อ incident
๕. Eradication & Recovery ๕.๑ แก้ไขสาเหตุ และผลกระทบจากการโจมตี ๕.๒ กู้คืนระบบ ข้อมูล และภาพลักษณ์จาก ความเสียหาย	ทีมรับมือและตอบสนองต่อ incident
๖. Post-incident ๖.๑ เก็บรักษาหลักฐานและบันทึกการ ดำเนินงาน ๖.๒ ปรับปรุง และพัฒนากระบวนการ กลไก แนวปฏิบัติในการรับมือ	ทีมรับมือและตอบสนองต่อ incident

ประกาศ ณ วันที่ ๙ ตุลาคม พ.ศ.๒๕๖๘

A handwritten signature in blue ink, consisting of two distinct, stylized characters.

(ผู้ช่วยศาสตราจารย์ ดร.ประไพ ศรีตามมา)
ผู้อำนวยการสำนักคอมพิวเตอร์



มหาวิทยาลัยราชภัฏบ้านสมเด็จเจ้าพระยา



BANSOMDEJCHAOPRAYA
RAJABHAT UNIVERSITY