



แผนรับมือภัยคุกคามทางไซเบอร์ วิทยาลัยเทคนิคกันทรลักษ์



คำนำ

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้ จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ งานศูนย์ข้อมูลและสารสนเทศ จึงได้จัดทำ "แผนรับมือเหตุภัยคุกคามทางไซเบอร์วิทยาลัยเทคนิคกันทรลักษณ์" เพื่อใช้เป็นแผนในการรับมือและฟื้นฟูบริการโครงสร้างพื้นฐานสำคัญด้านการจัดการเรียนการสอน ครู บุคลากร นักเรียน นักศึกษา ได้อย่างเป็นระบบ มีประสิทธิภาพและทันต่อเหตุการณ์

งานศูนย์ข้อมูลและสารสนเทศ
ฝ่ายแผนงานและความร่วมมือ
ตุลาคม ๒๕๖๗

สารบัญ

หลักการและเหตุผล	๑
วัตถุประสงค์	๑
ขอบเขต	๑
หน้าที่การทบทวนแผน	๑
หน้าที่ในการดำเนินการตามแผน	๑
ความเกี่ยวข้องกับเอกสารอื่น	๒
โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT)	๒
รูปแบบภัยคุกคามไซเบอร์	๓
ขั้นตอนการรับมือ	๔

แผนรับมือเหตุภัยคุกคามทางไซเบอร์วิทยาลัยเทคนิคกันทรลักษ์

๑. หลักการและเหตุผล

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้ของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการ กำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความ มั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.พ.ศ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อดำเนินการตาม พรบ. การรักษาความ มั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๖ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกันและแก้ไขปัญหที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบเครือข่ายคอมพิวเตอร์ ให้สามารถใช้งานได้

๒. วัตถุประสงค์

- ๒.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคามระบบสารสนเทศ
- ๒.๒ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
- ๒.๓ เพื่อให้การปฏิบัติราชการดำเนินไปได้อย่างมีประสิทธิภาพ
- ๒.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศของวิทยาลัยเทคนิคกันทรลักษ์

๓. ขอบเขต

แผนรับมือฯ ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ และข้อมูลดิจิทัลของวิทยาลัยเทคนิคกันทรลักษ์ รวมถึงบุคคลหรืออุปกรณ์ใด ๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว

๔. หน้าที่การทบทวนแผน

งานศูนย์ข้อมูลและสารสนเทศมีหน้าที่ทบทวนและขออนุมัติแผนรับมือฯ ฉบับนี้ถึงคณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์วิทยาลัยฯ

๕. หน้าที่ในการดำเนินการตามแผน

งานศูนย์ข้อมูลและสารสนเทศมีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย

๑. ฝ่ายแผนงานและความร่วมมือ
๒. ฝ่ายวิชาการ
๓. ฝ่ายบริหารทรัพยากร
๔. ฝ่ายพัฒนากิจการนักเรียน นักศึกษา

๖. ความเกี่ยวข้องกับเอกสารอื่น

๖.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์ วิทยาลัยเทคนิคกันทรลักษ์

๖.๒ นโยบายและแนวปฏิบัติด้านการคุ้มครองข้อมูลส่วนบุคคล วิทยาลัยเทคนิคกันทรลักษ์

๖.๓ ประกาศวิทยาลัยเทคนิคกันทรลักษ์ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.

๒๕๖๓

๖.๔ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ วิทยาลัยเทคนิคกันทรลักษ์

๗. นิยาม

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

เหตุการณ์คุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมีขอบเขตใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมีขอบเขตใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภัยอันตรายที่ใกล้จะถึงที่จะก่อให้เกิดหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

เหตุการณ์คุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุการณ์คุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๘ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘. โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Respo CIRT)

วิทยาลัยเทคนิคกันทรลักษ์ ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ในลักษณะแบบรวมศูนย์ ประกอบด้วย

๑. นางสาวทักษิณา ชมจันทร์	หัวหน้าทีมรับมือ	ผู้อำนวยการ
๒. นายสมศักดิ์ จันทานิตย์	รองหัวหน้าทีมรับมือ	รองผู้อำนวยการ
๓. นายณัฏพงศ์ โยธี	เจ้าหน้าที่รับมือ	หัวหน้างานศูนย์ฯ
๔. นายณัช มนตรี	เจ้าหน้าที่รับมือ	เจ้าหน้าที่งานศูนย์ฯ

๙. รูปแบบภัยคุกคามไซเบอร์

Malware คือ ซอฟต์แวร์หรือ Code ประเภทหนึ่งที่มีจุดประสงค์ในการผลิตออกมาเพื่อส่งผลกระทบต่อระบบคอมพิวเตอร์ที่ เมื่อถูกติดตั้งหรือเปิดในระบบคอมพิวเตอร์ Malware จะทำให้สามารถเข้าถึงทรัพยากรของระบบคอมพิวเตอร์ และอาจแชร์ข้อมูล ไปยังเครื่องคอมพิวเตอร์เครื่องอื่น ๆ ในเครือข่าย รวมถึงเซิร์ฟเวอร์ต่าง ๆ โดยมีพฤติกรรมแตกต่างกันตามที่ไม่ประสงค์ที่ทำการ ผลิตออกมา ชื่อเรียก Malware นั้นครอบคลุมถึงไวรัส (Virus) เวิร์ม (worms) โทรจัน (Trojans)

Web-based attacks คือ วิธีการโจมตีเหยื่อโดยผ่านช่องทางเว็บไซต์ โดยทำเว็บไซต์ หรือ Hack เว็บไซต์ที่มีช่องโหว่เพื่อแก้ไข เว็บไซต์โดยการใส่ code ที่ทำให้เหยื่อเมื่อเข้าเว็บไซต์ดังกล่าวแล้ว จะนำเหยื่อไปที่เป้าหมายปลายทางที่เป็น เว็บไซต์ที่ทำการวาง Malware ไว้เพื่อทำให้เครื่องคอมพิวเตอร์ของเหยื่อติด Malware

Phishing คือ วิธีการโจมตีเหยื่อผ่านทางช่องทางต่าง ๆ เช่น E-Mail, SMS, เว็บไซต์ หรือ ช่องทาง Social โดยวิธีการหลอกล่อเหยื่อด้วยวิธีการต่าง ๆ ที่ทำให้เหยื่อหลงเชื่อและให้ข้อมูลส่วนตัว เช่น Uername, Passw ข้อมูลสำคัญอื่น ๆ เพื่อนำข้อมูลดังกล่าวของเหยื่อไปใช้ในการทำธุรกรรม

Web application attacks Re วิธีการโจมตีเว็บไซต์เป้าหมายโดยอาศัยช่องโหว่ต่าง ๆ เช่น Code ของเว็บไซต์และ Web Server หรือ Database Server

Spam คือ วิธีการที่ผู้ส่ง หรือผู้ไม่ประสงค์ดีทำการส่งข้อมูล, ข้อความ, หรือโฆษณาต่าง ๆ ผ่านช่องทางต่าง ๆ ไปยังผู้รับ เช่น E-Mail. SMS. เว็บไซต์ หรือ ช่องทาง Social โดยเป็นการส่งจำนวนมากหรือส่งโดยที่ไม่ได้ขออนุญาตไปยังผู้รับ เพื่อสร้างความรำคาญหรือก่อกวน

DDoS (Distributed Denial of Service) คือ วิธีการโจมตีเป้าหมายที่เป็นเว็บไซต์, ระบบการระบบเครือข่าย โดยใช้เครื่องโจมตีที่เป็นต้นทางจำนวนมากยิงมาที่เป้าหมายเดียว ภายในเวลาเดียวกันจุดประสงค์เพื่อให้เว็บไซต์, ระบบการให้บริการ หรือระบบเครือข่ายไม่สามารถใช้งานได้

Data breach คือ เกิดการรั่วไหลของข้อมูลที่เกิดจากช่องโหว่ หรือการโจมตีเพื่อขโมยข้อมูลของแอปพลิเคชัน หรือระบบที่ให้บริการต่าง ๆ โดยที่เจ้าของข้อมูลหรือผู้ให้บริการแอปพลิเคชัน ไม่ทราบ ซึ่งผู้โจมตีต้องการนำข้อมูลไปขาย หรือเพื่อเรียกค่าไถ่ของชุดข้อมูล นั้นๆ

Insider threat คือ ภัยที่เกิดจากภายในบุคลากรภายในขององค์กร ซึ่งอาจจะเกิดจากความตั้งใจ หรือไม่ตั้งใจ ผ่านช่องทางการใช้งานปกติของบุคลากร เช่น เครื่องคอมพิวเตอร์ของบริษัท หรือ สมาร์ทโฟน เป็นต้น ซึ่ง Insider threat เป็นภัยประเภทที่มีความรุนแรงเนื่องจากภายในองค์กร อาจจะมีการป้องกันในระดับต่ำทำให้เกิดการโจมตีประเภทนี้ได้ง่าย และผลลัพธ์ของภัยนี้มีความรุนแรง

Botnets หรือ Robot Network คือ โปรแกรมที่ถูกเขียนขึ้นโดยผู้ไม่ประสงค์ดี ที่ทำการติดตั้งโปรแกรมแบบแฝงตัวอยู่ในเครื่องคอมพิวเตอร์ หรืออุปกรณ์ต่าง ๆ เพื่อรอรับคำสั่งให้ทำการโจมตีเป้าหมายหรือดำเนินการบางอย่างที่โปรแกรมไว้ ซึ่งส่วนมากเครื่องที่ Botnets แฝงตัวบนเครื่องของเหยื่อจะไม่ทราบว่ามีการติด BotBotnets จะไม่ทำงานตลอดเวลา จะทำงานก็ต่อเมื่อมีการเรียกจากผู้ผลิต (ผู้ไม่ประสงค์ดี)

Ransomware คือ Malware ประเภทหนึ่งที่ถูกติดตั้งที่เครื่องคอมพิวเตอร์แล้วจะหาวิธีการเข้ารหัสไฟล์ข้อมูลทั้งหมดในเครื่องทำให้ข้อมูลที่อยู่ในเครื่องไม่สามารถเปิดเพื่อใช้งานได้ ซึ่งจุดประสงค์ทำการล็อกไฟล์เพื่อที่จะเรียกค่าไถ่ของรหัสผ่านที่ใช้ในการปลดล็อกไฟล์เพื่อให้ไฟล์ที่คอมพิวเตอร์นั้นกลับมาใช้งานได้อีกครั้ง

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

ผู้บุกรุก (Hacker) ผู้ที่ไม่ได้รับอนุญาตในหารใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเป็นเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหาย จากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๑๐. ขั้นตอนการรับมือ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของวิทยาลัยฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึง นโยบายความมั่นคงปลอดภัยสารสนเทศทางไซเบอร์วิทยาลัยฯ ดังนี้

๑๐.๑ ขั้นการเตรียมการเพื่อให้วิทยาลัยฯ มีความพร้อมในการรับมือปัญหาภัยคุกคามทางไซเบอร์ตามที่ระบุ จึงได้ดำเนินการเตรียมความพร้อม ดังนี้

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

(๒) กำหนดโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

(๓) กำหนดเกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

(๔) ดำเนินการตามแนวปฏิบัติพื้นฐาน (Security Control Baselines) เพื่อเตรียมการและป้องกันการเกิดภัยคุกคามทางไซเบอร์ (preparation) ดังนี้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง	๑. การเตรียมความพร้อมด้านอุปกรณ์ ๑.๑ อุปกรณ์ป้องกันระบบเครือข่าย (Next Generation Firewall) ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ประเภท Dos/DDos BOTNET Phishing Hackers ทั้งนี้ อุปกรณ์ป้องกันระบบเครือข่ายที่จัดหาจากความสามารถในการเป็น Firewall แล้ว ยังต้องมีความสามารถอื่น ๆ เพิ่มเติม ได้แก่ ความสามารถในการตรวจจับผู้บุกรุก (IPS) ความสามารถในการคัดกรองเว็บไซต์อันตราย

<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง</p>	<p>๑.๒ ซอฟต์แวร์ตรวจสอบประสิทธิภาพระบบเครือข่าย (Network Monitoring Software) ใช้สำหรับตรวจจับความผิดปกติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์กลาง</p> <p>๑.๓ อุปกรณ์ web app firewall ใช้สำหรับป้องกันภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับระบบงานคอมพิวเตอร์ที่พัฒนาขึ้นมาให้บริการผ่าน web browser ได้แก่ การคุกคามทางไซเบอร์ประเภท Hacker โดยสามารถป้องกันเทคนิคการบุกรุก</p> <p>๑.๔ ซอฟต์แวร์สำรองข้อมูล ใช้สำหรับกระบวนการสำรองข้อมูล และการกู้ข้อมูลของระบบเครือข่ายคอมพิวเตอร์ รวมทั้งยังสามารถสำรองข้อมูลแบบเข้ารหัสได้</p>
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับวิกฤติ</p>	<p>๑.๕ อุปกรณ์จัดเก็บข้อมูลภายนอก (SAN Storage) เป็นอุปกรณ์ที่ใช้สำหรับติดตั้งระบบงานคอมพิวเตอร์ และในการรับมือทางไซเบอร์อุปกรณ์จัดเก็บข้อมูลภายนอกยังสามารถลดผลกระทบที่เกิดจาก Ransomsomware โดยจะใช้อุปกรณ์จัดเก็บข้อมูลภายนอกดังกล่าวจัดทำพื้นที่จัดเก็บกับข้อมูลส่วนกลางอย่างสม่ำเสมอ ซึ่งหากนำไฟล์สำคัญมาจัดเก็บเอาไว้ที่พื้นที่จัดเก็บข้อมูลส่วนกลางแม้ว่าจะเกิดภัยคุกคามไซเบอร์ประเภท Ransomware ก็สามารถนำข้อมูลสำคัญที่เก็บอยู่บนพื้นที่จัดเก็บข้อมูลส่วนกลางกลับมาได้</p> <p>๑.๖ ระบบงานคอมพิวเตอร์สำรอง ใช้ในกรณีไม่สามารถกู้ระบบงานคอมพิวเตอร์ขึ้นมาได้</p> <p>๑.๗ อุปกรณ์จัดเก็บ Log file ใช้สำหรับจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่เกิดขึ้นจากการใช้งานเครือข่ายคอมพิวเตอร์กลาง</p> <p>๑.๘ อุปกรณ์วิเคราะห์ Log file ใช้สำหรับวิเคราะห์ข้อมูลจราจรคอมพิวเตอร์ที่เกิดจากการใช้งานคอมพิวเตอร์กลาง ซึ่งข้อมูลที่ถูวิเคราะห์ดังกล่าวจะช่วยระบุถึงหมายเลข IP Address ของผู้โจมตี และลักษณะภัยคุกคามไซเบอร์ที่โจมตีระบบเครือข่ายคอมพิวเตอร์กลางและใช้ประกอบการทำรายงานให้แก่คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์</p> <p>๑.๙ ซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์แบบคอร์ปอเรต (Corporate AntivirusSoftware) ใช้สำหรับติดตั้งบนเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งสามารถป้องกันภัยคุกคามไซเบอร์ประเภท Malware, Computer Virus, Computer worm,Trojan, Ransomware, BOTNET และ Spam Mail</p> <p>๒. แผนการตรวจสอบการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ระบบเครือข่ายคอมพิวเตอร์กลาง สามารถรับมือกับภัยคุกคามทางไซเบอร์ที่มีการพัฒนาขึ้นตลอดเวลาจะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์มาตรวจสอบ โดยจะมีจำนวนครั้งในการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งในการตรวจสอบและประเมินความเสี่ยงนี้ อาจสามารถค้นหาภัยคุกคามไซเบอร์ประเภท Backdoor ที่ถูกซ่อนเอาไว้จากขั้นตอนการพัฒนากระบวนการทำงานคอมพิวเตอร์ได้</p>

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับไม่ร้ายแรง	๓. การเตรียมพร้อมด้านบุคลากร ๓.๑ การให้ความรู้เพื่อให้บุคลากรมีความรู้เกี่ยวกับภัยคุกคามทางไซเบอร์จะพิจารณาจ้างบริษัทผู้เชี่ยวชาญในการประเมินความเสี่ยงการรักษาความมั่นคงปลอดภัยไซเบอร์ ดำเนินการจัดฝึกอบรมให้ความรู้แก่บุคลากร ๓.๒ มีผู้ดูแลด้านการรักษาความมั่นคงปลอดภัยเครือข่าย และผู้ดูแลระบบคอมพิวเตอร์กลาง
กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับร้ายแรง	๔. การเตรียมความพร้อมด้านการสำรองข้อมูลและระบบคอมพิวเตอร์สำรองในกรณีภัยคุกคามทางไซเบอร์ ก่อเกิดความเสียหายแก่ระบบเครือข่ายคอมพิวเตอร์กลาง อย่างมากจนไม่สามารถทำงานได้เป็นเวลานานจะพิจารณาทางเลือกในการแก้ไขปัญหาโดยวิธีการกู้คืนข้อมูลที่เสียหาย หรือ เปิดใช้ระบบคอมพิวเตอร์สำรอง โดยมีเป้าหมายเพื่อให้ระบบคอมพิวเตอร์กลางสามารถใช้งานได้อย่างรวดเร็วที่สุด
กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับวิกฤติ	

๑๐.๒ ดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันทั่วถึงที่เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น โดยวิทยาลัยฯ ได้ดำเนินการตามประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังนี้

ระดับ	แนวปฏิบัติ
กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับไม่ร้ายแรง	๑ กำหนดช่องทางที่จะใช้ในการตรวจจับความผิดปกติได้อย่างเหมาะสมกับสภาพแวดล้อมที่ดูแล โดยสามารถพิจารณา "การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident" ๒. ดำเนินการวิเคราะห์ Incident ได้อย่างรวดเร็วและเหมาะสม ๓. การกำหนดจุดและวิธีการที่จะใช้ในการตรวจจับ Incident การตรวจจับ Incident จะขึ้นอยู่กับระบบที่ใช้งานอยู่และรูปแบบของพยายามในการโจมตีประกอบกับกลไกต่าง ๆ ที่ทำการปกป้องระบบอยู่เพราะโดยทั่วไประบบการป้องกันจะทำการแจ้งเตือน (Alert) หรือ เก็บบันทึกข้อมูล (Log) เพื่อ ใช้ในการวิเคราะห์หาความผิดปกติด้วย

ระดับ	แนวปฏิบัติ
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง</p>	<p>โดยลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น 2 ประเภท</p> <ul style="list-style-type: none"> • Precursor เป็นข้อมูลที่บ่งบอกว่า Incident จะเกิดขึ้นในอนาคต • Indicator เป็นข้อมูลที่บ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่ <p>ซึ่งการเลือกใช้อุปกรณ์ป้องกันและตรวจจับ นอกจากจะต้องพิจารณาความเหมาะสมกับระบบที่ต้องการจะ ป้องกันแล้ว ควรต้องมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ เป็นสำคัญและถูกต้องมากยิ่งขึ้น ซึ่งเทคนิคในการวิเคราะห์เหตุภัยคุกคามเมื่อได้รับแจ้งมีดังต่อไปนี้</p>
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับไม่ร้ายแรง</p>	<p>๔.การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติเมื่อได้รับแจ้ง</p> <p>การวิเคราะห์เหตุภัยคุกคามหรือความผิดปกติควรมีความถูกต้องแม่นยำและประสิทธิภาพ เพื่อให้การ ดำเนินการในขั้นตอนต่อไปสามารถดำเนินการได้เร็ว</p> <p>๔.๑ Profing (Baselining) Networks and Systems & Understand Normal Behavior ข้อมูลสถานะการทำงาน การตั้งค่า และการใช้งานปกติของระบบ จะทำให้ทราบ ได้เร็วขึ้นเมื่อมีพฤติกรรมผิดปกติเกิดขึ้นในระบบ</p>
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง</p>	<p>๔.๒ Log Retention Policy Log จากอุปกรณ์ต่าง ๆ เช่น IPDS, Work Servers, Network Devices เป็นต้น จะมีความสำคัญเป็นอย่างมากในการวิเคราะห์หาสาเหตุการโจมตี และ บันทึกเหตุการณ์เก็บไว้เพื่อหลักฐานทางกฎหมายหรือเรียกดูในอนาคต จึง ต้องมี การเก็บรักษาและป้องกันอย่างดี รวมถึงเก็บไว้เป็นระยะเวลาที่เหมาะสม ตอบ โจทย์ในด้านตอบสนองและเป็นไปตามกฎหมายข้อบังคับ</p>
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง</p>	<p>๔.๓ Perform Event Correlation การโจมตีโดยทั่วไปมักจะมีเส้นทางระบบเป้าหมายที่ผ่านอุปกรณ์ต่าง ๆ บนเครือข่าย ดังนั้นการวิเคราะห์ก็จำเป็นต้องใช้ข้อมูลจากทุกอุปกรณ์ ที่คาดว่า จะเกี่ยวข้องร่วมกัน (Correlation)เพื่อให้เห็นถึงเส้นทางของการโจมตี และสาเหตุที่แท้จริงที่ทำให้การบุกรุกประสบผลสำเร็จ</p> <p>๔.๔ Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการSynchronize เวลาให้ตรงกันอยู่เสมอ ไม่เช่นนั้นแล้วการ Correlate Eventจะทำได้ยากหรือไม่สามารถทำได้</p>
<p>กรณีบริการ ระบบ หรือ อุปกรณ์มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ระดับร้ายแรง</p>	<p>๔.๕ Sniff and Analyze Network Data ในหลาย ๆ กรณีการดักจับข้อมูลทางเครือข่าย ขณะเกิดเหตุเพื่อนำมาทำการ วิเคราะห์สามารถที่จะให้ข้อมูลเบาะแสที่สำคัญได้</p> <p>๔.๖ Seek Assistance เมื่อใดที่ทีมตอบสนองไม่สามารถดำเนินการวิเคราะห์ Incident เพื่อหาสาเหตุที่ แท้จริงเพื่อกำจัดผู้บุกรุกออกจากระบบได้ ก็สามารถใช้บริการให้ คำแนะนำปรึกษา จากภายนอกตามสมควรได้ เช่น CERT ต่าง ๆหรือบริการจากที่ปรึกษา ภายนอก เป็นต้น</p>

ระดับ	แนวปฏิบัติ
<p>กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับไม่ร้ายแรง</p> <p>กรณีบริการ ระบบ หรือ อุปกรณ์ มีแนวโน้มที่จะเกิดผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับร้ายแรง</p>	<p>๕. การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม มีการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ซึ่งจะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น โดยหน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้น ตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม ซึ่งการบันทึกข้อมูลอาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูล เช่น ระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์ขั้นตอนการจัดการ และแก้ไขเหตุ ภัยคุกคามเพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม</p> <p>๖. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของหน่วยงานและลดผลกระทบทางธุรกิจให้น้อยลงที่สุด</p> <p>๗. การวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจเชิงกลยุทธ์ เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัดของบริษัท และ ลดผลกระทบทางธุรกิจให้น้อยลงที่สุด</p> <p>๘. วิทยาลัยฯสามารถพิจารณาปัจจัยในเรื่องดังต่อไปนี้พิจารณาเพื่อกำหนด แนวทางในการติดต่อประสานงานและแจ้งข้อมูลให้กับผู้ที่เกี่ยวข้อง</p> <ul style="list-style-type: none"> • เป็นผู้ได้รับผลกระทบจาก Incident • เป็นผู้ที่ทำหน้าที่ตัดสินใจในการดำเนินการที่เกี่ยวข้องกับ Incident • เป็นผู้ที่ทำหน้าที่รับผิดชอบกำหนดนโยบายและแผน • เป็นผู้ที่ทำหน้าที่รับผิดชอบตามที่กฎหมายกำหนด <p>การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง บุคลากรหรือหน่วยงานที่ควรได้รับการ แจ้งเหตุภัยคุกคาม มีดังต่อไปนี้</p> <ul style="list-style-type: none"> • ผู้บริหาร (Top Management) • ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) • ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือ หัวหน้าหน่วยงาน


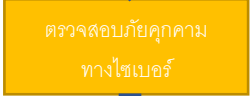
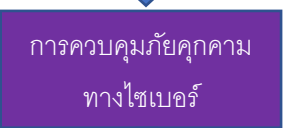

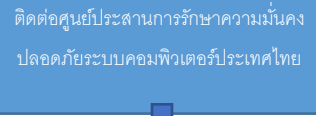
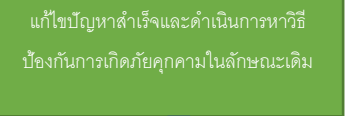


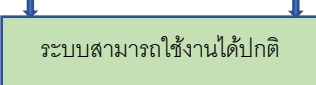
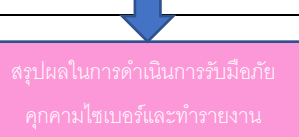
ระดับ	แนวปฏิบัติ
<p>กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับไม่ร้ายแรง</p> <p>กรณีบริการ ระบบ หรือ อุปกรณ์ มี แนวโน้มที่จะเกิด ผลกระทบเป็นภัยคุกคามทางไซเบอร์ ระดับร้ายแรง</p>	<p>รักษาความ มั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ (He Information Security)</p> <ul style="list-style-type: none"> ทีมรับมือและตอบสนองต่อเหตุการณ์อื่น ๆ ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอก (ตามความเหมาะสม) เจ้าของระบบงาน (System Owner) ฝ่ายทรัพยากรบุคคล (Human Resources) ฝ่ายสื่อสารองค์กร (สำหรับเหตุการณ์ที่จำเป็นต้องให้การประชาสัมพันธ์) ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย) ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team) ทีมรับมือและตอบสนองต่อเหตุการณ์วิกฤต (Crisis Management Team) หน่วยงานกำกับ (Regulators) / ทีม TI-CERT หน่วยงาน CERT (Computer Emergency Response Team) หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง (Law Enforcer)

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคาม ทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ เป็นการดำเนินการเพื่อระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery) โดยการดำเนินการดังกล่าวควร กำหนดให้สอดคล้องกับความรุนแรงและระดับของภัยคุกคามทางไซเบอร์แต่ละระดับจนกระทั่งสามารถกู้คืนพัยสินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ ซึ่งการดำเนินการในขั้นต้องกระทำควบคู่ไปกับการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ที่อาจมีการลุกลามหรือทวีความรุนแรงมากขึ้นเพื่อให้การระงับและการปราบปรามภัยคุกคามทางไซเบอร์ ตลอดจนการฟื้นฟูระบบงานที่ได้รับผลกระทบจากการเกิดคุกคามทางไซเบอร์ สอดคล้องกับสถานการณ์ที่เปลี่ยนแปลงไป ประกอบด้วยดำเนินการในเรี่

- (๑) จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
- (๒) เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
- (๓) ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์
- (๔) เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงกักกันที่กการยึดหลักฐานคอมพิวเตอร์ที่ได้มาหรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน
- (๕) ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี
- (๖) ดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๓ ในประกาศคณะกรรมการการรักษาความมั่นคง

ไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปรามประจักษ์ภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔

ทั้งนี้ขั้นตอนการปฏิบัติเมื่อเกิดภัยคุกคามทางไซเบอร์ของวิทยาลัยฯ มีขั้นตอนดังนี้

ขั้นตอน	รายละเอียด
 <p>ตรวจพบภัยคุกคามทางไซเบอร์</p>	มีการแจ้งเหตุจากผู้ใช้งานหรือตรวจจับการคุกคามทางไซเบอร์ได้จากอุปกรณ์ป้องกันระบบเครือข่าย หรือ เครื่องมือต่างๆ ตามที่กำหนด ซึ่งจะช่วยให้สามารถตรวจพบภัยคุกคามทางไซเบอร์ได้อย่างรวดเร็ว
 <p>ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์</p>	ตรวจสอบข้อมูลของภัยคุกคามทางไซเบอร์ และประเมินระดับภัยคุกคามตามที่กำหนดใน พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒
 <p>การควบคุมภัยคุกคามทางไซเบอร์</p>	ดำเนินการควบคุมภัยคุกคามทางไซเบอร์ ให้ส่งผลกระทบน้อยที่สุด และป้องกันไม่ให้เกิดการแพร่กระจายไปยังส่วนอื่นๆ ซึ่งในกรณีเร่งด่วน จะดำเนินการปิดระบบ หรือตัดการเชื่อมต่อของระบบคอมพิวเตอร์ชั่วคราว
 <p>แก้ไขปัญหา</p>	ดำเนินการแก้ไขหรือกำจัดภัยคุกคามทางไซเบอร์เบื้องต้นในทันที
 <p>ติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย</p>	ในกรณีที่ไม่สามารถแก้ไขปัญหาได้จึงดำเนินการติดต่อศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทยเพื่อขอคำแนะนำหรือช่วยเหลือ
 <p>แก้ไขปัญหาสำเร็จและดำเนินการหาวิธีป้องกันการเกิดภัยคุกคามในลักษณะเดิม</p>	หลังจากแก้ไขปัญหาภัยคุกคามไซเบอร์แล้ว จะดำเนินการตรวจหาช่องโหว่ โดยอุปกรณ์ตรวจสอบช่องโหว่ระบบเครือข่าย หรือเครื่องมืออื่นๆ และหาวิธีเพื่อป้องกันการเกิดภัยคุกคามไซเบอร์ในลักษณะเดิม
 <p>ทดสอบ</p>	ตรวจสอบการทำงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศว่าสามารถทำงานได้สมบูรณ์หรือไม่ ในกรณีที่พบว่าการทำงานไม่สมบูรณ์ หรือข้อมูลสำคัญเสียหายไปจะดำเนินการกู้คืนระบบงาน
 <p>กู้คืนระบบ</p>	ดำเนินการตามขั้นตอนการกู้คืนข้อมูลตามที่ระบบในแผนการสำรองและกู้คืนระบบ ในกรณีที่กู้คืนไม่ได้ จะพิจารณาเปิดใช้ระบบงานคอมพิวเตอร์สำรองและเร่งกู้ระบบงานคอมพิวเตอร์หลัก
 <p>ระบบสามารถใช้งานได้ตามปกติ</p>	เมื่อโครงสร้างพื้นฐานสำคัญทางสารสนเทศสามารถทำงานได้ตามปกติแล้วหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบสารสนเทศจะดำเนินการสรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์
 <p>สรุปผลในการดำเนินการรับมือภัยคุกคามไซเบอร์และทำรายงาน</p>	สรุปผลในการรับมือภัยคุกคามทางไซเบอร์ และแจ้งผลการดำเนินงานให้แก่ผู้เกี่ยวข้อง เช่น ผู้อำนวยการ ผู้บริหารตามระดับ

๑๐.๔ ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์

การดำเนินกิจกรรมที่เกี่ยวข้องภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์(Post-incident Activity)นั้น ให้จัดทำข้อกำหนดขั้นตอน วิธีปฏิบัติ ที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว เพื่อให้สามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่อง และพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไป โดยให้มีการประชุมหารือเพื่อแลกเปลี่ยนข้อมูล ความคิดเห็น ในการนำไปพัฒนาและปรับปรุงแนวทางในการรับมือและตอบสนองภัยคุกคามทางไซเบอร์ รวมทั้งการใช้ข้อมูล เพื่อประกอบการพิจารณาปรับปรุง นอกจากนี้ ต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้น นั้น อาจเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิด เกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไขเพิ่มเติม หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง โดยการเก็บข้อมูลบาง ประเภทนั้ อาจจำเป็นต้อง ดำเนินการตั้งแต่เมื่อมีการตรวจพบว่า มีภัยคุกคามทางไซเบอร์เกิดขึ้นเนื่องจากข้อมูล ดังกล่าวอาจสูญหายไปในช่วงที่ต้องระงับเหตุภัยคุกคามทางไซเบอร์นั้น หรืออาจถูกลบหรือทำลายโดยผู้โจมตี เมื่อมีการเก็บรวบรวมข้อมูล และหลักฐานที่จำเป็นแล้ว ให้นำข้อมูลและหลักฐานที่รวบรวมได้มาใช้ในการจัดทำ บันทึกรายการข้อมูลสถิติภัยคุกคามทางไซเบอร์โดยอาจจัดทำเป็นรายสัปดาห์หรือรายเดือน เพื่อเสนอต่อผู้ที่มีหน้าที่ดูแล รับผิดชอบภายในหน่วยงาน และกำหนดขั้นตอนที่หน่วยงานควรดำเนินการ เพื่อป้องกันไม่ให้เกิดภัยไซเบอร์ใน ลักษณะ ดังกล่าวขึ้นอีกในอนาคต

หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญ ดังนี้

๑.Assessment	การประเมินเพื่อหาจุดที่ต้องดำเนินการจัดเก็บหลักฐานของ incident ที่กำลังรับมือและตอบสนอง 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 หรือความอ่อนไหวต่อการสูญเสีย กระแสไฟฟ้าของ หลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มี กระแสไฟ คอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก ๓. ต้องบันทึก รายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติ อย่างละเอียด ๔. ต้องทำ การบันทึกหลักฐาน (Chain of Custody)
๓.Authentication	ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับ ต้นฉบับด้วยวิธี Cryptographic Hash
๔.Analysis & Report	วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือ เพื่อค้นหาสาเหตุของการเกิด Incident
๕.Archive	จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการ เคลื่อนย้าย

