ประกาศกรมป่าไม้
เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้ พ.ศ. ๒๕๖๗

อาศัยอำนาจตามความในมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ กรมป่าไม้ จึงจัดทำแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ พ.ศ. ๒๕๖๗ ดังต่อไปนี้

ข้อ ๑ วัตถุประสงค์และขอบเขต

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยแนวทางปฏิบัติฉบับนี้ จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์ ดังนั้น กรมป่าไม้ จึงจัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ พ.ศ. ๒๕๖๗ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ได้

ข้อ ๒ องค์ประกอบของแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ กรมป่าไม้ อ้างอิงจากพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์พ.ศ. ๒๕๖๒ มาตรา ๔๔ ซึ่งประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๑. แนวทางปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

โดยมีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐมีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งจากผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระภายนอกอย่างน้อยปีละหนึ่งครั้ง โดยมีขอบเขตของการตรวจสอบ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) กับบริการที่สำคัญที่หน่วยงานของรัฐ ที่สอดคล้องตามแผนรองรับสถานการณ์ฉุกเฉิน ที่จัดทำตามแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง (Business Continuity Plan : BCP) ของกรมป่าไม้

/๒.แนวทางปฏิบัติ...

๒.๒. แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

โดยมีวัตถุประสงค์เพื่อให้หน่วยงานของรัฐจำเป็นต้องรับทราบเมื่อทำการประเมินความเสี่ยงให้องค์กรต้องพิจารณากำหนดวัตถุประสงค์ในการบริหารความเสี่ยง ให้มีความสอดคล้องกับกลยุทธ์และความเสี่ยงที่องค์กรยอมรับได้ เพื่อวางเป้าหมายในการบริหารความเสี่ยงขององค์กรได้อย่างชัดเจนและเหมาะสม โดยเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉิน วางแผน ควบคุม แก้ไขความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดโอกาสที่จะก่อให้เกิดความเสียหายด้านความมั่นคงปลอดภัยไซเบอร์ที่ไม่ต้องการกับระบบสารสนเทศ

๒.๓. แผนรับมือภัยคุกคามทางไซเบอร์

เพื่อใช้เป็นแผนในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับกรมป่าไม้ โดยจะเป็นการกำหนดหน้าที่และความรับผิดชอบให้กับหน่วยงานต่างๆ ภายใต้สังกัดกรมป่าไม้ การกำหนดประเภทของเหตุภัยคุกคามทางไซเบอร์ การกำหนดความสัมพันธ์กับนโยบายและแนวปฏิบัติที่เกี่ยวข้อง การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมป่าไม้

องค์ประกอบของแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์แต่ละเรื่องที่กล่าวมาข้างต้นจะประกอบด้วยวัตถุประสงค์เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้สามารถใช้งานได้ ทำให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้ มีการปฏิบัติได้อย่างรวดเร็ว ถูกต้อง และมีประสิทธิภาพ ตามเอกสารแนบท้าย

ประกาศ ณ วันที่ ๒๓ พฤษภาคม พ.ศ. ๒๕๖๗

(นายนิกร ศิรโรจนานนท์)
รองอธิบดี ปฏิบัติราชการแทน
อธิบดีกรมป่าไม้

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ พ.ศ. ๒๕๖๗

แนบท้ายประกาศกรมป่าไม้ ลงวันที่ ๒๗ พฤษภาคม พ.ศ. ๒๕๖๗

เรื่อง แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้ พ.ศ. ๒๕๖๗

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้ พ.ศ. ๒๕๖๗

คำนำ

กรมป่าไม้เป็นหน่วยงานที่มีหน้าที่ ป้องกัน และรักษาพื้นที่ป่าไม้ให้คงอยู่เพิ่มพื้นที่ป่าเศรษฐกิจ สนับสนุนการเพิ่มพื้นที่สีเขียว และฟื้นฟูพื้นที่ป่าไม้ให้อุดมสมบูรณ์ ตอบสนองความต้องการทั้งด้านเศรษฐกิจ สังคม และสิ่งแวดล้อม บริหารจัดการทรัพยากรป่าไม้โดยการมีส่วนร่วม บริหารจัดการที่ดินป่าไม้อย่างเป็นระบบและเป็นธรรม เพื่อให้คนอยู่ร่วมกับป่าอย่างสมดุลและยั่งยืน วิจัยและพัฒนา เพื่อสร้างนวัตกรรม และถ่ายทอดเทคโนโลยีในการอนุรักษ์ และการใช้ประโยชน์ทรัพยากรป่าไม้ พัฒนาความสามารถเชิงรุกขององค์กร ทั้งระบบ กลไก ข้อมูลสารสนเทศ และปรับปรุงกฎระเบียบให้ทันสมัยให้เหมาะกับภาวการณ์ปัจจุบัน ได้มีการพัฒนาระบบสารสนเทศ ระบบฐานข้อมูล ระบบภูมิศาสตร์สารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ตลอดจนการให้บริการระบบเครือข่ายอินเทอร์เน็ต การประชุมออนไลน์ (Video Conference) และการติดต่อสื่อสารด้านเทคโนโลยีสารสนเทศในรูปแบบต่างๆ แก่บุคลากรของกรมป่าไม้ประชาชน และผู้ประกอบการ ให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว มีประสิทธิภาพ ถูกต้อง อีกทั้งยังมี การใช้บริการการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ เช่น กรมการปกครอง กรมศุลกากร สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น ซึ่งบริการดังข้างต้นที่ได้กล่าวมาเป็นระบบเทคโนโลยีสารสนเทศหลักของกรมป่าไม้ เพื่อพัฒนาไปสู่นโยบายไทยแลนด์ ๔.๐ และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย

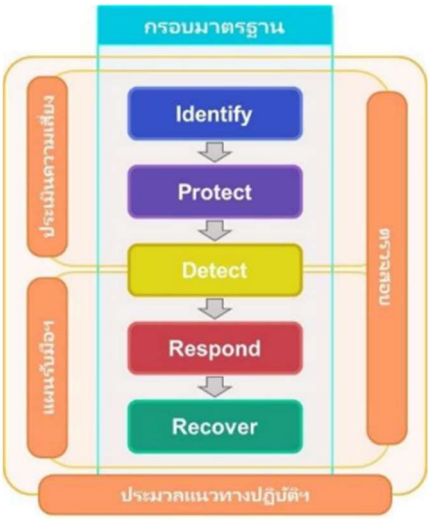
ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐ จัดทำแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้สอดคล้องกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ประกอบด้วย แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนรับมือเหตุภัยคุกคามทางไซเบอร์ ดังนั้น กรมป่าไม้ จึงได้จัดทำแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๗ เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้สามารถปฏิบัติได้อย่างรวดเร็ว มีประสิทธิภาพ และเป็นไปในทิศทางเดียวกัน สอดคล้องกับมาตรฐานสากล ที่สามารถป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ได้

สารบัญ

แนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์กรมป่าไม้

๑. หลักการและเหตุผล

ตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ กำหนดให้หน่วยงานของรัฐจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัย ไซเบอร์ โดยแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ที่จัดขึ้นฉบับนี้จัดทำขึ้นเพื่อให้สอดคล้องตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสน เทศ พ.ศ. ๒๕๖๔ ประกอบด้วย แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และแผนการรับมือภัยคุกคามทางไซเบอร์



รูปที่ ๑ ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อดำเนินการตาม พรบ.การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ มาตรา ๔๔ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ โดยการมุ่งเน้นการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบให้สามารถใช้งานได้

๒. วัตถุประสงค์

เพื่อให้การรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานมีการปฏิบัติได้อย่างรวดเร็ว ถูกต้อง และมีประสิทธิภาพ

๓. แนวทางปฏิบัติการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์

ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัย

ไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ ครั้ง ในกระบวนการจัดทำและผลกระทบของบริการที่สำคัญของหน่วยงานโดยมีขอบเขตของการตรวจสอบดังนี้

๓.๑ กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)

๓.๒ บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ ๓.๑

๔. แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

เพื่อให้สามารถประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ได้อย่างมีประสิทธิภาพและต่อเนื่อง จึงต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยต้องจัดให้มีการประเมินความเสี่ยงอย่างน้องปีละ ๑ ครั้ง ดังต่อไปนี้

๔.๑ การประเมินความเสี่ยง (Risk Assessment)

๔.๑.๑ การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่างๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงานระบบงาน บุคลากร หรือปัจจัยภายนอก

๔.๑.๒ การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม

๔.๑.๓ การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)

๔.๒ การจัดการความเสี่ยง (Risk Treatment)

ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกัน ความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับนอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง

๔.๓ การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้

๔.๔ การรายงานความเสี่ยง (Risk Reporting)

ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย

๕. แผนรับมือภัยคุกคามทางไซเบอร์

๕.๑ ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้

๕.๑.๑ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ

๕.๑.๒ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใดๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

๕.๑.๓ เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT

๕.๑.๔ ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

๕.๑.๕ การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)

๕.๑.๖ ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๕.๑.๗ ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่นๆ เพื่อสนับสนุนการสอบสวน

๕.๑.๘ ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๕.๑.๙ กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๕.๒ ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐ

๕.๓ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์อย่างน้อยปีละ ๑ ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ

๕.๔ ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่สำคัญของหน่วยงานของรัฐ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แผนปฏิบัติการด้านความมั่นคงปลอดภัยไซเบอร์ปรากฏตามภาคผนวก

๖. กรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ประกอบไปด้วย ๕ หัวข้อหลัก (ดังรูปที่ ๑) ดังนี้

๖.๑ การระบุความเสี่ยง (Identity) เป็นขั้นตอนแรกเพื่อระบุระบบสารสนเทศ ข้อมูล ทรัพย์สิน และกระบวนการต่างๆ ที่มีอยู่ภายใน รวมถึงการประเมินความเสี่ยงด้านไซเบอร์เพื่อค้นหาจุดอ่อนที่อาจถูกโจมตี เพื่อกำหนดเป้าหมาย ปรับแต่งมาตรการป้องกัน และวางแผนรับมือที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify) ดังนี้

๖.๑.๑ การจัดการทรัพย์สิน (Asset Management)

๖.๑.๒ การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)

๖.๑.๓ การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

๖.๑.๔ การจัดการผู้ให้บริการภายนอก (Third Party Management)

๖.๒ มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect) เป็นการวางมาตรการป้องกันเพื่อลดความเสี่ยง เช่น การติดตั้งระบบรักษาความปลอดภัยให้แข็งแกร่ง การควบคุมการเข้าถึงข้อมูลอย่างเข้มงวด การติดตั้งระบบป้องกันไวรัสและมัลแวร์ การสร้างนโยบายความปลอดภัยที่ชัดเจน และการอบรมพนักงานให้มีความรู้และทักษะในการรับมือกับภัยคุกคามทางไซเบอร์ โดยมีมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น ดังนี้

๖.๒.๑ การควบคุมการเข้าถึง (Access Control)

๖.๒.๒ การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

๖.๒.๓ การเชื่อมต่อระยะไกล (Remote Connection)

๖.๒.๔ สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

๖.๒.๕ การสร้างความตระหนักรู้ ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

๖.๒.๖ การแบ่งปันข้อมูล (Information Sharing)

๖.๓ มาตรการตรวจสอบ และเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect) การมีระบบตรวจสอบและเฝ้าระวังความผิดปกติซึ่งเปรียบเสมือการติดตั้งกล้องวงจรปิดภายในองค์กร ระบบเหล่านี้ เช่น SIEM (Security Information and Event Management) และเครื่องแสกนช่องโหว่ โดยเครื่องมือเหล่านี้จะช่วยให้สามารถระบุสัญญาณเตือนภัยของเหตุการณ์ด้านไซเบอร์ได้อย่างทันท่วงที เช่น การเข้าถึงระบบที่ผิดปกติ การแพร่กระจายของมัลแวร์ หรือพฤติกรรมที่น่าสงสัยอื่นๆ ซึ่งมีมาตรการ ดังนี้

๖.๓.๑ การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

๖.๔ มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond) เมื่อมีการตรวจพบเหตุการณ์ภัยคุกคาม ต้องมีแผนการรับมือที่ชัดเจนและรวดเร็วโดยแผนนี้จะครอบคลุมกระบวนการต่างๆ เช่น การระบุ สอบสวน ความคุมสถานการณ์ กำจัดภัยคุกคาม และลดผลกระทบ โดยมีเป้าหมายเพื่อหยุดยั้งการแพร่กระจายของภัยคุกคาม ปกป้องข้อมูลสำคัญ และฟื้นฟูระบบให้กลับมาใช้งานได้โดยเร็วที่สุด ซึ่งมีมาตรการดังนี้

๖.๔.๑ แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

๖.๔.๒ แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

๖.๔.๓ การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

๖.๕ มาตรการรักษา และฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover) หลังจากผ่านพ้นเหตุการณ์ภัยคุกคาม การฟื้นฟูระบบและข้อมูลถือเป็นสิ่งสำคัญ ซึ่งควรมีแผนสำรองข้อมูล (Backup) ที่อัปเดตอยู่เสมอ เพื่อให้สามารถกู้คืนข้อมูลที่สูญหายได้อย่างรวดเร็ว และต้องมีกระบวนการตรวจสอบและปรับปรุงระบบรักษาความปลอดภัยเพื่อป้องกันไม่ให้เหตุการณ์ลักษณะเดียวกันเกิดขึ้นอีก ดังนี้

๖.๕.๑ การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

๑. บทนำ

กรมป่าไม้ได้มีการพัฒนาระบบสารสนเทศ ระบบภูมิศาสตร์สารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ เพื่อให้ให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร แก่บุคลากรของกรมป่าไม้ ประชาชน และผู้ประกอบการ ให้สามารถเข้าถึงข้อมูลได้อย่างรวดเร็ว มีประสิทธิภาพ ถูกต้อง ทั้งนี้ยังมีการใช้บริการการเชื่อมโยงข้อมูลกับหน่วยงานอื่นๆ เช่น กรมการปกครอง กรมศุลกากร สำนักงานพัฒนาเศรษฐกิจจากฐานชีวภาพ (องค์การมหาชน) กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม เป็นต้น ซึ่งบริการดังข้างต้นที่ได้กล่าวมาเป็นเทคโนโลยีสารสนเทศหลักของกรมป่าไม้ เพื่อพัฒนาไปสู่นโยบายไทยแลนด์ ๔.๐ และแผนพัฒนารัฐบาลดิจิทัลของประเทศไทย โดยในปัจจุบันมีภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ จะอาศัยช่องโหว่ที่เกิดขึ้นในระบบ เจาะเข้ามาเพื่อขโมยข้อมูล ทำลายข้อมูล เข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ และทำให้ระบบเครือข่ายอินเทอร์เน็ตล่ม ซึ่งหากเกิดเหตุการณ์ดังกล่าวจะสร้างความเสียหายต่อระบบสารสนเทศ ระบบฐานข้อมูล ข้อมูลส่วนบุคคล และระบบเครือข่ายของกรมป่าไม้ได้

การตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เป็นกระบวนการเพื่อประเมินและตรวจสอบความมั่นคงปลอดภัยของระบบคอมพิวเตอร์ และระบบเครือข่ายของหน่วยงาน เพื่อตรวจหาความบกพร่องหรือจุดอ่อน ที่อาจเป็นช่องทางการเข้าถึงของผู้ไม่ประสงค์ดี (hackers) หรือการละเมิดความปลอดภัยอื่น ๆ ที่อาจส่งผลกระทบสร้างความเสียหายหน่วยงาน และประชาชน

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกรอบ มาตรการ และคุณสมบัติของผู้ตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ในการตรวจสอบและประมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๒.๒ เพื่อกำหนดหลักการตรวจสอบและประมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๓. กลุ่มเป้าหมาย

๓.๑ ผู้ตรวจสอบที่ได้รับการอนุมัติหรือแต่งตั้งอย่างเป็นทางการจากคณะกรรมการ

๓.๒ ผู้มีส่วนได้ส่วนเสีย เช่น หัวหน้าหน่วยธุรกิจ ผู้ขาย เจ้าของระบบ และหัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยข้อมูล เป็นต้น

๓.๓ ผู้ที่จำเป็นต้องรู้เกี่ยวกับความคาดหวังในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์สำหรับการตรวจสอบหน่วยงานของตน

๔. ขอบเขต

ครอบคลุมการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ตามมาตรา ๕๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมป่าไม้

๕. การอนุมัติผู้ตรวจสอบ

ผู้ตรวจสอบต้องได้รับการอนุมัติหรือแต่งตั้งโดยหน่วยงาน เพื่อดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ในหน่วยงาน โดยหน่วยงานและผู้ตรวจสอบจะต้องส่งแบบฟอร์มที่เกี่ยวข้องตามที่สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (สกมช.) กำหนด โดยใบสมัครจะสมบูรณ์ก็ต่อเมื่อแบบฟอร์มที่เกี่ยวข้องทั้งหมดและเอกสารประกอบที่ส่งมาของหน่วยงาน และผู้ตรวจสอบนั้นครบถ้วนและเป็นไปตามลำดับ

๕.๑ เกณฑ์การพิจารณาแบ่งออกเป็น ๒ ประการ ได้แก่

๕.๑.๑ ความเป็นอิสระและความสามารถที่สำนักงานตรวจสอบหรือทีมงาน (audit firm/team)

๕.๑.๒ ผู้ตรวจสอบ (auditors) ที่เสนอจำเป็นต้องปฏิบัติตาม

๕.๒ สำนักงานตรวจสอบหรือทีมงาน และผู้ตรวจสอบที่ได้รับการแต่งตั้ง มีคุณสมบัติดังนี้

๕.๒.๑ ไม่ควรอยู่ในตำแหน่งที่มีผลประโยชน์ทับซ้อน (Conflict of interest) ใด ๆ ไม่ว่าจะเกิดขึ้นจริง มีแนวโน้ม หรือได้รับรู้ ผลประโยชน์ทับซ้อน หมายถึง สถานการณ์ใด ๆ ที่ผลประโยชน์ของผู้ตรวจสอบอาจแทรกแซงการปฏิบัติหน้าที่ของผู้ตรวจสอบอย่างเป็นอิสระและมีวัตถุประสงค์

๕.๒.๒ ควรมีความสามารถทางเทคนิคที่จำเป็น เช่น คุณวุฒิวิชาชีพ/ใบรับรอง ทักษะ ความรู้และประสบการณ์ที่เกี่ยวข้อง เป็นต้น เพื่อดำเนินการตรวจสอบ

ทั้งนี้ หน่วยงานอาจพิจารณาแตกต่างไปตามที่หน่วยงานเห็นสมควร ในประเด็นต่อไปนี้

๑) จำนวนผู้ตรวจสอบของแต่ละหน่วยงาน

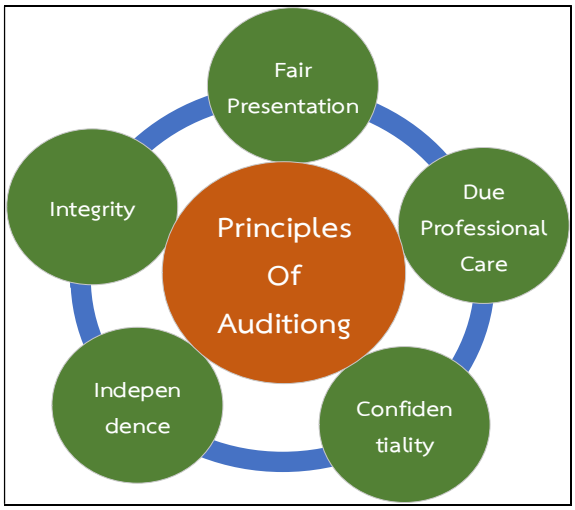
๒) ระยะเวลาในการขออนุญาต เช่น รายปีหรือตามรอบการตรวจสอบ เป็นต้น ในกรณีผู้ตรวจสอบของหน่วยงานที่ลงทะเบียนแล้วลาออกจากการเป็นพนักงานก่อนการดำเนินการตรวจสอบ หรือมีการเปลี่ยนแปลงพนักงานที่ลงทะเบียนไว้ ให้หน่วยงานแจ้ง สกมช. ภายใน ๓๐ วันนับจากวันที่การเปลี่ยนแปลงอย่างเป็นทางการของหน่วยงาน

๖. ความคาดหวังในการตรวจสอบ

ผู้ตรวจสอบต้องตรวจสอบอย่างสร้างสรรค์รัดกุมมีประสิทธิภาพ เพียงพอที่จะป้องกันความเสียหายและทันต่อเหตุการณ์ เน้นการตรวจสอบที่มีคุณภาพ คุ้มค่า เป็นไปตามมาตรฐาน โปร่งใส ถูกต้อง มีความน่าเชื่อถือ จะทำให้เกิดกระบวนการกำกับที่ดี (Good Governance) และความโปร่งใสในการปฏิบัติงาน (Transparency) โดยระบุความคาดหวังไว้ ๗ ด้าน ในหัวข้อ ๖.๑ ถึง ข้อ ๖.๗

๖.๑ หลักการตรวจสอบ

หลักการตรวจสอบควรยึดหลักการ ๕ ข้อดังต่อไปนี้ เพื่อให้ข้อสรุปการตรวจสอบที่เกี่ยวข้องและเพียงพอ ทั้งนี้ เพื่อช่วยให้ผู้ตรวจสอบ ซึ่งทำงานอย่างอิสระสามารถบรรลุข้อสรุปที่คล้ายคลึงกันในสถานการณ์ที่คล้ายคลึงกัน ดังภาพที่ ๑



ภาพที่ ๑ หลักการตรวจสอบ

๖.๑.๑ ความซื่อสัตย์ (Integrity) รากฐานของความเป็นมืออาชีพ

๑) ดำเนินการตรวจสอบด้วยความซื่อสัตย์และรับผิดชอบ

๒) มีความรู้ ทักษะ และมีความสามารถในการดำเนินการตรวจสอบ

๓) ดำเนินการตรวจสอบอย่างเป็นกลาง

๔) มีความยุติธรรม และเป็นกลางในการติดต่อสื่อสาร ระมัดระวังต่ออิทธิพลใด ๆ ที่อาจส่งผลต่อดุลยพินิจของผู้ตรวจสอบระหว่างการตรวจสอบ

๖.๑.๒ การนำเสนออย่างยุติธรรม (Fair Presentation) หน้าที่ในการรายงานตามความเป็นจริงและถูกต้อง

๑) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบ ข้อสรุปการตรวจสอบ และรายงานการตรวจสอบสะท้อนกิจกรรมการตรวจสอบตามความเป็นจริงและถูกต้อง

๒) รายงานอุปสรรคสำคัญที่พบในระหว่างการตรวจสอบและความเห็นที่แตกต่างระหว่างทีมตรวจสอบและผู้ตรวจประเมินที่ยังไม่ได้ข้อยุติ

๓) ตรวจสอบให้แน่ใจว่าการสื่อสารนั้นเป็นความจริง ถูกต้อง ตรงวัตถุประสงค์ ตรงเวลา ชัดเจนและครบถ้วน

๖.๑.๓ การปฏิบัติอย่างมืออาชีพ (Due Professional Care) การใช้ความรอบคอบและวิจารณญาณในการตรวจสอบ

๑) ใช้ความระมัดระวังอย่างเหมาะสมตามความสำคัญของงานและความเชื่อมั่นที่ผู้ตรวจสอบและผู้มีส่วนได้เสียอื่น ๆ มอบให้แก่ผู้ตรวจสอบ

๒) ใช้ดุลยพินิจอย่างมีเหตุผลในทุกสถานการณ์การตรวจสอบ

๖.๑.๔ การรักษาความลับ (Confidentiality) ความมั่นคงปลอดภัยของข้อมูล

๑) ใช้ดุลยพินิจในการใช้และปกป้องข้อมูลที่ได้รับระหว่างการตรวจสอบ

๒) ห้ามใช้ข้อมูลการตรวจสอบเพื่อประโยชน์ส่วนตัวหรือในทางที่เสียหายต่อผลประโยชน์ที่ชอบด้วยกฎหมายของผู้ตรวจสอบ

๓) จัดการกับข้อมูลที่ละเอียดอ่อนหรือเป็นความลับอย่างเหมาะสม

๖.๑.๕ ความเป็นอิสระ (Independence) พื้นฐานสำหรับความเป็นกลางของการตรวจสอบและความเที่ยงธรรมของข้อสรุปการตรวจสอบ

๑) ตรวจสอบความเป็นอิสระของกิจกรรมที่กำลังตรวจสอบ

๒) ดำเนินการในลักษณะที่ปราศจากอคติและผลประโยชน์ทับซ้อนในทุกกรณี

๓) รักษาความเป็นกลางตลอดกระบวนการตรวจสอบ

๔) ตรวจสอบให้แน่ใจว่าผลการตรวจสอบและข้อสรุปขึ้นอยู่กับหลักฐานการตรวจสอบ (audit evidence) เท่านั้น

๖.๒ วัตถุประสงค์ในการตรวจสอบ

๖.๒.๑ ตรวจสอบการปฏิบัติตามของหน่วยงานกับข้อกำหนดที่ระบุไว้ในประมวลแนวทางปฏิบัติและกรอบมาตรฐาน รวมถึงกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่ใช้บังคับที่เกี่ยวข้อง

๖.๒.๒ ประเมินความเพียงพอและประสิทธิผลของการควบคุมหรือมาตรการที่ใช้ในการปกป้องของหน่วยงาน ตามหลักการบริหารความเสี่ยง

๖.๓ ขอบเขตการตรวจสอบ

การตรวจสอบครอบคลุม ดังนี้

ขอบเขต	คำอธิบาย
หัวข้อการตรวจสอบ (Audit Subject)	หัวข้อการตรวจสอบควรครอบคลุมหน่วยงานทั้งหมดที่กำหนดภายใต้กฎหมาย
ระยะเวลาการตรวจสอบ (Audit Period)	ระยะเวลาการตรวจสอบขั้นต่ำควรมีการตรวจสอบอย่างน้อยปีละ ๑ ครั้ง
เกณฑ์การตรวจสอบ (Audit Criteria)	เกณฑ์การตรวจสอบควรรวมถึงการปฏิบัติตามกฎหมาย กฎหมายย่อย คำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔ แนวทางการตรวจสอบ

การตรวจสอบควรใช้ทั้งแนวทางการปฏิบัติตามข้อกำหนด (compliance approach) และตามความเสี่ยง (risk-based approach)

๖.๔.๑ การปฏิบัติตามข้อกำหนด

ดำเนินการทดสอบการปฏิบัติตามข้อกำหนดเพื่อยืนยันความเพียงพอและประสิทธิผลของการควบคุมที่ใช้ในหน่วยงาน เพื่อให้สอดคล้องกับพระราชบัญญัติ กฎหมายลำดับรอง หรือคำสั่งที่เป็นลายลักษณ์อักษรที่เกี่ยวข้อง

๖.๔.๒ การปฏิบัติตามความเสี่ยง

ระบุความเสี่ยงและภัยคุกคามที่หน่วยงานเผชิญ และตรวจสอบว่าการควบคุมที่วางไว้นั้นเหมาะสมเพื่อลดความเสี่ยงและภัยคุกคามที่ทราบหรือไม่

๖.๕ ข้อค้นพบการตรวจสอบ

ผู้ตรวจสอบควรเน้นสิ่งต่อไปนี้

๖.๕.๑ ข้อค้นพบการตรวจสอบใด ๆ ที่ระบุในระหว่างการตรวจสอบ

๖.๕.๒ เน้นการค้นหาอย่างเป็นระบบ (systemic finding) ซึ่งการค้นพบจะกระจายไปทั่วทั้งหน่วยงานซึ่งอาจเป็นจุดอ่อนในการออกแบบการควบคุม

๖.๕.๓ เน้นการค้นพบที่เกิดซ้ำ เช่น การค้นพบที่เกิดขึ้นจากการตรวจสอบในอดีตที่เกิดขึ้นซ้ำ ในการตรวจสอบในปัจจุบัน แม้ว่าจะดำเนินการแก้ไข (corrective action) แล้วก็ตาม

๖.๕.๔ เน้นแนวปฏิบัติที่ดี (good practices) ในด้านการกำกับดูแลและการควบคุม ซึ่งระบุไว้ในระหว่างการตรวจสอบ

๖.๕.๕ เมื่อเสนอข้อค้นพบการตรวจสอบ ผู้ตรวจสอบควรระบุคุณลักษณะของข้อค้นพบการตรวจสอบอย่างชัดเจน ต่อไปนี้

องค์ประกอบ	คำอธิบาย
สภาพหรือเงื่อนไข (Condition)	ถ้อยแถลงที่อธิบายผลลัพธ์ของการค้นพบการตรวจสอบ
เกณฑ์ (Criteria)	มาตรฐาน/ กฎ/ เกณฑ์มาตรฐาน (เช่น กฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ นโยบาย และแนวทางปฏิบัติที่ดีที่สุด) ที่ใช้เทียบกับสภาพหรือเงื่อนไขที่ตรวจสอบ
สาเหตุ (Cause)	สาเหตุที่แท้จริง (root cause) และเหตุผลที่สนับสนุนสำหรับสภาพหรือเงื่อนไขที่ตรวจสอบ
ผลกระทบ (Effect)	ผลกระทบและนัยสำคัญของสภาพหรือเงื่อนไขที่ตรวจสอบ (ทันทีในอนาคตหรือที่อาจเกิดขึ้น) ผู้ตรวจสอบควรเชื่อมโยงการค้นพบการตรวจสอบกับผลกระทบต่อบริการที่จำเป็นของหน่วยงาน ซึ่งฝ่ายบริหารคุ้นเคย เช่น ผลกระทบเชิงปริมาณ (เช่น ต้นทุน เวลา และการผลิต) และผลกระทบเชิงคุณภาพ (เช่น การบริการและการตัดสินใจที่ไม่เหมาะสม) สิ่งนี้ช่วยโน้มน้าวฝ่ายบริหารถึงความจำเป็นในการดำเนินการแก้ไข
คำแนะนำ (Recommendation)	แนะนำให้ดำเนินการแก้ไขสาเหตุเพื่อป้องกันการเกิดการตรวจสอบซ้ำซ้อน

๖.๖ สรุปผลการตรวจสอบ

ผู้ตรวจสอบควรให้ความเห็นและข้อสรุปในเรื่องต่อไปนี้

๖.๖.๑ ความเหมาะสมของความเห็นของฝ่ายบริหารในการตอบสนองต่อผลการตรวจสอบ

๖.๖.๒ ความเพียงพอและประสิทธิผลของการควบคุมที่จัดทำโดยหน่วยงานเพื่อจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน และโอกาสในการปรับปรุงเพื่อรักษาความมั่นคงปลอดภัยของหน่วยงาน

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร (Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารฉบับนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารฉบับนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ ๑) มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ๒) ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ๓) วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในข้อ ๖.๕ ของเอกสารฉบับนี้

เนื้อหา	คำอธิบาย
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในข้อ ๖.๖ ของเอกสารฉบับนี้

๖.๗ รูปแบบรายงานการตรวจสอบ

รายงานการตรวจสอบควรมีอย่างน้อย ดังต่อไปนี้

เนื้อหา	คำอธิบาย
บทสรุปผู้บริหาร(Executive Summary)	รายงานควรจัดให้มีการประเมินโดยรวมของข้อค้นพบที่บันทึกไว้ พร้อมด้วยคำอธิบายของปัญหา ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์และผลกระทบที่อาจเกิดขึ้นกับหน่วยงาน คำแนะนำ ความเห็นของฝ่ายบริหาร และการประเมินความเหมาะสมของความเห็นของฝ่ายบริหารของผู้ตรวจสอบ บทสรุปสำหรับผู้บริหารควรรวมถึงข้อสรุปของผู้ตรวจสอบเกี่ยวกับความเพียงพอโดยรวมและประสิทธิผลของการควบคุมในการจัดการกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ต่อหน่วยงาน
วัตถุประสงค์ (Purpose)	รายงานควรอธิบายถึงวัตถุประสงค์ของการดำเนินการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ (เช่น เพื่อปฏิบัติตามข้อผูกพันภายใต้พระราชบัญญัติความมั่นคงปลอดภัยไซเบอร์ เพื่อปฏิบัติตามคำแนะนำเฉพาะกิจที่ได้รับจาก กกม. ฯลฯ)
วัตถุประสงค์การตรวจสอบ (Audit Objective)	วัตถุประสงค์ในการตรวจสอบกำหนดไว้ในหัวข้อ ๖.๒ ของเอกสารฉบับนี้
ขอบเขตการตรวจสอบ (Audit Scope)	ขอบเขตการตรวจสอบกำหนดไว้ในส่วน ๖.๓ ของเอกสารฉบับนี้
ผู้มีส่วนได้ส่วนเสีย (Stakeholders)	ผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการตรวจสอบความมั่นคงปลอดภัยไซเบอร์และบทบาทและความรับผิดชอบควรระบุไว้อย่างชัดเจนในรายงาน
วิธีการและแนวทางการตรวจสอบ (Audit Methodology and Approach)	รายงานควรให้คำอธิบายว่าการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ดำเนินการอย่างไรเพื่อให้บรรลุวัตถุประสงค์ในการตรวจสอบ โดยเฉพาะอย่างยิ่ง คำอธิบายควรระบุ ๑) มีการพึ่งพางานของผู้ตรวจสอบรายอื่น (เช่น การตรวจสอบในอดีต) หรือผู้ประกอบวิชาชีพด้านการรับประกันความมั่นคงปลอดภัยไซเบอร์หรือไม่ และขอบเขตของการพึ่งพาดังกล่าว ๒) ประเภทของการวิเคราะห์และเทคนิคที่ใช้ในการตรวจสอบ (เช่น การสัมภาษณ์ คำแนะนำ การตรวจสอบเอกสาร) และ ๓) วิธีการสุ่มตัวอย่างที่นำมาใช้ (หากเลือกตัวอย่างเพื่อประเมินประสิทธิผลของการควบคุม)

เนื้อหา	คำอธิบาย
การค้นพบการตรวจสอบ (Audit Finding)	การค้นพบการตรวจสอบกำหนดไว้ในข้อ ๖.๕ ของเอกสารฉบับนี้
สรุปการตรวจสอบ (Audit Conclusion)	ข้อสรุปการตรวจสอบกำหนดไว้ในข้อ ๖.๖ ของเอกสารฉบับนี้

๗. ขั้นตอนการปฏิบัติในการตรวจสอบ

๗.๑ ผู้ตรวจสอบ ทำการวางแผน และจัดทำแผนการตรวจสอบ พร้อมทั้งจัดเตรียมทรัพยากรที่เกี่ยวข้อง

๗.๒ ผู้ตรวจสอบและคณะทำงานของหน่วยงาน ร่วมการประชุมเปิดการตรวจสอบ โดยมีวัตถุประสงค์ของการประชุมเปิดการตรวจสอบ ดังนี้

๗.๒.๑ เพื่อชี้แจงวัตถุประสงค์ ขอบเขต และแผนการตรวจสอบ

๗.๒.๒ การสรุปวิธีการตรวจสอบ เกณฑ์การพิจารณา และกิจกรรมที่จะทำการตรวจสอบ

๗.๒.๓ การกำหนดผู้รับผิดชอบหรือช่องทางการสื่อสาร

๗.๒.๔ การชี้แจงรูปแบบการรายงานและการปิดตรวจสอบ

๗.๒.๕ ยืนยันแผนการตรวจสอบ

๗.๓ ผู้ตรวจสอบดำเนินการตรวจสอบ โดยคณะทำงานทำหน้าที่ตอบข้อซักถาม และจัดเตรียมหลักฐานประกอบตามขอบเขตและข้อกำหนดประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

๗.๔ ผู้ตรวจสอบและคณะทำงาน ร่วมการประชุมปิดการตรวจสอบ และสรุปผลการตรวจสอบเบื้องต้น โดยมีวัตถุประสงค์ของการประชุมปิดการตรวจสอบ ดังนี้

๗.๔.๑ ยืนยันข้อค้นพบการตรวจสอบจากการตรวจสอบ

๗.๔.๒ ระดับความไม่สอดคล้องของข้อตรวจพบ

๗.๔.๓ ข้อเสนอแนะในการปรับปรุง

๗.๔.๔ สรุปผลการตรวจสอบ

๗.๔.๕ กำหนดการตรวจติดตาม (ถ้ามี)

๗.๕ ผู้ตรวจสอบจัดทำรายงานผลการตรวจสอบ และชี้แจงผลการตรวจสอบให้คณะทำงานรับทราบ

๗.๖ คณะทำงานรับทราบผลการตรวจสอบ

๗.๗ ผู้ตรวจสอบดำเนินการบันทึกความไม่สอดคล้อง จากข้อตรวจพบลงแบบฟอร์มรายงานความไม่สอดคล้อง (Non-conformity Report (NCR) Form) ของหน่วยงาน และจัดส่งรายงานการตรวจสอบให้กับหน่วยงานเฉพาะผู้ที่เกี่ยวข้องตามที่หน่วยงานกำหนด เพื่อรักษารักษาความลับ ในการตรวจสอบ

๗.๘ คณะทำงานนำเสนอผลการตรวจสอบให้ผู้บริหารระดับสูงของหน่วยงาน หรือคณะกรรมการตรวจสอบของหน่วยงาน หรือคณะกรรมการอื่น ๆ ที่ได้รับมอบหมายจากหน่วยงาน

๗.๙ คณะทำงาน ดำเนินการแก้ไขความไม่สอดคล้องจากข้อตรวจพบ โดยดำเนินการตามกระบวนการปฏิบัติการแก้ไขความไม่สอดคล้อง (Corrective Action Procedure) ของหน่วยงาน

๗.๑๐ ผู้ตรวจสอบดำเนินการติดตามการดำเนินการแก้ไขความไม่สอดคล้องของคณะทำงาน

แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

๑. บทนำ

๑.๑ ความสำคัญของการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ปัจจุบันเทคโนโลยีและระบบสารสนเทศ เป็นเครื่องมือสำคัญต่อการขับเคลื่อนองค์กร ให้มีความก้าวหน้าอย่างรวดเร็ว รวมทั้งการเปลี่ยนองค์กรเข้าสู่สังคมดิจิทัล (Transformation) และทำให้องค์กรต้องเผชิญกับความเสี่ยงจากภัยคุกคามทางไซเบอร์ (Cyber Threats) ที่มากขึ้น การรักษาความมั่นคงปลอดภัยต่อภัยคุกคามทางไซเบอร์ จึงมีบทบาทที่สำคัญต่อองค์กรเป็นอย่างมาก การมีความมั่นคงปลอดภัยจากภัยคุกคามทางไซเบอร์ที่มีความรัดกุมต่อระดับความเสี่ยง เพื่อเตรียมความพร้อมในการรับมือกับภัยคุกคาม ทางไซเบอร์รวมถึงการบริหารความเสี่ยงทั้งด้านบุคลากร กระบวนการ และเครื่องมือเทคโนโลยีสารสนเทศ เพื่อสร้างความเชื่อมั่นต่อผู้บริหาร บุคลากรของกรมป่าไม้ และประชาชน

การประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Assessment) เป็นขั้นตอนที่สำคัญของการบริหารความเสี่ยง คือ การประเมินความเสี่ยงที่มีประสิทธิภาพ โดยผลที่ได้จากการประเมินความเสี่ยงเป็นข้อมูลพื้นฐานที่จะจัดลำดับความสำคัญเกี่ยวกับการรักษาความปลอดภัยไซเบอร์ โดยสิ่งที่มีความเสี่ยงสูงควรได้รับการจัดการหรือรักษาความเสี่ยงนั้นก่อน เนื่องจากองค์กรไม่สามารถจัดการได้กับทุกความเสี่ยงที่มีได้ เพราะข้อจำกัดด้านงบประมาณและทรัพยากรที่มี

ดังนั้น จึงมีความจำเป็นสำหรับหน่วยงานในการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เหล่านี้อย่างมีประสิทธิภาพ ซึ่งเป็นส่วนสำคัญของกระบวนการจัดการความเสี่ยงระดับหน่วยงานของหน่วยงาน โดยการประเมินความเสี่ยง หน่วยงานจะสามารถ

- ระบุเหตุการณ์ สิ่งที่อาจผิดพลาด (What Could Go Wrong) ซึ่งมักเป็นผลมาจากการกระทำที่มุ่งร้ายโดยผู้คุกคาม และอาจนำไปสู่ผลลัพธ์ทางธุรกิจที่ไม่พึงประสงค์
- กำหนดระดับของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ต้องเผชิญ ความเข้าใจที่ดีเกี่ยวกับระดับความเสี่ยงจะช่วยให้หน่วยงานสามารถทุ่มเทการดำเนินการและทรัพยากรที่เพียงพอ เพื่อจัดการกับความเสี่ยงที่มีลำดับความสำคัญสูงสุด
- สร้างวัฒนธรรมที่ตระหนักถึงความเสี่ยงภายในหน่วยงาน การประเมินความเสี่ยงเป็นกระบวนการซ้ำ ๆ ที่เกี่ยวข้องกับการให้พนักงานมีส่วนร่วมคิดเกี่ยวกับความเสี่ยงด้านเทคโนโลยีและวิธีที่พนักงานดังกล่าวปรับให้สอดคล้องกับวัตถุประสงค์ทางธุรกิจ

๑.๒ ปัญหาโดยทั่วไป

ในขณะที่หน่วยงานต่าง ๆ ตระหนักดีว่าการประเมินความเสี่ยงเป็นส่วนสำคัญของแนวทางปฏิบัติในการประเมินความเสี่ยงของหน่วยงาน (Enterprise Risk assessment Practice) แต่หน่วยงานหลายแห่งยังประสบปัญหากับกระบวนการในการประเมินความเสี่ยงที่เหมาะสม ช่องว่างทั่วไปบางส่วนที่สังเกต ได้แก่

๑.๒.๑ การระบุสถานการณ์ความเสี่ยงที่ไม่ดี (Poor Articulation of Risk Scenarios) สถานการณ์ความเสี่ยงที่อธิบายถึงเหตุการณ์ “สิ่งที่อาจผิดพลาดได้ (What Could Go Wrong)” มักจะคลุมเครือและเป็นเรื่องทั่วไป โดยไม่ได้ระบุเหตุการณ์ภัยคุกคาม ช่องโหว่ ทรัพย์สิน และผลที่ตามมาที่เฉพาะเจาะจง เป็นผลให้การเข้าใจ

ขอบเขตของความเสี่ยง การเชื่อมโยงกับบริบทของหน่วยงาน หรือการระบุมาตรการเป้าหมายเพื่อจัดการกับความเสี่ยง กระทำได้ยาก

๑.๒.๒ การระบุความเสี่ยงโดยใช้วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบ (Identification of Risks Using a Compliance-oriented Approach) หลายหน่วยงานระบุความเสี่ยงจากจุดที่ประเมินการควบคุมความมั่นคงปลอดภัย (หรือขาดไป) คล้ายกับการดำเนินการตรวจสอบการปฏิบัติตามหรือการวิเคราะห์ช่องว่างเทียบกับชุดของมาตรฐานที่กำหนดไว้ วิธีการที่มุ่งเน้นการปฏิบัติตามกฎระเบียบเพื่อประเมินความเสี่ยงทำให้เกิดพฤติกรรม “รายการตรวจสอบ (Checklist)” ทำให้เกิดความเข้าใจผิดเกี่ยวกับความมั่นคงปลอดภัยว่าหน่วยงานจะไม่มีความเสี่ยงใด ๆ ตราบใดที่ปฏิบัติตามข้อกำหนดทั้งหมด

๑.๒.๓ การขาดการยอมรับความเสี่ยง (Absence of Risk Tolerance) หน่วยงานมักจะไม่บูรณาการแผนการจัดการความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์เข้ากับโปรแกรมการจัดการความเสี่ยงของหน่วยงาน ด้วยเหตุนี้ การยอมรับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ในระดับหน่วยงานจึงมักถูกละเลย และผู้บริหารต้องเผชิญกับความยากลำบากในการตัดสินใจเลือกระดับความเสี่ยงที่เหมาะสมที่จะนำมาใช้ในขณะที่ดำเนินการตามวัตถุประสงค์ทางธุรกิจของหน่วยงาน

๑.๒.๔ การกำหนดโอกาสเสี่ยงตามเหตุการณ์ที่เกิดขึ้นในอดีตหรือที่คาดไว้ (Determining Risk Likelihood Based on Historical or Expected Occurrences) หน่วยงานต่าง ๆ มักจะใช้การวัดเวลาหรือความถี่ (เช่น เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดไว้) เพื่อประเมินโอกาสเสี่ยงของตน แนวทางนี้ อาจไม่ถูกต้องเมื่อพิจารณาจากจำนวนครั้งที่เหตุการณ์เกิดขึ้นก่อนหน้านี้ โดยเฉพาะอย่างยิ่งเมื่อไม่มีข้อมูลเกี่ยวกับเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์ที่ผ่านมา ในบริบทของความมั่นคงปลอดภัยไซเบอร์ ความน่าจะเป็นของเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์นั้นไม่ขึ้นกับความถี่ของการเกิดขึ้นในอดีต

๑.๒.๕ จัดการกับความเสี่ยงด้วยการควบคุมหรือมาตรการที่ไม่เกี่ยวข้อง (Treating Risks With Irrelevant controls/measures) หน่วยงานอาจใช้แนวทางกว้าง ๆ ในการหามาตรการเพื่อลดความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่ระบุ ซึ่งส่งผลให้การดำเนินการควบคุมนั้นไม่ได้ระบุถึงสาเหตุที่แท้จริงอย่างสมบูรณ์ ซึ่งมักเกิดจากความเข้าใจหรือการอธิบายสถานการณ์ความเสี่ยงที่ไม่ดีพอ

๒. วัตถุประสงค์ กลุ่มเป้าหมาย และขอบเขต

๒.๑ วัตถุประสงค์

เพื่อให้คำแนะนำแก่หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ (หน่วยงาน) เกี่ยวกับวิธีดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม

๒.๒ กลุ่มเป้าหมายและขอบเขต

เพื่อใช้โดยผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอก ต่อไปนี้

๒.๒.๑ ผู้มีส่วนได้ส่วนเสีย (Stakeholders) เช่น หัวหน้าหน่วยธุรกิจ เจ้าของระบบ หัวหน้าเจ้าหน้าที่รักษาความมั่นคงปลอดภัยสารสนเทศ ฯลฯ ภายในหน่วยงาน

๒.๒.๒ ที่ปรึกษาภายนอกหรือผู้ให้บริการดำเนินการประเมินความเสี่ยงในนามของหน่วยงาน

๒.๒.๓ ขอบเขตของแนวทางฉบับนี้มุ่งเน้นไปที่กรอบความเสี่ยง การประเมิน และการจัดการเท่านั้น สำหรับหัวข้ออื่น ๆ เช่น การติดตามและการรายงานความเสี่ยง ซึ่งอยู่ภายใต้ขอบเขตที่กว้างขึ้นของการจัดการความเสี่ยง อยู่นอกเหนือขอบเขตของแนวทางฉบับนี้

๓. สร้างบริบทความเสี่ยง

การกำหนดบริบทของความเสี่ยงเป็นข้อกำหนดเบื้องต้นที่สำคัญสำหรับการประเมินความเสี่ยง ขั้นตอนนี้ทำให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียทั้งภายในและภายนอกที่เกี่ยวข้องในการดำเนินการประเมิน ความเสี่ยงมีความเข้าใจร่วมกันเกี่ยวกับวิธีกำหนดกรอบความเสี่ยง การยอมรับความเสี่ยงที่ต้องพิจารณา และความรับผิดชอบของเจ้าของความเสี่ยง

๓.๑ กำหนดความเสี่ยง

เป็นการระบุรายการความเสี่ยง ที่อาจเกิดขึ้นได้ทุกกรณีและสามารถเป็นต้นเหตุของการเกิดความเสียหาย ความล้มเหลว รวมถึงการลดโอกาสที่จะบรรลุความสำเร็จตามเป้าหมายของการปฏิบัติงานหรือกิจกรรม โดยความเสี่ยงถูกกำหนดให้เป็นผลลัพธ์ของ ๒ ปัจจัย คือ

- ความน่าจะเป็น (Likelihood) ของเหตุการณ์ภัยคุกคามที่เกิดขึ้นกับช่องโหว่ของทรัพย์สิน
- ผลกระทบที่เกิดขึ้น (Resulting Impact) จากการเกิดเหตุการณ์ภัยคุกคาม

Risk = Function (Likelihood, Impact)

ปัจจัยเสี่ยงแต่ละประการที่กล่าวถึงในคำจำกัดความได้อธิบายไว้ด้านล่าง

๓.๑.๑ เหตุการณ์ภัยคุกคาม (Threat Event)

เหตุการณ์ภัยคุกคาม หมายถึง สิ่งที่เกิดจากการที่ผู้โจมตีทำอันตรายต่อองค์กร เช่น แฮคเกอร์อาจทำอันตรายโดยการแก้ไขหน้าเว็บไซต์ขององค์กร เช่น การใช้บัญชีผู้ใช้ในทางที่ผิดหรือเกินกว่าที่ได้รับอนุญาต การแก้ไขข้อมูลที่สำคัญทั้งที่ตั้งใจและที่ไม่ได้ตั้งใจ การเจาะเข้าระบบโดยไม่ได้รับอนุญาต การทำลายระบบโดยไม่ได้ตั้งใจ การรบกวนระบบสื่อสารข้อมูลทั้งภายในและภายนอก และการบุกรุกเข้าห้องควบคุมโดยไม่ได้รับอนุญาต เป็นต้น

๓.๑.๒ ช่องโหว่ (Vulnerability)

ช่องโหว่ขององค์กรแบ่งออกเป็นประเภทต่างๆ ดังนี้

๑) ช่องโหว่ทางนโยบาย เป็นช่องโหว่ที่เกิดจากการบริหารจัดการ ซึ่งส่วนใหญ่เกิดจากการขาดกฎ ระเบียบ หรือกฎหมายที่บังคับ หรือห้ามการกระทำอย่างใดอย่างหนึ่ง

๒) ช่องโหว่จากการปฏิบัติงาน เป็นช่องโหว่ที่ที่อาจเกิดขึ้นจากการดำเนินการ จัดการความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบ สารสนเทศหรือใช้ข้อมูลต่าง ๆ ของสำนักงานเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิด ความเสียหายต่อข้อมูลสารสนเทศได้

๓) ช่องโหว่ทางเทคนิค เป็นช่องโหว่ที่เกิดจากข้อผิดพลาดของการเขียนโปรแกรม หรือการกำหนดค่าคอนฟิกที่ไม่สมบูรณ์หรือปลอดภัย

๔) ช่องโหว่ทางกายภาพ เป็นช่องโหว่ที่เกิดจากการป้องกันและรักษาความปลอดภัยทางกายภาพ เช่น การควบคุมการเข้าออกสถานที่ การล็อกประตูหน้าต่าง เครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ ที่มีอายุการใช้งานมานาน และยังไม่มีการจัดซื้อเครื่องใหม่มาทดแทน อาจทำให้เกิดความเสียหายต่อการทำงานได้ เช่น Hard Disk เสีย จะทำให้ข้อมูลสูญหายได้ เป็นต้น

๕) ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๑.๓ ความน่าจะเป็น (Likelihood)

ความน่าจะเป็น หมายถึง ความน่าจะเป็นที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ สามารถใช้ประโยชน์จากช่องโหว่ที่กำหนด (หรือชุดของช่องโหว่) ความน่าจะเป็นสามารถได้รับจากปัจจัยต่าง ๆ ได้แก่ ความสามารถในการค้นพบ (Discoverability) ความสามารถในการหาประโยชน์ (Exploitability) และความสามารถในการทำซ้ำ (Reproducibility)

๓.๑.๔ ผลกระทบ (Impact)

ผลกระทบหมายถึงขนาดหรือระดับของอันตรายที่เกิดจากเหตุการณ์ภัยคุกคามที่ใช้ประโยชน์จากช่องโหว่ (หรือชุดของช่องโหว่) ขนาดของความเสียหายสามารถประเมินได้จากมุมมองของประเทศ หน่วยงาน หรือบุคคล

๓.๒ กำหนดความเสี่ยงที่ยอมรับได้ (Determine Risk Tolerance)

ความเสี่ยงที่ยอมรับได้ (Risk Tolerance) หมายถึง ระดับของการรับความเสี่ยงที่ยอมรับได้เพื่อให้บรรลุวัตถุประสงค์ทางธุรกิจที่เฉพาะเจาะจง การกำหนดความเสี่ยงที่ยอมรับได้ช่วยให้ฝ่ายบริหารสามารถระบุได้ว่าหน่วยงานยินดียอมรับความเสี่ยงมากน้อยเพียงใด

การยอมรับความเสี่ยงที่ชัดเจนควรระบุ

- ความคาดหวังในการรักษาและติดตามความเสี่ยงเฉพาะประเภท
- ขอบเขตและเกณฑ์ของการรับความเสี่ยงที่ยอมรับได้

ตารางการยอมรับความเสี่ยง

ระดับความเสี่ยง (Risk Level)	คำอธิบายการยอมรับความเสี่ยง (Risk Tolerance Description)
น้อยมาก	เกิดเหตุไม่มีความสำคัญ
น้อย	เกิดเหตุเล็กน้อยที่แก้ไขได้
ปานกลาง	ระบบมีปัญหาและมีความสูญเสียไม่มาก
สูง	เกิดปัญหากับระบบ IT ที่สำคัญ และระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน
สูงมาก	เกิดความสูญเสียต่อระบบ IT ที่สำคัญทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลกรมป่าไม้

๓.๓ กำหนดบทบาทและความรับผิดชอบ (Define Roles and Responsibilities)

เพื่อให้แน่ใจว่าผู้มีส่วนได้ส่วนเสียตระหนักถึงบทบาทที่คาดหวังในแบบฝึกหัดการประเมินความเสี่ยง สิ่งสำคัญคือต้องระบุให้ชัดเจนล่วงหน้า บทบาทหลักในแบบฝึกหัดการประเมินความเสี่ยง ได้แก่

๓.๓.๑ หัวหน้าหน่วยงาน (Head of Organization)

ผู้บริหารระดับสูงสุดของกรมป่าไม้ (Chief Executive Office : CEO) มีภาระหน้าที่และความรับผิดชอบ (Responsibility and Accountability) โดยรวมในการทำให้มั่นใจว่าความเสี่ยงได้รับการจัดการอย่างเหมาะสมภายในระดับที่ยอมรับได้ของหน่วยงาน และยอมรับความเสี่ยงที่เหลืออยู่ทั้งหมด

๓.๓.๒ เจ้าของกระบวนการธุรกิจ (Business Owner)

สำนัก/กอง/ศูนย์/กลุ่ม ที่เป็นเจ้าของข้อมูลในระบบสารสนเทศ กรมป่าไม้ ที่รับผิดชอบในการตรวจสอบ

๓.๓.๓ ฟังก์ชั่นการบริหารความเสี่ยง (Risk Management Function)

สำนัก/กอง/ศูนย์/กลุ่ม / สำนักจัดการทรัพยากรป่าไม้ที่ ๑ – ๑๓ และสำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา

๓.๓.๔ ฟังก์ชั่นเทคโนโลยีและการดำเนินงาน (Technology and Operations Function)

ส่วนระบบคอมพิวเตอร์และเครือข่าย และส่วนระบบสารสนเทศและภูมิสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๓.๓.๕ ฟังก์ชั่นความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Function)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๔. ดำเนินการประเมินความเสี่ยง (CONDUCT RISK ASSESSMENT)

มีขั้นตอนหลักในการประเมินความเสี่ยง ได้แก่ ๑) การจัดการทรัพย์สิน (Asset Management) ๒) การระบุความเสี่ยง (Risk Identification) ๓) การวิเคราะห์ความเสี่ยง (Risk Analysis) และ ๔) การประเมินความเสี่ยง (Risk Evaluation)

รูปที่ ๑ กระบวนการดำเนินการประเมินความเสี่ยง

๔.๑ การจัดการทรัพย์สิน (Asset Management)

ทะเบียนทรัพย์สินประเภทฮาร์ดแวร์ -Network Device/Physical security

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑	HW-001	อุปกรณ์ค้นหาเส้นทาง Router	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Router	ห้อง Data Center
๒	HW-002	อุปกรณ์กระจายสัญญาณย่อย (Switch External)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๓	HW-003	อุปกรณ์ป้องกันเครือข่าย (Firewall)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Firewall	ห้อง Data Center
๔	HW-004	อุปกรณ์กระจายสัญญาณหลัก (Core Switch)	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๕	HW-005	อุปกรณ์ควบคุมอุปกรณ์กระจายสัญญาณเครือข่ายไร้สาย (Wireless Controller)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Wireless Controller	ห้อง Data Center
๖	HW-006	อุปกรณ์แจกหมายเลข IP และ DNS	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	DNS Server	ห้อง Data Center
๗	HW-007	อุปกรณ์บันทึกภาพแบบไอพี (Network Video Recorder)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Network Video Recorder	ห้อง Data Center
๘	HW-008	อุปกรณ์กระจายสัญญาณย่อย (DMZ Switch)	๔	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	ห้อง Data Center
๙	HW-009	เครื่องสแกนลายนิ้วมือ (Finger Scan)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Finger Scan	ห้อง Data Center
๑๐	HW-010	เครื่องสำรองไฟฟ้า ขนาด ๒๐ kVA	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑๑	HW-011	เครื่องสำรองไฟฟ้า ขนาด ๑๕ KVA	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center
๑๒	HW-012	เครื่องสำรองไฟฟ้า ขนาด ๑ KVA	๑๙	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	UPS	ห้อง Data Center
๑๓	HW-013	เครื่องปรับอากาศควบคุมอุณหภูมิและความชื้น	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Air	ห้อง Data Center
๑๔	HW-014	เครื่องตรวจจับควันความไวสูง	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Smoke Detector	ห้อง Data Center
๑๕	HW-015	เครื่องตรวจจับน้ำรั่วซึม	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Water Leak	ห้อง Data Center
๑๖	HW-016	เครื่องเฝ้าดูและแจ้งเตือนอัตโนมัติ (SMS Server)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	SMS Server	ห้อง Data Center
๑๗	HW-017	เครื่องวัดอุณหภูมิห้องปฏิบัติการคอมพิวเตอร์ (Data Center)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Room Temperature	ห้อง Data Center
๑๘	HW-018	อุปกรณ์กระจายสัญญาณไร้สาย (Wireless Access Point)	๘๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Access Point	อาคารภายในกรมป่าไม้
๑๙	HW-019	อุปกรณ์กระจายสัญญาณอาคาร (Core Switch BL)	๓	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	อาคารภายในกรมป่าไม้
๒๐	HW-019	อุปกรณ์กระจายสัญญาณ (Access Switch)	๓๐	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Switch	อาคารภายในกรมป่าไม้
๒๑	HW-020	กล้องโทรทัศน์วงจรปิดแบบไอพี (IP Camera)	๑๐	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	IP Camera	อาคารเทียมคมกฤส

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๒๒	HW-021	เครื่องกำเหนิดไฟฟ้า (Generator)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Generator	บริเวณด้านหน้า กองการอนุญาต
๒๓	HW-022	เครื่องควบคุมการสลับสัญญาณไฟฟ้า (ATS)	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	ATS	อาคารเทียมคมกฤส

ทะเบียนทรัพย์สินประเภทฮาร์ดแวร์ - Server/Storage/Backup

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๑	SV-001	HP ProLiant DL380G7	๕	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๒	SV-002	HP ProLiant DL380 G9	๔	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๓	SV-003	Storage HP MSA 2040	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Storage	ห้อง Data Center
๔	SV-004	HP ProLiant BL660c Gen8	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๕	SV-005	HP ProLiant BL6600c Gen9	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๖	SV-006	Storage HP	๑๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Storage	ห้อง Data Center
๗	SV-007	HP ProLiant DL 120 G5	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๘	SV-008	Acer R720 M2	๓	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	รายการ	จำนวน	ผู้รับผิดชอบ	ระบบ	กลุ่มทรัพย์สิน	ที่ตั้ง
๙	SV-009	IBM 520	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๐	SV-012	HP BL 680 G5	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๑	SV-011	HP BL 460c G6	๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center
๑๒	SV-012	BL 680 G7	๒	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	โครงสร้างพื้นฐานสารสนเทศ	Server	ห้อง Data Center

ทะเบียนทรัพย์สินประเภทข้อมูล - Data

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก/สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
๑	INFO-001	Source Code	โค้ดของระบบ	Confidential	Backup Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Source Code
๒	INFO-002	Data Backup	ข้อมูลสำรองระบบสารสนเทศ	Confidential	ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Data Backup
๓	INFO-003	Network Log File	ข้อมูลกิจกรรมต่างๆภายในระบบ	Confidential	SAN Server และ Backup Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Log File
๔	INFO-004	Network Diagram	ข้อมูลภาพโครงสร้างพื้นฐานระบบเครือข่าย	Confidential	PC Admin /ห้องศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Diagram

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อข้อมูล/สารสนเทศ	รายละเอียดข้อมูล/สารสนเทศ	ระดับชั้นความลับ	สื่อบันทึก/สถานที่จัดเก็บ	ผู้รับผิดชอบ	กลุ่มทรัพย์สิน
๕	INFO-005	Network Configuration	ข้อมูล Config Network	Confidential	File Server /ห้อง Data Center	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	Network Configuration

ทะเบียนทรัพย์สินระบบสารสนเทศและฐานข้อมูล - Web Application/Database

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อระบบสารสนเทศ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	App-001	ระบบเว็บไซต์กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒	App-002	ระบบด่านป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๓	App-003	ระบบเลื่อยโซ่ยนต์	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๔	App-004	ระบบจัดการป่าอย่างยั่งยืน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๕	App-005	ระบบทะเบียนสวนป่าออนไลน์	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๖	App-006	ระบบภูมิศาสตร์สารสนเทศเพื่อการบริหาร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๗	App-007	ระบบขอตรวจพิสูจน์ไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๘	App-008	ระบบแจกจ่ายกล้าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อระบบสารสนเทศ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๙	App-009	ระบบบริหารจัดการเรื่องร้องเรียน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๐	App-010	ระบบรับรองไม้ ผลิตภัณฑ์ไม้ และถ่านไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๑	App-011	ระบบอนุญาตส่งออกสินค้าไม้และผลิตภัณฑ์จากไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๒	App-012	ระบบพิทักษ์ไพร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๓	App-013	ระบบบัญชีข้อมูลกรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๔	App-014	ระบบพื้นที่ปลูกไม้มีค่า	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๕	App-015	ระบบบันทึกการปลูกต้นไม้ “รวมใจไทย ปลูกต้นไม้เพื่อแผ่นดิน”	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๖	App-016	ข้อมูลสารสนเทศกรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๗	App-017	ระบบฐานข้อมูลการบริหารกิจกรรมปลูกป่าและเพิ่มพื้นที่สีเขียว กระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๘	App-018	ระบบฐานข้อมูลงานวิจัย	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๑๙	App-018	ระบบบริหารจัดการป่าชุมชน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒๐	App-020	ระบบการขออนุญาตอุตสาหกรรมไม้ (e-Permit)	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App

ลำดับ	เลขทะเบียนทรัพย์สินสารสนเทศ	ชื่อระบบสารสนเทศ	ผู้รับผิดชอบ	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๒๑	App-021	ระบบเทคโนโลยีสารสนเทศการลดก๊าซเรือนกระจกภาคสมัครใจตามมาตรฐานของประเทศไทย จากการปลูก บำรุง อนุรักษ์ และฟื้นฟูป่าในพื้นที่ป่าไม้ กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒๒	App-022	ระบบจองที่พักป่านันทนาการ	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒๓	App-023	ระบบฐานข้อมูลความหลากหลายทางชีวภาพ กรมป่าไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒๔	App-024	ฐานข้อมูลรายการชนิดไม้	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Web App
๒๕	App-025	Forest4Thai	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Mobile App
๒๖	App-026	รวมใจไทยปลูกต้นไม้เพื่อแผ่นดิน	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Mobile App
๒๗	App-027	พิทักษ์ไพร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	SAN Server /ห้อง Data Center	Mobile App

๔.๒ ขั้นตอนที่ ๑: การระบุความเสี่ยง (Risk Identification)

งาน A: การระบุความเสี่ยง (Risk Identification)

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูล โดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๒. เว็บไซต์ และเว็บแอปพลิเคชันถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัปโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัปเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์ หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download Fileขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด
๖. ความเสี่ยงจากการถูกบุกรุกโดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัปเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม
				- ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัปเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ

- ทรัพย์สินสำคัญ (Crown Jewels) - ทรัพย์สินเหล่านี้มีความสำคัญต่อการบรรลุวัตถุประสงค์การดำเนินงานของกรมป่าไม้โดยรวม และมักจะเป็นสิ่งที่ผู้โจมตีต้องการแสวงหาประโยชน์

ลำดับ	ชื่อระบบสารสนเทศ/อุปกรณ์	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	ระบบเว็บไซต์กรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๒	ระบบอนุญาตส่งออกสินค้าไม้และผลิตภัณฑ์จากไม้กรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๓	ระบบบุคลากร เงินเดือน และสวัสดิการ	SAN Server /ห้อง Data Center	Web App
๔	ระบบงานบุคคลของพนักงานราชการ	SAN Server /ห้อง Data Center	Web App
๕	ระบบภูมิสารสนเทศเพื่อการบริหารกรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๖	อุปกรณ์ป้องกันเครือข่าย (Firewall)	ห้อง Data Center	Firewall
๗	อุปกรณ์กระจายสัญญาณหลัก (Core Switch)	ห้อง Data Center	Switch
๘	อุปกรณ์กระจายสัญญาณย่อย (DMZ Switch)	ห้อง Data Center	Switch
๙	อุปกรณ์ Info box อุปกรณ์แจกหมายเลข IP และ DNS	ห้อง Data Center	DNS
๑๐	อุปกรณ์ค้นหาเส้นทาง Router	ห้อง Data Center	Router

- ทรัพย์สินที่เกี่ยวข้อง (Stepping Stones) - ทรัพย์สินเหล่านี้เป็นทรัพยากรที่ผู้โจมตีต้องการควบคุมและใช้ประโยชน์เพื่อเปลี่ยนผ่านไปยังส่วนต่าง ๆ ของเครือข่ายก่อนที่จะไปถึงทรัพย์สินสำคัญ

ลำดับ	ชื่อระบบสารสนเทศ/อุปกรณ์	จัดเก็บอยู่ที่	กลุ่มทรัพย์สิน
๑	ระบบจัดเก็บบัญชีรายชื่อผู้ใช้งาน (AD)	ห้อง Data Center	Server
๒	ระบบสวนป่าออนไลน์	SAN Server /ห้อง Data Center	Web App
๓	ระบบแจกจ่ายกล้าไม้	SAN Server /ห้อง Data Center	Web App
๔	ระบบอนุญาตอุตสาหกรรมป่าไม้	SAN Server /ห้อง Data Center	Web App
๕	ระบบฐานข้อมูล	SAN Server /ห้อง Data Center	Data Base
๖	ระบบศูนย์ปฏิบัติการระดับกรม	SAN Server /ห้อง Data Center	Web App

งาน B: การสร้างแบบจำลองภัยคุกคาม (Threat Modelling)

เป็นกระบวนการจำลองเหตุภัยคุกคามที่อาจเกิดขึ้น เช่น ช่องโหว่เชิงโครงสร้าง เพื่อวิเคราะห์อย่างเป็นระบบเกี่ยวกับรูปแบบของการโจมตี เพื่อคาดการณ์รูปแบบการโจมตีที่เป็นไปได้ให้มากที่สุดและสินทรัพย์ที่ผู้โจมตีต้องการมากที่สุด โดยการสร้างแบบจำลองภัยคุกคามสามารถอธิบายถึง สินทรัพย์ที่มีมูลค่าสูงอยู่ที่ไหนในระบบ จุดที่เสี่ยงที่สุดในการถูกโจมตีคืออะไร ภัยคุกคามที่เป็นไปได้มากที่สุดคืออะไร และ มีรูปแบบการโจมตีอื่นอีกหรือไม่ที่ยังนึกไม่ถึง โดยทั่วไปแล้วมีการสร้างแบบจำลองภัยคุกคามบางรูปแบบในชีวิตประจำวันโดยไม่รู้ตัว บางคนใช้แบบจำลองภัยคุกคามในระหว่างการขับรถไปทำงานตอนเช้าเพื่อหลีกเลี่ยงอุบัติเหตุที่อาจเกิดขึ้น เป็นต้น โดยการสร้างแบบจำลองภัยคุกคามมีขั้นตอนต่อไปนี้

๑. การระบุขอบเขตและการจำแนกระบบ (Scope Identification and System Decomposition) – สิ่งเหล่านี้เป็นข้อกำหนดเบื้องต้นสำหรับการสร้างแบบจำลองภัยคุกคามที่แนะนำในงาน A

๒. การระบุภัยคุกคาม (Threat Identification) – หน่วยงานควรใช้แนวทางที่เป็นระบบเพื่อระบุเหตุการณ์ที่เป็นไปได้ที่ผู้โจมตีสามารถกระทำต่อทรัพย์สินได้

๓. การสร้างแบบจำลองการโจมตี (Attack Modelling) – หลังจากระบุเหตุการณ์ภัยคุกคามที่เกี่ยวข้องกับทรัพย์สินแต่ละรายการแล้ว หน่วยงานควรเชื่อมโยงเหตุการณ์เหล่านั้นเข้ากับลำดับการโจมตีที่เป็นไปได้ ทั้งนี้ การสร้างแบบจำลองการโจมตีอธิบายแนวทางการบุกรุกของผู้โจมตี เพื่อให้หน่วยงานสามารถระบุการควบคุมที่จำเป็นในการปกป้องระบบและจัดลำดับความสำคัญของการใช้งาน

งาน C: สร้างสถานการณ์ความเสี่ยง (Construct Risk Scenarios)

การสร้างสถานการณ์ความเสี่ยงเป็นงานสุดท้ายในการดำเนินการขั้นตอนการระบุความเสี่ยงให้เสร็จสมบูรณ์ งานนี้มีเป้าหมายเพื่อสร้างสถานการณ์ “สิ่งที่อาจผิดพลาด (What Could Go Wrong)” ที่ให้มุมมองที่สมจริงและสัมพันธ์กันของความเสี่ยงตามบริบททางธุรกิจ สภาพแวดล้อมของระบบ และภัยคุกคามที่เกี่ยวข้อง

สถานการณ์จำลองความเสี่ยงที่สร้างมาอย่างดีช่วยอำนวยความสะดวกในการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย และช่วยให้สามารถวิเคราะห์โครงสร้างความเสี่ยงในขั้นตอนต่อ ๆ ไป สถานการณ์ความเสี่ยงควรระบุองค์ประกอบหลัก ๔ ประการ ต่อไปนี้:

- ทรัพย์สิน (Asset) - สิ่งที่มีค่าที่ได้รับการระบุในงาน A

- เหตุการณ์ภัยคุกคาม (Threat event) - เหตุการณ์การโจมตีที่ระบุในงาน B

- ช่องโหว่ (Vulnerability) - จุดอ่อนในทรัพย์สินหรือกระบวนการที่สนับสนุนทรัพย์สินที่สามารถใช้ประโยชน์จากเหตุการณ์ภัยคุกคามที่ระบุได้ ช่องโหว่นี้อาจปรากฏขึ้นในช่วงที่ผ่านมาการตรวจสอบและ/หรือการทดสอบการเจาะ หรืออาจเกี่ยวข้องกับสภาพแวดล้อมเนื่องจากการใช้เทคโนโลยีบางอย่าง

- ผลที่ตามมา (Consequence) – ผลลัพธ์โดยตรงจากเหตุการณ์ภัยคุกคาม

ตัวอย่างของสถานการณ์ความเสี่ยงที่สร้างมาอย่างดีแสดงไว้ด้านล่าง

Legend: Threat Event | Vulnerability | Asset | Consequence

ผู้โจมตีทำการแทรก *SQL* บนเว็บแอปพลิเคชันเดิมที่ไม่ได้แพตช์เพื่อดาวน์โหลดเวชระเบียนผู้ป่วยที่มีความอ่อนไหว

Attacker performs an SQL injection on an **unpatched legacy web application** to **download sensitive patient medical records**.

รูปที่ ๑ เหตุการณ์ความเสี่ยง (Risk Scenario)

พนักงานภายในทำการหลอกลวงให้ชำระเงินเกินยอดเงินในบัญชีธนาคารในระบบการชำระเงินโดยไม่มีกำหนด ส่งผลให้เกิดการเบิกเกินบัญชีธนาคาร

Internal staff makes a fraudulent payment instruction exceeding bank account balance on the **payment system** with **no set limit, resulting in a bank overdraft**.

รูปที่ ๒ เหตุการณ์ความเสี่ยง

พนักงานที่ไม่ได้รับอนุญาตเข้าถึงเซิร์ฟเวอร์ SCADA โดยใช้ข้อมูลรับรองการเข้าสู่ระบบเริ่มต้นและดำเนินการคำสั่งปิดระบบเพื่อรบกวนการจ่ายน้ำไปยังฝั่งตะวันออกของกรุงเทพมหานครทั้งหมด

Unauthorised employee accesses the **SCADA server** using **default login credentials** and **execute shutdown command** to **disrupt the water supply to the entire east side of Bangkok.**

รูปที่ ๓ เหตุการณ์ความเสี่ยง

ผู้โจมตีส่งอีเมลฟิชชิ่งแบบเจาะจงกลุ่มเป้าหมายไปยังผู้ใช้ที่ไม่สงสัย ซึ่งเมื่อคลิกแล้ว จะทำให้บัญชีผู้ใช้ดำเนินการตรวจสอบสิทธิ์ *SMB* กับเซิร์ฟเวอร์ที่เป็นอันตรายและเปิดเผยข้อมูลประจำตัวที่แฮคไว้

Attacker delivers spear-phishing email to **unsuspecting user**, which when clicked, triggers the **user account** to **perform SMB authentication with malicious server** and **discloses hashed credentials.**

รูปที่ ๔ เหตุการณ์ความเสี่ยง

๔.๒ ขั้นตอนที่ ๒: การวิเคราะห์ความเสี่ยง (Risk Analysis)

การวิเคราะห์ความเสี่ยงเป็นการวิเคราะห์องค์ประกอบที่ประกอบกันเป็นสถานการณ์ความเสี่ยงแต่ละสถานการณ์เพื่อกำหนด

(๑) ความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น และ

(๒) ผลกระทบ (Impact) (เช่น ขนาดหรือระดับของอันตราย) ที่เกิดจากการเกิดสถานการณ์ความเสี่ยง

งาน A: กำหนดโอกาส (Determine Likelihood)

เหตุการณ์ในอดีตหรือเหตุการณ์ที่คาดว่าจะเกิดขึ้นมักถูกใช้เป็นตัวชี้วัดเพื่อวัดโอกาสเสี่ยง (เช่น เหตุการณ์คาดว่าจะเกิดขึ้นปีละครั้งหรือเกิดขึ้นครั้งเดียวในปีที่ผ่านมา) อย่างไรก็ตาม การใช้ตัวชี้วัดดังกล่าวเพื่อวัดแนวโน้มความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์อาจไม่เหมาะสม เนื่องจากลักษณะแบบพลวัตของภัยคุกคามทางไซเบอร์ ระบบที่ไม่เคยถูกบุกรุกมาก่อนไม่ได้หมายความว่าจะไม่ถูกบุกรุกในอนาคตตามคำแนะนำทั่วไป ความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ควรได้รับ การประเมินจากมุมมองของภัยคุกคามและช่องโหว่ วิธีหนึ่งในการพิจารณาความเป็นไปได้ของความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์คือการพิจารณาปัจจัยต่อไปนี้

- ความสามารถในการค้นพบ (Discoverability) – ฝ่ายตรงข้ามจะสามารถค้นพบช่องโหว่ของทรัพย์สินได้ง่ายเพียงใด ขึ้นอยู่กับความพร้อมใช้งานของข้อมูลเกี่ยวกับช่องโหว่และการเปิดเผยของทรัพย์สินที่มีช่องโหว่

- ความสามารถในการใช้ประโยชน์ (Exploitability) – ฝ่ายตรงข้ามจะใช้ประโยชน์จากช่องโหว่ของทรัพย์สินได้ง่ายแค่ไหน ขึ้นอยู่กับสิทธิ์การเข้าถึง ความซับซ้อนของเครื่องมือ ตลอดจนทักษะทางเทคนิคที่จำเป็นในการโจมตี

- ความสามารถในการทำซ้ำ (Reproducibility) – ฝ่ายตรงข้ามจะสามารถสร้างการโจมตีทรัพย์สินซ้ำได้ง่ายเพียงใด สิ่งนี้ขึ้นอยู่กับความซับซ้อนของการปรับแต่งการหาประโยชน์และสภาพแวดล้อมที่จำเป็นในการดำเนินการโจมตี

ภาพด้านล่าง คือตารางการประเมินตัวอย่างเพื่อพิจารณาแนวโน้มหรือโอกาส (Likelihood) ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ตามปัจจัยที่อธิบายไว้ข้างต้น สามารถทำตามขั้นตอนต่อไปนี้เพื่อให้ได้รับคะแนนความเป็นไปได้ของสถานการณ์ความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

(i) ให้คะแนนสำหรับแต่ละปัจจัยความน่าจะเป็น ๓ ระดับ (เช่น ๑ – ๓)

(ii) เฉลี่ยคะแนนและปัดเศษเป็นจำนวนเต็มที่ใกล้เคียงที่สุด

(iii) คะแนนสุดท้ายจะเป็นโอกาสของสถานการณ์ความเสี่ยง โดยระดับ ๓ คือ “มีแนวโน้มสูง” และ ๑ คือ “เป็นไปได้ยาก”

ตารางประเมินความเสี่ยงที่อาจเกิดขึ้น

Likelihood Rating	Discoverability	Exploitability	Reproducibility
High (๓)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการค้นหา/สแกนโดเมนสาธารณะสำหรับข้อมูลที่เผยแพร่ (เช่น Shodan, ExploitDB) ● สามารถถูกค้นพบและถูกโจมตีจากเครือข่ายภายนอก (รวมถึงอินเทอร์เน็ต)	การโจมตี: ● สามารถดำเนินการได้โดยไม่มีสิทธิ์การเข้าถึง (No Access Rights) ของเป้าหมาย ● สามารถทำได้ด้วยเครื่องมือที่หาได้ทั่วไป โดยไม่ต้องมีความรู้ด้านเทคนิค	การโจมตี: ● สามารถทำซ้ำได้ตามต้องการโดยไม่มีการกำหนดค่า (Configuration) หรือเงื่อนไขของเหตุการณ์ (Event Condition) ● สามารถทำซ้ำได้ตามต้องการโดยไม่ต้องปรับแต่งการหาประโยชน์ (Exploits) ที่เผยแพร่
Medium (๒)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการตรวจสอบการตอบสนอง พฤติกรรม และการสื่อสารของเป้าหมาย (เช่น การฟัซ (Fuzzing) กับแพ็กเก็ตเครือข่าย การดักจับเครือข่าย (Network Sniffing) ● สามารถถูกค้นพบและโจมตีจากภายในเครือข่ายย่อยหรือส่วนเครือข่ายเดียวกัน	การโจมตี: ● สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) ของเป้าหมาย (เช่น Admin/SYSTEM/ Root) ● สามารถดำเนินการได้ด้วยเครื่องมือที่เปิดเผยต่อสาธารณะ ซึ่งต้องใช้ความรู้ด้านเทคนิคในระดับกลาง	การโจมตี: ● สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์ที่คาดเดาได้บางอย่าง ● สามารถทำซ้ำได้ด้วยการปรับแต่งเฉพาะสำหรับเป้าหมาย
Low (๑)	ช่องโหว่ของเป้าหมาย: ● สามารถค้นพบได้โดยการดำเนินการและโต้ตอบกับการตั้งค่าปัจจุบันหรือที่คล้ายกันของเป้าหมาย	การโจมตี: ● สามารถดำเนินการได้ด้วยสิทธิ์การเข้าถึงพิเศษ (Privilege Access Rights) (เช่น Admin / SYSTEM / Root)	การโจมตี: ● สามารถทำซ้ำได้ตามเงื่อนไขเหตุการณ์สุ่มบางอย่าง

Likelihood Rating	Discoverability	Exploitability	Reproducibility
Low (๑) (ต่อ)	• สามารถถูกค้นพบและโจมตีด้วยการเข้าถึงแบบลอจิคัลโลคัล	• สามารถดำเนินการได้ด้วยเครื่องมือเฉพาะทางที่เปิดเผยต่อสาธารณะ ซึ่งต้องการความรู้ด้านเทคนิคขั้นสูงอาจต้องการรวมกันของการแสวงหาผลประโยชน์หลายอย่างร่วมกัน	• สามารถทำซ้ำได้ในทางทฤษฎีหรือด้วยการพิสูจน์การใช้ประโยชน์จากแนวคิดที่เผยแพร่

รายงานการประเมินความเสี่ยง

โดยวิเคราะห์จากปัจจัยความน่าจะเป็น (Likelihood) ของสถานการณ์ความเสี่ยงที่เกิดขึ้น ให้คะแนนตามระดับ ๑ ถึง ๓ (๑ เป็น “เป็นไปได้ยาก” ๒ “ปานกลาง” และ ๓ คือ “มีแนวโน้มสูง”) แสดงดังตารางต่อไปนี้

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๑
๒. เว็บไซต์ และเว็บแอปพลิเคชัน ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัปโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัปเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์	๒
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๓
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๓
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจาก	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ความน่าจะเป็น
Hacker	การปฏิบัติงาน	- ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัปเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข		patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัปเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๑

งาน B: กำหนดผลกระทบ (Determine Impact)

โดยทั่วไป การแสดงสถานการณ์ความเสี่ยงอาจส่งผลต่อการรักษาความลับ (Confidentiality) ความสมบูรณ์ (Integrity) และ/หรือความพร้อมใช้งาน (Availability) ของทรัพย์สิน (เช่น ข้อมูล อุปกรณ์ การดำเนินงาน) การโจมตีใด ๆ ของทรัพย์สินจะแปลเป็นผลกระทบในสาม (๓) ระดับต่อไปนี้

- ระดับชาติ (National) – ในระดับประเทศ ผลกระทบอาจถูกมองว่าเป็นอันตรายต่อความมั่นคงและเศรษฐกิจของประเทศ

- หน่วยงาน (Organisational) – ในระดับหน่วยงาน ผลกระทบอาจถูกมองว่าเป็นการหยุดชะงักในการดำเนินธุรกิจ ความเสียหายต่อชื่อเสียงและการสูญเสียทางการเงิน

- บุคคล (Individual) - ในระดับบุคคล ผลกระทบสามารถมองได้ว่าเป็นการสูญเสียชีวิต และการบาดเจ็บ

ตารางด้านล่าง คือ ตารางประเมินสำหรับการพิจารณาผลกระทบของความเสี่ยงในระดับคะแนน ๑ ถึง ๓ (โดยระดับคะแนน ๓ คือ “รุนแรงมาก” ระดับคะแนน ๒ คือ “ปานกลาง” และ ๑ คือ “เล็กน้อย”) ที่จะเกี่ยวข้องกับ

- เกี่ยวข้องกับบริบททางธุรกิจ (Relevant to business context) – เชื่อมโยงคำอธิบายกับวัตถุประสงค์ทางธุรกิจของหน่วยงานหรือวัดผลงาน

- ไม่กำกวม (Unambiguous) - ใช้คำอธิบายที่เป็นเลขฐานสองหรือที่มีช่วงเชิงปริมาณ (เช่น การรั่วไหลของข้อมูลที่ถูกจัดประเภทเป็น “ความลับ” หรือทำให้การบริการของลูกค้ามากกว่าร้อยละ ๕๐ หยุดชะงัก)

- มุมมองที่หลากหลาย (Multi-perspectives) – ระบุประเภทย่อยของผลกระทบจากแต่ละระดับจาก ๓ ระดับ (เช่น ระดับประเทศ หน่วยงาน และบุคคล)

ตารางคำอธิบายทั่วไปสำหรับการพิจารณาผลกระทบของความเสี่ยง

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	**ผลกระทบที่อาจเกิดขึ้น (potential impact)***		
	ต่ำ	**กลาง**	**สูง**
ด้านการรักษาความลับ (Confidentiality)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or SecondaryNational Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

วัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security Objective)	ผลกระทบที่อาจเกิดขึ้น (potential impact)*		
	ต่ำ	กลาง	สูง
	มีผลกระทบต่อข้อมูลที่ลับ (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐ)	มีผลกระทบต่อข้อมูลที่ลับมาก (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรง)	มีผลกระทบต่อข้อมูลที่ลับที่สุด (ข้อมูลข่าวสารลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายแก่ประโยชน์แห่งรัฐอย่างร้ายแรงที่สุด)
ด้านการรักษาความถูกต้องครบถ้วน (Integrity)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การแก้ไขหรือทำลายข้อมูลโดยไม่ได้รับอนุญาตอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)
ด้านการรักษาสภาพพร้อมใช้งาน (Availability)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบน้อยหรืออย่างจำกัด (Limited) และเกิดผลประโยชน์แห่งชาติสำคัญน้อย (Less Important or Secondary National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรง (Serious) และเกิดผลประโยชน์แห่งชาติที่สำคัญ (Important National Interests)	การหยุดชะงักของการเข้าถึงหรือการใช้ข้อมูลข่าวสารหรือระบบสารสนเทศอาจส่งผลกระทบอย่างร้ายแรงมาก (Severe or Catastrophic) และเกิดผลประโยชน์แห่งชาติสำคัญยิ่ง (Extremely Important National Interests)

ตารางเกณฑ์การประเมินผลกระทบ

ด้านผลกระทบ	ระดับผลกระทบ		
	ต่ำ	กลาง	สูง
การเงินหรือทรัพย์สิน	ไม่เกินหนึ่งล้านบาท	ไม่เกินหนึ่งร้อยล้านบาท	เกินกว่าหนึ่งร้อยล้านบาทขึ้นไป
อันตรายต่อชีวิต ร่างกายหรืออนามัย	ไม่มีผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อชีวิต ร่างกายหรืออนามัย	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย ไม่เกินหนึ่งพันคน	ผู้ใช้บริการหรือผู้มีส่วนได้เสียได้รับผลกระทบต่อร่างกายหรืออนามัย เกินกว่าหนึ่งพันคนหรือต่อชีวิตตั้งแต่หนึ่งคน
ผู้ใช้บริการหรือผู้มีส่วนได้เสียที่อาจได้รับ ความเสียหายนอกจากอันตรายต่อชีวิต ร่างกาย หรืออนามัย	ไม่เกินหนึ่งหมื่นคน	เกินกว่าหนึ่งหมื่นคนแต่ไม่เกินหนึ่งแสนคน	เกินกว่าหนึ่งแสนคน
ความสามารถในการดำเนินการตามหน้าที่ของหน่วยงาน	ไม่มีผลกระทบหรือมีผลกระทบต่อการดำเนินการตามหน้าที่ของหน่วยงานเพียงเล็กน้อย	การดำเนินการตามหน้าที่หลักของหน่วยงานด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	การดำเนินการตามหน้าที่หลักของหน่วยงานต้องหยุดชะงักไม่ต่อเนื่อง และไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน
ความมั่นคงของรัฐ	ไม่มีผลกระทบต่อความมั่นคงของรัฐ	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐด้อยประสิทธิภาพลงมาก แต่ยังอยู่ในระดับที่สามารถกู้คืนให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน	ระบบคอมพิวเตอร์หรือโครงสร้างสำคัญทางสารสนเทศที่เกี่ยวข้องกับความมั่นคงของรัฐต้องหยุดชะงัก ไม่ต่อเนื่องและไม่สามารถกู้คืนระบบให้กลับมาดำเนินการตามปกติได้ภายในระยะเวลาตามแผนกู้คืนระบบของหน่วยงาน เป็นผลให้ไม่สามารถทำงานหรือให้บริการได้

สถานการณ์ความเสี่ยงแต่ละสถานการณ์อาจได้รับการประเมินให้มีการจัดอันดับผลกระทบที่แตกต่างกันในด้านการรักษาความลับ ความสมบูรณ์ และความพร้อมใช้งาน คะแนนที่มีผลกระทบสูงสุดควรถือเป็นคะแนนสุดท้าย

รายงานการประเมินความเสี่ยง การกำหนดผลกระทบให้คะแนนตามระดับ ๑ ถึง ๓ (ระดับคะแนน ๑ คือ “ต่ำ” ระดับคะแนน ๒ คือ “ปานกลาง” และระดับคะแนน ๓ คือ “สูง”)

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๓
๒. เว็บไซต์ และเว็บแอปพลิเคชัน ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์ หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัปโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๒

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัปเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์	๒
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๓
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๑

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	ผลกระทบ
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัปเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	๓
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัปเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๓

๔.๓ ขั้นตอนที่ ๓: การประเมินความเสี่ยง (Risk Evaluation)

การประเมินความเสี่ยงเป็นเรื่องเกี่ยวกับการกำหนดและทำความเข้าใจความสำคัญของระดับความเสี่ยง และประกอบด้วยภารกิจดังต่อไปนี้:

- กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)
- ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

งาน A: กำหนดและจัดลำดับความสำคัญของความเสี่ยง (Determine and Prioritise Risk)

ดังที่กล่าวไว้ในหัวข้อที่ ๓ ความเสี่ยง คือ โอกาสที่เหตุการณ์ภัยคุกคามหนึ่ง ๆ จะใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สิน และทำให้เกิดผลกระทบ โดยสามารถนำเสนอเป็นแผนภาพโดยใช้เมทริกซ์ความเสี่ยง แสดงดังภาพด้านล่างเป็นตัวอย่างเมทริกซ์ความเสี่ยง ๓ ต่อ ๓ สำหรับกำหนดระดับความเสี่ยงสำหรับแต่ละสถานการณ์ความเสี่ยง โดยที่ระดับความเสี่ยงเป็นการคูณของ “โอกาสเป็นไปได้” และ “ผลกระทบ” ซึ่งกำหนดจากขั้นตอนการวิเคราะห์ความเสี่ยง (หัวข้อ ๔.๒)

IMPACT				
	High (๓)	M๓๑	H๓๒	H๓๓
	Medium (๒)	L๒๑	M๒๒	H๒๓
	Low (๑)	L๑๑	L๑๒	L๑๓
		Low (๑)	Medium (๒)	High (๓)
		LIKELIHOOD		

รูปที่ ๒ เมทริกซ์ความเสี่ยง ๓ คูณ ๓ สำหรับกำหนดระดับความเสี่ยง

สำหรับแต่ละระดับความเสี่ยงที่ได้รับ ให้เปรียบเทียบกับระดับการยอมรับความเสี่ยงที่กำหนดโดยหน่วยงาน สถานการณ์ความเสี่ยงที่มีระดับความเสี่ยงสูงกว่าระดับที่ยอมรับได้ต้องได้รับการจัดลำดับความสำคัญสำหรับการรักษาจนกว่าระดับความเสี่ยงจะอยู่ภายในระดับที่ยอมรับได้ เมื่อจัดลำดับความสำคัญของความเสี่ยงในการรักษา ควรกำหนดระยะเวลาที่คาดหวังไว้ด้วย

รายงานการประเมินความเสี่ยง แสดงดังตารางต่อไปนี้

ระดับความเสี่ยง = ผลกระทบ *x* โอกาสเกิด โดยระดับการประเมิน นั้น C I และ A หมายถึง *Confidentiality Availability* และ *Integrity* ตามลำดับ การตอบ *Yes* ใน *C I* หรือ *A* หมายถึง การเกิดผลกระทบต่อการรักษาความลับ *(C)* การเกิดผลกระทบต่อความสมบูรณ์ของข้อมูล *(I)* หรือการเกิดผลกระทบต่อสภาพพร้อมใช้ *(A)* ตามลำดับ และการตอบ *No* หมายถึง ไม่ได้รับผลกระทบ

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูล โจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	Yes	Yes	Yes	๓	๑	๓
๒. เว็บไซต์ และเว็บแอปพลิเคชัน ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มี	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https	Yes	Yes	Yes	๓	๒	๖

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
		ความทนทานต่อการถูกโจมตีจากผู้ไม่ประสงค์ดี (Secure Coding) - การอัปโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย	แม่ข่าย	- กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่						
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	ความเสี่ยงด้านเทคนิค /ความเสี่ยงจากการปฏิบัติงาน	- ขาดการอัปเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์	Yes	Yes	Yes	๒	๒	๔
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	ความเสี่ยงด้านเทคนิค	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์ - การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	- ผู้ใช้งาน - ผู้ดูแลระบบ - ระบบสารสนเทศ - ระบบฐานข้อมูล - เครื่องคอมพิวเตอร์แม่ข่าย	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	Yes	Yes	Yes	๓	๓	๙

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	ความเสี่ยงจากการปฏิบัติงาน	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- ผู้ใช้งาน - ระบบสารสนเทศ - ระบบฐานข้อมูล เข้าสู่ระบบ Domain ไม่ได้ - การเข้าถึงระบบเครือข่ายช้า	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	Yes	Yes	Yes	๑	๑	๓
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	ความเสี่ยงด้านเทคนิค / ความเสี่ยงจากการปฏิบัติงาน	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัปเดต ทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- ระบบฐานข้อมูล - ระบบสารสนเทศ	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall	Yes	Yes	Yes	๓	๒	๖

ความเสี่ยง (ภาวะคุกคาม)	ประเภทความเสี่ยง	ปัจจัยเสี่ยง (จุดอ่อนของระบบ)	ผลกระทบ /ผู้ได้รับผลกระทบ	แนวทางการควบคุม	การวิเคราะห์ความเสี่ยง					
					ระดับผลกระทบ			ผลกระทบ	โอกาสเกิด	ระดับความเสี่ยง
					C	I	A			
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	ความเสี่ยงด้านเทคนิค	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัปเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเทอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- ผู้ใช้งาน - ผู้ดูแลระบบ - เครื่องคอมพิวเตอร์แม่ข่าย - อุปกรณ์เครือข่าย - ระบบฐานข้อมูล - ระบบสารสนเทศ	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	Yes	Yes	Yes	๓	๑	๓

งาน B: ทำเอกสารเกี่ยวกับความเสี่ยง (Document Risk)

การประเมินความเสี่ยงจะไม่สมบูรณ์หากไม่มีเอกสารประกอบ ผลลัพธ์จากขั้นตอนก่อนหน้าจะต้องได้รับการบันทึกไว้อย่างชัดเจนในทะเบียนความเสี่ยงเพื่อการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย การลงทะเบียนความเสี่ยงเป็นบันทึกของสถานการณ์ความเสี่ยงทั้งหมดที่ระบุ รวมถึงระดับความเสี่ยงที่กำหนด การลงทะเบียนความเสี่ยงเป็นเอกสารที่มีชีวิตซึ่งได้รับการตรวจสอบและปรับปรุงให้ทันสมัย (update) เป็นประจำ เพื่อให้แน่ใจว่าฝ่ายบริหารของหน่วยงานมีภาพปัจจุบันเกี่ยวกับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานเมื่อทำการตัดสินใจโดยแจ้งความเสี่ยง ควรมีอย่างน้อยดังต่อไปนี้

- สถานการณ์ความเสี่ยง (Risk Scenario) – สถานการณ์ที่แสดงให้เห็นว่าเหตุการณ์ภัยคุกคามสามารถใช้ประโยชน์จากช่องโหว่ที่อาจเกิดขึ้นของทรัพย์สินเพื่อสร้างผลกระทบในทางลบได้อย่างไร

- วันที่ระบุความเสี่ยง (Identification Date) – วันที่ที่ระบุสถานการณ์ความเสี่ยง

- มาตรการที่มีอยู่ (Existing Measures) – มาตรการปัจจุบันที่มีอยู่เพื่อจัดการกับสถานการณ์ความเสี่ยง

- ความเสี่ยงในปัจจุบัน (Current Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากพิจารณามาตรการที่มีอยู่ (เช่น ความเสี่ยงโดยธรรมชาติ (Inherent Risk) โดยใช้มาตรการที่มีอยู่)

- แผนจัดการความเสี่ยง (Treatment Plan) – กิจกรรมที่วางแผนไว้ (เช่น การใช้มาตรการเพิ่มเติม) และระยะเวลาในการจัดการกับความเสี่ยงในปัจจุบันให้อยู่ในระดับที่ยอมรับได้ (เช่น ภายในระดับการยอมรับความเสี่ยงของหน่วยงาน)

- สถานะความคืบหน้า (Progress Status) – สถานะของการดำเนินการตามแผนจัดการความเสี่ยง

- ความเสี่ยงที่คงเหลืออยู่ (Residual Risk) – ระดับความเสี่ยงที่กำหนด (การรวมกันของความเป็นไปได้และผลกระทบ) ของสถานการณ์ความเสี่ยงหลังจากดำเนินการตามแผนจัดการความเสี่ยง (เช่น ความเสี่ยงปัจจุบันที่มีมาตรการเพิ่มเติม)

- เจ้าของความเสี่ยง (Risk Owner) – บุคคลหรือกลุ่มที่รับผิดชอบในการดูแลให้ความเสี่ยงที่เหลืออยู่อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

รายงานการประเมินความเสี่ยงมีองค์ประกอบอย่างน้อย ๘ ประการ ได้แก่ ๑) สถานการณ์ความเสี่ยง ๒) วันที่ระบุ ๓) มาตรการที่มีอยู่ ๔) ความเสี่ยงปัจจุบัน ๕) แผนจัดการความเสี่ยง ๖) สถานะความคืบหน้า ๗) ความเสี่ยงที่เหลืออยู่ และ ๘) เจ้าของความเสี่ยง ดังตารางด้านล่างนี้

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูลโดยผู้ไม่ประสงค์ดี (Hacker)	เมษายน ๒๕๖๗	- ความเสี่ยงจากระบบฐานข้อมูลมีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการบุกรุกระบบฐานข้อมูลจากภายนอก ลักลอบแก้ไขเปลี่ยนแปลงข้อมูลโจรกรรมข้อมูล - ข้อมูลถูกทำลาย โดยไวรัสคอมพิวเตอร์ - ไม่มีระบบสำรองเมื่อระบบหลักเสียหาย	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่	๙๐ %	- โปรแกรมระบบฐานข้อมูลเก่า ล้าสมัย - เครื่องแม่ข่ายฐานข้อมูล (Server) และเครื่องจัดเก็บข้อมูล (Storage) เก่า และไม่ได้รับการบำรุงรักษาอย่างต่อเนื่อง	ศทส
๒. เว็บไซต์ และเว็บแอปพลิเคชัน ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	เมษายน ๒๕๖๗	- ความเสี่ยงจากโปรแกรมสำเร็จรูปที่ใช้พัฒนาเว็บไซต์หรือปลั๊กอิน มีช่องโหว่เกิดขึ้น - ความเสี่ยงจากการไม่มีแนวทางการพัฒนาซอฟต์แวร์ที่มีความทนทานต่อการถูกโจมตีจากผู้ไม่	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘	๑๐๐ %	- เว็บแอปพลิเคชันเก่า ขาดการปรับปรุง Source code ให้ทันสมัยและปลอดภัย	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
		ประสงค์ดี (Secure Coding) - การอัปโหลดข้อมูล หรือไฟล์ที่ติดไวรัสขึ้นสู่ระบบ - การตั้งรหัสผ่านที่ไม่ปลอดภัย		ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่			
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	เมษายน ๒๕๖๗	- ขาดการอัปเดตโปรแกรมอย่างสม่ำเสมอ - การใช้โปรแกรมไม่ถูกลิขสิทธิ์	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟต์แวร์ถูกลิขสิทธิ์	๔๐%	ซอฟต์แวร์และระบบปฏิบัติการส่วนใหญ่ไม่สามารถอัปเดตเพื่อปิดช่องโหว่ได้	ศทส
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	เมษายน ๒๕๖๗	- การนำอุปกรณ์อื่นมาเชื่อมต่อเข้าระบบ เช่น Flash drive, Handy drive - มีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตหรือเว็บไซต์ที่ไม่เหมาะสม - การเปิด e-mail ที่ไม่รู้จักแหล่งที่มา เช่น มีโฆษณาแปลก ๆ บนเว็บบราวเซอร์, มีโฆษณาขายสินค้าในระบบอีเมล์	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอและจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์	๔๐%	มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่ยังไม่ครอบคลุมเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องลูกข่าย	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
		- การ Download File ที่สุ่มเสี่ยงต่อการติดไวรัสคอมพิวเตอร์	ประจำปี พ.ศ. ๒๕๖๖				
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	เมษายน ๒๕๖๗	- ผู้ใช้ขาดความระมัดระวังในการเข้าใช้ระบบสารสนเทศ เช่น การมอบหมายให้ผู้อื่นใช้รหัสผ่านของตนเองเข้าใช้ระบบหรือใช้งานแทน - ผู้ใช้งานเกินความจำเป็น เช่น ผู้ใช้บริการ Download File ขนาดใหญ่ , เปิดเว็บไซต์ที่ใช้ Bandwidth สูง	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด	๕๐ %	ผู้ใช้งานมีสิทธิ์เป็น Admin ของเครื่องซึ่งทำให้สามารถติดตั้งโปรแกรม หรือ Virus, Malware จะสามารถเขียนไฟล์ หรือสร้างตัวเองลงในเครื่องได้โดยไม่ต้องขอใช้สิทธิ์	ศทส
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	เมษายน ๒๕๖๗	- การตั้งค่าอุปกรณ์เครือข่ายไม่ปลอดภัยรัดกุม - รหัสผ่านคาดเดาได้ง่าย - ไม่มีอุปกรณ์ป้องกันภัยคุกคาม เช่น IPS, Antivirus, Web Filter - ระบบปฏิบัติการไม่อัปเดตทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้าน	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและ patch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความ	๙๐ %	ผู้ไม่ประสงค์ดี (Hacker) ยังสามารถใช้ช่องโหว่ ที่เกิดขึ้นในระบบเครือข่าย ระบบสารสนเทศ เพื่อเข้าแก้ไขข้อมูล ทำลายข้อมูล โดยไม่ได้รับอนุญาตยังสามารถทำงานได้ในบางระบบสารสนเทศ ซึ่งหน่วยงานควรจัดหา	ศทส

สถานการณ์ความเสี่ยง	วันที่ระบุ	ความเสี่ยงปัจจุบัน	แผนจัดการความเสี่ยง	มาตรการที่มีอยู่	สถานะความคืบหน้า	ความเสี่ยงที่เหลืออยู่	เจ้าของความเสี่ยง
			สารสนเทศกรมป่าไม้ ประจำปี พ.ศ. ๒๕๖๖	ปลอดภัย เช่น Firewall		ระบบหรืออุปกรณ์ด้านการป้องกันภัยคุกคามทางไซเบอร์มาเพื่อป้องกัน	
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	เมษายน ๒๕๖๗	- การตั้งค่าอุปกรณ์ผิดพลาด - อุปกรณ์เครื่องคอมพิวเตอร์แม่ข่ายชำรุดเสียหาย - ระบบปฏิบัติการไม่อัปเดตข้อมูลทำให้มีช่องโหว่ที่ยังไม่ได้แก้ไข - ความเสี่ยงจากไวรัสคอมพิวเตอร์ที่มาจากระบบเครือข่ายอินเตอร์เน็ต - ความเสี่ยงจากการโจมตีของผู้ไม่หวังดี เช่น Hacker - สาย LAN ชำรุดเสียหาย	- มีแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ - มีแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) - มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้ ประจำปี พ.ศ. ๒๕๖๖	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ	๑๐๐%	-	ศทส

๕. ตอบสนองต่อความเสี่ยง

หลังจากประเมินความเสี่ยงที่ระบุแล้ว (เช่น ความเสี่ยงในปัจจุบัน) ขั้นตอนต่อไปคือการระบุและกำหนดแนวทางการดำเนินการต่อไปเพื่อรักษาความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ของหน่วยงาน

๕.๑ ประเภทของตัวเลือกการตอบสนองความเสี่ยง (Types of Risk Response Options)

มีตัวเลือกการตอบสนองความเสี่ยง จำนวน ๔ ตัวเลือก ที่ต้องพิจารณา

(๑) ยอมรับ (Accept)

การยอมรับความเสี่ยงหมายถึงการรับความเสี่ยงตามที่เป็นอยู่โดยไม่ต้องดำเนินการเพิ่มเติมเพื่อลดความเสี่ยง ความเสี่ยงควรได้รับการยอมรับเมื่ออยู่ในระดับที่ยอมรับได้ของหน่วยงานเท่านั้น

(๒) หลีกเลี่ยง (Avoid)

การหลีกเลี่ยงความเสี่ยงหมายถึงการยุติการกระทำหรือกิจกรรมที่ทำให้หน่วยงานมีความเสี่ยงที่ระบุ สิ่งนี้อาจดูรุนแรง แต่อาจเป็นแนวทางปฏิบัติที่ดีที่สุดหากความเสี่ยงมีมากกว่าผลประโยชน์

ตัวอย่าง: การไม่ทำธุรกรรมการชำระเงินออนไลน์เป็นตัวอย่างของการหลีกเลี่ยงความเสี่ยงที่ผู้โจมตีจะลักลอบใช้ธุรกรรมเพื่อชำระเงินที่เป็นการฉ้อโกง

(๓) โอนย้าย (Transfer)

การโอนความเสี่ยงหมายถึงการแบ่งปันความเสี่ยงส่วนหนึ่งกับบุคคลหรือหน่วยงานอื่น เช่น โดยทั่วไปตัวเลือกการความเสี่ยงแบบนี้จะลดองค์ประกอบ “ผลกระทบ” ของความเสี่ยง

ตัวอย่าง: การซื้อประกันทางไซเบอร์หรือการจ้างดำเนินการบางอย่างเป็นตัวอย่างของการแบ่งปันความเสี่ยงกับบุคคลที่สาม

(๔) การลดความเสี่ยง (Mitigate)

การลดความเสี่ยงหมายถึงการวางมาตรการเพื่อลดระดับความเสี่ยง ซึ่งสามารถทำได้โดยผ่านการปรับใช้การควบคุมความมั่นคงปลอดภัย

ตัวอย่าง: การใช้ไฟร์วอลล์เพื่อจำกัดทราฟฟิกเครือข่ายเป็นตัวอย่างในการลดความเสี่ยงของระบบในการสื่อสารกับเซิร์ฟเวอร์ภายนอกที่เป็นอันตราย

ทั้งนี้ ไม่ว่าจะใช้ตัวเลือกการตอบสนองความเสี่ยงใด ผู้บริหารระดับสูง (ผู้ที่มีระดับอำนาจหน้าที่และความรับผิดชอบที่เหมาะสม) ภายในหน่วยงานจะต้องอนุมัติการตอบสนองความเสี่ยงที่เลือกอย่างเป็นทางการ และตัดสินใจอย่างมีวิจารณญาณเพื่อยอมรับความเสี่ยงที่เหลืออยู่

๕.๒ การเลือกการดำเนินการตอบสนองความเสี่ยงที่เหมาะสม (Choosing the Appropriate Risk Response Actions)

หน่วยงานหลายแห่งมักจะจัดการกับความเสี่ยงด้วยการลดความเสี่ยงด้วยการลงทุนในการควบคุมความมั่นคงปลอดภัยและทางแก้ไขปัญหาทางเทคนิคที่มีค่าใช้จ่ายสูง อย่างไรก็ตาม หน่วยงานควรสำรวจการรักษาความเสี่ยงด้วยการหลีกเลี่ยงหรือถ่ายโอนเป็นทางเลือกที่เป็นไปได้ซึ่งอาจมีความคุ้มค่าตัวอย่างเช่น เพื่อจัดการกับความเสี่ยงของการถูกบุกรุกของระบบเมื่อพนักงานเข้าถึงเว็บไซต์ที่เป็นอันตราย หน่วยงานต่าง ๆ อาจต้องพิจารณาหลีกเลี่ยงความเสี่ยงโดยการทำให้เข้าถึงระบบอินเทอร์เน็ตลดลงหรือจำกัดการเข้าถึงระบบอินเทอร์เน็ต แทนที่จะลดความเสี่ยงด้วยการปรับใช้ทางแก้ไขปัญหาป้องกันปลายทางที่มีราคาแพง

เมื่อหน่วยงานเลือกที่จะจัดการกับความเสี่ยงด้วยการลดความเสี่ยง จำเป็นต้องตรวจสอบให้แน่ใจว่าการควบคุมความมั่นคงปลอดภัยที่ใช้มีความเกี่ยวข้องและเหมาะสมกับความเสี่ยงที่กำลังจัดการ ทั้งนี้ตามคำแนะนำทั่วไป การควบคุมจะถือว่าเหมาะสมและเกี่ยวข้องกับความเสี่ยง คือ การลดความเสี่ยงหรือการลดผลกระทบจากความเสี่ยง

๖. การจัดการความเสี่ยง

จากนโยบายของกรมป่าไม้ ระดับความเสี่ยงที่ยอมรับได้ ≤ ๓ โดยกำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการความเสี่ยง คือ ความเสี่ยงที่มีระดับความเสี่ยงสูง ตั้งแต่ ๓ ขึ้นไป ส่วนความเสี่ยงที่มีระดับความเสี่ยงต่ำกว่า ๓ ถือว่ามีความเสี่ยงค่อนข้างต่ำอาจจะนำมาดำเนินการจัดการความเสี่ยงในแผนบริหารความเสี่ยงหรือไม่ก็ได้การดำเนินการจัดการความเสี่ยงเป็นดังตารางต่อไปนี้

ความเสี่ยง (ภาวะคุกคาม)	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	วิธีควบคุม	แนวทางการควบคุม
๑. ระบบฐานข้อมูลเสียหาย หรือมีการเปลี่ยนแปลงข้อมูล โดยผู้ไม่ประสงค์ดี (Hacker)	๓	มีแผนรองรับความเสี่ยง	ลด	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - มีการเข้ารหัสลับของระบบฐานข้อมูล - บำรุงรักษาระบบฐานข้อมูลอย่างสม่ำเสมอ - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๒. เว็บไซต์ และเว็บแอปพลิเคชัน ถูกแก้ไขข้อมูลโดยไม่ได้รับอนุญาต	๔	มีแผนรองรับความเสี่ยง	ลด	- สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด - บำรุงรักษาระบบอย่างสม่ำเสมอ - เปิดการใช้งาน https - กำหนดรหัสผ่านให้มีความปลอดภัย ไม่น้อยกว่า ๘ ตัวอักษร ที่มีอักษรตัวเล็ก ตัวใหญ่ ตัวเลข และอักขระพิเศษ - มีการทดสอบการเจาะระบบเพื่อปิดช่องโหว่
๓. โปรแกรมประยุกต์เกิดช่องโหว่ของโปรแกรม	๔	มีแผนรองรับความเสี่ยง	ลด	- ตรวจสอบการทำงานของโปรแกรมอย่างสม่ำเสมอ - ใช้ซอฟแวร์ถูกลิขสิทธิ์
๔. ความเสี่ยงจากไวรัสคอมพิวเตอร์หรือมัลแวร์	๙	มีแผนรองรับความเสี่ยง	ลด	- ติดตั้งระบบป้องกันไวรัสและมีการตรวจสอบอย่างสม่ำเสมอ และจัดทำรายงานประจำเดือน - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - ต้องอัปเดตโปรแกรมป้องกันไวรัสและ Patch อย่างสม่ำเสมอ - สร้างความรู้ความเข้าใจให้ผู้ใช้งาน ตระหนักถึงภัยคุกคามคอมพิวเตอร์

ความเสี่ยง (ภาวะคุกคาม)	ค่าระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	วิธีควบคุม	แนวทางการควบคุม
๕. ความเสี่ยงที่เกิดจากการใช้งานของผู้ใช้บริการ	๓	มีแผนรองรับความเสี่ยง	ลด	- สร้างความตระหนักในเรื่องนโยบาย และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ เช่น จำกัดสิทธิ์ในการใช้งานสื่อ Social Network - ปฏิบัติตามแนวนโยบายหรือระเบียบด้านสารสนเทศอย่างเคร่งครัด
๖. ความเสี่ยงจากการถูกบุกรุก โดยผู้ไม่ประสงค์ดี หรือ Hacker	๖	มีแผนรองรับความเสี่ยง	ลด	- ติดตั้งระบบตรวจสอบการบุกรุกเครือข่าย และติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและpatch อย่างสม่ำเสมอ - ติดตั้ง patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ - ติดตั้งอุปกรณ์รักษาความปลอดภัย เช่น Firewall
๗. ความเสี่ยงต่อระบบสำรองข้อมูลไม่สามารถกู้คืนระบบได้	๓	มีแผนรองรับความเสี่ยง	ลด	- จัดหาอุปกรณ์สำรองเพื่อให้สามารถใช้ทดแทนทำให้ปฏิบัติงานได้ตามปกติ - ติดตั้งระบบตรวจสอบการใช้งานเครือข่าย - ตรวจสอบและบำรุงรักษาเครื่องระบบสำรองข้อมูลอย่างสม่ำเสมอ - จัดเก็บข้อมูลที่สำรองไว้ด้วย External Harddisk สม่ำเสมอ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

๑.หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผน ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายในหรือ ผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ ต่อเครื่องแม่ข่าย ระบบสารสนเทศ ฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์ของกรมป่าไม้ โดยการดำเนินงานตามแผน ในการตรวจสอบ ควบคุม ป้องกัน และแก้ไขปัญหาที่เกิดจากภัยคุกคามทางไซเบอร์ รวมถึงการกู้คืนระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ให้สามารถใช้งานได้ต่อเนื่อง

๒.วัตถุประสงค์

๒.๑ เพื่อใช้เป็นแผนในการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศของกรมป่าไม้

๒.๒ เพื่อสร้างความเชื่อมั่นให้ผู้ใช้งานระบบเครือข่ายของกรมป่าไม้ ได้รับการปกป้องต่อภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ

๒.๓ เพื่อกำหนดมาตรการ นโยบาย และกลไกในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศ และการรับมือในภาวะฉุกเฉินเพื่อแก้ไขปัญหา

๒.๔ เพื่อเป็นแนวทางในการดำเนินงานของหน่วยงานภายในกรมป่าไม้ ที่เกี่ยวข้องในการปรับปรุงพัฒนาระบบสารสนเทศ และการให้ความรู้แก่บุคคลากรทางไซเบอร์และผู้ใช้งานระบบเครือข่ายของกรมป่าไม้ ให้มีความรู้ในเรื่องภัยคุกคามทางไซเบอร์ เพื่อสามารถป้องกันตนเองจากภัยคุกคามต่างๆ การรายงานเหตุภัยคุกคามทางไซเบอร์ และขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ ตามขอบเขตของระบบสารสนเทศที่กำหนดไว้ รวมไปถึงการสื่อสารไปยังผู้มีส่วนได้ส่วนเสีย เพื่อลดผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของกรมป่าไม้

๓. ขอบเขต

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ ใช้รับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้นต่อระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ใดๆ และบุคคล ที่เข้าถึงระบบสารสนเทศของกรมป่าไม้ ที่ติดตั้งอยู่ในห้อง Data Center ของกรมป่าไม้ ชั้น ๓ อาคารเทียมคมกฤส กรมป่าไม้

๔. หน้าที่การทบทวนแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีหน้าที่ทบทวนแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ และเสนอขออนุมัติแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ต่ออธิบดีกรมป่าไม้

๕. หน้าที่ในการดำเนินการตามแผน

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีหน้าที่เป็นผู้รับผิดชอบหลักในการดำเนินการตามแผนรับมือฯ ฉบับนี้ โดยมีหน่วยงานสนับสนุนประกอบด้วย

๕.๑ สำนักบริหารกลาง
๕.๒ สำนักป้องกันรักษาป่าและควบคุมไฟป่า
๕.๓ สำนักจัดการป่าชุมชน
๕.๔ สำนักวิจัยและพัฒนาการป่าไม้
๕.๕ สำนักส่งเสริมการปลูกป่า
๕.๖ สำนักจัดการที่ดินป่าไม้
๕.๗ สำนักแผนงานและสารสนเทศ
๕.๘ สำนักการป่าไม้ต่างประเทศ
๕.๙ สำนักโครงการพระราชดำริและกิจการพิเศษ
๕.๑๐ สำนักเศรษฐกิจการป่าไม้
๕.๑๑ สำนักจัดการป่านันทนาการ
๕.๑๒ กองการอนุญาต
๕.๑๓ สำนักจัดการทรัพยากรป่าไม้ที่ ๑ – ๑๓
๕.๑๔ สำนักจัดการทรัพยากรป่าไม้สาขาทุกสาขา
๕.๑๕ กลุ่มนิติการ
๕.๑๖ กลุ่มพัฒนาระบบบริหาร
๕.๑๗ กลุ่มตรวจสอบภายใน
๕.๑๘ กลุ่มงานจริยธรรม

๖. รายละเอียดการบังคับใช้เอกสาร

๖.๑. รายละเอียดของเอกสาร (Document control and review)

รายละเอียดของเอกสาร (Document control)	
ผู้จัดทำเอกสาร (Author)	นายทนงศักดิ์ มนตรี
ผู้ดำเนินการตามเอกสาร (Owner)	ทุกหน่วยงานในกรมป่าไม้
วันที่จัดทำเอกสาร (Date created)	๒๕ เมษายน ๒๕๖๗

รายละเอียดของเอกสาร (Document control)	
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	พฤษภาคม ๒๕๖๗
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	รองอธิบดีกรมป่าไม้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ของกรมป่าไม้
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	พฤษภาคม ๒๕๖๘

๖.๒. การเปลี่ยนแปลงเอกสาร (Version control)

รุ่น (Version)	วันที่อนุมัติ (Date of Approval)	ผู้อนุมัติ (Approved by)	สถานะ (Description of change)
๑		รองอธิบดีกรมป่าไม้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ของกรมป่าไม้	อนุมัติ

๗. เอกสารและกรอบมาตรฐานที่เกี่ยวข้อง

๗.๑ ประกาศกรมป่าไม้ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมป่าไม้ ประจำปี พ.ศ. ๒๕๖๖

๗.๒ ประกาศกรมป่าไม้ เรื่อง แนวนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๖

๗.๓ แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๗

๗.๔ แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)

๗.๕ แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖

๘. นิยาม

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

๘.๒ เหตุภัยคุกคามทางไซเบอร์ (Cyber incident) หมายความว่า เหตุการณ์ที่มีผลเชิงลบที่เกิดจากการกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่อาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๘.๓ ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๘.๔ เหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญ หมายความว่า เหตุภัยคุกคามทางไซเบอร์ที่ปรากฏต่อระบบสารสนเทศ และเป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙ ซึ่งคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติได้กำหนดลักษณะของภัยคุกคามทางไซเบอร์ไว้ตามมาตรา ๖๐ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

๘.๕ ซอฟต์แวร์ประสงค์ร้าย (Malicious Software) หรือที่เรียกโดยทั่วไปว่ามัลเวร์ (Malware) ซึ่งเป็นโปรแกรมที่มีการทำงานที่มุ่งประสงค์ร้ายต่อคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์

๘.๖ ไวรัสคอมพิวเตอร์ (Computer Virus) เป็นมัลแวร์ชนิดหนึ่ง ที่สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่น ๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต ซึ่งไวรัสคอมพิวเตอร์จะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยใช้พาหะ เช่น แฟลชไดรฟ์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๘.๗ หนอนคอมพิวเตอร์ (Computer worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัสตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอปพลิเคชัน จากนั้นจึงทำการคัดลอกตัวเองเข้าไปฝังตัวโดยใช้ช่องโหว่ดังกล่าว

๘.๘ ม้าโทรจัน (Trojan horse) เป็นมัลแวร์ชนิดหนึ่ง ที่มีจุดประสงค์เพื่อบุกรุก เข้าถึง และควบคุมเครื่องคอมพิวเตอร์จากระยะไกล ดำเนินการเปลี่ยนแปลง ทำลายไฟล์ข้อมูลสำคัญ หรือทำการคัดลอกข้อมูลดังกล่าว ส่งให้แก่ผู้คุกคามผ่านระบบเครือข่ายอินเตอร์เน็ต ซึ่งข้อมูลสำคัญที่ผู้คุกคามต้องการ อาจเป็นชื่อผู้ใช้ รหัสผ่าน เลขที่บัญชีธนาคาร และข้อมูลส่วนบุคคล อื่นๆ ลักษณะของการติดตั้งม้าโทรจันจะเหมือนกับไวรัสคอมพิวเตอร์คืออาศัยพาหนะ ซึ่งอาจมาจากแฟลชไดรว์ หรือทางอีเมล์

๘.๙ สปายแวร์ (Spyware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเทอร์เน็ต โดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้น สามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม ซึ่งส่วนใหญ่แล้วบันทึก

เว็บไซต์ที่ผู้ใช้เข้าถึงและส่งไปยังบริษัทโฆษณาต่าง ๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต

๘.๑๐ ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลดล็อคเพื่อกู้ข้อมูลคืนมา ผู้ใช้งานจะต้องทำการจ่ายเงินตามข้อความ “เรียกค่าไถ่” ที่ปรากฏ

๘.๑๑ การโจมตีแบบ DoS/DDoS มีจุดประสงค์เพื่อทำให้เครื่องคอมพิวเตอร์แม่ข่าย (Server) หยุดทำงาน หากเครื่องคอมพิวเตอร์ที่โจมตีมีเครื่องเดียว เรียกว่าการโจมตีแบบ Denial of Service (DoS) แต่หากมีเครื่องคอมพิวเตอร์ที่โจมตีมีมากกว่า ๑ เครื่อง และกระทำพร้อม ๆ กัน ไม่ว่าจะโดยตั้งใจหรือไม่ตั้งใจ จะเรียกว่าการโจมตีแบบ Distributed Denial of Service (DDoS)

๘.๑๒ Botnet เป็นกลุ่มของอุปกรณ์ที่ติดมัลแวร์และถูกเปลี่ยนเป็น Bot (ย่อมาจาก Robot) ไม่ว่าจะเป็นอุปกรณ์คอมพิวเตอร์ เว็บแคม เราท์เตอร์ หรืออุปกรณ์ IOT อื่น ๆ เพื่อรอรับคำสั่งจากผู้บุกรุก (Hacker) โดยผู้บุกรุก (Hacker) จะนำ Botnet ที่มีไปใช้ในการโจมตีขนาดใหญ่ เช่นการทำ DDoS เป็นต้น

๘.๑๓ Phishing คือการหลอกลวงทางอินเทอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง

๘.๑๔ ผู้บุกรุก (Hacker) หมายถึง ผู้ที่ไม่ได้รับอนุญาตในการใช้งานระบบ แต่พยายามลักลอบเข้ามาใช้งานด้วยวัตถุประสงค์ต่าง ๆ ไม่ว่าจะเพื่อโจรกรรมข้อมูล ผลกำไร หรือความพอใจส่วนบุคคลก็ตาม ความเสียหายจากผู้บุกรุกเป็นภัยคุกคามที่หนัก

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายทนงศักดิ์ XXXX	๒๔ ชั่วโมง/ ๗ วัน	๐๙ ๑๒๑๕ XXXX	รับแจ้งเหตุ	ประสานหน่วยงานที่เกี่ยวข้อง
๒	นายณภัทร์ XXXX	๒๔ ชั่วโมง/ ๗ วัน	๐๙ ๕๗๑๓ XXXX	รับแจ้งเหตุ	ประสานหน่วยงานที่เกี่ยวข้อง

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

กรมป่าไม้ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายสัมพันธ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๖๔๕๓ XXXX	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นางสาวสพินนา XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ XXXX	รองหัวหน้าทีมรับมือฯ (Deputy team manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
	นางสาวณัฏฐิณี XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๐๙๗๑ XXXX		
	นายทนงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ XXXX		
	นายประพันธ์พงษ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ XXXX		
๓	นายวีร์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ XXXX	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือหน่วยงานเจ้าของระบบสารสนเทศให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
	นายดำรงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๐๙๘๔ XXXX		
	นางสาวนรนันท์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๕๘๒๓ XXXX		
	นางสาวชณัฐจิตต์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๗๙๒ XXXX		

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
	นายณภัทร์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๕๗๑๓ XXXX		
	นายกิตติทัศน์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ XXXX		
	นางสาวปรียานุช XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๒๖๓๕ XXXX		
๔	นายทนงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ XXXX	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
	นายประพันธ์พงษ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ XXXX		
	นายวีร์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ XXXX		
๕	นายทนงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ XXXX	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบาย แผนงาน และคำสั่งที่เกี่ยวข้อง
	นางสาวสพินนา XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ XXXX		
	นางสาวณัฏฐิณี XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๐๙๗๑ XXXX		
	นายประพันธ์พงษ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ XXXX		

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๖	นายทนงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ XXXX	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
	นายวีร์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ XXXX		
	นายณภัทร์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๕๗๑๓ XXXX		
๗	นายวิจารณ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๖ ๔๓๕๖ XXXX	ผู้เชี่ยวชาญด้านกฎหมาย	-ทำหน้าที่ตามนโยบายแผนงานและคำสั่งที่เกี่ยวข้อง - แจ้งความดำเนินคดี และรายงานเหตุภัยคุกคามทางไซเบอร์
๘	นางสาวสพินนา XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ XXXX	ผู้บริหารจัดการความเสี่ยง	- ทำหน้าที่ตามนโยบาย แผนงานและคำสั่งที่เกี่ยวข้อง
	นายทนงศักดิ์ XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ XXXX		- ทำหน้าที่ประเมินผลกระทบความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๙	นางสาวจีราภา XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๒๘๕๒ XXXX	ผู้รับผิดชอบด้านสื่อสารองค์กร	ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ตารางที่ ๒ ทีมสนับสนุนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายอำนาจ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒-๓ ต่อ ๕๘๔๒	สำนักบริหารกลาง	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๒	นายทรงศักดิ์ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ต่อ ๕๐๕๑	สำนักป้องกันรักษาป่าและควบคุมไฟป่า	
๓	นางนันทนา XXXX	โทรศัพท์: ๐ ๒๕๗๙ ๗๕๘๕	สำนักจัดการป่าชุมชน	
๔	ดร. สุวรรณ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ต่อ ๕๔๗๔	สำนักวิจัยและพัฒนาการป่าไม้	
๕	นายอนันต์ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒-๓ ต่อ ๕๕๒๙	สำนักส่งเสริมการปลูกป่า	
๖	นายศักดา XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒-๓ ต่อ ๕๗๓๒, ๕๗๕๗	สำนักจัดการที่ดินป่าไม้	

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๗	นางวิสุตรา XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ๓ ต่อ ๕๖๗๑	สำนักแผนงานและสารสนเทศ	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๘	นายสุทธิรัตน์ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ๓ ต่อ ๕๒๐๙	กองการอนุญาต	
๙	นายบุญสุธีย์ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ๓ ต่อ ๕๒๔๙	สำนักเศรษฐกิจการป่าไม้	
๑๐	นายวีรวัฒน์ XXXX	โทรศัพท์: ๐ ๒๕๖๑ ๔๒๙๒ ๓ ต่อ ๕๕๓๔	สำนักจัดการป่านันทนาการ	

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

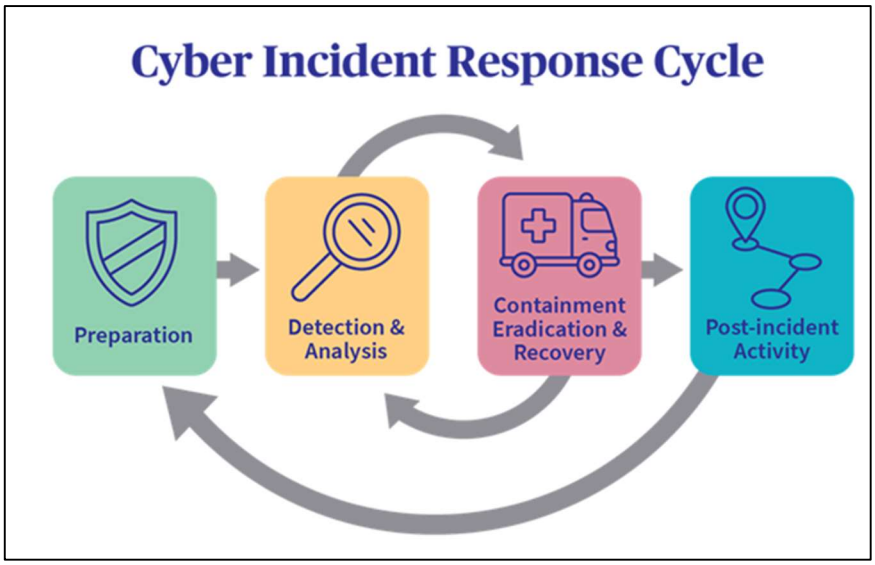
ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	-	๑. Email : thaicert@ncsa.or.th ๒. โทรศัพท์ ๐๒ ๑๑๔ ๓๕๓๑ (๒๔ ชั่วโมง)	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ
๒	-	โทรศัพท์ ๐ ๒๒๖๕ ๖๒๔๗	ศูนย์เทคโนโลยีดิจิทัลและอากาศยาน สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	หน่วยงานกำกับดูแล
๔	นายเกรียงไกร XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๓๑๓๘ XXXX	บริษัท อินเทอร์แอคทีฟ อินฟอร์เมชั่น ซิสเต็มส์ จำกัด	บริษัทรับจ้างบำรุงรักษาระบบงาน
๕	นางสาวสพินนา XXXX	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ XXXX	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส.)	ดูแลด้านการคุ้มครองข้อมูลส่วนบุคคลกรมป่าไม้

๙.๔ โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure)

กรมป่าไม้มีแผนผังโครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ของบุคลากรภายในทีมรับมือฯ ผู้บริหารหน่วยงาน หน่วยงานกำกับดูแล หน่วยงานรับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ตามกฎหมาย และหน่วยงานภายนอก

๑๐. ขั้นตอนการรับมือ

แผนรับมือฯ ฉบับนี้ ประกอบด้วยขั้นตอนการรับมือเหตุภัยคุกคามทางไซเบอร์ตามข้อ ๑๙.๑ ในประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ และประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ รวมถึงประกาศกรมป่าไม้ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กรมป่าไม้ ประจำปี พ.ศ. ๒๕๖๖ และแผนอื่นๆ ดังนี้



ภาพที่ ๑ ขั้นตอนการรับมือ

๑๐.๑ ขั้นการเตรียมการ (preparation)

เป็นการดำเนินมาตรการเพื่อเตรียมการในการป้องกันและลดความเสี่ยงจากเหตุภัยคุกคามทางไซเบอร์ (Preparation) เป็นสิ่งที่จะต้องทำในระยะเริ่มต้น เพื่อเตรียมความพร้อมเมื่อต้องเผชิญเหตุ ได้แก่

๑๐.๑.๑ จัดฝึกอบรมการสร้างความตระหนักรู้ (Awareness Training) ด้านความมั่นคงปลอดภัยไซเบอร์แก่บุคคลากรของกรมป่าไม้ อย่างน้อยปีละ ๑ ครั้ง

๑๐.๑.๒ ส่งเจ้าหน้าที่เข้ารับการฝึกอบรมด้านความมั่นคงปลอดภัยไซเบอร์เชิงลึก และการทดสอบการเจาะระบบแก่เจ้าหน้าที่ที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง

๑๐.๑.๓ ตั้งค่าระบบสารสนเทศ เว็บไซต์ ฐานข้อมูล ระบบปฏิบัติการ และอุปกรณ์เครือข่าย ให้มีความมั่นคงปลอดภัย โดยการปิดช่องโหว่ที่เกิดขึ้น พร้อมกับการทำ Secure coding

๑๐.๑.๔ ให้มีการติดตั้งโปรแกรมป้องกันไวรัส สำหรับเครื่องลูกข่าย และเครื่องแม่ข่ายให้ครอบคลุมทุกเครื่องภายในกรมป่าไม้ส่วนกลาง

๑๐.๑.๕ จัดให้มีการซ้อมแผนการเผชิญเหตุภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ ครั้ง

๑๐.๑.๖ มีการจัดหา Next Gen Firewall เพื่อป้องกันระบบเครือข่าย

๑๐.๑.๗ มีการเช่าระบบสำรองข้อมูลเพื่อสำรองข้อมูลสารสนเทศของกรมป่าไม้

๑๐.๑.๘ จัดเตรียมทีมรับมือเหตุการณ์ภัยคุกคามทางไซเบอร์ ได้แก่

๑) หัวหน้าทีมรับมือฯ (Team manager)

๒) รองหัวหน้าทีมรับมือฯ (Deputy team manager)

๓) เจ้าหน้าที่รับมือฯ (Incident lead)

๔) เจ้าหน้าที่เทคนิค (Technical lead)

๕) เจ้าหน้าที่ควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ (Officers control the effects of cyber threats)

๖) เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)

๗) ผู้ทดสอบเจาะระบบ (Penetration tester)

๘) ผู้เชี่ยวชาญด้านกฎหมาย (Legal expert)

๙) ผู้บริหารจัดการความเสี่ยง (Risk management person)

๑๐) ผู้รับผิดชอบด้านสื่อสารองค์กร (Person responsible for corporate

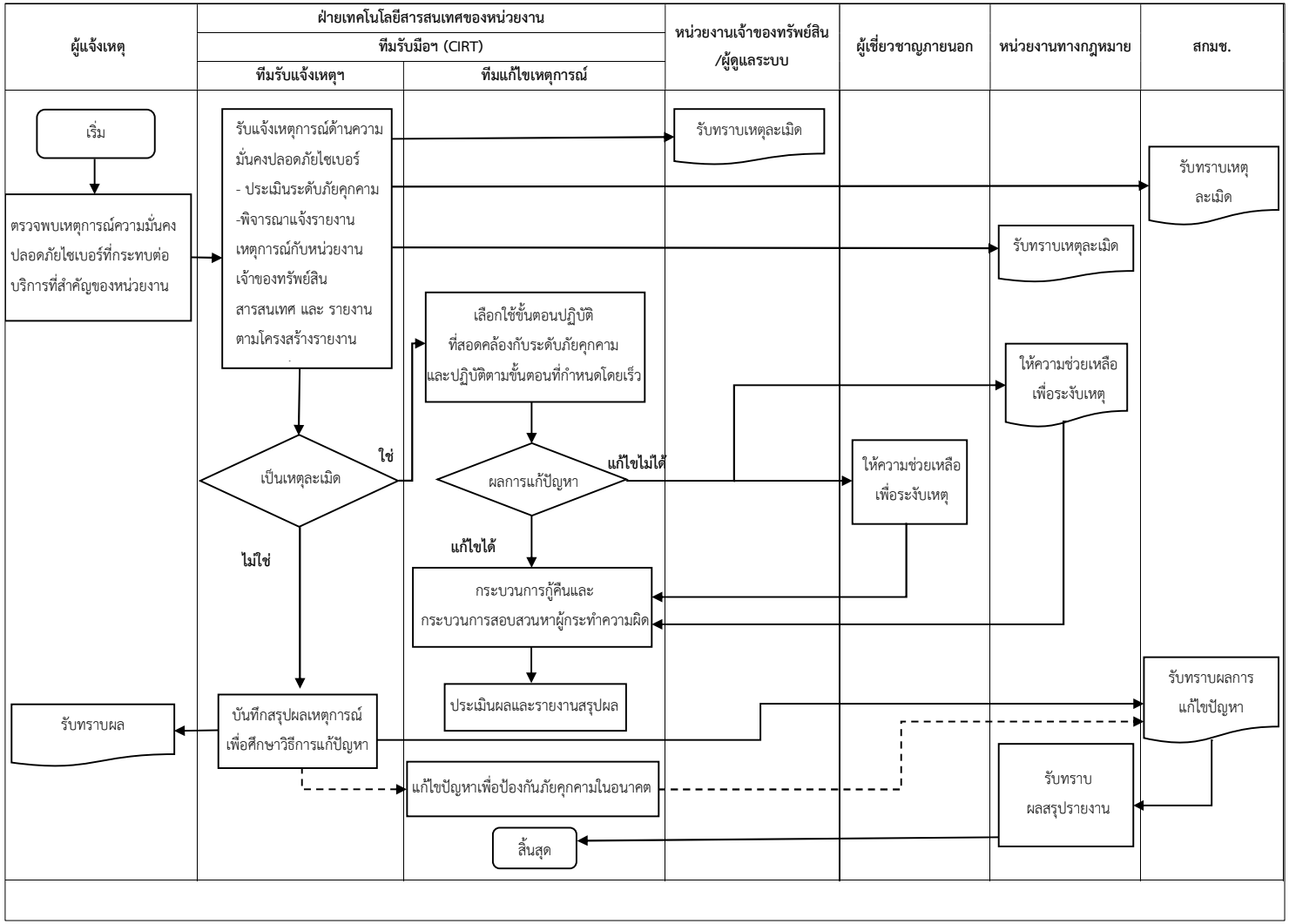
๑๐.๑.๙ จัดเตรียมช่องทางการแจ้งเหตุการณ์ภัยคุกคามทางไซเบอร์

๑๐.๑.๑๐ จัดเตรียมช่องทางการติดตามสถานการณ์ ของเหตุการณ์ภัยคุกคามทางไซเบอร์ ที่ได้รับแจ้ง

๑๐.๑.๑๑ จัดเตรียมห้องประชุม

๑๐.๑.๑๒ จัดเตรียมสถานที่จัดเก็บหลักฐาน ข้อมูลและพยานอื่นๆ ที่สำคัญ

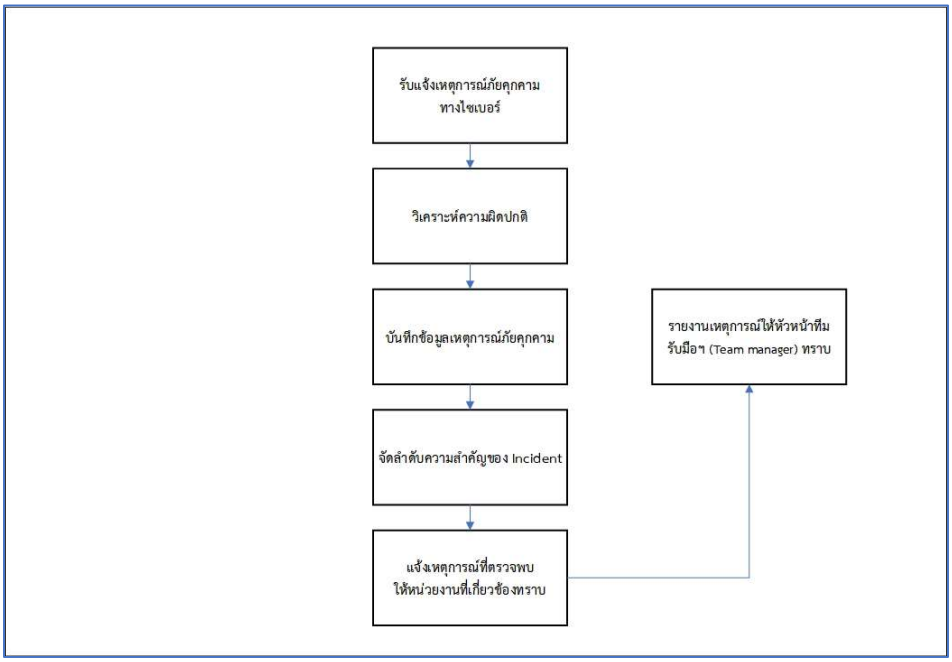
๑๐.๑.๑๓ จัดทำแผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ของกรมป่าไม้ ดังภาพที่ ๒



ภาพที่ ๒ แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity incident Response)

๑๐.๒ ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

เป็นการดำเนินการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis) ซึ่งเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น ประกอบด้วยการดำเนินการตามเอกสารแนบท้าย ๒ ตารางที่ ๒.๒ ในประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติเรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปรามและระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ ดังภาพที่ ๓



ภาพที่ ๓ ขั้นการตรวจจับ และวิเคราะห์ภัยคุกคามทางไซเบอร์

แม้ว่าหน่วยงานจะจัดให้มีมาตรการต่าง ๆ เพื่อป้องกันหรือควบคุมมิให้เกิดภัยคุกคามทางไซเบอร์ขึ้นแล้วก็ตาม แต่หน่วยงานก็ยังคงต้องเตรียมความพร้อมอยู่เสมอเพื่อรับมือกับสถานการณ์ภัยคุกคามทางไซเบอร์ที่ไม่อาจหลีกเลี่ยงได้การดำเนินมาตรการในการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) จึงเป็นสิ่งจำเป็นที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทันท่วงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๑๐.๒.๑ การตรวจจับ incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกในการปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท ดังนี้

- Precursor เป็นข้อมูลบ่งบอกว่า incident จะเกิดขึ้นในอนาคต

- Indicator เป็นข้อมูลบ่งบอกว่า incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกันและต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการ แจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑๐.๒.๑.๑ ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือนเมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่ายและ Host การตรวจเจอ Malware ในระบบเป็นข้อบ่งชี้ได้ทั้งที่กำลังพยายามโจมตีและการโจมตีได้สำเร็จแล้ว

๓) Third-Party บริการสอดส่องดูแลความผิดปกติที่เกิดขึ้นกับระบบ หรือระบบของหน่วยงาน ถูกนำไปโจมตีระบบอื่น ๆ ภายนอกองค์กรซึ่งบ่งบอกได้ว่าระบบภายในหน่วยงานได้ถูกยึดครองโดยผู้ไม่ประสงค์ดี และนำไปใช้สร้างความเสียหาย

๑๐.๒.๑.๒ ประเภท Log

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

๒) Network Device Log อุปกรณ์เครือข่ายที่มีการบันทึกข้อมูลที่ผ่านเข้าออกเครือข่าย สามารถถูกใช้ในการตรวจจับเหตุการณ์ภัยคุกคามบางอย่างได้ขึ้นอยู่กับประเภทของ Log และ Rule set ที่ใช้ในการวิเคราะห์

๑๐.๒.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็นข้อบ่งชี้ภัยคุกคามได้

๑๐.๒.๑.๔ บุคคลที่ทำหน้าที่แจ้งเตือนบุคคลภายในองค์กร บุคลากรทุกตำแหน่งสามารถเข้ารับการฝึกฝน เพื่อช่วยสอดส่องดูแล

๑๐.๒.๒ การวิเคราะห์ภัยคุกคามเพื่อให้การดำเนินการต่อไปสามารถทำได้เร็วและถูกต้อง ใช้การวิเคราะห์ความผิดปกติเมื่อได้รับแจ้งดังนี้

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

๑๐.๒.๒.๒ Clock Synchronization อุปกรณ์ทุกชิ้นบนเครือข่ายต้องได้รับการ Synchronize เวลาให้ ตรงกันอยู่เสมอเพื่อทำให้การ Correlate Event ทำได้ง่าย

๑๐.๒.๒.๓ Sniff and Analyze Network Data ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ข้อมูล

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

๑๐.๒.๓ การวิเคราะห์ผลกระทบและความรุนแรง เพื่อจัดลำดับความสำคัญของ Incident และช่วยในการตัดสินใจ เชิงกลยุทธ์เพื่อดำเนินการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้นได้อย่างเหมาะสมภายใต้ทรัพยากรที่มีอยู่อย่างจำกัด และลดผลกระทบทางธุรกิจให้น้อยลงที่สุด การกำหนดแนวทางในการวิเคราะห์ผลกระทบและการจัดลำดับความสำคัญของ Incident โดยอย่างน้อยควรครอบคลุมในด้านผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อข้อมูล (Information Impact) และความสามารถในการฟื้นฟูระบบ (Recoverability)

๑๐.๒.๓.๑ ผลกระทบต่อการให้บริการ (Functional Impact) ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม พิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที ซึ่งรวมถึงผลกระทบทางด้านการปฏิบัติงานของระบบการให้บริการต่าง ๆ ซึ่งส่งผลโดยตรงต่อการดำเนินธุรกิจ (Impact to Business) ที่ทำให้เกิดความขัดข้องหรือเสียหายต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้นโดยระดับของ Functional Impact มีดังนี้

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

๑๐.๒.๓.๒ ผลกระทบต่อข้อมูล (Information Impact) ผลกระทบต่อข้อมูล จะพิจารณา 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 หรือทำลายโดยไม่ได้รับอนุญาต

๑๐.๒.๓.๓ ความสามารถในการฟื้นฟูระบบ (Recoverability) ความสามารถในการฟื้นฟูระบบจะพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศเช่น ระบบ ข้อมูล เป็นต้น ที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถ หรือความยากง่ายในการฟื้นฟูระบบ รวมทั้งทรัพยากรที่จำเป็นต้องใช้โดยระดับของ Recoverability Effort มีดังนี้

- Regular เวลาในการกู้คืนสามารถคาดการณ์ได้ โดยใช้ทรัพยากรที่มี
- Supplemented เวลาในการกู้คืนสามารถคาดการณ์ได้ แต่ต้องมีการจัดหาทรัพยากรเพิ่ม
- Extended เวลาในการกู้คืนไม่สามารถคาดการณ์ได้ ต้องใช้ทรัพยากรและความช่วยเหลือจากภายนอก
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๑๐.๒.๔ เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ให้ทีมรับแจ้งเหตุบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ตามแบบฟอร์มบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ในภาคผนวก ๑

๑๐.๒.๕ เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ได้จัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย พร้อมระบุรายละเอียดพร้อมเวลาที่เกิดเหตุและระยะเวลาที่ใช้ ลงวันที่และลงนามโดยผู้มีหน้าที่จัดการรับมือเหตุการณ์นั้นๆ เพื่อให้มั่นใจได้ว่าเหตุการณ์ความปลอดภัยทางไซเบอร์ที่เกิดขึ้นจะได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม ตามแบบฟอร์มบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) ในภาคผนวก ๒

๑๐.๒.๖ กรณีที่เกิดเหตุภัยคุกคามทางไซเบอร์ให้เจ้าหน้าที่รายงานภัยคุกคามทางไซเบอร์ที่เกิดขึ้นกับบริการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติทราบ ตามแบบฟอร์ม ภาคผนวก ๓ และรายงานภัยคุกคามตามแบบฟอร์ม ภาคผนวก ๔ และจัดทำและส่งรายงานสรุปจำนวนเหตุภัยคุกคามทางไซเบอร์ทั้งหมดที่ได้เกิดขึ้นกับข้อมูลหรือระบบสารสนเทศของกรมป่าไม้ในแต่ละปี ภายในวันที่ ๓๑ มกราคม ของปีถัดไป ให้สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ โดยให้แยกสถิติหมวดหมู่ตามแบบฟอร์ม ภาคผนวก ๕

๑๐.๓ ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ ทีมรับมือจะดำเนินการดังนี้ เพื่อให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกูคืนทรัพยสินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ

๑๐.๓.๑ จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- 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 ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

๑๐.๓.๒ เรียกใช้งานกระบวนการกู้คืน (Recovery Process)

หลังจากดำเนินการควบคุมความเสียหาย กำจัดสาเหตุของภัยคุกคามเสร็จเรียบร้อยแล้ว จะเข้าสู่กระบวนการฟื้นฟูระบบให้เข้าสู่สภาวะการทำงานปกติ โดยดำเนินการดังต่อไปนี้

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

-Restore ข้อมูลกลับเข้าระบบจาก Back Up Storage

๑๐.๓.๓ ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์

๑๐.๓.๔ เก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน

๑๐.๓.๕ ดำเนินการตามระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ให้บริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี

๑๐.๔. ขั้นการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident activity)

หน่วยงานควรกำหนดขั้นตอน วิธี ปฏิบัติ หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจนซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไขจุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น อาจเข้าลักษณะเป็นความผิดตามประมวล กฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง ประกอบด้วยการดำเนินการในเรื่องดังต่อไปนี้

(๑) ทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ

๑๐.๕. การจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

หน่วยงานจะต้องจัดทำรายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ซึ่งจะช่วยให้แนวทางแก่หน่วยงานเกี่ยวกับขั้นตอนสำคัญที่ควรดำเนินการ โดยหน่วยงานสามารถใช้ข้อมูลเพื่อประกอบการพิจารณาความเหมาะสมในการจัดทำรายการตรวจสอบของตนเองได้ (รายละเอียดปรากฏตามภาคผนวก ๕)

แบบประเมินความสอดคล้อง
ของประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ กรมป่าไม้

คำชี้แจง :

๑. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ ประกอบด้วย ประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ

๒. เนื่องจากมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ประกอบกับประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ จะต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานให้สอดคล้องกับประกาศดังกล่าว ทั้งในส่วนของประมวลแนวทางปฏิบัติ จำนวน ๓ ข้อ และกรอบมาตรฐาน จำนวน ๑๕ ข้อ ซึ่งอาจมีเอกสารที่ต้องดำเนินการเป็นจำนวนมาก สำนักงานจึงกำหนดให้หน่วยงานเริ่มดำเนินการในส่วนของประมวลแนวทางปฏิบัติทั้ง ๓ ข้อก่อน <u>โดยให้แล้วเสร็จภายในวันที่ ๑๕ กันยายน ๒๕๖๖</u> ทั้งนี้ สำนักงานจะได้พิจารณาแจ้งให้หน่วยงานได้ดำเนินการจัดทำในส่วนของกรอบมาตรฐานเป็นลำดับต่อไป

๓. แบบประเมินนี้ มีวัตถุประสงค์เพื่อช่วยให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญสารสนเทศ นำไปใช้ในการประเมินว่าประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน มีความสอดคล้องกับประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ จำนวน ๓ ข้อ ตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. ๒๕๖๔ หรือไม่

๔. การประเมินความสอดคล้องนี้ กรมป่าไม้จำเป็นต้องอ้างถึงหลักฐานที่ชัดเจนว่าได้มีการดำเนินการอย่างไร พร้อมแนบหลักฐานดังกล่าวไปยังสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ ทั้งนี้ <u>กรมป่าไม้ปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive data)</u> และการประเมินโดยกรมป่าไม้เป็นเพียงการประเมินขั้นต้นเท่านั้น <u>ยังไม่ถือว่าได้มีการจัดทำแผนรับมือฯ สอดคล้องกับประกาศดังกล่าวข้างต้น</u> จนกว่าสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ จะได้ตรวจสอบแล้วเสร็จ และแจ้งเป็นหนังสือรับรองกลับไปยังหน่วยงานเป็นลายลักษณ์อักษร แล้วเท่านั้น

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑๗.๑	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศ ทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้	✓		กรมป่าไม้ได้มีหนังสือลับ ที่ ทส ๑๖๑๒.๓/๘๒๒ ลงวันที่ เรื่องขอรับการทดสอบความมั่นคปลอดภัยของระบบเครื่องแม่ข่ายและเว็บไซต์
	(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	✓		- แผนบริหารควมเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้ ปีงบประมาณ พ.ศ. 2566 ลิงก์ :https://shorturl.at/ckyPZ - แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. 2566 (Business Continuity Plan: BCP) ลิงก์ :https://shorturl.at/ruyQV - แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) ลิงก์: https://shorturl.at/ejlyQ
	(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)	✓		- ตามแผนบริหารควมเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้ ปีงบประมาณ พ.ศ. 2566 ลิงก์ :https://shorturl.at/ckyPZ
	(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด	✓		ตามเอกสารฉบับนี้ ประกอบด้วย - แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
๑๗.๒	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย		✓	-
๑๗.๓	ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่นให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการ		✓	-

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	ดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่จากวันที่ได้รับรายงานการตรวจสอบโดยแผนการดำเนินการแก้ไขต้องมีรายละเอียดอย่างน้อย ดังนี้			
	(ก) ให้รายละเอียดการดำเนินการแก้ไขที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการเพื่อจัดการกับการไม่ปฏิบัติตาม และ		✓	-
	(ข) กำหนดระยะเวลาสำหรับการดำเนินการตามที่ระบุไว้ในข้อ ๑๗.๓ (ก)		✓	-
๑๗.๔	ในกรณีที่ กกม. เห็นสมควรให้ปรับปรุงแผนการดำเนินการแก้ไข ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศดำเนินการและส่งแผนการดำเนินการแก้ไขที่ได้รับการปรับปรุงแล้วไปยังสำนักงานภายในระยะเวลาที่ กกม. กำหนด พร้อมส่งทั้งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย		✓	-
๑๗.๕	เมื่อแผนการดำเนินการแก้ไขได้รับความเห็นชอบจาก กกม. หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะดำเนินการตามแผนการดำเนินการแก้ไขดังกล่าว และดำเนินการแก้ไขทั้งหมดให้แล้วเสร็จภายในกำหนดระยะเวลาตามที่ระบุไว้ เพื่อให้ผ่านเกณฑ์การพิจารณาของ กกม.		✓	-
	การประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
	หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศต้องกำหนดนโยบายการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อยดังต่อไปนี้	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๑๘.๑	การประเมินความเสี่ยง (Risk Assessment)			
	(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์ และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุ มาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	(ข) การวิเคราะห์ความเสี่ยง (Risk Analysis) ต้องเข้าใจและวิเคราะห์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อหาแนวทางในการจัดการความเสี่ยงที่เหมาะสม	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	(ค) การประเมินค่าความเสี่ยง (Risk Evaluation) ต้องประเมินถึงโอกาสที่ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์จะเกิดขึ้นและผลกระทบต่อการปฏิบัติงานและการดำเนินธุรกิจ รวมถึงกำหนดระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ (Risk Appetite)	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๑๘.๒	การจัดการความเสี่ยง (Risk Treatment)			
	ต้องมีแนวทางจัดการ ควบคุม และป้องกันความเสี่ยงที่เหมาะสมสอดคล้องกับผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้ความเสี่ยงที่เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	นอกจากนี้ต้องกำหนดดัชนีชี้วัดความเสี่ยงที่สำคัญ (Key Risk Indicator: KRI) ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวข้องกับการดำเนินธุรกิจ ให้สอดคล้องกับความสำคัญของความมั่นคงปลอดภัยไซเบอร์แต่ละงาน เพื่อใช้ติดตามและทบทวนความเสี่ยง	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๑๘.๓	การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)			
	ต้องมีกระบวนการที่มีประสิทธิภาพในการติดตาม และทบทวนความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้อยู่ภายใต้ระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ที่กำหนดไว้	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๑๘.๔	การรายงานความเสี่ยง (Risk Reporting)			
	ต้องรายงานระดับความเสี่ยงและผลการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ต่อคณะกรรมการของหน่วยงานที่ได้รับมอบหมายเป็นประจำ เช่น ตามรอบการประชุมของคณะกรรมการของหน่วยงานที่ได้รับมอบหมาย	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น	✓		อยู่ระหว่างดำเนินการตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	แผนการรับมือภัยคุกคามทางไซเบอร์			
๑๙.๑	ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ และกฎหมายย่อยใด ๆ ที่ทำขึ้นภายใต้กฎหมายดังกล่าว ตลอดจนภาระหน้าที่ในการรายงานภายใต้กฎหมาย และข้อกำหนดด้านกฎระเบียบที่เกี่ยวข้องกับโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ค) เกณฑ์และขั้นตอนในการเรียกใช้งาน (Activate) การตอบสนองต่อเหตุการณ์และ CIRT	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ง) ขั้นตอนจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(จ) การเรียกใช้งานกระบวนการกู้คืน (Recovery Process)	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ฉ) ขั้นตอนในการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ช) ขั้นตอนการเก็บรักษาหลักฐาน (Preservation of Evidence) ก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ซ) ระเบียบวิธีการมีส่วนร่วม (Engagement Protocols) กับบุคคลภายนอก หรือแนวปฏิบัติการบริหารจัดการบุคคลภายนอก ซึ่งรวมถึงรายละเอียดการติดต่อ ตัวอย่างเช่น ผู้ขายสำหรับบริการด้านนิติวิทยาศาสตร์/การกู้คืนและการบังคับใช้กฎหมายเพื่อดำเนินคดี และ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
๑๙.๒	ต้องตรวจสอบให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์ได้รับการสื่อสารอย่างมีประสิทธิผลไปยังบุคลากรที่เกี่ยวข้องทั้งหมดที่สนับสนุนบริการสำคัญของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
๑๙.๓	ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยนับแต่วันที่แผนได้รับการอนุมัติ	✓		อยู่ระหว่างดำเนินการตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
๑๙.๔	ต้องทบทวนแผนการรับมือภัยคุกคามทางไซเบอร์ เมื่อมีการเปลี่ยนแปลงอย่างมีนัยสำคัญในสภาพแวดล้อมการปฏิบัติการทางไซเบอร์ของบริการที่ สำคัญของหน่วยงานของรัฐและ หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ หรือข้อกำหนดในการตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	✓		อยู่ระหว่างดำเนินการตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

ลงชื่อ .....

(นายนิกร ศิรโรจนานนท์)

รองอธิบดีกรมป่าไม้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม

(DCIO) ของกรมป่าไม้

ภาคผนวก

ภาคผนวก ๑

แบบฟอร์มบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนองต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงานความคืบหน้าครั้งถัดไป :		

ภาคผนวก ๒

แบบฟอร์มบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)
ตัวอย่าง ๑๒/๑/๖๖ – ๐๙.๐๐ น.	*ทีมรับมือฯ ตรวจสอบพบภัยคุกคามลักษณะ Phishing ทำให้เกิด Ransomware เข้าสู่ระบบเครือข่ายภายในหน่วยงาน*

ภาคผนวก ๓

ข้อมูลที่ต้องแจ้ง

ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น
๑. ข้อมูลการประสานงาน ชื่อหน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม วันที่และเวลาที่แจ้ง
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล ตำแหน่งงาน ชื่อหน่วยงาน อีเมล โทรศัพท์ (ที่ทำงาน / มือถือ)
๔. ความต่อเนื่องของเหตุภัยคุกคาม ☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม
๕. ลักษณะภัยคุกคามทางไซเบอร์ ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงานหรือไม่ เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐) ☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข) ☐ ยังไม่สามารถระบุได้

๖. หมวดหมู่ของภัยคุกคาม (แจ้งได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)

* อ้างอิงหมวดหมู่ตามภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์ มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์แต่ละระดับ พ.ศ. ๒๕๖๔ (ทั้งนี้ ภัยคุกคามทางไซเบอร์หมวดหมู่ที่ ๐ หมวดหมู่ที่ ๑ และหมวดหมู่ที่ ๙ ไม่เข้าข่ายเป็นภัยคุกคามทางไซเบอร์ที่ต้องรายงาน)

ภาคผนวก ๔

แบบรายงานภัยคุกคามทางไซเบอร์

ส่วนที่ ๑

หมวด ก. ข้อมูลการประสานงานและผลการตรวจสอบภัยคุกคามเบื้องต้น

หมายเลขอ้างอิง (สำหรับเจ้าหน้าที่ สกมช.): โปรดระบุ

หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี): โปรดระบุ

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม

ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: โปรดระบุ

ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม

ชื่อ-นามสกุล: โปรดระบุ ตำแหน่งงาน: โปรดระบุ

ชื่อหน่วยงาน: โปรดระบุ อีเมล: โปรดระบุ

โทรศัพท์ (ที่ทำงาน / มือถือ) : โปรดระบุ

ก๓. ความต่อเนื่องของเหตุภัยคุกคาม

☐ เหตุภัยคุกคามใหม่ ☐ การรายงานข้อมูลต่อเนื่องจากเหตุภัยคุกคามเดิม

ก๔. ลักษณะภัยคุกคามทางไซเบอร์

ระบบที่ได้รับผลกระทบมีความสำคัญต่อพันธกิจหลักของหน่วยงาน

☐ ใช่ ☐ ไม่ใช่

เหตุการณ์ที่เกิดขึ้นเกิดจากภัยคุกคามทางไซเบอร์ ในระดับใด (มาตรา ๖๐)

☐ ไม่ร้ายแรง ☐ ร้ายแรง ☐ วิกฤต (ก) ☐ วิกฤต (ข)

☐ ยังไม่สามารถระบุได้

หมวด ข. ข้อมูลการตรวจพบภัยคุกคามไซเบอร์

ข๑. วัน เวลา ที่เกิดเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม

วันที่ : เลือกวันที่ เวลา : โปรดระบุ

ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ

☐ ยังไม่ได้แจ้ง ☐ แจ้งแล้ว _____

ข๓. หมวดหมู่ของภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

หมวดหมู่*	คำอธิบาย
☐ หมวดหมู่ที่ ๒	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)
☐ หมวดหมู่ที่ ๓	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยของหน่วยงาน (Non-Compliance Activity)
☐ หมวดหมู่ที่ ๔	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)
☐ หมวดหมู่ที่ ๕	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)
☐ หมวดหมู่ที่ ๖	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)
☐ หมวดหมู่ที่ ๗	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)
☐ หมวดหมู่ที่ ๘	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)
☐ อื่น ๆ	โปรดระบุ

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

ข๔. ข้อมูลเบื้องต้นเกี่ยวกับระบบคอมพิวเตอร์ คอมพิวเตอร์ บริการ หรือข้อมูลที่ได้รับผลกระทบ:

สถานที่ตั้งของเครื่อง ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น จังหวัด ตำบล ตึก ห้อง):

โปรดระบุ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ

ฮาร์ดแวร์ ซอฟต์แวร์ที่ได้รับผลกระทบ (โปรดระบุรายละเอียด เช่น ผู้ผลิตหรือยี่ห้อ รุ่นของเครื่องคอมพิวเตอร์): โปรดระบุรายละเอียด

มีผลกระทบต่อการสื่อสาร (ทางโทรศัพท์ หรือ การใช้งานเครือข่าย): โปรดระบุ

รายละเอียดอื่น ๆ: โปรดระบุ

หมวด ค: ข้อมูลการรับมือภัยคุกคาม

ค๑. สถานการณ์หรือการแก้ไขเหตุภัยคุกคาม (เลือกได้มากกว่า ๑ รายการ)

☐ เพิ่งพบเหตุการณ์ ☐ อยู่ในขั้นตอนการขอความช่วยเหลือ

☐ อยู่ในขั้นตอนการสอบสวน ☐ กำลังลุกลาม

☐ อยู่ในขั้นตอนการระงับภัย ☐ สามารถระงับภัยได้แล้ว

☐ รายงานปิดเหตุการณ์ภัยคุกคามแล้ว ☐ อื่น ๆ: โปรดระบุ

ค๒. สิ่งที่ได้ดำเนินการหรือได้แก้ไขไปแล้ว

☐ ยังไม่ได้ดำเนินการแก้ไขใด ๆ ☐ ยกเลิกการเชื่อมต่อระบบออกจากเครือข่ายแล้ว

☐ ตรวจสอบข้อมูลจราจร (Log) แล้ว ☐ ตรวจสอบโปรแกรม (แฟ้ม binaries/.exe) แล้ว

☐ กู้คืนกลับมาด้วยระบบหรือข้อมูลสำรองที่ตรวจสอบความถูกต้องแล้ว

☐ รายละเอียดการแก้ไขภัยคุกคามที่เกิดขึ้นเพิ่มเติม: โปรดระบุ

ค๓. รายละเอียดการรับมือภัยคุกคามอื่น ๆ (ถ้ามี)

โปรดระบุ

ส่วนที่ ๒

หมวด ง : รายละเอียดภัยคุกคาม

ง๑. ข้อมูลการตรวจจับและการวิเคราะห์

ง๑.๑ วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access)

วันที่: เลือกวันที่ **เวลา:** โปรดระบุ **ไม่ทราบ:** ☐

ง๑.๒ ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์

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

โปรดระบุ

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

โปรดระบุ

รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด):

โปรดระบุ

ง๑.๓ รายละเอียดผลกระทบจากเหตุภัยคุกคาม (ระบุผลกระทบที่มีเกิดขึ้นต่อ ระบบ คน หรือข้อมูล)

จำนวนระบบ บริการ หรือสินทรัพย์ที่เป็นโครงสร้างพื้นฐานสำคัญทางสารสนเทศที่ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

ทรัพย์สินที่สำคัญอื่น ๆ ที่อาจได้รับผลกระทบ: โปรดระบุ

จำนวนผู้ได้รับผลกระทบ (โดยประมาณ): โปรดระบุ

มูลค่าความเสียหาย (โดยประมาณ): โปรดระบุ

ในกรณีที่ข้อมูลที่ระบุตัวบุคคลได้รั่วไหล (หรือถูกขโมย):

จำนวนบุคคลที่เป็นเจ้าของข้อมูล : โปรดระบุ

ชนิดของข้อมูล (เลือกทุกข้อที่ใช่):

☐ ข้อมูลไบโอเมตริกซ์ ☐ ข้อมูลการติดต่อ

☐ ข้อมูลการเงิน ☐ ข้อมูลบุคลากรของรัฐ

☐ หมายเลขบัตรประชาชน ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ

☐ ข้อมูลทางการแพทย์

☐ อื่น ๆ : โปรดระบุ

จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ

ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

๑.๔ รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)

หมายเลข CVE: โปรดระบุ

ช่องโหว่ที่ถูกใช้จู่โจม: โปรดระบุ

การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อจู่โจมขยายผลไปยังระบบหรือเครื่องอื่น:
โปรดระบุ

อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า ๑ รายการ)

☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ

☐ บัญชีผู้ใช้ถูกสร้างขึ้นมาใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ

☐ การจู่โจมด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ

☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ)

☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ

☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ

☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย

☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง

☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก

☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย

☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ

☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ

☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การจู่โจมให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS)

☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ผิดปกติ

☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น

☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ

☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility)

☐ สิ่งที่ผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ

ง๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน **(เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)** โปรดระบุ
ง๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ
ง๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู
ง๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ
ง๒.๒ การคาดการณ์ความสามารถฟื้นฟู โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู
ง๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)
ง๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ
ง๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ
ง๓.๓ บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ

ภาคผนวก ๕

แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ ๑ สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์

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

ข้อ ๒ สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ ๓ สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์

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

ภาคผนวก ๕

ตัวอย่าง : รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)		
๑	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
๑.๑	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
๑.๒	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
๑.๓	ดำเนินการสืบค้นข้อมูล (เช่น search engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
๑.๔	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
๒	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
๓	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)		
๔	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
๕	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	
๖	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
๗	ทำการกำจัดสาเหตุ (Eradicate the incident)	
๗.๑	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
๗.๒	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
๗.๓	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (detection and analysis)	
๘	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	

รายการตรวจสอบการจัดการเหตุการณ์		Complete
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	