ประกาศกรมป่าไม้
เรื่อง แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศและข้อมูลของกรมป่าไม้ เป็นภารกิจสำคัญที่ต้องดำเนินการอย่างเป็นระบบ เพื่อให้สามารถป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุภัยคุกคามทางไซเบอร์ได้อย่างเหมาะสม ลดผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศ ข้อมูลสำคัญ และภารกิจของหน่วยงาน ตลอดจนสนับสนุนให้การดำเนินงานของกรมป่าไม้เป็นไปอย่างต่อเนื่อง มีประสิทธิภาพและเชื่อถือได้

เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้เป็นไปอย่างเหมาะสม สอดคล้องกับมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ซึ่งเป็นกรอบในการบริหารจัดการความมั่นคงปลอดภัยด้านไซเบอร์อย่างเป็นระบบ และอาศัยอำนาจตามความในมาตรา ๓๒ แห่งพระราชบัญญัติระเบียบบริหารราชการแผ่นดิน พ.ศ. ๒๕๓๔ และที่แก้ไขเพิ่มเติม กรมป่าไม้จึงกำหนดแผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ เพื่อให้หน่วยงานและบุคลากรในสังกัดถือปฏิบัติ กรมป่าไม้จึงประกาศไว้ ดังนี้

๑. ประกาศนี้เรียกว่า “แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้”

๒. การจัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑ เพื่อกำหนดแนวทางและขั้นตอนในการรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ให้เป็นระบบและมีประสิทธิภาพ

๒.๒ เพื่อเตรียมความพร้อมในการป้องกัน ตรวจจับ วิเคราะห์ และตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์ได้อย่างทันท่วงที

๒.๓ เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องในการบริหารจัดการเหตุการณ์ด้านไซเบอร์อย่างชัดเจน

๒.๔ เพื่อให้การดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ของกรมป่าไม้สอดคล้องกับกฎหมาย มาตรฐาน และแนวปฏิบัติที่เกี่ยวข้อง

๒.๕ เพื่อสร้างความเชื่อมั่นให้แก่ผู้ใช้งานและประชาชนว่าระบบสารสนเทศของกรมป่าไม้มีความปลอดภัย น่าเชื่อถือ และสามารถให้บริการได้อย่างต่อเนื่อง

๓. ให้หน่วยงานและบุคลากรในสังกัดกรมป่าไม้ถือปฏิบัติตามแผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้ รวมทั้งดำเนินการทบทวนและปรับปรุงแผนให้สอดคล้องกับสถานการณ์ภัยคุกคามทางไซเบอร์ เทคโนโลยี และกฎหมายที่เกี่ยวข้องอย่างต่อเนื่อง

๔. ให้ใช้แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้ ตามแนบท้ายประกาศนี้

๕. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

(นายนิกร ศิรโรจนานนท์)
อธิบดีกรมป่าไม้

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้

แนบท้ายประกาศกรมป่าไม้ ลงวันที่ ๒๙ พฤษภาคม พ.ศ. ๒๕๖๙

เรื่อง แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ กรมป่าไม้

คำนำ

ตามที่พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ ได้มีผลบังคับใช้ โดยมีวัตถุประสงค์เพื่อกำหนดนโยบาย มาตรการ และแนวทางในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงของรัฐ เศรษฐกิจ และการให้บริการสาธารณะของประเทศนั้น กรมป่าไม้ ในฐานะหน่วยงานของรัฐจึงมีหน้าที่ต้องดำเนินการให้สอดคล้องกับบทบัญญัติของกฎหมายดังกล่าว

ทั้งนี้ ตามมาตรา ๔๔ แห่งพระราชบัญญัติดังกล่าว กำหนดให้หน่วยงานของรัฐต้องจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สอดคล้องกับนโยบายและแผนระดับชาติ รวมถึงมาตรา ๕๘ ที่กำหนดให้หน่วยงานต้องมีการตรวจสอบ ประเมิน และดำเนินการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์อย่างเหมาะสม พร้อมทั้งรายงานเหตุการณ์ต่อหน่วยงานที่เกี่ยวข้องโดยเร็ว

นอกจากนี้ ยังต้องปฏิบัติตามประกาศและแนวทางที่ออกโดยคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ และหน่วยงานกำกับดูแลที่เกี่ยวข้อง เช่น หลักเกณฑ์และวิธีการรายงานภัยคุกคามทางไซเบอร์ ซึ่งกำหนดให้หน่วยงานของรัฐต้องมีการเฝ้าระวัง ตรวจสอบ และรายงานเหตุภัยคุกคามทางไซเบอร์อย่างเป็นระบบและทันเวลา

ดังนั้น กรมป่าไม้จึงได้จัดทำแผนรับมือเหตุภัยคุกคามทางไซเบอร์ฉบับนี้ขึ้น เพื่อใช้เป็นกรอบแนวทางในการป้องกัน ตรวจจับ ตอบสนอง และฟื้นฟูจากเหตุการณ์ด้านความมั่นคงปลอดภัยไซเบอร์อย่างมีประสิทธิภาพ สอดคล้องตามบทบัญญัติของกฎหมาย และมาตรฐานที่เกี่ยวข้อง อันจะช่วยลดความเสี่ยงและผลกระทบที่อาจเกิดขึ้นต่อระบบสารสนเทศและภารกิจหลักของหน่วยงาน

แผนฉบับนี้ยังมุ่งเน้นการเสริมสร้างความรู้ ความตระหนัก และความพร้อมของบุคลากรในการรับมือกับภัยคุกคามทางไซเบอร์ที่มีความซับซ้อนและเปลี่ยนแปลงอย่างรวดเร็ว เพื่อให้การดำเนินงานของกรมป่าไม้เป็นไปอย่างมั่นคง ปลอดภัย และสร้างความเชื่อมั่นให้แก่ประชาชนและผู้มีส่วนได้ส่วนเสียต่อไป

พฤษภาคม ๒๕๖๙

สารบัญ

แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

๑. หลักการและเหตุผล

แผนรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมป่าไม้ ฉบับนี้ จัดทำขึ้นเพื่อให้เป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.๒๕๖๒ ที่กำหนดให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์โดยเร็ว ซึ่งอย่างน้อยต้องประกอบด้วยเรื่อง (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง และ (๒) แผนการรับมือภัยคุกคามทางไซเบอร์ เพื่อรับมือกับภัยคุกคามทางไซเบอร์ที่มีรูปแบบการโจมตีแบบใหม่ๆ 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

รายละเอียดของเอกสาร (Document control)	
วันที่จัดทำเอกสาร (Date created)	๒๐ กุมภาพันธ์ ๒๕๖๘
ผู้ตรวจสอบความถูกต้องของเอกสาร (Last reviewed by)	ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
วันที่ตรวจสอบความถูกต้องของเอกสาร (Last date reviewed)	
ผู้อนุมัติเอกสาร และวันที่อนุมัติเอกสาร (Endorsed by and date)	รองอธิบดีกรมป่าไม้ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) ของกรมป่าไม้
วันที่จะต้องมีการตรวจสอบเอกสารครั้งถัดไป (Next review due date)	

๖.๒. การเปลี่ยนแปลงเอกสาร (Version control)

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

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 โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรม

ไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่อาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

๘.๓ ภัยคุกคามทางไซเบอร์ (Cyber threat) หมายความว่า การกระทำหรือการดำเนินการใด ๆ โดยมิชอบ โดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึง ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ 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 แฟลชไดรว์ติดไวรัส หรือไฟล์คอมพิวเตอร์ติดไวรัส เป็นต้น

๘.๗ หนอนคอมพิวเตอร์ (Computer Worm) เป็นมัลแวร์ชนิดหนึ่ง สามารถคัดลอกตัวเอง ติดตั้งตัวเองในเครื่องคอมพิวเตอร์อื่นๆ โดยที่เจ้าของเครื่องคอมพิวเตอร์ไม่อนุญาต โดยหนอนคอมพิวเตอร์จะต่างกับไวรัส ตรงที่ไวรัสจะแพร่กระจายตัวเองไปสู่เครื่องคอมพิวเตอร์เครื่องอื่น ๆ โดยอาศัยพาหะ แต่หนอนคอมพิวเตอร์จะใช้วิธีสแกนเครื่องคอมพิวเตอร์ที่อยู่ในระบบเครือข่ายและตรวจหาช่องโหว่ของระบบปฏิบัติการหรือช่องโหว่ของแอพพลิเคชั่น 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 ที่มีวัตถุประสงค์เพื่อบันทึกการกระทำของผู้ใช้บนเครื่องคอมพิวเตอร์และส่งผ่านอินเตอร์เน็ต โดยที่ผู้ใช้ไม่ได้รับทราบ โปรแกรมแอบดักข้อมูลนั้น สามารถรวบรวมข้อมูล สถิติการใช้งานจากผู้ใช้ได้หลายอย่างขึ้นอยู่กับการออกแบบของโปรแกรม ซึ่งส่วนใหญ่แล้วบันทึกเว็บไซต์ที่ผู้ใช้เข้าถึงและส่งไปยังบริษัทโฆษณาต่าง ๆ บางโปรแกรมอาจบันทึกว่าผู้ใช้พิมพ์อะไรบ้าง เพื่อพยายามค้นหารหัสผ่าน หรือเลขหมายบัตรเครดิต

๘.๑๐ ซอฟต์แวร์เรียกค่าไถ่ (Ransomware) เป็นมัลแวร์ชนิดหนึ่ง ที่มีพฤติกรรมเข้ารหัสไฟล์ต่างๆ ที่อยู่บนเครื่องคอมพิวเตอร์ไม่ว่าจะเป็นไฟล์เอกสาร รูปภาพ วิดีโอ ผู้ใช้งานจะไม่สามารถเปิดไฟล์ใด ๆ ได้เลย หากไฟล์

เหล่านั้นถูกเข้ารหัส ซึ่งการถูกเข้ารหัสก็หมายความว่าจะต้องใช้คีย์ในการปลอดล็อคเพื่อกู้ข้อมูลคืนมา 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 คือการหลอกลวงทางอินเตอร์เน็ต เพื่อขอข้อมูลที่สำคัญ เช่น รหัสผ่าน หรือหมายเลขบัตรเครดิต โดยการส่งข้อความผ่านทางอีเมลหรือเมสเซนเจอร์ ตัวอย่างของการฟิชชิง เช่น การบอกแก่ผู้รับปลายทางว่าเป็นธนาคารหรือบริษัทที่น่าเชื่อถือ และแจ้งว่ามีสาเหตุทำให้คุณต้องเข้าสู่ระบบ และใส่ข้อมูลที่สำคัญใหม่ โดยเว็บไซต์ที่ลิงก์ไปนั้น จะมีหน้าตาคล้ายคลึงกับเว็บที่กล่าวถึง

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

๙. บทบาทหน้าที่และโครงสร้างทีมรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

๙.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นายทนงศักดิ์ มนตรี	๒๔ ชั่วโมง/ ๗ วัน	๐๙ ๑๒๑๕ ๑๙๔๙	รับแจ้งเหตุ	ประสานหน่วยงานที่เกี่ยวข้อง
๒	นายวีร์ ศรีทิพโพธิ์	๒๔ ชั่วโมง/ ๗ วัน	๐๘ ๖๔๖๗ ๘๙๑๙	รับแจ้งเหตุ	ประสานหน่วยงานที่เกี่ยวข้อง
๓	นายณภัทร์ ดลเสถียร	๒๔ ชั่วโมง/ ๗ วัน	๐๙ ๕๗๑๓ ๓๐๘๐	รับแจ้งเหตุ	ประสานหน่วยงานที่เกี่ยวข้อง

๙.๒ โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT)

กรมป่าไม้ใช้โมเดลโครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ในลักษณะแบบรวมศูนย์ ประกอบด้วย

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	นางสาวสพินนา อ่อนเพ็ง	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ ๖๕๐๙	หัวหน้าทีมรับมือฯ (Team Manager)	ทำหน้าที่สื่อสารกับผู้บริหารของหน่วยงาน
๒	นายดำรงศักดิ์ ธนีบุญ	เบอร์โทรศัพท์มือถือ : ๐๘ ๐๙๘๔ ๔๒๕๒	รองหัวหน้าทีมรับมือฯ (Deputy Team Manager)	ทำหน้าที่แทนกรณีหัวหน้าทีมรับมือฯ ไม่อยู่/ไม่สามารถปฏิบัติงานได้
	นางสาวณัฏฐิณี ปิ่นเนียม	เบอร์โทรศัพท์มือถือ : ๐๙ ๐๙๗๑ ๘๐๘๑		
	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙		
	นายประพันธ์พงษ์ คงศรีรอด	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ ๔๓๙๑		
๓	นายวีร์ ศรีทิพโพธิ์	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ ๘๙๑๙	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือหน่วยงานเจ้าของระบบสารสนเทศให้สามารถควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์ได้
	นายณภัทร์ ดลเสถียร	เบอร์โทรศัพท์มือถือ : ๐๙ ๕๗๑๓ ๓๐๘๐		
	นายกิตติทัศน์ สุริยา	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ ๔๓๙๕		
	นางสาวปรียานุช กิจสิทธิโชค	เบอร์โทรศัพท์มือถือ : ๐๖ ๒๖๓๕ ๖๓๙๔		

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๔	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙	เจ้าหน้าที่เทคนิคฯ (Technical lead)	ทำหน้าที่ให้ความเห็นเกี่ยวกับแนวทางที่เหมาะสมในการควบคุมผลกระทบจากภัยคุกคามทางไซเบอร์
	นายประพันธ์พงษ์ คงศรีรอด	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ ๔๓๙๑		
	นายวีร์ ศรีทิพโพธิ์	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ ๘๙๑๙		
๕	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙	เจ้าหน้าที่ด้านการปฏิบัติตามกฎหมาย (Compliance)	ทำหน้าที่ตามนโยบาย แผนงาน และคำสั่งที่เกี่ยวข้อง
	นางสาวสพินนา อ่อนเพ็ง	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ ๖๕๐๙		
	นางสาวณัฏฐิณี ปิ่นเนียม	เบอร์โทรศัพท์มือถือ : ๐๙ ๐๙๗๑ ๘๐๘๑		
	นายประพันธ์พงษ์ คงศรีรอด	เบอร์โทรศัพท์มือถือ : ๐๖ ๓๙๐๖ ๔๓๙๑		
๖	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙	ผู้ทดสอบเจาะระบบ	ทำหน้าที่ตามนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน
	นายวีร์ ศรีทิพโพธิ์	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ ๘๙๑๙		
	นายณภัทร์ ดลเสถียร	เบอร์โทรศัพท์มือถือ : ๐๙ ๕๗๑๓ ๓๐๘๐		
๗	ผู้อำนวยการกลุ่มนิติการ	โทรศัพท์ : ๐๒๕๖๑๔๒๙๒ ต่อ ๕๖๗๐	ผู้เชี่ยวชาญด้านกฎหมาย	-ทำหน้าที่ตามนโยบาย แผนงาน และคำสั่งที่เกี่ยวข้อง - แจ้งความดำเนินคดีและรายงานเหตุภัยคุกคามทางไซเบอร์
๘	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙	ผู้บริหารจัดการความเสี่ยง	- ทำหน้าที่ตามนโยบาย แผนงาน และคำสั่งที่เกี่ยวข้อง

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๙	นายทนงศักดิ์ มนตรี	เบอร์โทรศัพท์มือถือ : ๐๙ ๑๒๑๕ ๑๙๔๙	ประเมินความเสี่ยงและผลกระทบ	- ทำหน้าที่ประเมินผลกระทบความเสี่ยงเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์
	นายวีร์ ศรีทิพโพธิ์	เบอร์โทรศัพท์มือถือ : ๐๘ ๖๔๖๗ ๘๙๑๙		
๑๐	ผู้อำนวยการส่วนประชาสัมพันธ์และเผยแพร่	เบอร์โทรศัพท์มือถือ : ๐๙ ๒๘๕๒ ๕๖๖๙	ผู้รับผิดชอบด้านสื่อสารองค์กร	ประชาสัมพันธ์ไปยังผู้มีส่วนได้ส่วนเสียเกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ นอกจากทีมรับมือฯ ดังกล่าวข้างต้น ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ดังนี้

ตารางที่ ๒ ทีมสนับสนุนรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๑	ผู้อำนวยการสำนักบริหารกลาง	โทรศัพท์: ๐-๒๕๖๑-๔๒๙๒-๓ ต่อ ๕๘๔๒	สำนักบริหารกลาง	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๒	ผู้อำนวยการสำนักป้องกันรักษาป่าและควบคุมไฟป่า	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒ ต่อ ๕๐๕๑	สำนักป้องกันรักษาป่าและควบคุมไฟป่า	
๓	ผู้อำนวยการสำนักจัดการป่าชุมชน	โทรศัพท์: ๐๒-๕๗๙-๗๕๘๕	สำนักจัดการป่าชุมชน	
๔	ผู้อำนวยการสำนักวิจัยและพัฒนาการป่าไม้	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒ ต่อ ๕๔๗๔	สำนักวิจัยและพัฒนาการป่าไม้	
๕	ผู้อำนวยการสำนักส่งเสริมการปลูกป่า	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒-๓ ต่อ ๕๕๒๙	สำนักส่งเสริมการปลูกป่า	

๖	ผู้อำนวยการสำนักจัดการที่ดินป่าไม้	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒-๓ ต่อ ๕๗๓๒, ๕๗๕๗	สำนักจัดการที่ดินป่าไม้	

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	ความรับผิดชอบ
๗	ผู้อำนวยการสำนักแผนงานและสารสนเทศ	โทรศัพท์: ๐-๒๕๖๑-๔๒๙๒-๓ ต่อ ๕๖๗๑	สำนักแผนงานและสารสนเทศ	ทำหน้าที่ควบคุมผลกระทบจากภัยคุกคาม
๘	ผู้อำนวยการกองกาอนุญาต	โทรศัพท์: ๐-๒๕๖๑-๔๒๙๒-๓ ต่อ ๕๒๐๙	กองการอนุญาต	
๙	ผู้อำนวยการสำนักเศรษฐกิจการป่าไม้	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒-๓ ต่อ ๕๒๔๙	สำนักเศรษฐกิจการป่าไม้	
๑๐	ผู้อำนวยการสำนักจัดการป่านันทนาการ	โทรศัพท์: ๐๒-๕๖๑๔๒๙๒-๓ ต่อ ๕๕๓๔	สำนักจัดการป่านันทนาการ	

๙.๓ หน่วยงานภายนอกที่เกี่ยวข้อง

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
๑	สำนักงานคณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ National Cyber Security Agency - NCSA	๑. อีเมล: saraban@ncsa.or.th ๒. โทรศัพท์. ๐๒ ๑๔๒ ๖๘๘๘	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ
๒	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team – ThaiCERT)	๑.อีเมล : thaicert@ncsa.or.th ๒. โทรศัพท์ ๐๒-๑๑๔-๓๕๓๑ (๒๔ ชั่วโมง)	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	เป็นหน่วยงานรับผิดชอบงานตามพระราชบัญญัติ
๓	ศูนย์เทคโนโลยีดิจิทัลและอากาศยานสำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและ	โทรศัพท์ ๐ ๒๒๖๕ ๖๒๔๗	สำนักงานปลัดกระทรวงทรัพยากรธรรมชาติและสิ่งแวดล้อม	หน่วยงานกำกับดูแล

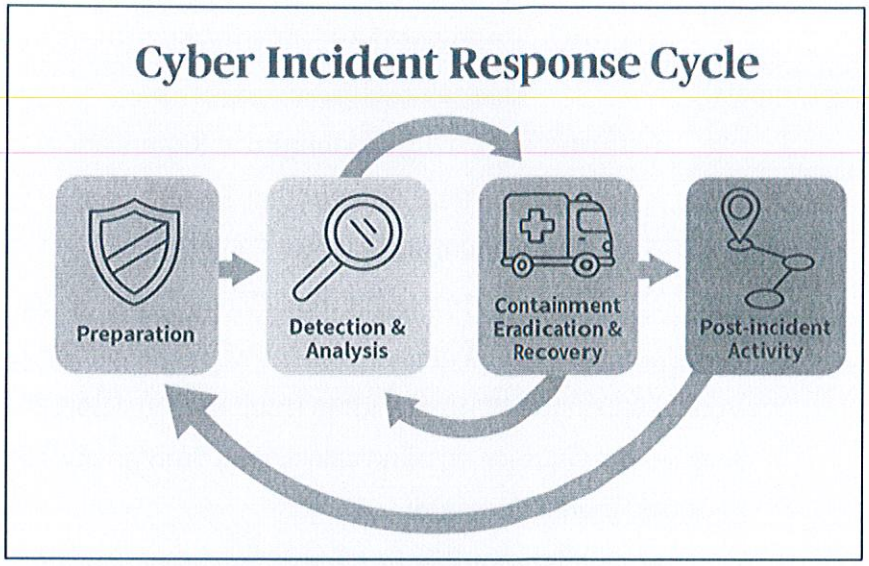
ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
	สิ่งแวดล้อม			
๔	นายเกรียงไกร อัศวรักษ์	เบอร์โทรศัพท์มือถือ : ๐๙ ๓๑๓๘ ๖๙๖๙	บริษัท อินเทอร์แอคทีฟ อินฟอร์เมชั่น ซิสเต็มส์ จำกัด	บริษัทรับจ้างบำรุงรักษาระบบงาน
๕	นางสาวสพินนา อ่อนเพ็ง	เบอร์โทรศัพท์มือถือ : ๐๙ ๗๐๐๓ ๖๕๐๙	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (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 และอุปกรณ์เครือข่ายให้มีความมั่นคงปลอดภัย 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

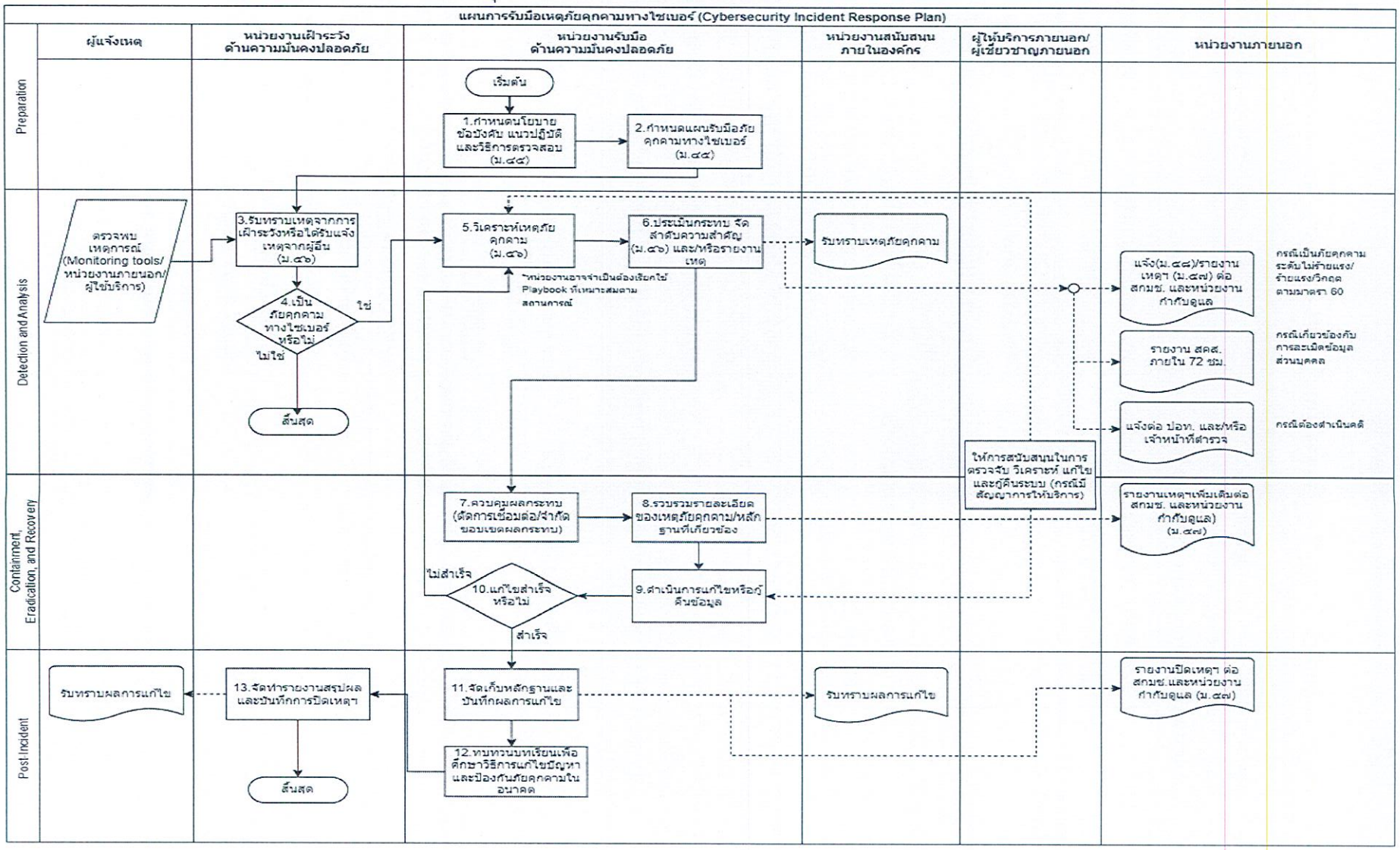
๑๐.๑.๑๑ จัดเตรียมห้องประชุม

๑๐.๑.๑๒ จัดเตรียมสถานที่จัดเก็บหลักฐาน ข้อมูลและพยานอื่นๆ ที่สำคัญ

๑๐.๑.๑๓ จัดทำแผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ของกรมป่าไม้ ดังภาพที่ ๒

แผนการรับมือเหตุภัยคุกคามทางไซเบอร์และขั้นตอนการรับมือภัยคุกคามแต่ละประเภท

ภาพที่ ๒ แผนผังโครงสร้างขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ของกรมป่าไม้



คำอธิบายแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

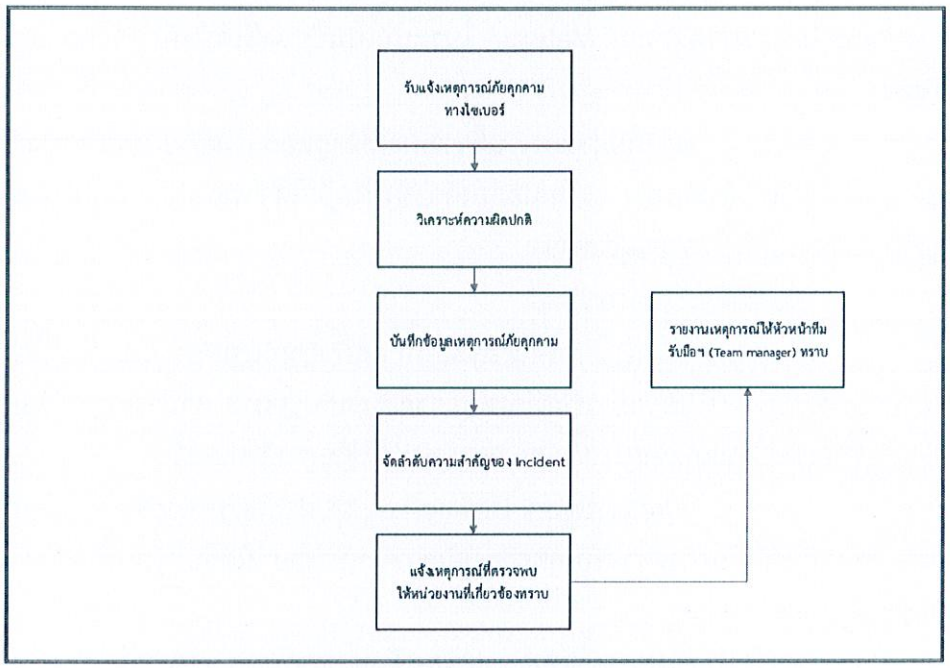
ลำดับ	หัวข้อ	คำอธิบาย
ขั้นตอนการเตรียมการ (Preparation)		
๑	กำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย ร่วมกับผู้บริหารของหน่วยงานกำหนดนโยบาย ข้อบังคับ แนวปฏิบัติ และวิธีการตรวจสอบด้านความมั่นคงปลอดภัย โดยสอดคล้องตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (ตามมาตรา ๑๓ วรรคหนึ่ง (๔))
๒	กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ (ม.๔๕)	หน่วยงานรับมือด้านความมั่นคงปลอดภัย กำหนดแผนรับมือภัยคุกคามทางไซเบอร์ โดยระบุภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับหน่วยงาน กำหนดขั้นตอนและวิธีการในการรับมือกับเหตุการณ์ภัยคุกคามทางไซเบอร์ กำหนดผู้รับผิดชอบในแต่ละขั้นตอน และกำหนดให้มีการทดสอบแผนรับมือภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ
ขั้นตอนการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)		
๓	รับทราบเหตุจากการเฝ้าระวังหรือได้รับแจ้งเหตุจากผู้อื่น (ม.๕๖)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ได้รับทราบเหตุจากการเฝ้าระวัง (Monitoring Tools) หรือได้รับแจ้งเหตุจากผู้อื่นที่ตรวจพบเหตุการณ์ เช่น หน่วยงานภายนอกหรือผู้ใช้บริการ
๔	เป็นภัยคุกคามทางไซเบอร์หรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาเหตุการณ์ว่าเป็นภัยคุกคามทางไซเบอร์หรือไม่
๕	วิเคราะห์เหตุภัยคุกคาม	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาประเภทของภัยคุกคาม หมวดหมู่ของภัยคุกคาม รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม ข้อมูล จำนวนระบบ บริการ หรือสินทรัพย์ที่ได้รับผลกระทบ
๖	ประเมินกระทบ และจัดลำดับความสำคัญ (ม.๕๖)	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ดำเนินการประเมินกระทบ และจัดลำดับความสำคัญของเหตุภัยคุกคาม รวมถึงเลือกแนวทางในการรับมือกับเหตุภัยคุกคามทางไซเบอร์

ลำดับ	หัวข้อ	คำอธิบาย
		หมายเหตุ: หน่วยงานอาจจำเป็นต้องเรียกใช้ Playbook ที่เหมาะสมตามสถานการณ์ ๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุภัยคุกคามทางไซเบอร์ต่อหน่วยงานต่าง ๆ ■ กรณีเป็นภัยคุกคามระดับไม่ร้ายแรง/ร้ายแรง/วิกฤตตามมาตรา ๖๐ หน่วยงานต้องแจ้งเหตุภัยคุกคาม (มาตรา ๕๘) (แบบฟอร์ม ก.๑ หรือมีข้อมูลเทียบเท่า) และ/หรือรายงานเหตุภัยคุกคาม (มาตรา ๕๗) (แบบฟอร์ม ก.๒) ต่อ สกมช. และหน่วยงานกำกับดูแล ■ กรณีเกี่ยวข้องกับการละเมิดข้อมูลส่วนบุคคล หน่วยงานอาจต้องแจ้งไปยัง สคส. ■ กรณีมีความจำเป็นต้องดำเนินคดีเนื่องจากเหตุนั้นเหตุนั้นเข้าลักษณะเป็นความผิดตามประมวลกฎหมายอาญา หรือพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และที่แก้ไข เพิ่มเติม (ถ้ามี) หรือกฎหมายอื่น ๆ ที่เกี่ยวข้อง หน่วยงานอาจต้องแจ้งไปยัง ปอท. และ/หรือเจ้าหน้าที่ตำรวจ เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้น
ขั้นตอนการระงับภัยคุกคาม ปราบปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery)		
๗	ควบคุมผลกระทบ (ตัดการเชื่อมต่อ/จำกัดขอบเขตผลกระทบ)	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย ควรจำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ ทำการกำจัดสาเหตุ (Eradicate The Incident) กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคาม อื่น ๆ
๘	รวบรวมรายละเอียดของเหตุภัยคุกคาม/หลักฐานที่เกี่ยวข้อง	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย บันทึกเหตุการณ์ และดำเนินการจัดเก็บรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืน ซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์ อื่น ๆ เพื่อสนับสนุนการสอบสวน

ลำดับ	หัวข้อ	คำอธิบาย
		๒. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย รายงานเหตุการณ์เพิ่มเติมต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๙	ดำเนินการแก้ไขหรือกู้คืนข้อมูล	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เรียกใช้งานกระบวนการกู้คืน (Recovery Process)
๑๐	แก้ไขสำเร็จหรือไม่	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย พิจารณาว่าระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งานแล้วหรือไม่ หากยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ ให้ดำเนินการต่อที่ขั้นตอนที่ ๑๑ หากยังไม่สามารถแก้ไขได้ ให้ดำเนินการขั้นตอนที่ ๕ ซ้ำเพื่อวิเคราะห์ภัยคุกคามทางไซเบอร์อีกครั้ง
ขั้นตอนการดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๑๑	จัดเก็บหลักฐานและบันทึกผลการแก้ไข	๑. หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย เก็บรักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี ๒. บันทึกผลการแก้ไขเหตุภัยคุกคามและวิธีการแก้ไขเพื่อจัดเก็บเป็นบทเรียน ๓. รายงานปิดเหตุการณ์ต่อ สกมช. และหน่วยงานกำกับดูแล (ม.๕๗) (แบบฟอร์ม ก.๒)
๑๒	ทบทวนบทเรียนเพื่อศึกษาวิธีการแก้ไขปัญหา และป้องกันภัยคุกคามในอนาคต	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว และกำหนดแนวทางในการป้องกันการเกิดเหตุซ้ำ หรือป้องกันภัยคุกคาม อื่น ๆ ที่มีลักษณะคล้ายคลึงกันในอนาคต
๑๓	จัดทำรายงานสรุปผลและบันทึกการปิดเหตุฯ	หน่วยงานเฝ้าระวังด้านความมั่นคงปลอดภัย จัดทำรายงานสรุปผลและบันทึกการปิดเหตุการณ์ รวมถึงแจ้งผลการแก้ไขไปยังผู้เกี่ยวข้องให้รับทราบ

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) จึงเป็นสิ่งจำปนที่จะช่วยให้หน่วยงานสามารถบรรเทาความเสี่ยงที่ยังคงเหลืออยู่ และสามารถแจ้งเตือนได้อย่างทัน ทวงทีเมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้น

๑๐.๒.๑ การตรวจจับ Incident จะขึ้นอยู่กับระบบงานที่ใช้อยู่ รูปแบบของความพยายามโจมตี และกลไกใน การปกป้องระบบ เพราะระบบการป้องกันจะแจ้งเตือน (Alert) หรือเก็บบันทึกข้อมูล (Log) เพื่อใช้ในการวิเคราะห์ หาความผิดปกติและมีการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบ ลักษณะของข้อมูลแจ้งเตือนที่ใช้ในการตรวจจับแบ่งได้เป็น ๒ ประเภท

- Precursor เป็นข้อมูลบ่งบอกว่า Incident จะเกิดขึ้นในอนาคต

- Indicator เป็นข้อมูลบ่งบอกว่า Incident ได้เคยเกิดขึ้นหรือกำลังเกิดขึ้นอยู่

อุปกรณ์ที่ใช้เพื่อการป้องกันและตรวจจับต้องพิจารณาตามความเหมาะสมกับระบบที่ต้องการ ป้องกันและต้องทำการปรับ Fine Tune เพื่อให้มีความเหมาะสมกับสภาพการใช้งานของระบบนั้น ๆ ซึ่งข้อมูลการแจ้งเตือนเพื่อตรวจจับการบุกรุกระบบคอมพิวเตอร์และเครือข่ายมีดังนี้

๑๐.๒.๑.๑ ประเภท Alert

๑) IPS ระบบที่ทำหน้าที่ตรวจจับและป้องกันการโจมตีในระบบเครือข่าย มีการแจ้งเตือน เมื่อพบสิ่งที่ตรงกับวิธีการโจมตีที่ระบบรู้จัก

๒) Anti-Malware ทำหน้าที่ตรวจจับโปรแกรมประสงค์ร้าย ทำงานทั้งในระดับเครือข่าย และ 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 ที่ใช้ในการ วิเคราะห์

๑๐.๒.๑.๓ ข้อมูลจากแหล่งสาธารณะข้อมูลช่องโหว่และวิธีการโจมตีระบบรูปแบบใหม่สามารถถูกใช้เป็น ข้อบ่งชี้ภัยคุกคามได้

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 ทำการดักจับข้อมูลทางเครือข่ายเพื่อนำมาวิเคราะห์ ข้อมูล

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) ที่ทำให้เกิดความขัดข้องหรือเสียหาย ต่อธุรกิจ ซึ่งหากไม่ได้รับการแก้ไขโดยเร็วอาจจะมีผลเสียมากยิ่งขึ้น โดยระดับของ 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 หรือทำลายโดยไม่ได้ รับอนุญาต

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 ต้องใช้ทรัพยากรและความช่วยเหลือ จากภายนอก ๙
- Not Recoverable การกู้คืนไม่สามารถทำได้ ใช้กับสถานการณ์ที่ข้อมูลได้รั่วไหลสู่สาธารณะแล้ว เป็นต้น ให้ใช้วิธีการติดตามและจำกัดการแพร่กระจายรวมถึงการเยียวยาผลกระทบ

๑๐.๒.๔ เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ ให้ทีมรับแจ้งเหตุบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ตามแบบฟอร์มบันทึกรายงานสถานการณ์เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ ในภาคผนวก ๑

๑๐.๒.๕ เมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ได้จัดให้มีการจัดทำบันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation) โดยบันทึกข้อมูลเกี่ยวกับเหตุการณ์ความปลอดภัยทางไซเบอร์ทุกขั้นตอนตั้งแต่ตรวจพบเหตุการณ์จนถึงกระบวนการสุดท้าย 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 การรับมือภัยคุกคาม การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication, and Recovery)

เมื่อมีภัยคุกคามทางไซเบอร์เกิดขึ้นหรือ ทีมรับมือจะดำเนินการดังนี้ เพื่อให้สอดคลองกับความรุนแรง และระดับของภัยคุกคามทางไซเบอร์แต่ละระดับ จนกระทั่งสามารถกูคืนทรัพยสินสำคัญทางสารสนเทศให้กลับมาดำเนินงานหรือให้บริการได้ตามปกติ

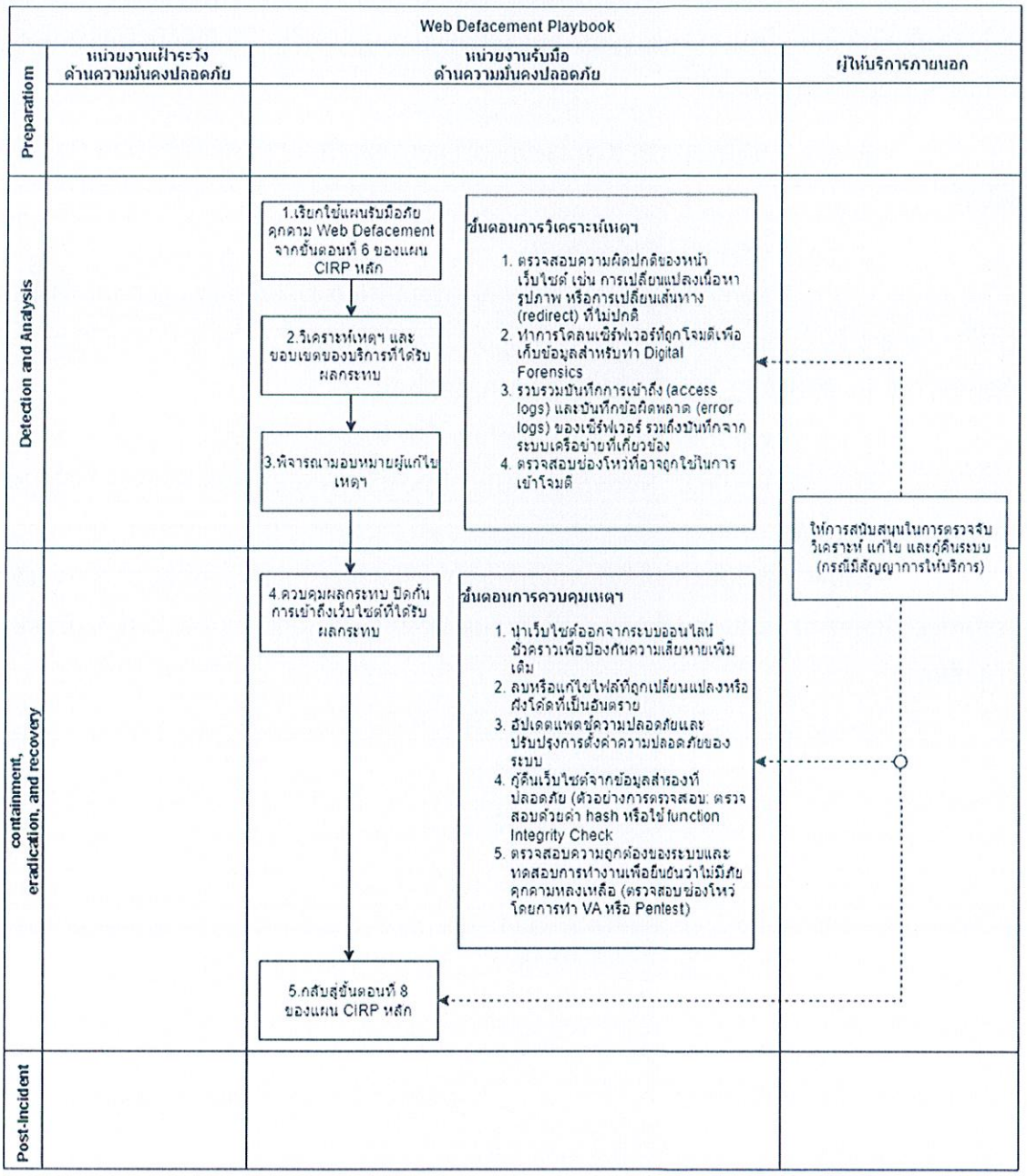
๑๐.๓.๑ จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

- 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

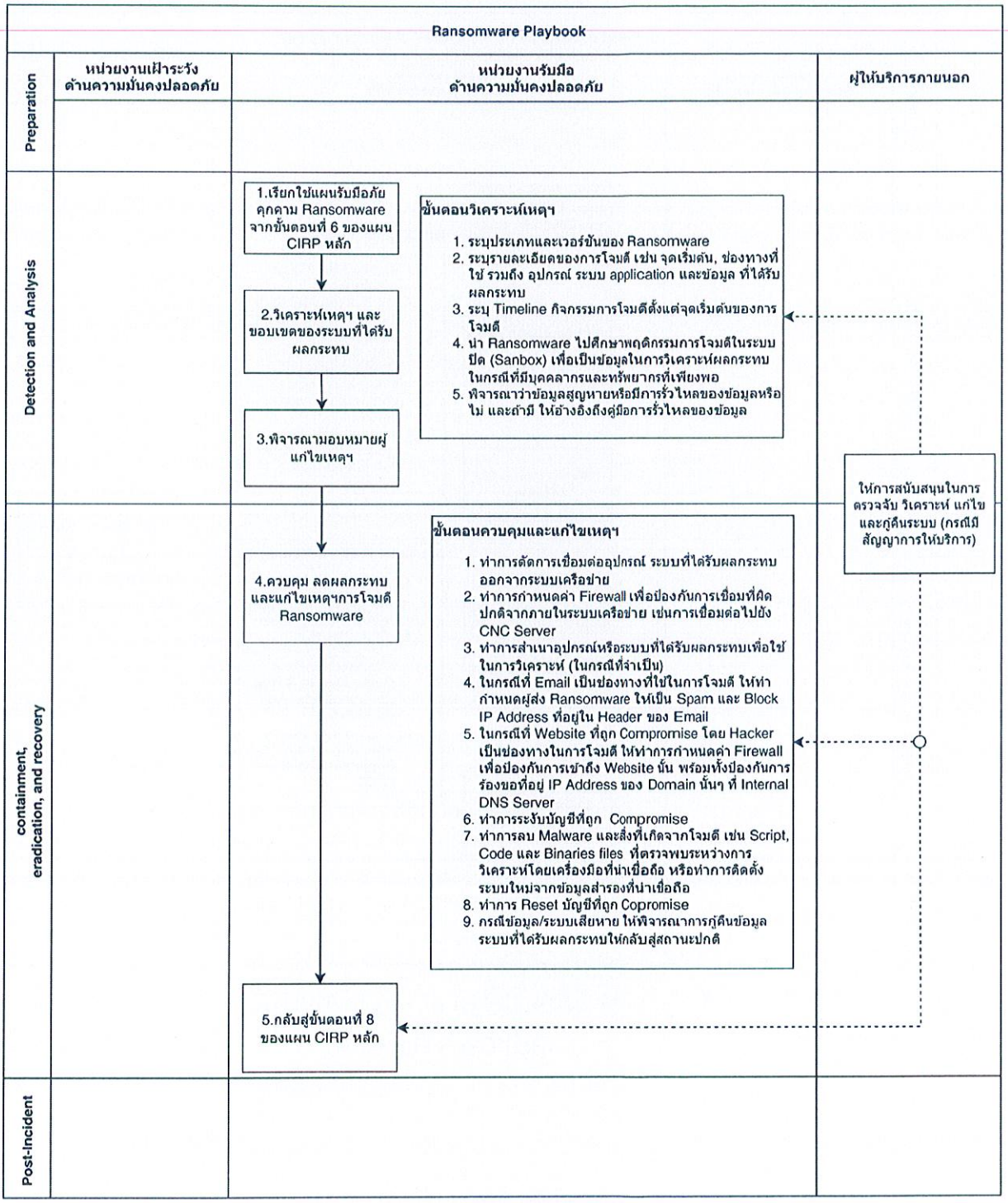
๑๐.๓.๒ ขั้นตอนการรับมือภัยคุกคาม ที่ส่งผลกระทบต่อระบบสารสนเทศและระบบเครือข่าย ดังนี้

๑๐.๓.๒.๑ ขั้นตอนการรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook) ดังภาพที่ ๔



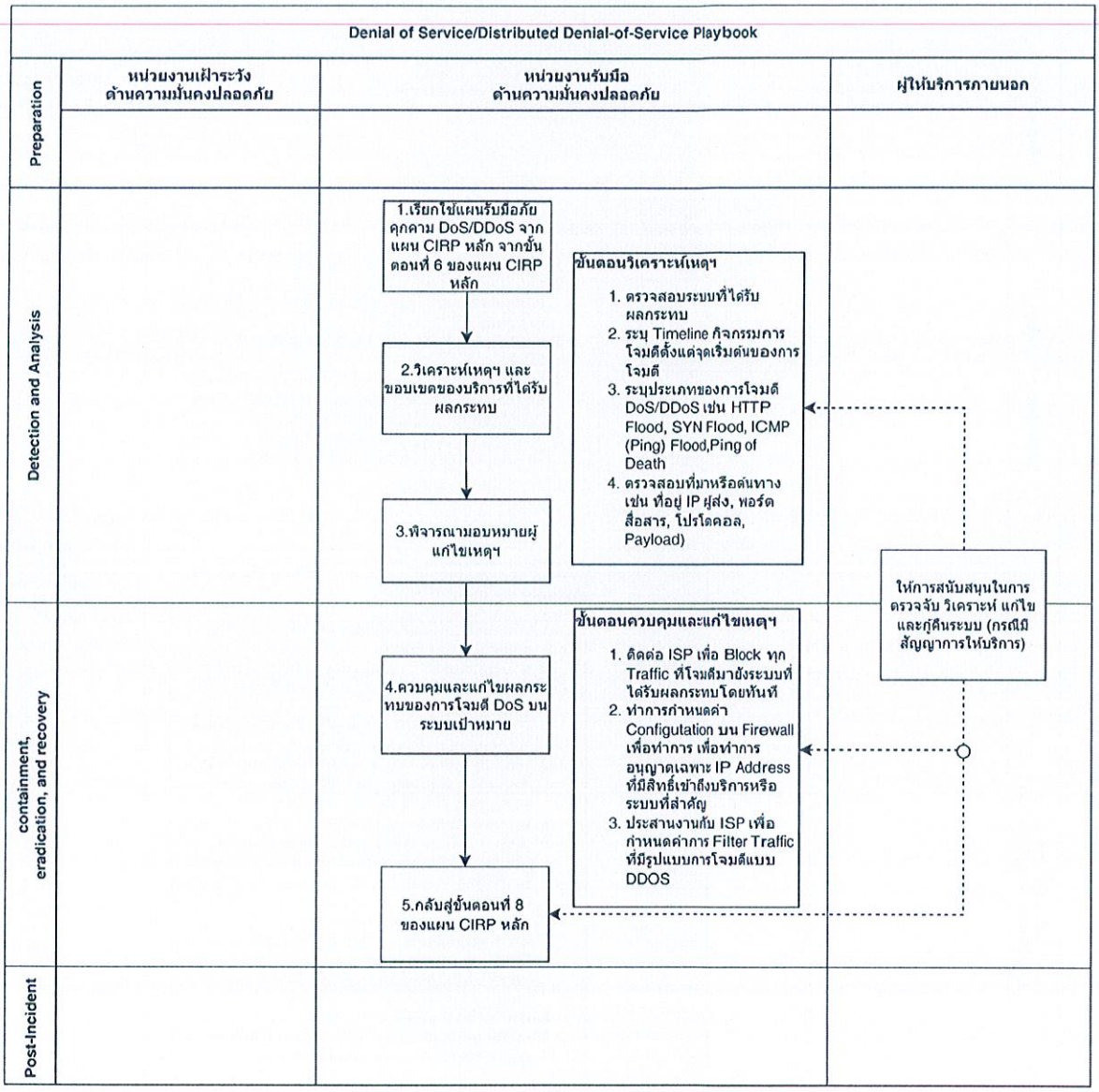
ภาพที่ ๔ การรับมือภัยคุกคามแบบ Web Defacement (Web Defacement Playbook)

๑๐.๓.๒.๒ ขั้นตอนการรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook) ดังภาพที่ ๕



ภาพที่ ๕ การรับมือภัยคุกคามแบบ Ransomware (Ransomware Playbook)

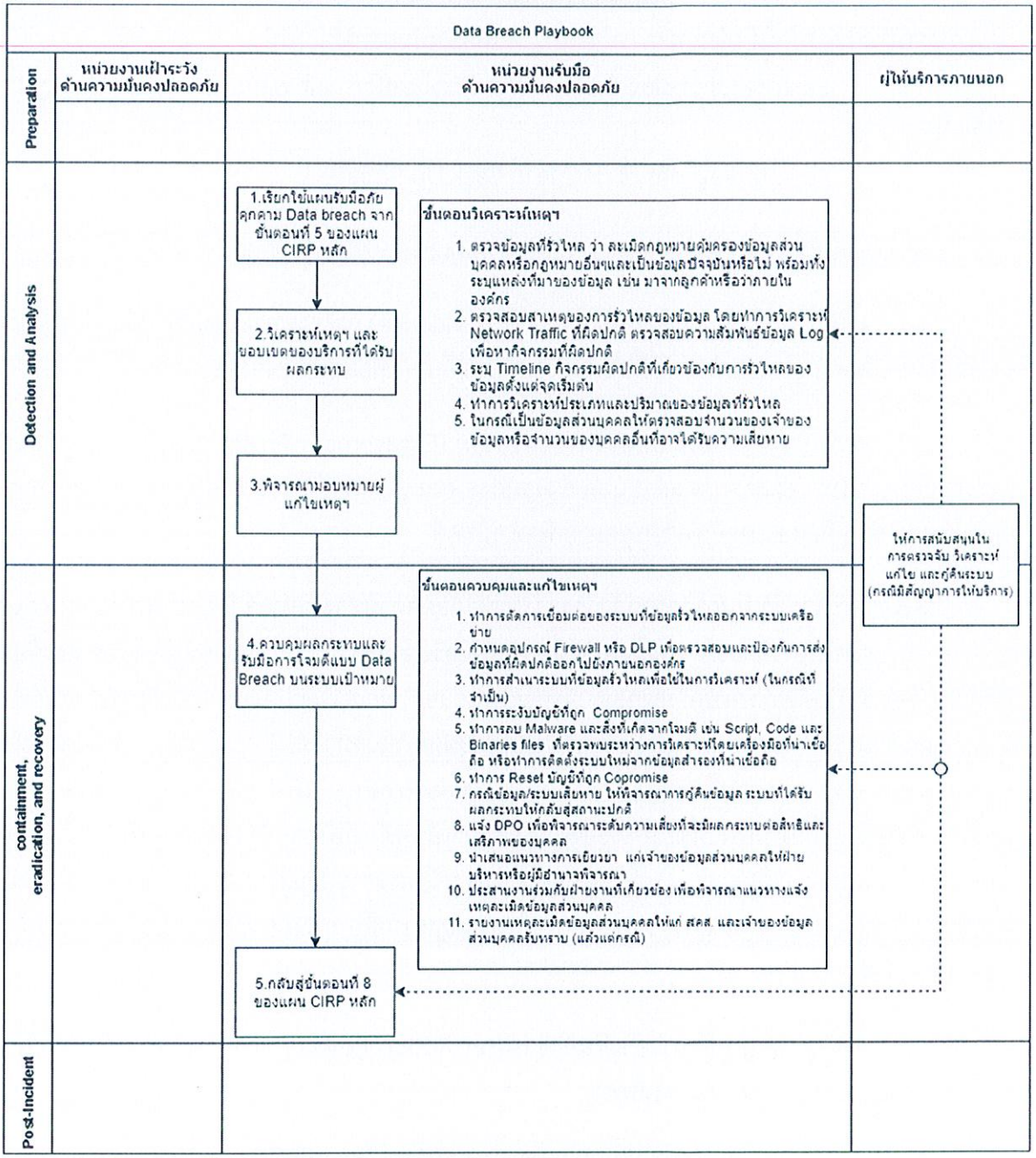
๑๐.๓.๒.๓ ขั้นตอนการรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook) ดังภาพที่ ๖



ภาพที่ ๖ การรับมือภัยคุกคามแบบ Denial of Service/Distributed Denial-of-Service (DoS/DDoS Playbook)

๑๐.๓.๒.๔ ขั้นตอนการรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)

ดังภาพที่ ๗



ภาพที่ ๗ การรับมือภัยคุกคามแบบ Data Breach (Data Breach Playbook)

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 หรือกำหนดนโยบายภายในที่เกี่ยวข้องเพื่อให้มีแนวทางที่ชัดเจน ซึ่งการปฏิบัติตามมาตรการดังกล่าว จะช่วยให้หน่วยงานสามารถเรียนรู้จากเหตุภัยคุกคามทางไซเบอร์ที่ผ่านมา และสามารถหาแนวทางเพื่อแก้ไข จุดบกพร่องและพัฒนาแนวทางรับมือกับภัยคุกคามทางไซเบอร์ต่อไปในอนาคต นอกจากนี้หน่วยงานต้องเก็บ รักษาข้อมูลและพยานหลักฐานที่จำเป็น เพื่อใช้ในกระบวนการทางนิติวิทยาศาสตร์ หรือใช้ในกรณีที่ต้องการร้องทุกข์หรือดำเนินคดี เนื่องจากภัยคุกคามทางไซเบอร์ที่เกิดขึ้นนั้นอาจเข้าลักษณะเป็นความผิดตามประมวล 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 โดยให้แล้วเสร็จภายในวันที่ ๑๕ กันยายน ๒๕๖๖ ทั้งนี้ สำนักงานจะได้พิจารณาแจ้งให้หน่วยงานได้ดำเนินการจัดทำในส่วนของกรอบมาตรฐานเป็นลำดับต่อไป

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

๔. การประเมินความสอดคล้องนี้ หน่วยงานจำเป็นต้องอ้างถึงหลักฐานที่ชัดเจนว่าได้มีการดำเนินการอย่างไร พร้อมแนบหลักฐานดังกล่าวมายังสำนักงาน ทั้งนี้ หน่วยงานของท่านอาจพิจารณาปิด (Masking) ส่วนของข้อมูลที่มีความอ่อนไหว (Sensitive Data) ได้ และการประเมินโดยหน่วยงานของท่านเป็นเพียงการประเมินขั้นต้นเท่านั้น ยังไม่ถือว่าได้มีการจัดทำแผนรับมือฯ สอดคล้องกับประกาศดังกล่าวข้างต้น จนกว่าสำนักงานจะได้ตรวจสอบแล้วเสร็จ และแจ้งเป็นหนังสือรับรองกลับไปยังหน่วยงานเป็นลายลักษณ์อักษรแล้วเท่านั้น

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	แผนการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์			
๑๗.๑	ต้องจัดให้มีการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์โดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศทั้งโดยผู้ตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระภายนอก อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง โดยมีขอบเขตของการตรวจสอบ ดังนี้	✓		กรมป่าไม้ได้มีหนังสือ ที่ ลงวันที่ เรื่องขอความอนุเคราะห์ (สกมช.) ดำเนินการตรวจสอบช่องโหว่
	(ก) กระบวนการจัดทำและผลการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA)	✓		- แผนบริหารควมเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๖ ลิ้ง :https://shorturl.at/ckyPZ - แผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๖๖ (Business Continuity Plan: BCP) ลิ้ง:https://shorturl.at/ruyQV - แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) ลิ้ง:https://shorturl.at/ejlyQ
	(ข) บริการที่สำคัญที่หน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศเป็นเจ้าของและใช้บริการ ตามผลการวิเคราะห์ในข้อ (ก)	✓		- ตามแผนบริหารควมเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมป่าไม้ ปีงบประมาณ พ.ศ. ๒๕๖๖ ลิ้ง :https://shorturl.at/ckyPZ
	(ค) การปฏิบัติตามพระราชบัญญัตินี้ และประมวลแนวทางปฏิบัตินี้และหลักปฏิบัติใด ๆ ที่เกี่ยวข้องกับประมวลแนวทางปฏิบัติ มาตรฐานการปฏิบัติงาน และที่คณะกรรมการประกาศกำหนด	✓		ตามเอกสารฉบับนี้ ประกอบด้วย - แนวทางการตรวจสอบด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
๑๗.๒	หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดส่งผลสรุปรายงานการตรวจสอบด้านความมั่นคงปลอดภัยไซเบอร์ต่อสำนักงานภายในกำหนด ๓๐ (สามสิบ) วันนับแต่วันที่ดำเนินการแล้วเสร็จตามที่กำหนดไว้ในมาตรา ๕๔ พร้อมทั้งส่งสำเนาให้หน่วยงานควบคุมหรือกำกับดูแลด้วย		✓	-
๑๗.๓	ในกรณีที่การตรวจสอบดำเนินการภายใต้มาตรา ๕๔ ระบุการไม่ปฏิบัติตามข้อ ๑๗.๑ เว้นแต่ กกม. จะระบุเป็นลายลักษณ์อักษรเป็นอย่างอื่น ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศส่งแผนการดำเนินการแก้ไขไปยังสำนักงานภายในกำหนด 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 ตามที่ระบุไว้ในนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคง	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	ปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้ครอบคลุมเรื่องโครงสร้างองค์กรและบทบาทหน้าที่ของผู้ที่เกี่ยวข้องในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ และต้องนำนโยบายดังกล่าวมาจัดทำระเบียบวิธีปฏิบัติและกระบวนการในการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ โดยต้องจัดให้มีการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง ต้องประกอบด้วยรายละเอียดอย่างน้อย ดังต่อไปนี้			
๑๘.๑	การประเมินความเสี่ยง (Risk Assessment)			
	(ก) การระบุความเสี่ยง (Risk Identification) ต้องระบุถึงความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ซึ่งรวมถึงความเสี่ยงจากภัยคุกคามทางไซเบอร์และช่องโหว่ต่าง ๆ โดยความเสี่ยงดังกล่าวอาจมีสาเหตุมาจากกระบวนการปฏิบัติงาน ระบบงาน บุคลากร หรือปัจจัยภายนอก	✓		ตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	(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 เพื่อให้ความเสี่ยงที่	✓		ตามเอกสารในฉบับนี้

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	เหลืออยู่ (Residual Risk) อยู่ในระดับความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ที่ยอมรับได้ โดยต้องคำนึงถึงความสมดุลระหว่างต้นทุนในการป้องกันความเสี่ยงและผลประโยชน์ที่คาดว่าจะได้รับ			- 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	✓		อยู่ระหว่างดำเนินการตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	ทั้งนี้ ต้องทบทวนระเบียบวิธีปฏิบัติและกระบวนการบริหารความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง และทุกครั้งที่มีการเปลี่ยนแปลงอย่างมีนัยสำคัญ เช่น กรณีที่มีการเปลี่ยนแปลงของระบบความมั่นคงปลอดภัยไซเบอร์ ความเสี่ยง มาตรฐานสากล อย่างมีนัยสำคัญ เป็นต้น	✓		อยู่ระหว่างดำเนินการตามเอกสารในฉบับนี้ - แนวทางปฏิบัติการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
	แผนการรับมือภัยคุกคามทางไซเบอร์			
๑๙.๑	ต้องจัดทำแผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ที่กำหนดว่าควรตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์อย่างไร โดยแผนการรับมือภัยคุกคามทางไซเบอร์ต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	(ก) โครงสร้างทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber Incident Response Team: CIRT) รวมถึงบทบาทและความรับผิดชอบที่กำหนดไว้อย่างชัดเจนของสมาชิกในทีมแต่ละคนและรายละเอียดการติดต่อ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
	(ข) โครงสร้างการรายงานเหตุการณ์ (Incident Reporting Structure) ซึ่งกำหนดว่าหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจะปฏิบัติตามภาระหน้าที่ในการรายงานภายใต้พระราชบัญญัติ 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

ข้อ	รายการ	สถานะปัจจุบัน		หลักฐาน*
		มี	ไม่มี	
	(ฌ) กระบวนการทบทวนหลังการดำเนินการ (After-Action Review Process) เพื่อระบุและแนะนำให้ปรับปรุงการดำเนินการเพื่อป้องกันการเกิดซ้ำ	✓		ตามเอกสารในฉบับนี้ - แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมป่าไม้
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 .....

(นายพงศ์ พยัคฆ์)

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 : ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) วันที่และเวลาที่แจ้ง : ๑๓ มิถุนายน ๒๕๖๘ เวลา ๑๖.๕๗ น
๒. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม กรมป่าไม้ ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม : กรมป่าไม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ๖๑ ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐
๓. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล นายทนงศักดิ์ มนตรี และนายวีร์ ศรีทิพโพธิ์ ตำแหน่งงาน นักวิชาการคอมพิวเตอร์ชำนาญการ ชื่อหน่วยงาน กรมป่าไม้ อีเมล tanongtpl@gmail.com, wee.s@forest.go.th โทรศัพท์ (ที่ทำงาน / มือถือ) ๐๙๑๒๑๕๑๙๔๙, ๐๘๖๔๖๗๘๙๑๙
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.): - **หน่วยงานที่รับผิดชอบติดตามเหตุภัยคุกคาม (ถ้ามี):** ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ศปช.) สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) **วันที่:** ๑๓ มิถุนายน ๒๕๖๘ **เวลา:** ๑๖ ๕๗ น
ก๑. ด้านภารกิจหรือบริการของหน่วยงาน และ ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม ชื่อหน่วยงานที่เกิดเหตุภัยคุกคาม: กรมป่าไม้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่อยู่ของหน่วยงานหรือหน่วยงานย่อยที่เกิดเหตุภัยคุกคาม: กรมป่าไม้ ๖๑ ถนนพหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพมหานคร ๑๐๙๐๐
ก๒. ข้อมูลการติดต่อสำหรับการประสานงานเหตุภัยคุกคาม ชื่อ-นามสกุล นายทนงศักดิ์ มนตรี และนายวีร์ ศรีทิพโพธิ์ ตำแหน่งงาน นักวิชาการคอมพิวเตอร์ชำนาญการ ชื่อหน่วยงาน กรมป่าไม้ อีเมล tanongtpl@gmail.com, wee.s@forest.go.th โทรศัพท์ (ที่ทำงาน / มือถือ) ๐๙๑๒๑๕๑๙๔๙, ๐๘๖๔๖๗๘๙๑๙
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 ๑๓ มิถุนายน ๒๕๖๘ เวลา :๑๖.๕๗ **วัน เวลา ที่หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศทราบเหตุภัยคุกคาม** ๑๓ มิถุนายน ๒๕๖๘ เวลา :๑๖.๕๗
ข๒. วัน เวลา ที่แจ้งเหตุภัยคุกคามให้หน่วยงานควบคุมหรือกำกับดูแลทราบ ☐ ยังไม่ได้แจ้ง ☑ แจ้งแล้ว __๑๔ มิถุนายน ๒๕๖๘_____
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: เครื่องแม่ข่ายห้อง Data Center กรมป่าไม้ และระบบสารสนเทศที่ติดตั้งบนระบบคลาว์ดภาครัฐ

ชื่อผู้ให้บริการเครือข่ายที่ให้บริการแก่ระบบ บริการ หรือข้อมูลที่ได้รับผลกระทบ :

โปรดระบุ -

บริการของระบบ ข้อมูล หรือสินทรัพย์ที่ได้รับผลกระทบ (เช่น บริการการโอนเงิน):

โปรดระบุ ระบบสารสนเทศหลักกรมป่าไม้ ตามไฟล์เอกสาร ๑

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 – ในเบื้องต้นได้แจ้งผู้ใช้งานให้เปลี่ยนรหัสผ่านที่มากกว่า ๘ อักษรแล้ว

ส่วนที่ ๒
หมวด ง : รายละเอียดภัยคุกคาม
ง๑. ข้อมูลการตรวจจับและการวิเคราะห์
ง๑.๑ <u>วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ</u> (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

๑.๕ รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การจู่โจมครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการจู่โจม, Attack vector, เทคนิคหรือเครื่องมือที่ผู้จู่โจมใช้ ฯลฯ)

โปรดระบุ

๑.๖ รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ

๒. ข้อมูลการระงับ ปราบปราม และฟื้นฟู

๒.๑ รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ

๒.๒ การคาดการณ์ความสามารถฟื้นฟู

โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู

๓. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)

๓.๑ วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ **เวลา:** โปรดระบุ

๓.๒ การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ

๓.๓ 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)	
สวิตช์ (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)	
๘.๑	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
๘.๒	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
๘.๓	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
๙	จัดทำรายงานการติดตามผล	
๑๐	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	