

แผนการชกซ้อมและรับมือ ภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ ของสำนักงานนโยบายและแผนการขนส่งและจราจร



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



สนช www.otp.go.th



แผนการซักซ้อมและรับมือภัยความเสี่ยง
ด้านความมั่นคงปลอดภัยไซเบอร์
สำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

คำนำ

ปัจจุบันที่เทคโนโลยีดิจิทัลพัฒนาไปอย่างรวดเร็ว ทำให้เกิดความเสี่ยงจากภัยคุกคามทางไซเบอร์ในรูปแบบต่างๆ ซึ่งสามารถเกิดขึ้นได้ตลอดเวลา และส่งผลกระทบต่อการใช้งานระบบเทคโนโลยีสารสนเทศของ สนช. ได้แก่ ระบบคอมพิวเตอร์และอุปกรณ์ ระบบงานสารสนเทศ ระบบเครือข่าย และระบบฐานข้อมูล รวมถึงทำให้การปฏิบัติงานต้องหยุดชะงัก หรือไม่สามารถดำเนินงานได้ตามปกติ ซึ่งเหตุการณ์ดังกล่าวอาจเกิดจากปัจจัยที่ควบคุมได้ และปัจจัยที่อยู่เหนือการควบคุม อาจเกิดจากธรรมชาติ เช่น น้ำท่วม แผ่นดินไหว หรือเกิดจากฝีมือมนุษย์ เช่น การโจรกรรม การก่อการร้าย การแอบเข้าถึงและละเมิดข้อมูล ซึ่งอาจเกิดขึ้นครั้งเดียว วันเดียว หรือหลายวันติดต่อกันก็ได้ อาจรุนแรงหรือไม่รุนแรง แต่ก็ก่อให้เกิดผลเสียหายต่อชีวิตและทรัพย์สิน หรือส่งผลกระทบต่อนาฬิกาชีวิตความน่าเชื่อถือขององค์กร จึงจำเป็นต้องมีดำเนินการเพื่อให้ระบบเทคโนโลยีสารสนเทศมีความพร้อม สามารถให้บริการระบบงานสารสนเทศได้ทั้งในสถานการณ์ปกติและในสถานการณ์ฉุกเฉิน

สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) ได้ตระหนักถึงความสำคัญของการให้บริการระบบเทคโนโลยีสารสนเทศและข้อมูล จึงได้นำผลการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยทางไซเบอร์ของ สนข. มากำหนดเป็นแผนบริหารทางธุรกิจ (Business Continuity Management : BCM) และความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) เพื่อกำหนดแนวทางปฏิบัติในการรับมือ ป้องกัน และแก้ไขปัญหาจากสถานการณ์ภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ สนข. ได้อย่างทันทั่วถึง เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและข้อมูลของ สนข. ทั้งนี้ เพื่อให้เกิดการนำองค์ความรู้และแนวทางปฏิบัติในการรับมือภัยความเสี่ยงมาสู่การเตรียมความพร้อมในการรับมือภัยคุกคามทางไซเบอร์ สนข. จึงได้จัดทำแผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ขึ้นมาขับเคลื่อนให้มีกิจกรรมการซักซ้อมการป้องกันและรับมือความเสี่ยงและภัยคุกคามทางไซเบอร์ที่อาจเกิดขึ้นและมีผลการทบทวนระบบสารสนเทศของหน่วยงาน เพื่อให้เกิดความพร้อมต่อการตอบสนอง และลดความเสี่ยงที่จะเกิดขึ้นให้เหลือน้อยที่สุดต่อไป

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
บทที่ ๑ บทนำ	๑
๑.๑ หลักการและเหตุผล	๑
๒.๒ จุดประสงค์	๑
๑.๓ ขอบเขตการดำเนินงาน	๑
บทที่ ๒ การวิเคราะห์และประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ	๓
๒.๑ การวิเคราะห์และประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๓
๒.๒ การกำหนดขั้นตอนและแนวทางควบคุมความเสี่ยง	๕
๒.๓ การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน	๖
๒.๔ การกำหนดกระบวนการแก้ไขปัญหาและสถานการณ์ฉุกเฉิน	๘
บทที่ ๓ แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข.	๑๐
๓.๑ การจัดเตรียมความพร้อมในการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์	๑๑
๓.๒ แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข.	๑๑
บทที่ ๔ การสรุปผลการดำเนินงาน	๑๖
๔.๑ สรุปผลการจัดทำแผน	๑๖
๔.๒ การทบทวนแผน	๑๖
๔.๓ การติดตามและรายงานผล	๑๖

ภาคผนวก - เอกสารประกอบ

บทที่ ๑ บทนำ

๑.๑ หลักการและเหตุผล

ปัจจุบัน สำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) มีการนำเทคโนโลยีดิจิทัลมาใช้เพื่อช่วยสนับสนุนการบริหารจัดการงานราชการ ให้สามารถปฏิบัติงานได้อย่างสะดวก รวดเร็ว ซึ่งระบบเทคโนโลยีสารสนเทศและข้อมูลหน่วยงานนั้น ถือเป็นทรัพย์สินสำคัญของทางราชการที่ต้องใช้ในการดำเนินงานตามภารกิจ จึงมีความจำเป็นอย่างยิ่งที่จะต้องได้รับการปกป้องดูแลให้ปลอดภัยจากภัยคุกคามทางไซเบอร์ที่กำลังรุนแรง และมุ่งเป้าหมายมาที่ระบบเทคโนโลยีสารสนเทศของหน่วยงานภาครัฐ ทำให้ สนข. มีความเสี่ยงต่อทรัพย์สิน หรือส่งผลกระทบต่อภาพลักษณ์ความน่าเชื่อถือขององค์กร ดังนั้น เพื่อให้ สนข. มีความมั่นคงปลอดภัยจากภัยคุกคามและความเสี่ยงจากภัยคุกคามทางไซเบอร์ รวมถึงทำให้ระบบงานสามารถดำเนินงานได้อย่างต่อเนื่องไม่หยุดชะงัก สนข. จึงจำเป็นต้องมีการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ และนำผลลัพธ์ที่ได้มากำหนดเป็นมาตรการการดำเนินการและวิธีในการป้องกันภัยทางไซเบอร์ให้แก่ทรัพย์สินสารสนเทศสำคัญของ สนข.

ทั้งนี้ การเตรียมความพร้อมรับมือและแก้ไขสถานการณ์ฉุกเฉินจากภัยคุกคามทางไซเบอร์ จำเป็นต้องมีการนำผลการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนข. ที่มีระดับความเสี่ยงสูง มากำหนดเป็นแผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ขึ้นเพื่อให้เกิดการฝึกซ้อม รับมือ และสามารถแก้ไขสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นจนส่งผลกระทบต่อซึ่งระบบเทคโนโลยีสารสนเทศและข้อมูลของ สนข. ให้เกิดความรู้ ความเข้าใจ และสามารถดำเนินการแก้ไขปัญหาได้อย่างมีประสิทธิภาพ

๑.๒ จุดประสงค์

๑.๒.๑ เพื่อเตรียมความพร้อมรับมือและแก้ไขสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๑.๒.๒ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๑.๒.๓ เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๑.๒.๔ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันทั่วทั้งที่

๑.๓ ขอบเขตการดำเนินงาน

แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ที่จัดทำขึ้นใช้เป็นแนวทางปฏิบัติในการรับมือและแก้ไขสถานการณ์ที่เป็นความเสี่ยงระดับสูง ซึ่งอาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ และทำให้เกิดผลกระทบในการให้บริการสารสนเทศของ สนข. ดังนี้

- ๑.๓.๑ การวิเคราะห์และประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- ๑.๓.๒ การกำหนดขั้นตอนและแนวทางควบคุมความเสี่ยง
- ๑.๓.๓ การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
- ๑.๓.๔ การกำหนดกระบวนการแก้ไขปัญหาและสถานการณ์ฉุกเฉิน
- ๑.๓.๕ การซักซ้อมรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์
- ๑.๓.๖ การสรุปและรายงานผล

บทที่ ๒

การวิเคราะห์และประเมินความเสี่ยงด้านระบบเทคโนโลยีสารสนเทศ

๒.๑ การวิเคราะห์และประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

สนข. ได้มีการประเมินเสี่ยงด้านเทคโนโลยีสารสนเทศตามแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ สรุปผลได้ดังนี้

ตารางที่ ๒-๑ ผลการประเมินเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข.

ลำดับที่	รหัส	กิจกรรม/ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑	๐๑๘	ละเมิดลิขสิทธิ์โปรแกรมมอร์รดิประโยชน์ (Utilities Program)	๕	๓	๑๕	สูงมาก
๒	๐๑๕	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	๓	๕	๑๕	สูงมาก
๓	๐๑๖	ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	๓	๕	๑๕	สูงมาก
๔	๐๒	ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ	๓	๓	๙	สูง
๕	๐๑๙	ข้อมูลสำคัญรั่วไหล	๒	๔	๘	สูง
๖	๐๒๓	ผู้ใช้งาน (Users) ไม่มีความรู้ ความชำนาญ และทักษะการใช้งานระบบ	๔	๒	๘	สูง
๗	๐๑๗	เกิดช่องโหว่ของซอฟต์แวร์ขาดการบำรุงรักษา หรือเกิดช่องโหว่ของโปรแกรม	๒	๓	๖	ปานกลาง
๘	๐๑๔	เครื่องคอมพิวเตอร์แม่ข่ายชำรุด/เสียหาย/ค้าง/ดับ หรือไม่สามารถให้บริการได้	๒	๓	๖	ปานกลาง
๙	๐๒๔	การเชื่อมอีเมลหรือหน้าเว็บไซต์ปลอมเพื่อหลอกลวง (Mail Phishing)	๓	๒	๖	ปานกลาง
๑๐	๐๑	ไฟไหม้ห้องปฏิบัติการศูนย์ข้อมูล (Data Center)	๑	๕	๕	ปานกลาง
๑๑	๐๔	ไม่มีแผนต่อเนื่องกรณีเกิดสถานการณ์ภัยพิบัติ/ความไม่สงบทางการเมือง/ชุมนุมประท้วง	๑	๕	๕	ปานกลาง
๑๒	๐๕	การถูกบุกรุกหรือเข้าถึงพื้นที่หวงห้าม	๑	๕	๕	ปานกลาง
๑๓	๐๗	ขาดแผนรองรับระบบฮาร์ดแวร์ภายในศูนย์ปฏิบัติการระบบแม่ข่าย และเครือข่ายคอมพิวเตอร์ สนข.	๑	๕	๕	ปานกลาง
๑๔	๐๒๖	ผู้ใช้งานไม่ออกจากระบบเมื่อไม่ใช้งาน	๕	๑	๕	ปานกลาง

ลำดับที่	รหัส	กิจกรรม/ความเสี่ยง	โอกาส ความถี่ (๑)	ผลกระทบ ความรุนแรง (๒)	ระดับ คะแนน (๑) X (๒)	ระดับ ความเสี่ยง
๑๕	๐๖	ไม่มีการควบคุม/จัดทำบัญชี/ปรับปรุงบัญชีทรัพย์สินของอุปกรณ์เทคโนโลยีและการสื่อสาร	๑	๔	๔	ปานกลาง
๑๖	๐๑๓	ทรัพยากรของเครื่องคอมพิวเตอร์แม่ข่าย หรือระบบฐานข้อมูลไม่เพียงพอ	๒	๒	๔	ปานกลาง
๑๗	๐๘	ขาดการบริหารจัดการสิทธิ์การใช้งานอุปกรณ์เทคโนโลยีสารสนเทศในทุก ๆ ระดับผู้ใช้งาน	๑	๓	๓	ต่ำ
๑๘	๐๑๒	การรักษาความมั่นคงปลอดภัยของผู้ปฏิบัติงานจากระยะไกลไม่ทั่วถึง	๑	๓	๓	ต่ำ
๑๙	๐๒๐	การนำเข้าข้อมูลผิดพลาดไม่ครบถ้วน หรือไม่เป็นปัจจุบัน	๑	๓	๓	ต่ำ
๒๐	๐๒๑	การจ้างบุคคลภายนอก ที่ขาดความรู้ ความชำนาญ ความเชี่ยวชาญดูแลบำรุงรักษาระบบ/พัฒนาระบบ	๑	๓	๓	ต่ำ
๒๑	๐๓	การควบคุมอุณหภูมิ/ความชื้นภายในห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และระบบเครือข่ายคอมพิวเตอร์ของ สนช.	๒	๑	๒	ต่ำ
๒๒	๐๙	ระบบเครือข่ายไม่เพียงพอต่อการให้บริการ	๑	๒	๒	ต่ำ
๒๓	๐๒๒	บุคลากรด้านไอทีมีความรู้ ความเข้าใจด้านเทคโนโลยี ๆ ไม่เพียงพอ	๑	๒	๒	ต่ำ
๒๔	๐๒๕	การเฝ้าระวังข้อมูลจากการใช้เครือข่ายเดียวกันกับบุคคลน่าสงสัย	๑	๒	๒	ต่ำ
๒๕	๐๒๗	งบประมาณไม่เพียงพอสำหรับดำเนินโครงการ	๑	๒	๒	ต่ำ
๒๖	๐๑๐	ขาดการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่	๑	๑	๑	ต่ำ
๒๗	๐๑๑	ความเสี่ยงจากการจัดหาคอมพิวเตอร์และอุปกรณ์ไม่เหมาะสมกับลักษณะงาน	๑	๑	๑	ต่ำ
๒๘	๐๒๘	ไม่สามารถดำเนินโครงการที่กำหนดไว้ตามแผนดิจิทัลฯ	๑	๑	๑	ต่ำ
๒๙	๐๒๙	กระบวนการจัดซื้อจัดจ้างการบำรุงรักษาระบบไม่เป็นไปตามแผน/อนุมัติโครงการล่าช้า	๑	๑	๑	ต่ำ
๓๐	๐๓๐	ไม่สามารถปฏิบัติตามกฎหมายและระเบียบที่เกี่ยวข้อง	๑	๑	๑	ต่ำ
๓๑	๐๓๑	การเปลี่ยนแปลงนโยบายด้านเทคโนโลยีสารสนเทศของหน่วยงาน	๑	๑	๑	ต่ำ

จากผลการประเมินความเสี่ยงฯ พบว่ามีปัจจัยเสี่ยงทั้งสิ้น ๓๑ ปัจจัย แบ่งเป็น ปัจจัยเสี่ยงที่มีคะแนนอยู่ในระดับสูง จำนวน ๓ รายการ ระดับค่อนข้างสูง จำนวน ๓ รายการ ระดับค่อนข้างต่ำ จำนวน ๑๐ รายการ และระดับต่ำ จำนวน ๑๕ รายการ ทำให้ต้องมีการดำเนินการจัดการความเสี่ยง โดยความเสี่ยงที่อยู่ในระดับสูงเป็นระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที ความเสี่ยงระดับค่อนข้างสูง เป็นระดับที่ไม่สามารถยอมรับได้ ต้องจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้ต่อไป ความเสี่ยงระดับค่อนข้างต่ำ เป็นระดับที่สามารถยอมรับได้ แต่ต้องมีการควบคุมเพื่อป้องกันไม่ให้ความเสี่ยงเคลื่อนย้ายไปยังระดับที่ยอมรับไม่ได้ และความเสี่ยงระดับต่ำเป็นระดับที่สามารถยอมรับได้โดยไม่ต้องควบคุมความเสี่ยงหรือไม่ต้องการจัดการเพิ่มเติม

๒.๒ การกำหนดขั้นตอนและแนวทางควบคุมความเสี่ยง

จากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. มีรายการ/กิจกรรม ที่มีความเสี่ยงระดับ “สูง” จำนวน ๓ กิจกรรม ซึ่งเป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที ดังนี้

ตารางที่ ๒-๒ ประเด็นและแนวทางการควบคุมความเสี่ยงด้านเทคโนโลยีสารสนเทศระดับ “สูง”

ประเด็นความเสี่ยง/กิจกรรม	แนวทางจัดการ/กิจกรรมควบคุม	เป้าหมาย/ผลสำเร็จของการดำเนินการกิจกรรมตามแนวทางการจัดการความเสี่ยง
๐๑๘ ละเมิดลิขสิทธิ์โปรแกรมอรรถประโยชน์ (Utilities Program)	<ul style="list-style-type: none"> - สร้างความตระหนักในเรื่องนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศและการทำงานซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - กระตุ้นให้เกิดการปฏิบัติตามนโยบายหรือระเบียบฯ อย่างจริงจัง - ส่งเสริมให้ใช้โปรแกรมอรรถประโยชน์แบบ OpenSource แทนโปรแกรมที่มีค่าใช้จ่ายเกี่ยวกับลิขสิทธิ์ - จัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย 	<ul style="list-style-type: none"> - เจ้าหน้าที่ของ สนข. มีความเข้าใจเกี่ยวกับโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย - เจ้าหน้าที่ของ สนข. มีความตระหนักรู้และไม่ใช้งานโปรแกรมที่ละเมิดลิขสิทธิ์ - มีการจัดหาโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย
๐๑๕ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)	<ul style="list-style-type: none"> - มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ 	<ul style="list-style-type: none"> - ระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายของ สนข. มีความมั่นคงปลอดภัย

ประเด็นความเสี่ยง/กิจกรรม	แนวทางจัดการ/ กิจกรรมควบคุม	เป้าหมาย/ผลสำเร็จ ของการดำเนินการกิจกรรม ตามแนวทางการจัดการความเสี่ยง
	<ul style="list-style-type: none"> - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ 	
๐๑๖ ถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)	<ul style="list-style-type: none"> - มีการติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย เช่น IPS, Firewall - ตรวจสอบการตั้งค่าของอุปกรณ์รักษาความปลอดภัยระบบเครือข่าย (IPS, Firewall) อย่างสม่ำเสมอ - ตรวจสอบ ติดตาม และเฝ้าระวังการบุกรุกเครือข่ายอย่างสม่ำเสมอ - ติดตามข่าวสารภัยคุกคามทางไซเบอร์อย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัส - ติดตั้ง Patch ของระบบปฏิบัติการอย่างสม่ำเสมอ - เปลี่ยนรหัสผ่านตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ - ทดสอบช่องโหว่ของโปรแกรม - กำหนดมาตรฐานในการพัฒนาโปรแกรมให้มีความปลอดภัย 	<ul style="list-style-type: none"> - ระบบสารสนเทศและฐานข้อมูลของ สนข. มีความมั่นคงปลอดภัย

จากผลการประเมินความเสี่ยงฯ พบว่า มีความเสี่ยงระดับ “สูง” จำนวน ๓ กิจกรรม ซึ่งเป็นความเสี่ยงที่อยู่ในระดับที่ไม่สามารถยอมรับได้ จำเป็นต้องเร่งจัดการความเสี่ยงให้อยู่ในระดับที่ยอมรับได้โดยทันที สนข. จึงควรคัดเลือกกิจกรรมที่มีความเสี่ยงดังกล่าว มากำหนดเป็นแผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ ต่อไป

๒.๓ การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

ตามแผนการรับมือเหตุภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) ของ สนข. ได้กำหนดโครงสร้างและบทบาทของทีรับมือเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ไว้ ดังนี้

๒.๓.๑ ผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายในหน่วยงาน กำหนดไว้ดังนี้

ตารางที่ ๒-๓ รายชื่อทีรับมือแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ภายใน ของ สนข.

ลำดับ	ชื่อ – นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	หน้าที่ และ ความรับผิดชอบ
๑	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๙๔ ๙๑๕ ๑๕๓๖	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์
๒	นายพิสิฐ ป้อมทอง นวช.คอมฯ ชก. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๙๔ ๓๑๐ ๐๒๐๘	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

ลำดับ	ชื่อ - นามสกุล	ระยะเวลาในการปฏิบัติงาน	ช่องทางการติดต่อสื่อสาร	หน้าที่	หน้าที่ และ ความรับผิดชอบ
๓	นายชัยวัฒน์ ธรรมาสถิตนุกูล นวช.คอมฯ ชก. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๘๑ ๒๐๖ ๕๒๕๔	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์
๔	นายทรงเกียรติ ตะเภาทอง นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๙๗ ๒๔๕ ๕๓๔๒	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์
๕	นางสาวรุ่งทิพย์ ศรีบุญชู นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๘๗ ๔๓๒ ๕๖๒๕	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์
๖	นางสาวชนันดา ดวงพรม นวช.คอมฯ ปก. ศทท.	๒๔ ชั่วโมง/๗ วัน	โทร. ๐๙๓ ๕๓๖ ๖๓๖๔	เจ้าหน้าที่รับมือฯ (Incident lead)	เป็นผู้รับแจ้งเหตุการณ์ ความมั่นคงปลอดภัยไซเบอร์

๒.๓.๒ ผู้รับผิดชอบรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT) กำหนดไว้ดังนี้

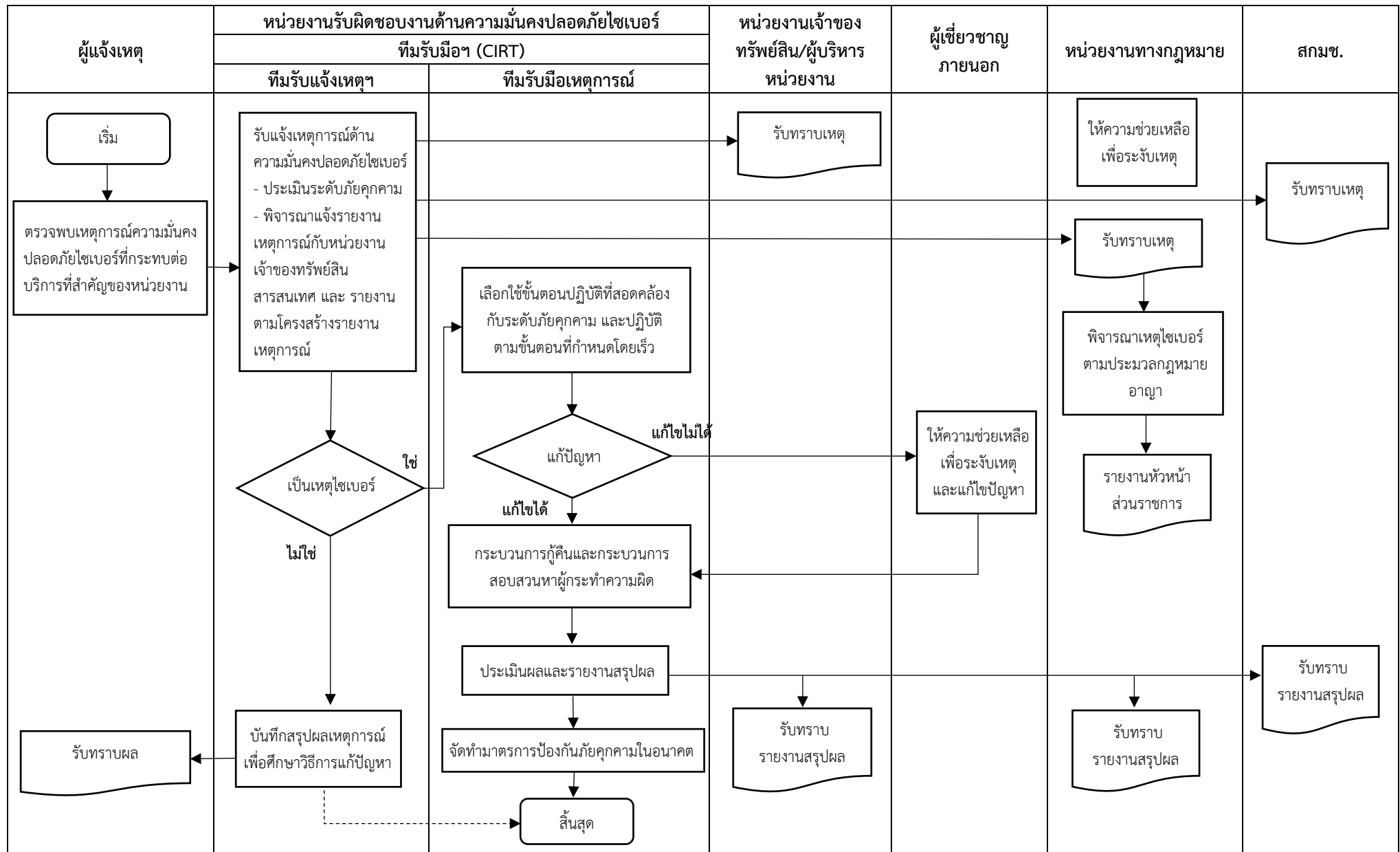
ตารางที่ ๒-๔ รายชื่อทีมรับมือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ (Cyber incident Response Team : CIRT) ของ สนช.

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	หน้าที่ และ ความรับผิดชอบ
๑	นางสาวจิรังค์ ห้วยหงษ์ทอง ผอ.ศทท. ในฐานะผู้บริหารจัดการ ความมั่นคงปลอดภัยสารสนเทศ (Head of Information Security) ประจำ สนช.	ภายใน : ๔๐๐๘ มือถือ : ๐๘๑ ๑๓๘ ๓๘๔๐ email : Jirungruk.hua@otp.go.th	หัวหน้าทีมรับมือฯ (Team manager)	ทำหน้าที่สื่อสารกับ ผู้บริหารเทคโนโลยี สารสนเทศของหน่วยงาน
๒	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. หน.กพค. ศทท.	ภายใน : ๔๕๑๕ มือถือ : ๐๙๔ ๙๑๕ ๑๕๓๖ email : narit.mai@otp.go.th	รองหัวหน้าทีม รับมือฯ (Team Deputy manager)	ทำหน้าที่ช่วยเหลือ สนช. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๓	นายพิสิฐ ป้อมทอง นวช.คอมฯ ชก. ศทท.	ภายใน : ๔๕๑๐ มือถือ : ๐๘๔ ๓๑๐ ๐๒๐๘ email : pitit.pom@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนช. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๔	นายชัยวัฒน์ ธรรมาสถิตนุกูล นวช.คอมฯ ชก. ศทท.	ภายใน : ๔๐๑๔ มือถือ : ๐๘๑ ๒๐๖ ๕๒๕๔ email : chaiwat.tha@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนช. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๕	นายทรงเกียรติ ตะเภาทอง นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๔๕ มือถือ : ๐๙๗ ๒๔๕ ๕๓๔๒ email : srongkiat.tap@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนช. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้

ลำดับ	ชื่อ - นามสกุล	ช่องทางการติดต่อสื่อสาร	หน้าที่	หน้าที่ และ ความรับผิดชอบ
๖	นางสาวรุ่งทิพย์ ศรีบุญชู นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๘๑ มือถือ : ๐๘๗ ๔๗๒ ๕๖๒๕ email : roongthip.sri@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๗	นางสาวชนันดา ดวงพรหม นวช.คอมฯ ปก. ศทท.	ภายใน : ๔๐๘๑ มือถือ : ๐๙๓ ๕๓๖ ๖๓๖๔ email : chananda.dua@otp.go.th	เจ้าหน้าที่รับมือฯ (Incident leader)	ทำหน้าที่ช่วยเหลือ สนข. ให้สามารถควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์ได้
๘	นายณฤทธิ์ มัยรัตน์ นวช.คอมฯ ขพ. หน.กพค. ศทท.	ภายใน : ๔๕๑๕ มือถือ : ๐๙ ๔๙๑๕ ๑๕๓๖ email : narit.mai@otp.go.th	เจ้าหน้าที่เทคนิคฯ (Technical leader)	ทำหน้าที่ให้ความเห็น เกี่ยวกับแนวทาง ที่เหมาะสมในการควบคุม ผลกระทบจากภัยคุกคาม ทางไซเบอร์

๒.๔ การกำหนดกระบวนการแก้ไขปัญหาและสถานการณ์ฉุกเฉิน

จากการประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศของ สนข. พบว่า สนข. มีรายการ/กิจกรรม ที่มีความเสี่ยงระดับ “สูง” ควรมีการเฝ้าระวังและเตรียมความพร้อมในการรับมือเมื่อเกิดเหตุฉุกเฉินหรือสถานการณ์จริง สนข. จึงนำมากำหนดเป็นขั้นตอนการดำเนินการแก้ไขปัญหาและรับมือสถานการณ์ฉุกเฉิน ดังนี้



บทที่ ๓

แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนช.

๓.๑ การจัดเตรียมความพร้อมในการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์

ศทท. เป็นหน่วยงานหลักในการดำเนินงานด้านเทคโนโลยีสารสนเทศและการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนช. ต้องมีการจัดเตรียมความพร้อมของอุปกรณ์และเครื่องมือต่าง ๆ ที่ใช้ในกิจกรรมการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อให้การดำเนินการซักซ้อมฯ เป็นไปอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ดังนี้

๓.๑.๑ การจัดเตรียมสถานที่

ต้องจัดเตรียมสถานที่สำหรับดำเนินการฝึกซ้อมรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ เช่น ห้องศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร ห้องปฏิบัติการศูนย์ข้อมูล (Data Center) และห้องประชุมของ สนช. เป็นต้น

๓.๑.๒ การจัดเตรียมอุปกรณ์

ต้องจัดเตรียมอุปกรณ์ที่จำเป็นต้องใช้งานสำหรับการฝึกซ้อมตามแผนการซักซ้อมฯ เช่น เครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์โน้ตบุ๊ก ระบบเครือข่าย โปรแกรมหรือไดรเวอร์ และอุปกรณ์สำรองข้อมูล เป็นต้น

๓.๑.๓ การจัดเตรียมหัวข้อการซักซ้อม

ต้องมีการกำหนดหัวข้อการฝึกซ้อมให้สอดคล้องกับการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงาน รวมถึงขั้นตอนการปฏิบัติต่าง ๆ และแบบฟอร์มการบันทึกข้อมูลที่เกี่ยวข้อง

๓.๑.๔ การจัดเตรียมบุคลากร

ต้องจัดให้มีการประชุมหรือการชี้แจงบุคลากรที่จะเข้าร่วมการฝึกซ้อม เพื่อให้มั่นใจได้ว่าผู้เข้าร่วมการฝึกซ้อมทุกคนจะเข้าใจถึงขอบเขตของการฝึกซ้อม แนวทางและการปฏิบัติในการฝึกซ้อม รวมถึงหน้าที่และความรับผิดชอบของตนได้อย่างชัดเจน เพื่อไม่ให้เกิดความสับสนและสามารถดำเนินการซักซ้อมได้อย่างมีประสิทธิภาพ

๓.๑.๕ การจัดเตรียมการประสานงาน

ต้องมีการแจ้งผู้ที่เกี่ยวข้องหรือผู้ที่ได้รับผลกระทบจากการซักซ้อมแต่ละครั้ง เพื่อให้ทราบถึงกำหนดการซักซ้อม และไม่เกิดความสับสนในการปฏิบัติงานตามปกติ

๓.๒ แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนช.

ในปีงบประมาณ พ.ศ. ๒๕๖๙ ได้กำหนดแผน หัวข้อ และขั้นตอนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของ สนช. ไว้ดังนี้

๓.๒.๑ แผนการซักซ้อมการถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
๑. ได้รับแจ้ง/ตรวจพบเจอเหตุภัยคุกคามทางไซเบอร์	ทีมผู้รับแจ้งเหตุฯ	๑. รับแจ้งเหตุ ๒. บันทึกการแจ้งเหตุภัยทางไซเบอร์ที่เกิดขึ้น	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๒. ดำเนินการตรวจสอบว่าเป็นเหตุภัยคุกคามทางไซเบอร์หรือไม่	ทีมผู้รับแจ้งเหตุฯ	๑. ตรวจสอบเหตุ ๒. บันทึกผลการตรวจสอบเหตุภัยทางไซเบอร์ที่เกิดขึ้น ๓. หากพบว่าไม่เป็นเหตุภัยคุกคามทางไซเบอร์ให้สรุปผลเหตุการณ์	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๓. แจ้งเหตุการณ์ถูกโจมตีจากภัยคุกคามทางไซเบอร์ให้ทีมรับมือเหตุการณ์ฯ	ทีมผู้รับแจ้งเหตุฯ	๑. แจ้งเหตุการณ์ถูกโจมตีจากภัยคุกคามทางไซเบอร์ให้ทีมรับมือเหตุการณ์ฯ ทราบ	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๔. วิเคราะห์และแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์	ทีมรับมือเหตุการณ์ฯ	๑. ระบุผลกระทบหรือควบคุมขอบเขตของภัยคุกคามทางไซเบอร์ที่เกิดขึ้นโดยเร็วที่สุด ๒. วิเคราะห์สาเหตุและผลกระทบของเหตุการณ์ที่เกิดขึ้น	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรม เหตุการณ์ความปลอดภัยทาง ไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
		๓. ดำเนินการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ๔. บันทึกผลการดำเนินการตอบสนองต่อเหตุภัยทางไซเบอร์ ๕. การขอความช่วยเหลือจากหน่วยงานภายนอกเมื่อไม่สามารถแก้ไขเหตุภัยทางไซเบอร์ที่เกิดขึ้น			
๕. กระบวนการกู้คืน	ทีมรับมือเหตุการณ์ฯ	๑. ดำเนินการกู้คืนระบบงานสารสนเทศ หรือระบบฐานข้อมูล ๒. บันทึกผลการกู้คืนระบบงาน	- บันทึกรายงานสถานการณ์/เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถดำเนินการได้ ระบุ	(ใส่ระยะเวลาดำเนินการในขั้นตอนนี้)
๕. การสรุปผลเหตุการณ์และการบันทึกผลการแก้ไขปัญหา	ทีมรับมือเหตุการณ์ฯ	๑. สรุปผลการดำเนินการแก้ไขปัญหาภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ๒. บันทึกผลการแก้ไขปัญหา	- บันทึกรายงานสถานการณ์/เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถดำเนินการได้ ระบุ	(ใส่ระยะเวลาดำเนินการในขั้นตอนนี้)
๖. การแจ้งและรายงานผลการแก้ไขปัญหา	ทีมรับมือเหตุการณ์ฯ	๑. รายงานผลให้ทีมผู้รับแจ้งเหตุฯ ๒. รายงานผลให้เจ้าของทรัพย์สิน/ผู้บริหารหน่วยงาน ๓. รายงานผลให้หน่วยงานอื่นที่เกี่ยวข้อง (ถ้ามี)		☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถดำเนินการได้ ระบุ	(ใส่ระยะเวลาดำเนินการในขั้นตอนนี้)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
๗. การสรุปผลเหตุการณ์	ทีมผู้รับแจ้งเหตุฯ ทีมรับมือเหตุการณ์ฯ	๑. ตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ๒. สรุปผลเหตุการณ์ เช่น สาเหตุ ความรุนแรง ผลกระทบ ขั้นตอนการ แก้ไขปัญหา อุปสรรค การกู้คืน แนวทางการป้องกันเหตุในอนาคต และรายละเอียดของผู้ได้รับ ผลกระทบ	- รายการตรวจสอบ การจัดการเหตุการณ์ (Incident Handling Checklist) - รายละเอียดภัยคุกคาม - แบบรายงานสรุปภัยคุกคาม ทางไซเบอร์ในหนึ่งรอบปี	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)

๓.๒.๒ แผนการซักซ้อมการถูกโจมตีโดยบุคคลที่ไม่มีสิทธิ์เจาะระบบหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูล (Database)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
๑. ได้รับแจ้ง/ตรวจพบเจอเหตุภัยคุกคาม ทางไซเบอร์	ทีมผู้รับแจ้งเหตุฯ	๑. รับแจ้งเหตุ ๒. บันทึกการแจ้งเหตุภัยทางไซเบอร์ ที่เกิดขึ้น	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๒. ดำเนินการตรวจสอบว่าเป็นเหตุ ภัยคุกคามทางไซเบอร์หรือไม่	ทีมผู้รับแจ้งเหตุฯ	๑. ตรวจสอบเหตุ ๒. บันทึกผลการตรวจสอบเหตุ ภัยทางไซเบอร์ที่เกิดขึ้น ๓. หากพบว่าไม่เป็นเหตุภัยคุกคาม ทางไซเบอร์ให้สรุปผลเหตุการณ์	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
๓. แจ้งเหตุการณ์ฉุกเฉินจากภัยคุกคามทางไซเบอร์ให้ทีมรับมือเหตุการณ์ฯ	ทีมผู้รับแจ้งเหตุฯ	๑. แจ้งเหตุการณ์ฉุกเฉินจากภัยคุกคามทางไซเบอร์ให้ทีมรับมือเหตุการณ์ฯ ทราบ	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๔. วิเคราะห์และแก้ไขสถานการณ์ภัยคุกคามทางไซเบอร์	ทีมรับมือเหตุการณ์ฯ	๑. ระบุผลกระทบหรือความ ขอบเขตของภัยคุกคามทางไซเบอร์ ที่เกิดขึ้นโดยเร็วที่สุด ๒. วิเคราะห์สาเหตุและผลกระทบ ของเหตุการณ์ที่เกิดขึ้น ๓. ดำเนินการแก้ไขปัญหาภัยคุกคาม ทางไซเบอร์ที่เกิดขึ้น ๔. บันทึกผลการดำเนินการตอบสนอง ต่อเหตุภัยทางไซเบอร์ ๕. การขอความช่วยเหลือจาก หน่วยงานภายนอกเมื่อไม่สามารถ แก้ไขเหตุภัยทางไซเบอร์ที่เกิดขึ้น	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรม เหตุการณ์ความปลอดภัยทาง ไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๕. กระบวนการกู้คืน	ทีมรับมือเหตุการณ์ฯ	๑. ดำเนินการกู้คืนระบบงาน สารสนเทศ หรือระบบฐานข้อมูล ๒. บันทึกผลการกู้คืนระบบงาน	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรม เหตุการณ์ความปลอดภัยทาง ไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)

ขั้นตอน / กิจกรรม	ผู้รับผิดชอบ	การดำเนินการ	เอกสาร และการบันทึก รายงานสถานการณ์	ผลการดำเนินการ	ระยะเวลา ดำเนินการ
๕. การสรุปผลเหตุการณ์และการบันทึก ผลการแก้ไข้ปัญหา	ทีมรับมือเหตุการณ์ฯ	๑. สรุปผลการดำเนินการแก้ไข้ปัญหา ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น ๒. บันทึกผลการแก้ไข้ปัญหา	- บันทึกรายงานสถานการณ์/ เหตุการณ์ความมั่นคง ปลอดภัยไซเบอร์ - บันทึกข้อมูลกิจกรรม เหตุการณ์ความปลอดภัยทาง ไซเบอร์	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๖. การแจ้งและรายงานผลการแก้ไข้ปัญหา	ทีมรับมือเหตุการณ์ฯ	๑. รายงานผลให้ทีมผู้รับแจ้งเหตุฯ ๒. รายงานผลให้เจ้าของทรัพย์สิน/ ผู้บริหารหน่วยงาน ๓. รายงานผลให้หน่วยงานอื่นที่ เกี่ยวข้อง (ถ้ามี)		☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)
๗. การสรุปผลเหตุการณ์	ทีมผู้รับแจ้งเหตุฯ ทีมรับมือเหตุการณ์ฯ	๑. ตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist) ๒. สรุปผลเหตุการณ์ เช่น สาเหตุ ความรุนแรง ผลกระทบ ขั้นตอนการ แก้ไข้ปัญหา อุปสรรค การกู้คืน แนวทางการป้องกันเหตุในอนาคต และรายละเอียดของผู้ได้รับ ผลกระทบ	- รายการตรวจสอบ การจัดการเหตุการณ์ (Incident Handling Checklist) - รายละเอียดภัยคุกคาม - แบบรายงานสรุปภัยคุกคาม ทางไซเบอร์ในหนึ่งรอบปี	☐ ดำเนินการแล้วเสร็จ ☐ ไม่สามารถ ดำเนินการได้ ระบุ	(ใส่ระยะเวลา ดำเนินการ ในขั้นตอนนี้)

บทที่ ๔

การสรุปผลการดำเนินงาน

๔.๑ สรุปผลการจัดทำแผน

แผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ประจำปีงบประมาณ พ.ศ. ๒๕๖๙ จัดทำขึ้นเพื่อเตรียมความพร้อมในการรับมือและแก้ไขสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของ สนข. สร้างความเข้าใจในการบริการจัดการงานด้านความมั่นคงปลอดภัยไซเบอร์ แก่ผู้บริหารและผู้ปฏิบัติเมื่อต้องรับมือกับเหตุภัยคุกคามทางไซเบอร์ และใช้เป็นกรอบแนวทางในการรับมือ และแก้ไขปัญหาเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์แก่ระบบเทคโนโลยีสารสนเทศของ สนข. ทั้งนี้ เพื่อให้ระบบสารสนเทศของมีเสถียรภาพ มีความพร้อมในการให้บริการได้ตลอดเวลา ภายใต้การกำกับดูแลของผู้บริหาร ด้านความมั่นคงปลอดภัยทางไซเบอร์ของ สนข. (Head of Cybersecurity) และผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงระดับกรม (DCIO) ประจำปี สนข.

๔.๒ การทบทวนแผน

การจัดทำแผนการซักซ้อมและรับมือภัยความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ สนข. ควรมีการทบทวน หรือปรับปรุง อย่างน้อยปีละ ๑ ครั้ง เพื่อให้สอดคล้องกับสถานการณ์ภัยความเสี่ยงที่เกิดขึ้นในปัจจุบัน หรือ ทุกครั้งที่มีการปรับปรุงแผนการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ แผนการรับมือเหตุ ภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan) และแผนแก้ไขปัญหาจากสถานการณ์ ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)

๔.๓ การติดตามและรายงานผล

กำหนดให้ผู้รับผิดชอบรายงานผลการดำเนินการซักซ้อมฯ ให้ผู้บริหารจัดการความมั่นคงปลอดภัย สารสนเทศ (Head of Information Security) ประจำปี สนข. ทราบ เพื่อรายงานสรุปให้ผู้บริหาร เทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) ทราบ เป็นลำดับขั้นไป และหากมีเหตุฉุกเฉินร้ายแรง ต้องรีบรายงานให้ผู้บริหารสูงสุดของหน่วยงานทราบโดยทันที

ภาคผนวก
เอกสารประกอบ

๑. แบบบันทึกรายงานสถานการณ์/เหตุการณ์ความมั่นคงปลอดภัยไซเบอร์

วันที่ :	เวลา :	ผู้บันทึกรายงาน : ติดต่อ :
วันและเวลาที่เกิดเหตุการณ์ :		
สถานะเหตุการณ์ปัจจุบัน :		
ประเภทเหตุการณ์ :		
ระดับความรุนแรง :		
รายละเอียดเหตุการณ์ :		
ผลกระทบที่เกิดขึ้น :		
ความเสียหายที่เกิดขึ้น :		
การรายงานเหตุการณ์ :		
หน่วยงานที่ขอความช่วยเหลือ :		
การดำเนินการตอบสนอง ต่อเหตุการณ์ :		
รายละเอียดเพิ่มเติม :		
ผู้จัดการรับมือฯ เหตุการณ์ :		
ข้อมูลติดต่อผู้จัดการรับมือฯ เหตุการณ์ :		
วันและเวลาที่มีรายงาน ความคืบหน้าครั้งถัดไป :		

๒. บันทึกข้อมูลกิจกรรมเหตุการณ์ความปลอดภัยทางไซเบอร์ (Incident Documentation)

วันที่และเวลา	บันทึกกิจกรรมที่เกิดขึ้น (ข้อเท็จจริง, สถานการณ์ที่เกิดขึ้น, การตัดสินใจ, ผลกระทบ)

หมวด ง : รายละเอียดภัยคุกคาม
ง1. ข้อมูลการตรวจจับและการวิเคราะห์
ง1.1 วัน เวลา ที่ผู้โจมตีได้เริ่มต้นเข้าถึงระบบ (System Access) วันที่: เลือกวันที่ เวลา: โปรดระบุ ไม่ทราบ: ☐
ง1.2 ข้อมูลการพบเห็นเหตุภัยคุกคามทางไซเบอร์ รายละเอียดแหล่งที่มา หรือต้นเหตุของเหตุภัยคุกคาม (เท่าที่ทราบ เช่น คน, ความผิดพลาดของระบบ, ภัยธรรมชาติ, การโจรกรรม, ความผิดพลาดจากคนนอกองค์กร): โปรดระบุ บุคคล วิถี หรือเครื่องมือที่ตรวจพบภัยคุกคาม (เช่น ผู้ใช้, ผู้ดูแลระบบ, โปรแกรม Anti-virus, IDS, การวิเคราะห์ข้อมูลจราจรทางคอมพิวเตอร์, ไม่ทราบ): โปรดระบุ รายละเอียดของปัญหาลักษณะคล้ายกันที่หน่วยงานเคยพบมาก่อน (ถ้ามี โปรดระบุรายละเอียด): โปรดระบุ
ง1.3 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 (เลือกทุกข้อที่ใช้): <div style="display: flex; flex-wrap: wrap;"> <div style="width: 50%;"> ☐ ข้อมูลไบโอเมตริกซ์ </div> <div style="width: 50%;"> ☐ ข้อมูลการติดต่อ </div> <div style="width: 50%;"> ☐ ข้อมูลการเงิน </div> <div style="width: 50%;"> ☐ ข้อมูลบุคลากรของรัฐ </div> <div style="width: 50%;"> ☐ หมายเลขบัตรประชาชน </div> <div style="width: 50%;"> ☐ ข้อมูลการติดต่อกับหน่วยงานต่าง ๆ </div> <div style="width: 50%;"> ☐ ข้อมูลทางการแพทย์ </div> <div style="width: 50%;"> ☐ อื่น ๆ : โปรดระบุ </div> </div> จำนวนข้อมูล (Record) ที่ได้รับผลกระทบ: โปรดระบุ ผลกระทบอื่น ๆ ที่เกิดขึ้น: โปรดระบุ

<p>ง1.4 รายละเอียดของระบบ หรือข้อมูลที่ได้รับผลกระทบ (Information of Affected System)</p> <p>หมายเลข CVE: โปรดระบุ</p> <p>ช่องโหว่ที่ถูกใช้โจมตี: โปรดระบุ</p> <p>การใช้ระบบหรือเครื่องที่ได้รับผลกระทบเป็นฐานเพื่อโจมตีขยายผลไปยังระบบหรือเครื่องอื่น:</p> <p>โปรดระบุ</p> <p>อาการหรือสิ่งผิดปกติ (เลือกได้มากกว่า 1 รายการ)</p> <div> ☐ ระบบล่ม ☐ รายการข้อมูลจราจรทางคอมพิวเตอร์ที่ผิดปกติ </div> <div> ☐ บัญชีผู้ใช้ถูกสร้างขึ้นใหม่โดยไม่ทราบสาเหตุ หรือ บัญชีผู้ใช้มีความผิดปกติ </div> <div> ☐ การโจมตีด้วยวิศวกรรมสังคม (Social Engineering) ทั้งที่สำเร็จและไม่สำเร็จ </div> <div> ☐ ประสิทธิภาพของระบบด้อยลง (ทั้งที่รู้ว่าเป็นเพราะเหตุภัยคุกคามและที่ไม่รู้สาเหตุ) </div> <div> ☐ การเปลี่ยนแปลงใน DNS หรือ กฎของ Router หรือกฎไฟร์วอลล์ โดยไม่ทราบสาเหตุ </div> <div> ☐ การยกระดับสิทธิ์การเข้าถึงระบบโดยไม่ทราบสาเหตุ </div> <div> ☐ การตรวจพบการทำงานของโปรแกรมหรืออุปกรณ์ Sniffer เพื่อจับการรับส่งข้อมูลภายในเครือข่าย </div> <div> ☐ การเข้าใช้งานครั้งสุดท้ายของผู้ใช้ที่ไม่สอดคล้องกับการใช้งานครั้งสุดท้ายที่เกิดขึ้นจริง </div> <div> ☐ การแจ้งเตือนจากเครื่องมือตรวจจับการบุกรุก </div> <div> ☐ การเข้ามาลาดตระเวน (Probing) หรือการเรียกดู (Browsing) ที่น่าสงสัย </div> <div> ☐ รูปแบบการใช้งานที่ผิดปกติ ☐ การเปลี่ยนแปลงขนาดไฟล์ไปจากเดิมแบบผิดปกติ </div> <div> ☐ ความพยายามที่จะเขียนไฟล์ของระบบ ☐ การเปลี่ยนแปลงวันที่ของไฟล์ไปจากเดิมแบบผิดปกติ </div> <div> ☐ การแก้ไขหรือลบข้อมูลที่ผิดปกติ ☐ การโจมตีให้เกิดการปฏิเสธการให้บริการ (DOS, DDOS) </div> <div> ☐ ไฟล์ใหม่ถูกสร้างขึ้นโดยไม่ทราบสาเหตุ ☐ การใช้งานหรือมีกิจกรรมที่เกิดในเวลาที่ไม่ปกติ </div> <div> ☐ การแก้ไขหน้าเว็บ ☐ การสร้างแฟ้มข้อมูล setuid หรือ setgid ใหม่ที่ผิดปกติเกิดขึ้น </div> <div> ☐ การเปลี่ยนแปลงในไดเรกทอรีและแฟ้มข้อมูลของระบบปฏิบัติการที่ผิดปกติ </div> <div> ☐ การตรวจพบโปรแกรมเจาะระบบ (Crack utility) </div> <div> ☐ สิ่งผิดปกติไปจากเดิมอื่น ๆ: โปรดระบุ </div>
<p>ง1.5 รายละเอียดของเหตุภัยคุกคามตามลำดับเวลา ตั้งแต่การโจมตีครั้งแรก จนถึงปัจจุบัน (เช่น ลำดับของการโจมตี, Attack vector, เทคนิคหรือเครื่องมือที่ผู้โจมตีใช้ ฯลฯ)</p> <p>โปรดระบุ</p>
<p>ง1.6 รายละเอียดอื่น ๆ ที่พบเกี่ยวข้องกับเหตุภัยคุกคาม: โปรดระบุ</p>
<p>ง2. ข้อมูลการระงับ ปรามปราม และฟื้นฟู</p>
<p>ง2.1 รายละเอียดการดำเนินการเพื่อแก้ไขเหตุภัยคุกคาม: โปรดระบุ</p>
<p>ง2.2 การคาดการณ์ความสามารถฟื้นฟู โปรดระบุรายละเอียดการฟื้นฟู ทรัพยากรที่ต้องใช้และที่ต้องการเพิ่ม และประมาณระยะเวลาการฟื้นฟู</p>
<p>ง3. ข้อมูลกิจกรรมภายหลังการแก้ปัญหา (ถ้ามี)</p>
<p>ง3.1 วัน เวลา ที่เหตุภัยคุกคามสิ้นสุด วันที่: เลือกวันที่ เวลา: โปรดระบุ</p>
<p>ง3.2 การดำเนินการเพื่อป้องกันเหตุภัยคุกคามที่คล้ายคลึงกัน: โปรดระบุ</p>
<p>ง3.3 บทเรียนที่ได้จากเหตุภัยคุกคาม: โปรดระบุ</p>

แบบรายงานสรุปภัยคุกคามทางไซเบอร์ในหนึ่งรอบปี

ข้อ 1 สถิติรายปีจำแนกตามหมวดหมู่ของภัยคุกคามทางไซเบอร์¹

หมวดหมู่	คำอธิบาย	จำนวน
0	เหตุการณ์จำลองและการฝึกซ้อมของหน่วยงาน (Training and Exercises)	
1	การพยายามเข้าถึงระบบที่ไม่สำเร็จ (Unsuccessful Activity Attempt)	
2	การพยายามบุกรุกเพื่อสำรวจข้อมูลองค์กรเพื่อโจมตี (Reconnaissance)	
3	การดำเนินการที่ไม่เป็นไปตามมาตรฐานความปลอดภัยที่หน่วยงานกำหนด (Non-Compliance Activity)	
4	การบุกรุกโดยการใช้มัลแวร์ (Malicious Logic)	
5	การบุกรุกในระดับผู้ใช้งาน (User Level Intrusion)	
6	การบุกรุกในระดับผู้ควบคุมระบบ (Root Level Intrusion)	
7	การบุกรุกที่ทำให้ไม่สามารถเข้าไปใช้บริการได้ (Denial of Service)	
8	เหตุการณ์ที่อยู่ระหว่างการวิเคราะห์สอบสวน (Investigating)	
9	เหตุการณ์ผิดปกติที่ได้รับการวิเคราะห์แล้วว่าไม่ใช่เหตุการณ์ที่เป็นภัยคุกคาม (Explained Anomaly)	

ข้อ 2 สถิติรายปีจำแนกตามทรัพย์สินที่ได้รับผลกระทบ

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

ข้อ 3 สถิติรายปีจำแนกตามระดับภัยคุกคามทางไซเบอร์²

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

¹ หมวดหมู่ตามข้อ 1 ของภาคผนวกท้ายประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เรื่อง ลักษณะภัยคุกคามทางไซเบอร์
มาตรการป้องกัน รับมือ ประเมิน ปราบปราม และระงับภัยคุกคามทางไซเบอร์ แต่ละระดับ พ.ศ.2564

² ระดับภัยคุกคามทางไซเบอร์ตามมาตรา 60 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

รายการตรวจสอบการจัดการเหตุการณ์ (Incident Handling Checklist)

รายการตรวจสอบการจัดการเหตุการณ์		Complete
ขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)		
1	ตรวจสอบว่ามีเหตุการณ์เกิดขึ้นหรือไม่	
1.1	วิเคราะห์ตรวจจับสัญญาณเหตุการณ์ความปลอดภัยทางไซเบอร์	
1.2	ค้นหาข้อมูลเพิ่มเติมที่มีความสัมพันธ์กัน	
1.3	ดำเนินการสืบค้นข้อมูล (เช่น Search Engines, ฐานข้อมูลอื่น ๆ เป็นต้น)	
1.4	ทันทีที่ผู้จัดการรับมือฯ เหตุการณ์เชื่อว่ามีเหตุการณ์เกิดขึ้น ให้เริ่มบันทึกการสอบสวนและรวบรวมหลักฐาน	
2	จัดลำดับความสำคัญในการจัดการเหตุการณ์ตามระดับความรุนแรงของภัยคุกคามที่เกิดขึ้น	
3	รายงานเหตุการณ์ดังกล่าวต่อผู้บริหารและหน่วยงานภายนอกที่เกี่ยวข้อง	
ขั้นการระงับภัยคุกคาม ปรามปราม และฟื้นฟูระบบงานที่ได้รับผลกระทบ (Containment, Eradication and Recovery)		
4	บันทึกเหตุการณ์, จัดเก็บและดูแลรักษาหลักฐานเกี่ยวกับเหตุการณ์ทั้งหมดก่อนเริ่มกระบวนการกู้คืนซึ่งรวมถึงการได้มาของบันทึกการยึดหลักฐานคอมพิวเตอร์ที่ได้มา หรืออุปกรณ์อื่น ๆ เพื่อสนับสนุนการสอบสวน	
5	จำกัดขอบเขต (Containment) ผลกระทบของเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยไซเบอร์	
6	ดำเนินการสอบสวน (Investigate) สาเหตุและผลกระทบของเหตุการณ์	
7	ทำการกำจัดสาเหตุ (Eradicate the Incident)	
7.1	ระบุช่องโหว่ของระบบที่โดนโจมตีและบรรเทาผลกระทบที่เกิดขึ้น	
7.2	กำจัด หรือลบมัลแวร์ และสาเหตุภัยคุกคามอื่นๆ	
7.3	หากมีการตรวจพบว่ามีระบบใหม่ได้รับผลกระทบ (เช่น การติดมัลแวร์ใหม่) ให้ทำซ้ำขั้นตอนการตรวจจับและการวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)	
8	เรียกใช้งานกระบวนการกู้คืน (Recovery Process)	
8.1	ระบบที่ได้รับผลกระทบจากภัยคุกคามกลับสู่สถานะพร้อมใช้งาน	
8.2	ยืนยันว่าระบบที่ได้รับผลกระทบกลับมาทำงานได้ตามปกติ	
8.3	หากจำเป็น ให้ดำเนินการติดตามสถานการณ์ต่อไป เพื่อค้นหาเหตุการณ์ความมั่นคงปลอดภัยไซเบอร์ที่อาจเกี่ยวข้องในอนาคต	
การดำเนินการภายหลังการแก้ปัญหาภัยคุกคามทางไซเบอร์ (Post-Incident Activity)		
9	จัดทำรายงานการติดตามผล	
10	จัดการประชุมทบทวนบทเรียนที่เกิดจากเหตุการณ์ดังกล่าว	

ผู้จัดทำร่าง

๑. นายพิสิษฐ์ ป้อมทอง
นักวิชาการคอมพิวเตอร์ชำนาญการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

๒. นายทรงเกียรติ ตะเภาทอง
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
กลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

ที่ปรึกษา

๑. นางสาวจิรัชก ห้วยหงษ์ทอง
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร
๒. นายนฤฤทธิ์ มัยรัตน์
นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร