กรอบมาตรฐานทางไซเบอร์

(Cyber Security Framework)

รหัสเอกสาร 000 – 001 เวอร์ชั่น 1.0

ประเภทเอกสาร เผยแพร่ ประกาศครั้งที่ 01

ประเภทชั้นความลับ ลำดับหน้า

ชื่อเอกสาร กรอบมาตรฐานด้านความมั่นคงทางไซเบอร์ (Cyber Security Framework)

การอนุมัติเอกสาร

ผู้จัดทำ	ผู้สอบทาน	ผู้อนุมัติ
นางสาวณรัณภัช แสงทอง ลงนาม: (_____) ตำแหน่ง ผู้อำนวยการส่วนคอมพิวเตอร์และเครือข่าย วันที่ ___/_____/_____	นายประสงค์ ธัมมะปาละ ลงนาม: (_____) ตำแหน่ง ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร วันที่ ___/_____/_____	นายบุญธรรม เลิศสุขีเกษม ลงนาม: (_____) ตำแหน่ง อธิบดีกรมป้องกันและบรรเทาสาธารณภัย วันที่ ___/_____/_____/

ลำดับการประกาศใช้และประวัติการปรับปรุงเอกสาร

ครั้งที่	เวอร์ชั่น	คำอธิบายและเหตุผลในการแก้ไข	วันประกาศใช้	
			เริ่มใช้	ยกเลิก

สารบัญ

1. วัตถุประสงค์

เพื่อกำหนดกรอบแนวคิด รวมถึงวิธีปฏิบัติของระบบการบริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Management) สำหรับนำไปใช้กับการดำเนินงาน และการจัดการด้านเทคโนโลยีสารสนเทศของกรมป้องกันและบรรเทาสาธารณภัยที่ครอบคลุม

2. ขอบเขต

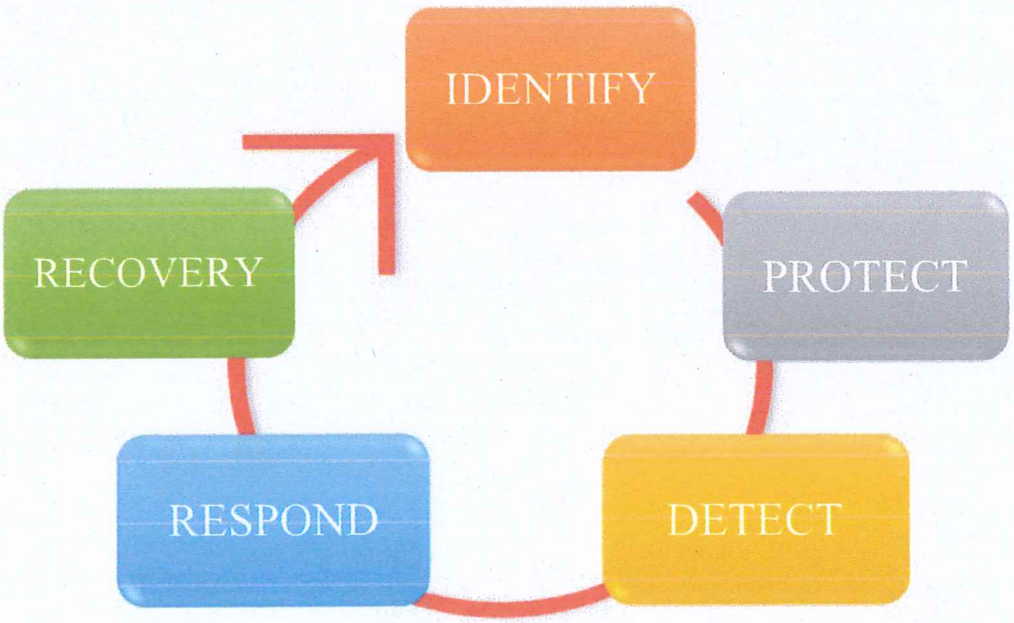
เพื่อกำหนดกรอบ และวิธีปฏิบัติสำหรับการทำงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) สำหรับบริหารจัดการระบบเทคโนโลยีสารสนเทศที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย

3. คำนิยาม

คำนิยาม	ความหมาย
โครงสร้างพื้นฐานสำคัญทางสารสนเทศ	คอมพิวเตอร์หรือระบบคอมพิวเตอร์ ซึ่งหน่วยงานของรัฐหรือหน่วยงานเอกชน ใช้ในกิจการของตนที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยของรัฐ ความปลอดภัยสาธารณะ ความมั่นคงเศรษฐกิจของประเทศ หรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ
หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ(หน่วยงาน CII)	หน่วยงานของรัฐหรือหน่วยงานเอกชน ซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
หน่วยงานควบคุมหรือกำกับดูแล	หน่วยงานของรัฐ หน่วยงานเอกชน หรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่ และอำนาจในการในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐ หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
บริการที่สำคัญ	ภารกิจ หรือบริการของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศตามมาตรา ๔๙
สำนักงาน	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
กกม.	คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์

4. กรอบการดำเนินการ

กรอบการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Framework) จัดทำขึ้นตามประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564 ซึ่งสามารถสรุปกิจกรรมที่จะต้องดำเนินการต่าง ๆ ได้ดังต่อไปนี้



ภาพที่ 1 กรอบมาตรฐานด้านการรักษาความมั่นคงทางไซเบอร์

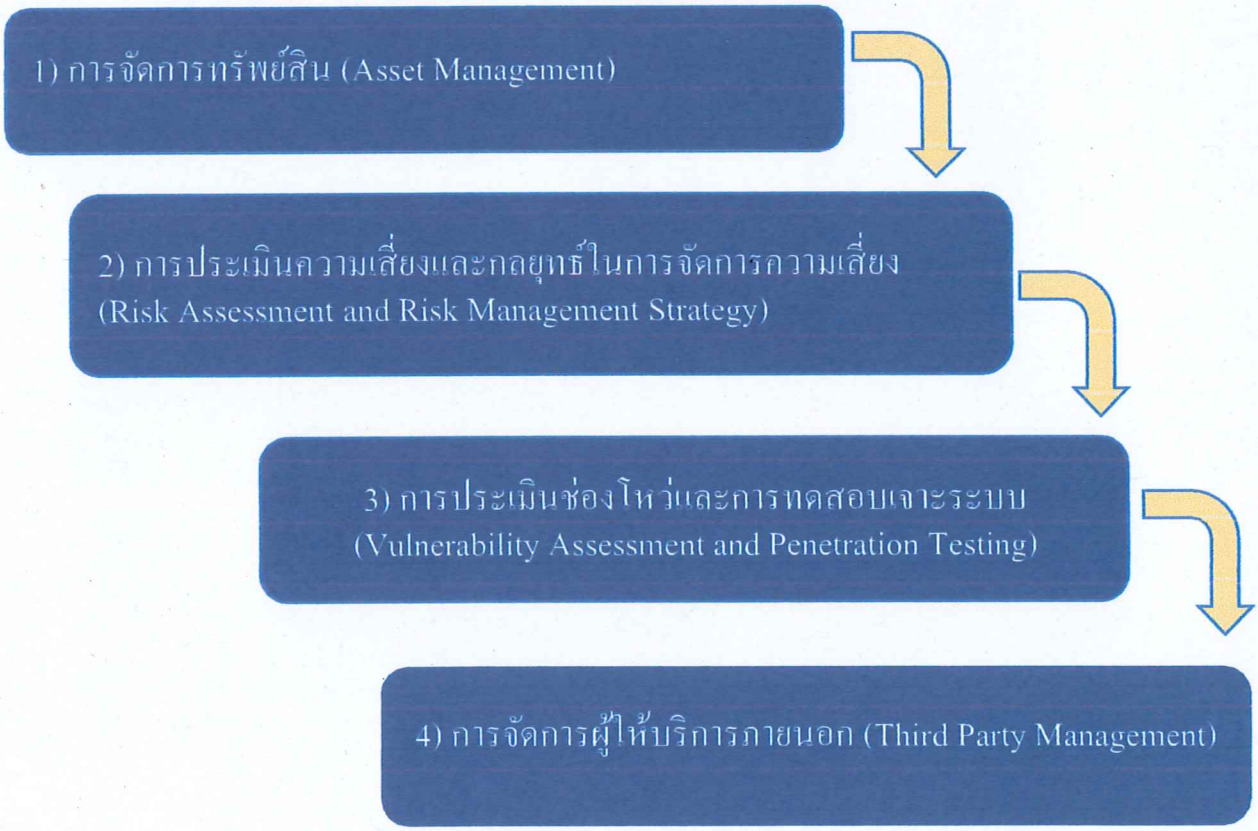
กิจกรรมตามกรอบมาตรฐาน

รายละเอียดของแต่ละกิจกรรมมีดังนี้

1. การระบุความเสี่ยงที่อาจจะเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ข้อมูลที่เกี่ยวข้องกับระบบความพิวเตอร์ ทรัพย์สินและชีวิตร่างกายของบุคคล (Identify)
2. มาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)
3. มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)
4. มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)
5. มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

1. <u>กิจกรรมการระบุความเสี่ยง (Identify)</u>

รายละเอียดของกิจกรรมนี้ จะประกอบไปด้วยกระบวนการดำเนินงาน 4 ขั้นตอน ดังนี้:



ภาพที่ 2 การระบุความเสี่ยง (Identify)

1) **การจัดการทรัพย์สิน (Asset Management)**

- ต้องจัดทำทะเบียนทรัพย์สิน (Inventory) ที่ระบุทรัพย์สินของบริการที่สำคัญ และต้องทบทวนทะเบียนทรัพย์สินให้เป็นปัจจุบัน โดยรายละเอียดทะเบียนทรัพย์สิน จะต้องมีข้อมูลอย่างน้อย ดังนี้
  - ชื่อ/คำอธิบายของทรัพย์สิน ของบริการที่สำคัญ
  - ฟังก์ชันที่สำคัญของทรัพย์สิน ของบริการที่สำคัญ
  - การระบุ และการจัดลำดับความสำคัญของทรัพย์สิน ของบริการที่สำคัญ
  - ตำแหน่งทางกายภาพของทรัพย์สิน ของบริการที่สำคัญ
  - การขึ้นต่อกันของทรัพย์สิน ของบริการที่สำคัญ บนระบบ/เครือข่ายภายใน และ/หรือภายนอก
- ต้องระบุขอบเขตเครือข่ายของบริการที่สำคัญ และระบบคอมพิวเตอร์ที่เชื่อมต่อโดยตรงและมีนัยสำคัญ (Direct and Significant Interface)
- ต้องมีการตรวจสอบ และปรับปรุงทะเบียนทรัพย์สินอย่างน้อยปีละ 1 ครั้ง หากมีการเปลี่ยนแปลงใด ๆ กับทรัพย์สินของบริการที่สำคัญ
- ต้องดำเนินการประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ของบริการที่สำคัญ ซึ่งรวมถึงรายการทั้งหมดที่ระบุไว้ในทะเบียนทรัพย์ อย่างน้อยปีละ 1 ครั้ง

2) **การประเมินความเสี่ยงและกลยุทธ์ในการจัดการความเสี่ยง (Risk Assessment and Risk Management Strategy)**

- ต้องดำเนินการประเมินความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ ตามเกณฑ์ประเมินความเสี่ยงด้านรักษาความมั่นคงปลอดภัยไซเบอร์ที่กำหนดไว้ในการบริหารความเสี่ยง (Risk Management) ตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการประกาศกำหนด
- ต้องดำเนินการปรับปรุงทะเบียนความเสี่ยง โดยจัดทำเอกสารซึ่งมีรายละเอียดที่ระบุไว้อย่างน้อยดังต่อไปนี้
  - วันที่ระบุความเสี่ยง (Data the Risk is identify)
  - คำอธิบายความเสี่ยง (Description of the Risk)
  - โอกาสที่จะเกิดขึ้น (Likelihood of Occurrence)
  - ความรุนแรงของเหตุการณ์ (Severity of the Occurrence)
  - การจัดการความเสี่ยง (Risk Treatment)
  - เจ้าของความเสี่ยง (Risk Owner)
  - สถานะของการจัดการความเสี่ยง (Status of Risk Treatment)
  - ความเสี่ยงที่เหลือ (Residual Risk)

3) การประเมินช่องโหว่และการทดสอบเจาะระบบ (Vulnerability Assessment and Penetration Testing)

- ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ โดยอ้างอิงตามหลักการบริหารความเสี่ยง เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม โดยครอบคลุมบริการที่สำคัญซึ่งเป็น
  - ระบบเทคโนโลยีสารสนเทศ (Information Technology (IT) system)
- ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการประเมินช่องโหว่แต่ละรายการ ประกอบด้วย
  - การประเมินความมั่นคงปลอดภัยของโฮสต์ (Host Security Assessment)
  - การประเมินความมั่นคงปลอดภัยของเครือข่าย (Network Security Assessment)
  - การตรวจสอบความมั่นคงปลอดภัยของสถาปัตยกรรม (Architecture Security Review)
- ต้องดำเนินการประเมินช่องโหว่ของบริการที่สำคัญ เพื่อระบุจุดอ่อนด้านความมั่นคงปลอดภัยและการควบคุม สำหรับการดำเนินการทดสอบระบบใหม่ใด ๆ ที่เชื่อมต่อกับบริการที่สำคัญ หรือการดำเนินการเปลี่ยนแปลงระบบที่สำคัญใดๆ ของบริการที่สำคัญ โดยการเปลี่ยนแปลงระบบที่สำคัญ ได้แก่ การเพิ่มโมดูลแอปพลิเคชัน (Adding New Application Module) การปรับปรุงระบบและการปรับเปลี่ยนเทคโนโลยี เป็นต้น
- ควรพิจารณาดำเนินการทดสอบเจาะระบบ (Penetration Testing) ของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเตอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบ หรือความเสี่ยงจากการทดสอบเจาะระบบด้วย
- ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบในส่วนของโฮสต์ เครือข่าย และแอปพลิเคชัน ของบริการที่สำคัญ โดยเฉพาะอย่างยิ่ง ระบบเทคโนโลยีสารสนเทศ (Information Technology: IT) ที่เชื่อมต่อกับอินเตอร์เน็ต (Internet Facing) ให้สอดคล้องกับระดับของความเสี่ยง และพิจารณาผลกระทบหรือความเสี่ยงจากการทดสอบเจาะระบบด้วย
- ต้องตรวจสอบให้แน่ใจว่าขอบเขตของการทดสอบเจาะระบบ (Scope of a Penetration Test) รวมถึงการทดสอบเจาะระบบในส่วนของโฮสต์ เครือข่าย และแอปพลิเคชันของบริการที่สำคัญ โดยเฉพาะอย่างยิ่งทุกระบบที่มีการเชื่อมต่ออินเตอร์เน็ตโดยตรง (Internet Facing)
- ควรพิจารณาดำเนินการทดสอบเจาะระบบอย่างน้อยปีละ 1 ครั้ง ตามความจำเป็นเพื่อตรวจสอบความถูกต้องของระบบรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญ รวมถึงก่อนที่จะทำการทดสอบระบบใหม่ หรือการเปลี่ยนแปลงของระบบที่สำคัญ เช่น โมดูลการปรับปรุงระบบ และการปรับเปลี่ยนเทคโนโลยี เป็นต้น

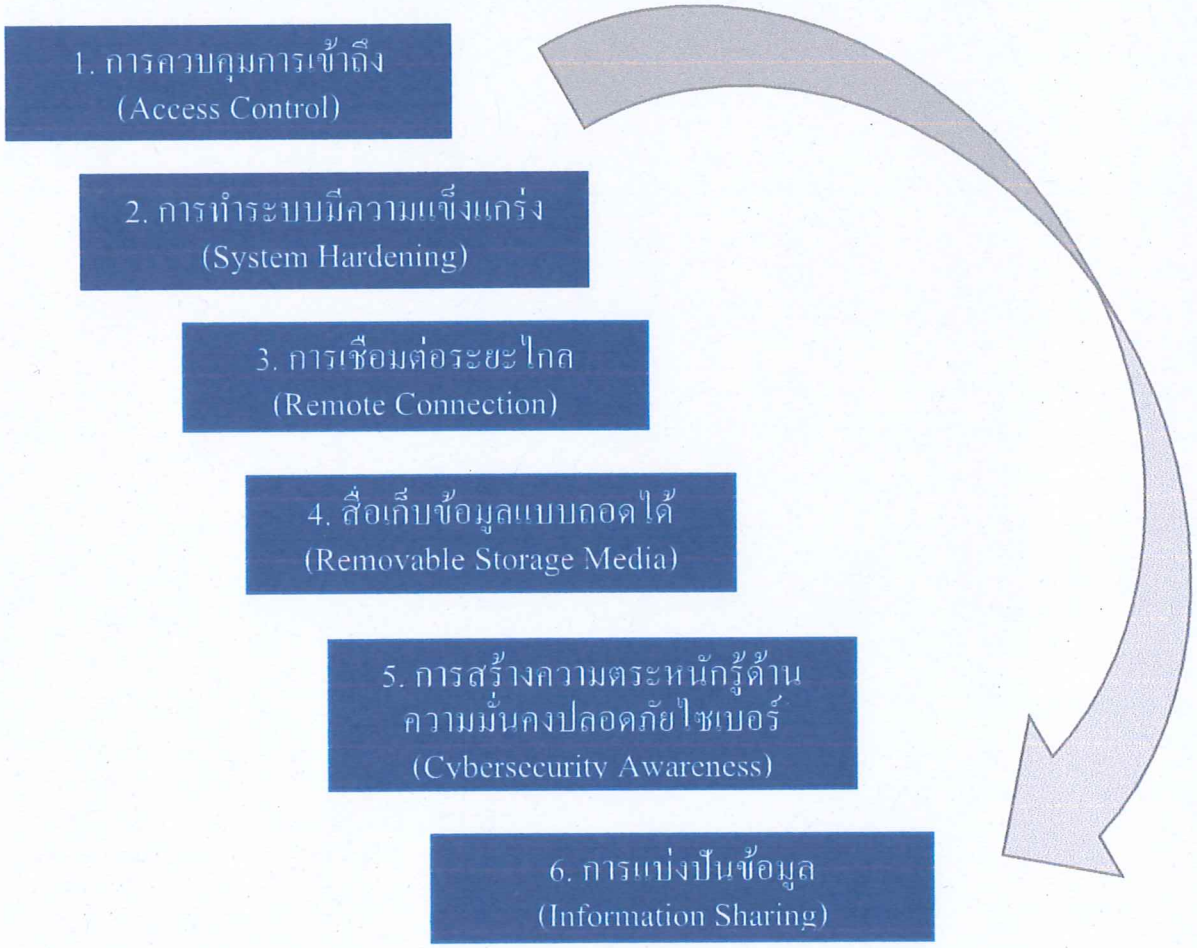
- ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบ และผู้ทดสอบเจาะระบบ (Penetration Testers) ที่จะทำการทดสอบเจาะระบบ บนโครงสร้างพื้นฐานสำคัญสารสนเทศ มีการรับรองและได้รับประกาศนียบัตร (Accreditation and Certification) ที่เป็นที่ยอมรับในอุตสาหกรรม และเป็นอิสระจากระบบที่ทำการทดสอบเจาะระบบ ทั้งนี้ คุณสมบัติของผู้ทดสอบเจาะระบบให้เป็นไปตามหลักเกณฑ์และวิธีการที่หน่วยงานควบคุมหรือกำกับดูแลกำหนด
- ต้องตรวจสอบให้แน่ใจว่าการทดสอบเจาะระบบทั้งหมดโดยผู้ให้บริการทดสอบเจาะระบบ ดำเนินการภายใต้การดูแลของกรมป้องกันและบรรเทาสาธารณภัย
- ต้องสร้างกระบวนการ เพื่อติดตามและจัดการกับช่องโหว่ที่ระบุในผลการประเมินช่องโหว่และในผลการทดสอบเจาะระบบ อีกทั้งต้องดำเนินการตรวจสอบว่าช่องโหว่ที่ระบุทั้งหมดได้รับการแก้ไขอย่างเพียงพอ
- หากได้รับการร้องขอจาก กกม. หรือสำนักงาน จะต้องส่งสำเนารายงานสรุปผลการทดสอบเจาะระบบ เพื่อประโยชน์ในการประเมินระดับความเสี่ยงด้านความมั่นคงปลอดภัยไซเบอร์ของหน่วยงานดังกล่าว ไปยังสำนักงาน ภายในกำหนด วัน นับแต่วันที่ได้รับหนังสือ

4) การจัดการผู้ให้บริการภายนอก (Third Party Management)

- ต้องรับผิดชอบ (Responsible) และมีภาระรับผิดชอบ (Accountable) ต่อการดูแลรักษาความมั่นคงปลอดภัยไซเบอร์ของกรมป้องกันและบรรเทาสาธารณภัย แม้ว่าผู้ให้บริการภายนอกจะดำเนินงานใด ๆ ก็ตามในส่วนของบริการที่สำคัญ
- ต้องมีการกำหนด ข้อกำหนดด้านความมั่นคงปลอดภัยไซเบอร์ เพื่อลดความเสี่ยงที่เกี่ยวข้องกับการเข้าถึงกระบวนการจัดเก็บ การสื่อสาร และการดำเนินการของโครงสร้างพื้นฐานสำคัญทางสารสนเทศของผู้ให้บริการภายนอก ในส่วนข้อตกลงระดับการให้บริการ (Service Level Agreement) หรือเงื่อนไขของสัญญากับผู้ให้บริการภายนอก โดยข้อกำหนดจะต้องคำนึงถึงรายละเอียดอย่างน้อย ดังต่อไปนี้
  - ประเภทของผู้ให้บริการภายนอก ที่เข้าถึงทรัพย์สินของบริการที่สำคัญ ตามความต้องการหรือตามภารกิจขององค์กร รวมถึงโปรไฟล์ด้านความเสี่ยงในการรักษาความมั่นคงปลอดภัยไซเบอร์
  - ภาระหน้าที่ของผู้ให้บริการภายนอก ในการปกป้องบริการที่สำคัญหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ จากภัยคุกคามทางไซเบอร์
  - ความเสี่ยงที่เกี่ยวข้องกับบริการ และอื่น ๆ ที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ
  - สิทธิ์ของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ในการตรวจสอบความมั่นคงปลอดภัยไซเบอร์ ของผู้ให้บริการภายนอก

2. <u>กิจกรรมการกำหนดมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)</u>

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 6 ขั้นตอน ดังนี้:



ภาพที่ 3 การกำหนดมาตรการป้องกันความเสี่ยงที่อาจจะเกิดขึ้น (Protect)

1) การควบคุมการเข้าถึง (Access Control)

- ต้องดำเนินการตรวจสอบให้แน่ใจว่า การเข้าถึงบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณะภัย ถูกจำกัดไว้ที่
  - บุคลากร และกิจกรรมที่ได้รับอนุญาตเท่านั้น
  - อุปกรณ์ และอินเทอร์เฟซ (Interface) ที่ได้รับอนุญาตเท่านั้น

- ในส่วนที่เกี่ยวกับภาระหน้าที่การตรวจสอบการเข้าถึงบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัยต้องกำหนดให้แต่ละบุคลากร กิจกรรม และกระบวนการที่ได้รับอนุญาตเท่านั้น และมีการใช้เทคนิคการตรวจสอบสิทธิ์ที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile) สำหรับแต่ละโหมดการเข้าถึงบริการที่สำคัญ
- ต้องเก็บรักษาบันทึกการเข้าถึงทั้งหมด (Logs of All Access) และความพยายามทั้งหมดในการเข้าถึงบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย และตรวจสอบบันทึกเหล่านี้ ให้สอดคล้องกับความถี่ หรือความสม่ำเสมอของกิจกรรมการเข้าถึงดังกล่าว
- ต้องตรวจสอบให้แน่ใจว่าการเข้าถึงอินเทอร์เฟซ (Interface) ของบริการที่สำคัญ (เช่น USB, พอร์ตอนุกรม) และการเข้าถึงทางลอจิคอล (Logical) มีการกำกับดูแลโดย
  - ทำภายใต้การดูแลของกรมป้องกันและบรรเทาสาธารณภัย เท่านั้น
  - ดำเนินการทั้งหมดในสถานที่หากเป็นไปได้

2) การทำให้ระบบมีความแข็งแกร่ง (System Hardening)

- ต้องสร้างมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) สำหรับระบบปฏิบัติการ แอปพลิเคชัน และอุปกรณ์เครือข่ายทั้งหมดของบริการที่สำคัญที่สอดคล้องกับโปรไฟล์ความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Risk Profile)
- มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ต้องมีหลักการรักษาความมั่นคงปลอดภัยอย่างน้อย ดังต่อไปนี้
  - สิทธิพิเศษในการเข้าถึงน้อยที่สุด (Least Access Privilege)
  - การแบ่งแยกหน้าที่ (Separation of Duties)
  - การบังคับใช้นโยบายความซับซ้อนของรหัสผ่าน
  - การลบบัญชีที่ไม่ได้ใช้
  - การลบบริการและแอปพลิเคชันที่ไม่จำเป็น เช่น การลบคอมไพเลอร์ (Removal of Compiler) และแอปพลิเคชันสนับสนุนผู้ให้บริการภายนอก (Vendor Support Application)
  - การปิดพอร์ตเครือข่ายที่ไม่ได้ใช้งาน
  - การป้องกันมัลแวร์ (Malware)
  - การปรับปรุงซอฟต์แวร์ และแพตซ์ (Patch) ความมั่นคงปลอดภัยของระบบอย่างทันการณ์และเหมาะสม

- ต้องตรวจสอบให้แน่ใจว่ามีการใช้มาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ตามที่ระบุไว้ ก่อนที่จะมีทรัพย์สินใด ๆ เชื่อมต่อหรือเมื่อมีการเปลี่ยนแปลงหรือปรับปรุงบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย
- ต้องตรวจสอบมาตรฐานการกำหนดค่าขั้นต่ำด้านความมั่นคงปลอดภัย (Security Baseline Configuration Standards) ของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ามาตรฐานเหล่านี้ยังคงมีประสิทธิภาพต่อภัยคุกคามทางไซเบอร์
- ต้องจัดทำกระบวนการจัดการเปลี่ยนแปลง (Change Management Process) เพื่ออนุญาตและตรวจสอบความถูกต้องของการเปลี่ยนแปลงระบบทั้งหมดที่มีต่อบริการที่สำคัญ ของหน่วยงานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

3) การเชื่อมต่อระยะไกล (Remote Connection)

- ต้องตรวจสอบให้แน่ใจว่าการเชื่อมต่อระยะไกลทั้งหมดมายังบริการที่สำคัญกรมป้องกันและบรรเทาสาธารณภัย มีมาตรการรักษาความปลอดภัยไซเบอร์ที่มีประสิทธิ์ภาพเพื่อป้องกันและตรวจจับการเข้าถึงโดยไม่ได้รับอนุญาต
- สำหรับการเชื่อมต่อระยะไกลกับบริการที่สำคัญกรมป้องกันและบรรเทาสาธารณภัย ต้องปฏิบัติตามแนวทางปฏิบัติ ดังต่อไปนี้
  - ในกรณีที่เป็นไปได้ ให้เปิดใช้งานการเชื่อมต่อไปยังระบบ เมื่อจำเป็นเท่านั้น
  - ในกรณีที่เป็นไปได้ ให้ใช้เทคนิคการพิสูจน์ตัวตน (Authentication Techniques) ที่มีความมั่นคงปลอดภัยในการส่ง (Transmission Security) และความสมบูรณ์ของข้อความ (Message Integrity) ที่แข็งแกร่ง
  - ใช้การเข้ารหัสสำหรับการเชื่อมต่อเครือข่ายทั้งหมด เช่น https, ssh, scp เป็นต้น
  - ไม่อนุญาตให้เชื่อมต่อระยะไกลจากการใช้คำสั่งระบบ (Issuing System Commands) ที่จะส่งผลกระทบต่อการดำเนินการบริการที่สำคัญกรมป้องกันและบรรเทาสาธารณภัย เว้นแต่จะได้รับอนุญาตอย่างชัดเจนเนื่องจากความต้องการของหน่วยงานเท่านั้น
    จำกัดการไหลของข้อมูล เฉพาะฟังก์ชันขั้นต่ำที่จำเป็นสำหรับการเชื่อมต่อเท่านั้น

4) สื่อเก็บข้อมูลแบบถอดได้ (Removable Storage Media)

- ต้องตรวจสอบให้แน่ใจว่ามีการใช้การควบคุมอย่างเข้มงวด ในการเชื่อมต่อสื่อบันทึกข้อมูลแบบถอดได้และอุปกรณ์คอมพิวเตอร์แบบพกพา (เช่น แล็ปท็อป) กับบริการที่สำคัญกรมป้องกันและบรรเทาสาธารณภัยโดยใช้มาตรการอย่างน้อย ดังนี้

- ในกรณีที่มีการใช้งานบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย ให้ปิดใช้งานพอร์ตการเชื่อมต่อภายนอกทั้งหมด (เช่น พอร์ต USB) ที่รองรับสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา และเปิดใช้งานเมื่อจำเป็นเท่านั้น
- ใช้สื่อบันทึกข้อมูลที่ได้รับอนุญาต จากกรมป้องกันและบรรเทาสาธารณภัย เท่านั้น
- ตรวจสอบว่าสื่อบันทึกข้อมูลแบบถอดได้ และอุปกรณ์คอมพิวเตอร์พกพาทั้งหมดไม่มีมัลแวร์ก่อนที่จะเชื่อมต่อกับบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย

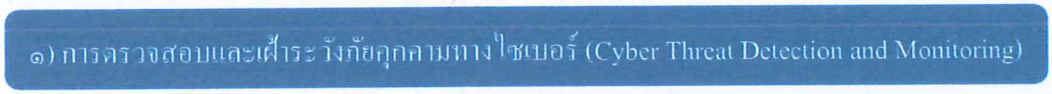
- ต้องเข้ารหัสข้อมูลในส่วนข้อมูลที่มีความละเอียดอ่อนทั้งหมดของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัยบนสื่อบันทึกข้อมูลแบบถอดได้

5) การสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness)

- ต้องให้ความสำคัญกับแผนงานในการสร้างตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Awareness) สำหรับพนักงาน ผู้รับเหมา และผู้ให้บริการภายนอก บุคคลที่สามที่สามารถเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศได้ โดยจะต้องมีรายละเอียดอย่างน้อย ดังต่อไปนี้
  - กิจกรรมให้ความรู้แก่บุคลากรทุกประเภท ได้แก่
    - พนักงานใหม่ (New Employees)
    - ผู้ใช้และผู้บริหาร (Users and Management)
    - เจ้าหน้าที่สนับสนุนโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ผู้ให้บริการ IT และ ICS
    - ผู้ขาย ผู้รับเหมา และผู้ให้บริการ (Vendors, Contractors and Service Providers)
      - การเผยแพร่ความรับผิดชอบของกลุ่ม และบุคคลตามลำดับ สำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย
      - การตระหนักรู้กฎหมายความมั่นคงปลอดภัยไซเบอร์ กฎ ระเบียบ นโยบาย แนวปฏิบัติมาตรฐาน และขั้นตอนที่เกี่ยวข้องกับการใช้งาน และการเข้าถึงโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
      - การสื่อสารอย่างสม่ำเสมอ และทันท่วงที ครอบคลุมเนื้อหาสำหรับการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์ และภัยคุกคามทางไซเบอร์ ผลกระทบ และการบรรเทาผลกระทบ
- ต้องทบทวนแผนงานในการสร้างความตระหนักรู้ด้านความมั่นคงปลอดภัยไซเบอร์อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าเนื้อหาของแผนงานยังคงเป็นปัจจุบันและมีรายละเอียดที่เกี่ยวข้องเหมาะสม

3. กิจกรรมกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 1 ขั้นตอน ดังนี้:



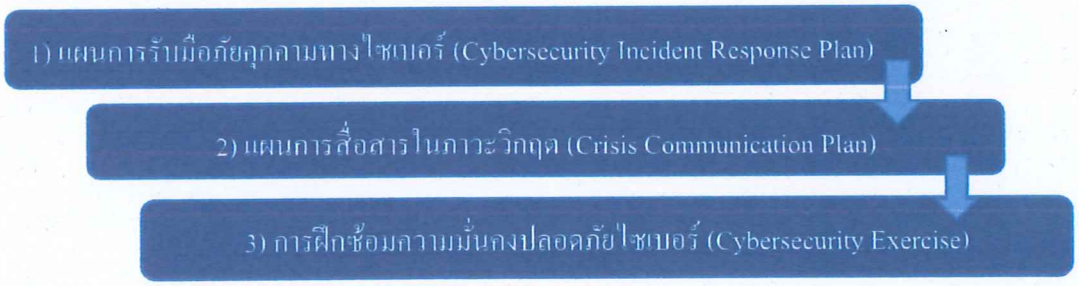
ภาพที่ 4 การกำหนดมาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Detect)

1) การตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์ (Cyber Threat Detection and Monitoring)

- ต้องสร้างกลไกและกระบวนการเพื่อ
  - ตรวจจับเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ทั้งหมดที่เกี่ยวข้องกับบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย
  - การจัดประเภทและวิเคราะห์เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่ตรวจพบ
  - การระบุว่ามีภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เกี่ยวกับบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย หรือไม่
- ต้องดำเนินการทบทวนกลไก และกระบวนการ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่ากลไกและกระบวนการต่าง ๆ ยังคงมีประสิทธิภาพ

4. กิจกรรมการกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามไซเบอร์ (Respond)

รายละเอียดของกิจกรรมนี้ ประกอบไปด้วยกระบวนการ 3 ขั้นตอน ดังนี้:



ภาพที่ 5 การกำหนดมาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์ (Respond)

1) แผนการรับมือภัยคุกคามทางไซเบอร์ (Cybersecurity Incident Response Plan)

ต้องมีการจัดทำ สื่อสาร ฝึกซ้อม ทบทวน และปรับปรุง แผนการรับมือภัยคุกคามทางไซเบอร์ตามที่ระบุไว้ในประมวลแนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ อย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าแผนการรับมือภัยคุกคามทางไซเบอร์สามารถดำเนินการได้อย่างมีประสิทธิภาพและประสิทธิผล

2) แผนการสื่อสารในภาวะวิกฤต (Crisis Communication Plan)

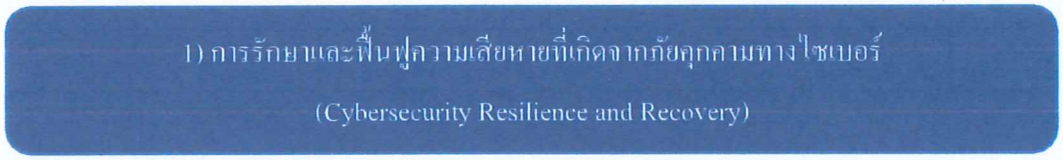
- ต้องจัดทำแผนการสื่อสารในภาวะวิกฤต เพื่อตอบสนองต่อวิกฤตที่เกิดจากเหตุการณ์
- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต มีการดำเนินการต่อไปนี้
  - จัดตั้งทีมสื่อสารในภาวะวิกฤต เพื่อเปิดใช้งานในช่วงวิกฤต
  - ระบุสถานการณ์จำลองเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ที่เป็นไปได้และแผนการดำเนินการที่เกี่ยวข้อง
  - ระบุกลุ่มเป้าหมาย และผู้มีส่วนได้ส่วนเสียสำหรับสถานการณ์จำลองเหตุการณ์ ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์แต่ละประเภท
  - ระบุโฆษกหลักและผู้เชี่ยวชาญด้านเทคนิคที่จะเป็นตัวแทนขององค์กรเมื่อกล่าวแถลงกับสื่อมวลชน
  - ระบุแพลตฟอร์ม/ช่องทางการเผยแพร่ที่เหมาะสม (เช่น สื่อดั้งเดิมและโซเชียลมีเดีย) สำหรับการเผยแพร่ข้อมูล
- ต้องตรวจสอบให้แน่ใจว่าแผนการสื่อสารในภาวะวิกฤต รวมถึงการประสานงานระหว่างทุกฝ่ายที่ได้รับผลกระทบเพื่อให้แน่ใจว่ามีการตอบสนองที่ประสานกันและสอดคล้องกันในช่วงวิกฤต
- ต้องดำเนินการฝึกซ้อมแผนการสื่อสารในภาวะวิกฤตอย่างน้อยปีละ 1 ครั้ง เพื่อให้แน่ใจว่าสามารถสื่อสารและเผยแพร่ข้อมูลได้อย่างทันท่วงทีและมีประสิทธิผลในช่วงวิกฤตอันเนื่องมาจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์

3) การฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ (Cybersecurity Exercise)

- กรมป้องกันและบรรเทาสาธารณภัย ต้องมีส่วนร่วมในการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ หากได้รับคำสั่งเป็นลายลักษณ์อักษรให้ทำ โดยคณะกรรมการการฝึกซ้อมการรักษาความมั่นคงปลอดภัยไซเบอร์ดังกล่าว อาจดำเนินการได้ทั้งในระดับชาติหรือระดับภาคส่วน กรมป้องกันและบรรเทาสาธารณภัย ต้องตรวจสอบให้แน่ใจว่าบุคลากรที่เกี่ยวข้อง ที่ระบุไว้ในแผนการรับมือภัยคุกคามทางไซเบอร์ มีส่วนร่วม ในการฝึกซ้อมความมั่นคงปลอดภัยไซเบอร์ดังกล่าว
- ต้องปฏิบัติตามคำขอใด ๆ ของคณะกรรมการ เพื่อให้ข้อมูลที่เกี่ยวข้องกับบริการที่สำคัญ กรมป้องกันและบรรเทาสาธารณภัย เพื่อวัตถุประสงค์ในการวางแผนและดำเนินการฝึกซ้อมรับมือกับภัยคุกคามทางไซเบอร์ ข้อมูลที่คณะกรรมการอาจร้องขอภายใต้ข้อนี้รวมถึงแผนการรับมือภัยคุกคามทางไซเบอร์และแผนการสื่อสารในภาวะวิกฤต และขั้นตอนการปฏิบัติงานมาตรฐานที่เกี่ยวข้องกับการดำเนินงานของบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย

5. กิจกรรมการกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

รายละเอียดของกิจกรรมนี้ ประกอบได้ด้วยกระบวนการ 1 ขั้นตอน ดังนั้น:



ภาพที่ 6 การกำหนดมาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Recover)

1) การรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์ (Cybersecurity Resilience and Recovery)

- ต้องจัดทำแผนความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP) เพื่อให้แน่ใจว่าบริการที่สำคัญของกรมป้องกันและบรรเทาสาธารณภัย สามารถให้บริการที่จำเป็นต่อไปได้ในกรณีที่เกิดการหยุดชะงัก เนื่องจากเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์ เพื่อให้สามารถใช้ปฏิบัติงานได้จริง รวมถึงสอบทานแผนของผู้ให้บริการภายนอก เพื่อพิจารณาความสอดคล้องกับแผนของหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ เช่น ความสอดคล้องกันของขอบเขตคำนิยามและการกำหนดระยะที่สำคัญ : Maximum Tolerable Period of Disruption (MTPD), Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) เป็นต้น
- ต้องตรวจสอบให้แน่ใจว่ามีการฝึกซ้อม BPC อย่างน้อยปีละ 1 ครั้ง เพื่อประเมินประสิทธิภาพของ BCP ต่อภัยคุกคามทางไซเบอร์และเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์