พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พันตำรวจเอก ณัทกฤช พรหมจันทร์

ศูนย์ประสานการรักษาความมั่นคงปลอดภัยแห่งชาติระบบคอมพิวเตอร์

NCSA National Cybersecurity Agency

Agenda

01 ความเป็นมา สาระสำคัญ พ.ร.บ.การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ พ.ศ. ๒๕๖๒

02 คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

03 ภารกิจ หน้าที่ เป้าหมายของหน่วยงาน

NCSA National Cybersecurity Agency

ความเป็นมา

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

- ประกาศในราชกิจจานุเบกษา เมื่อวันที่ ๒๗ พฤษภาคม ๒๕๖๒
- มีผลใช้บังคับ ตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เป็นต้นไป

การเฝ้าระวัง → การปกป้อง → การรับมือ → ลดความเสี่ยง

สาระสำคัญ

รวมจำนวน ๘๓ มาตรา

บททั่วไป
(วันบังคับใช้/นิยาม/ผู้รักษาการ)

หมวด ๑
คณะกรรมการ

- กมช.
  นรม. เป็นประธานฯ
  - กกม.
    รมว.ดศ.
    เป็นประธานฯ
  - คณะกรรมการ ๓ คน
    ดำเนินการรับมือภัยที่
    เร่งด่วนได้ทันที

หมวด ๓
การรักษา
ความมั่นคงปลอดภัยไซเบอร์

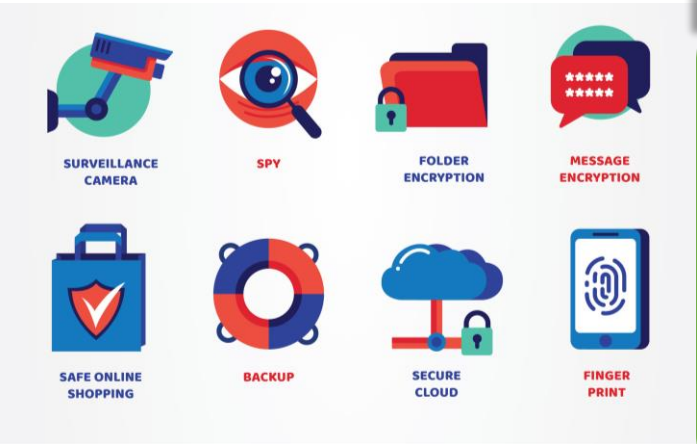
- ส่วนที่ ๑ นโยบายและแผน
- ส่วนที่ ๒ การบริหารจัดการ
- ส่วนที่ ๓ โครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- ส่วนที่ ๔ การรับมือภัยคุกคามทางไซเบอร์

บทเฉพาะกาล

หมวด ๒
สำนักงานคณะกรรมการการรักษา
ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด ๔
บทกำหนดโทษ

สาระสำคัญ



หลักการสำคัญของพระราชบัญญัติ

มุ่งที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ

วันบังคับใช้

ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป

(มีผลใช้บังคับ ตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เป็นต้นไป)

คำนิยามที่สำคัญ

➢ “ภัยคุกคามทางไซเบอร์”

หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมิชอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์โดยมุ่งหมายให้เกิดการประทุษร้ายต่อระบบคอมพิวเตอรข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และเป็นภยันตรายที่ใกล้จะถึงที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

➢ “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

➢ “หน่วยงานควบคุมหรือกำกับดูแล”

หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชนหรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

การรักษาความมั่งคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
(กมช.)

คณะกรรมการบริหารสำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
(กกม.)

สำนักงาน
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เลขาธิการ
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

โครงสร้างพื้นฐานสำคัญทางสารสนเทศ (CCI)

กมช.
ประกาศกำหนด
CII ๘ ด้าน

(๑) ด้านความมั่นคงของรัฐ

(๒) ด้านบริการภาครัฐที่สำคัญ

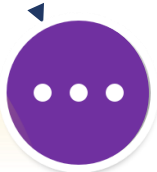
(๓) ด้านการเงินการธนาคาร

(๔) ด้านเทคโนโลยีสารสนเทศและโทรคมนาคม

(๕) ด้านการขนส่งและโลจิสติกส์

(๖) ด้านพลังงานและสาธารณูปโภค

(๗) ด้านสาธารณสุข



(๘) ด้านอื่น ตามที่ กมช. ประกาศกำหนดเพิ่มเติม

NCSA National Cybersecurity Agency

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

ประธาน =>นรม.

กรรมการโดยตำแหน่ง

1. รมว.กระทรวงกลาโหม
2. รมว.กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
3. ปลัดกระทรวงการคลัง
4. ปลัดกระทรวงยุติธรรม
5. ผู้บัญชาการตำรวจแห่งชาติ
6. เลขาธิการสภาความมั่นคงแห่งชาติ

กรรมการผู้ทรงคุณวุฒิ จำนวนไม่เกิน 7 คน (คณะรัฐมนตรีเป็นผู้แต่งตั้ง)

1. ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
2. ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
3. ด้านการคุ้มครองข้อมูลส่วนบุคคล
4. ด้านวิทยาศาสตร์
5. ด้านวิศวกรรมศาสตร์
6. ด้านกฎหมาย
7. ด้านการเงิน
8. ด้านอื่นที่เกี่ยวข้อง

- **เสนอนโยบาย**
- **จัดทำแผนปฏิบัติการ**
- **การกำหนดมาตรการ แนวทาง และประกาศหลักเกณฑ์ต่างๆ**
- **แต่งตั้ง/ถอดถอนเลขาธิการ**

เลขานุการ => เลขาธิการ

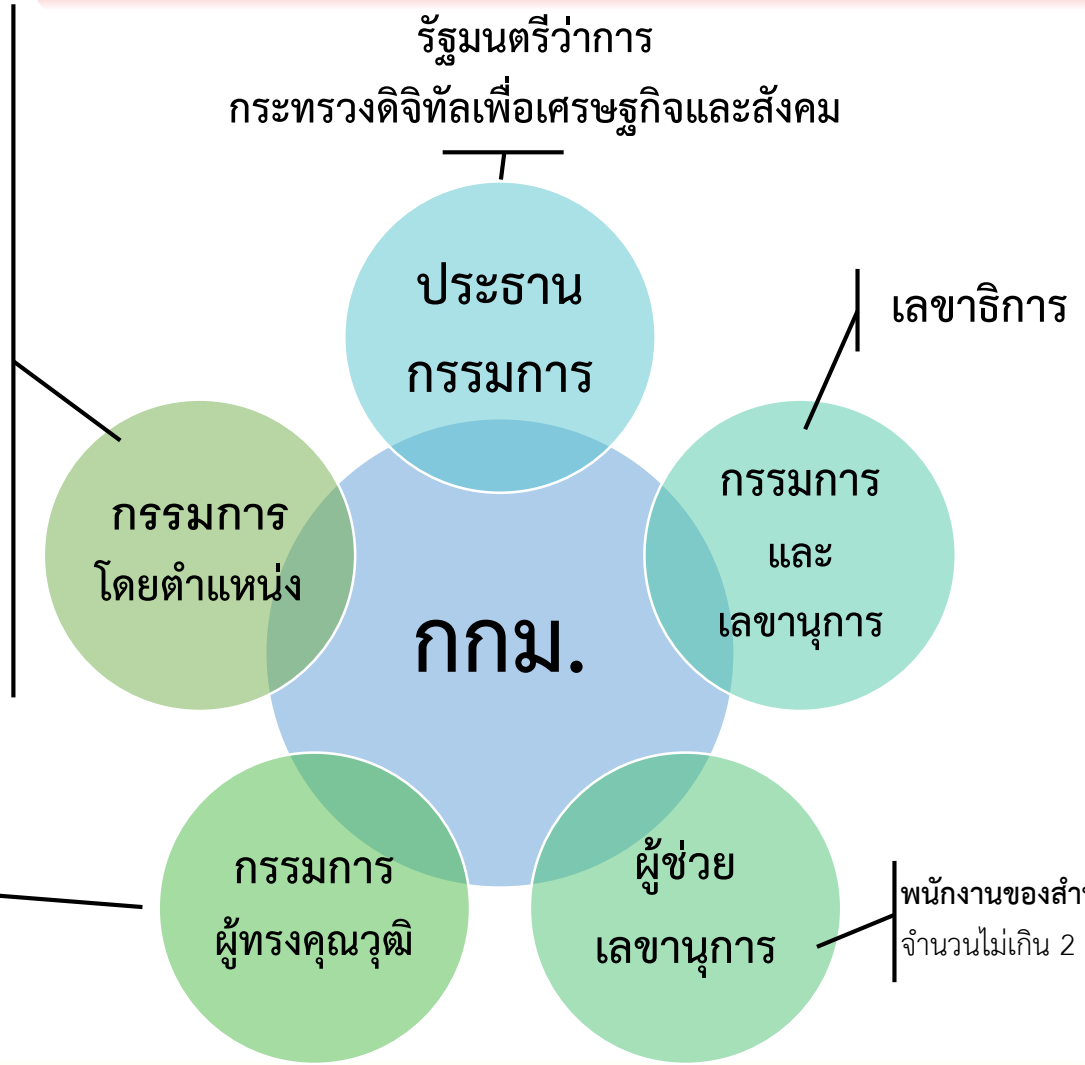
ผู้ช่วยเลขานุการไม่เกิน 2 คน (สกมช.)

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

จำนวน 13 คน

1. ปลัดกระทรวงการต่างประเทศ
2. ปลัดกระทรวงคมนาคม
3. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
4. ปลัดกระทรวงพลังงาน
5. ปลัดกระทรวงมหาดไทย
6. ปลัดกระทรวงสาธารณสุข
7. ผู้บัญชาการตำรวจแห่งชาติ
8. ผู้บัญชาการทหารสูงสุด
9. เลขาธิการสภาความมั่นคงแห่งชาติ
10. ผู้อำนวยการสำนักข่าวกรองแห่งชาติ
11. ผู้ว่าการธนาคารแห่งประเทศไทย
12. เลขาธิการสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
13. เลขาธิการคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และกิจการโทรคมนาคมแห่งชาติ



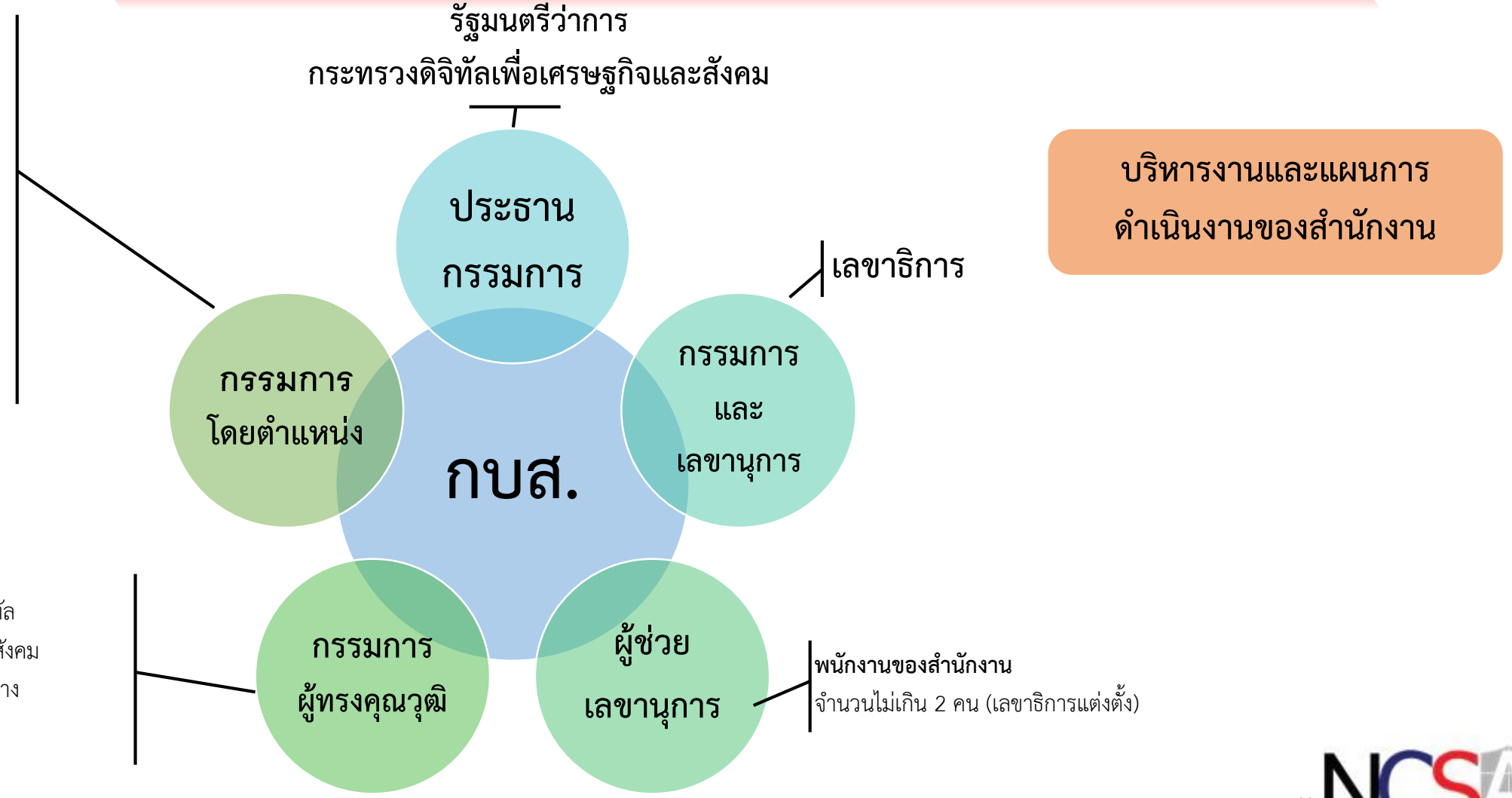
จำนวนไม่เกิน 4 คน
(คณะกรรมการแต่งตั้ง)
มีความรู้ ความเชี่ยวชาญ และประสบการณ์เป็นที่ประจักษ์ และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์

พนักงานของสำนักงาน
จำนวนไม่เกิน 2 คน (เลขาธิการแต่งตั้ง)

- กำกับดูแลศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
- กำหนดประมวลแนวทางปฏิบัติกรอบมาตรฐานหน้าที่ CII

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)



จำนวนไม่เกิน 6 คน

วาระการดำรงตำแหน่งคราวละ 4 ปี
(คณะรัฐมนตรีเป็นผู้แต่งตั้ง)

1. ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
2. ด้านเทคโนโลยีสารสนเทศและการสื่อสาร
3 .ด้านเศรษฐศาสตร์
4. ด้านสังคมศาสตร์
5. ด้านกฎหมาย
6. ด้านบริหารธุรกิจ
7. ด้านอื่นที่เกี่ยวข้อง

จำนวน 4 คน

1. ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
2. อธิบดีกรมบัญชีกลาง
3. เลขาธิการ ก.พ.
4. เลขาธิการ ก.พ.ร.

บริหารงานและแผนการดำเนินงานของสำนักงาน

พนักงานของสำนักงาน
จำนวนไม่เกิน 2 คน (เลขาธิการแต่งตั้ง)

NCSA National Cybersecurity Agency

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- เป็นหน่วยงานธุรการของ คกก. ทั้ง 3 คณะ
- ส่งเสริม สนับสนุน งานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- ปฏิบัติการ ประสานงานเฝ้าระวัง แจ้งเตือน ให้ความช่วยเหลือ
- จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
- เป็นศูนย์กลางในการรวบรวมและวิเคราะห์ข้อมูลด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ รวมทั้งเผยแพร่ข้อมูลที่เกี่ยวข้องกับความเสี่ยงและเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ให้แก่หน่วยงานของรัฐและหน่วยงานเอกชน
- ศึกษาและวิจัยข้อมูลที่จำเป็นสำหรับการรักษาความมั่นคงปลอดภัยไซเบอร์ รวมทั้งดำเนินการอบรมและฝึกซ้อมการรับมือกับภัยคุกคามทางไซเบอร์ให้แก่หน่วยงานที่เกี่ยวข้องเป็นประจำ
- ฝึกอบรมเพื่อยกระดับทักษะความเชี่ยวชาญในการปฏิบัติหน้าที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
- รายงานความคืบหน้าและสถานการณ์เกี่ยวกับการปฏิบัติตามพระราชบัญญัตินี้

นโยบายและแผน (มาตรา ๔๑ – ๔๔)

นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ ต้องมีเป้าหมายและแนวทางอย่างน้อย ดังต่อไปนี้

๑	การบูรณาการการจัดการในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ
๒	การสร้างมาตรการและกลไกเพื่อพัฒนาศักยภาพในการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์
๓	การสร้างมาตรการในการปกป้องโครงสร้างพื้นฐานสำคัญทางสารสนเทศของประเทศ
๔	การประสานความร่วมมือระหว่างภาครัฐ เอกชน และประสานความร่วมมือระหว่างประเทศเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์
๕	การวิจัยและพัฒนาเทคโนโลยีและองค์ความรู้ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์
๖	การพัฒนาบุคลากรและผู้เชี่ยวชาญด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ทั้งภาครัฐและเอกชน
๗	การสร้างความตระหนักและความรู้ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
๘	การพัฒนาระเบียบและกฎหมายเพื่อการรักษาความมั่นคงปลอดภัยไซเบอร์

แผนย่อย ป้องกันและแก้ไขปัญหาความมั่นคงทางไซเบอร์

กลยุทธ์ / ยุทธวิธีในการแก้ไขปัญหา

ภาพรวมแผนงาน ของ สกมช.

ปี 64

- ได้รับงบประมาณดำเนินการตั้งแต่ปี 63
- IDENTIFY / PROTECT / DETECT / RESPONSE / RECOVER
- 10% อยู่ระหว่างดำเนินการ
- LOADING... รอการจัดสรรงบประมาณดำเนินการปี 64

01 กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการ ในภาพรวม

การจัดทำแผนตาม พ.ร.บ.ไซเบอร์
- นโยบายและแผน
- แผนปฏิบัติการ
- นโยบายบริหารจัดการ (รัฐ และ CII)
- ประมวลแนวทางปฏิบัติ และกรอบมาตรฐานไซเบอร์

02 จัดองค์กร โครงสร้าง อำนาจหน้าที่ ขีดความสามารถ

- การจัดตั้ง สกมช.
- กมช.
- กกม.

03 กำหนดระบบบริหารจัดการ ในแต่ละระดับให้ชัดเจน

ดำเนินงานตามนโยบาย แผนงาน และมติของ กมช. กกม.

04 เสริมสร้างและพัฒนาระบบการรายงาน ในสถานการณ์ฉุกเฉิน

LOADING...

- ระบบ Help Desk ของ NationalCERT
- การประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์
- จัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)

05 ยกระดับแนวความคิดในการปกป้อง CII

LOADING...

- การจัดตั้งศูนย์อบรม Cybersecurity Training Center
- ยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ (Cyber Security Self-Assessment)
- ส่งเสริมและสนับสนุนการตรวจประเมินมาตรฐานขั้นต่ำ (Baseline)

06 พัฒนาการป้องกันแก้ไขปัญหาการเผยแพร่ข้อมูลที่กระทบต่อความมั่นคง

LOADING...

สร้างทีมปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team: CPT)

07 สร้างความตระหนักรู้ให้แก่ประชาชน และหน่วยงาน

LOADING...

- เผยแพร่และสร้างความเข้าใจในนโยบายและกฎระเบียบที่เกี่ยวข้องด้านการรักษาความมั่นคงปลอดภัยไซเบอร์

10%

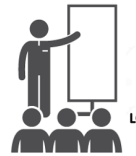
การจัดกิจกรรม/นิทรรศการ Cybersecurity Open Forum

08 ปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง

LOADING...

จัดทำนโยบายและแผนตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

09 พัฒนาศักยภาพบุคลากรและเทคโนโลยี ให้ทันสมัยพร้อมรองรับสถานการณ์



LOADING...

- จัดการแข่งขันทักษะทางไซเบอร์ (Cyber Top Talent)
- พัฒนาหลักสูตรและส่งเสริมการศึกษาร่วมกับสถาบันการศึกษาในทุกระดับ

10%

- เร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

National Cybersecurity Agency

01 กำหนดแนวความคิด มาตรการ มาตรฐาน ระบบบริหารจัดการ ในภาพรวม

การจัดทำแผนตาม พ.ร.บ.ไซเบอร์

- นโยบายและแผน - แผนปฏิบัติการ - นโยบายบริหารจัดการ (หน่วยงานรัฐ และ CII) - ประมวลแนวทางปฏิบัติและกรอบมาตรฐานไซเบอร์

(ร่าง) นโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2564-2568

VISION	วิสัยทัศน์	บริการที่สำคัญของประเทศไทยมีความมั่นคงปลอดภัยไซเบอร์ เพื่อความยั่งยืนทางเศรษฐกิจและสังคม			
4 STRATEGIES		ยุทธศาสตร์ 1	ยุทธศาสตร์ 2	ยุทธศาสตร์ 3	ยุทธศาสตร์ 4
		สร้างศักยภาพของหน่วยงานระดับชาติ ให้มีคุณภาพและมาตรฐาน	สร้างบริการภาครัฐ และโครงสร้างพื้นฐานสำคัญทางสารสนเทศให้มีความมั่นคงปลอดภัยไซเบอร์ และฟื้นคืนสู่สภาพปกติได้	บูรณาการความร่วมมือเพื่อเตรียมความพร้อมในการรับมือทางไซเบอร์ และฟื้นคืนสู่สภาพปกติได้	สร้างขีดความสามารถในการรักษาความมั่นคงปลอดภัยไซเบอร์ของประเทศ (คน องค์ความรู้ และเทคโนโลยี)
11 FOCUS AREAS		1.1 เพิ่มขีดความสามารถในการรับมือและตอบสนองต่อเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์	2.1 กำหนดมาตรการรักษาความมั่นคงปลอดภัยขั้นต่ำ CII	3.1 ส่งเสริมและสนับสนุนความร่วมมือระหว่างภาครัฐและเอกชน	4.1 เพิ่มบุคลากรที่มีความสามารถด้านความมั่นคงปลอดภัยไซเบอร์
		1.2 ส่งเสริมและสนับสนุนการแบ่งปันข้อมูลภัยคุกคาม	2.2 กำหนดโครงสร้างการกำกับดูแลและกรอบกฎหมายสำหรับ CII	3.2 ประสานความร่วมมือระหว่างประเทศเพื่อรับมือภัยคุกคาม	4.2 สร้างความตระหนักและทักษะด้านความมั่นคงปลอดภัยไซเบอร์ให้กับพลเมืองไทยและธุรกิจ
37 KEY INITIATIVES		1.3 ส่งเสริมและสนับสนุนความมั่นคงปลอดภัยไซเบอร์ขององค์กรที่ให้บริการที่สำคัญ	2.3 ปกป้องระบบของรัฐบาล (ข้อมูลและเครือข่าย)		4.3 ส่งเสริมและสนับสนุนการวิจัยและพัฒนานวัตกรรมในภาคความมั่นคงปลอดภัยไซเบอร์
		12 โครงการ	9 โครงการ	7 โครงการ	9 โครงการ

64 → 65

ยกร่างแล้วเสร็จ เตรียมนำเสนอ กมช. กกม. ประกาศบังคับใช้

ประสานหน่วยงานที่เกี่ยวข้อง กลไก ติดตามประเมินผล

02 จัดองค์กร โครงสร้าง อำนาจหน้าที่ ขีดความสามารถ

เล่ม ๑๓๖ ตอนที่ ๖๙ ก ราชกิจจานุเบกษา ๒๗ พฤษภาคม ๒๕๖๒

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน
หมวด ๒
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

มาตรา ๒๐ ให้มีสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ เป็นหน่วยงานของรัฐ มีฐานะเป็นนิติบุคคล และไม่เป็นส่วนราชการตามกฎหมายว่าด้วยระเบียบบริหารราชการแผ่นดิน หรือรัฐวิสาหกิจตามกฎหมายว่าด้วยวิธีการงบประมาณหรือกฎหมายอื่น

มาตรา ๒๑ กิจการของสำนักงานไม่อยู่ภายใต้บังคับแห่งกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยแรงงานสัมพันธ์ กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน แต่พนักงานและลูกจ้างของสำนักงานต้องได้รับประโยชน์ตอบแทนไม่น้อยกว่าที่กำหนดไว้ในกฎหมายว่าด้วยการคุ้มครองแรงงาน กฎหมายว่าด้วยประกันสังคม และกฎหมายว่าด้วยเงินทดแทน

มาตรา ๒๒ ให้สำนักงานรับผิดชอบงานธุรการ งานวิชาการ งานการประชุม และงานเลขานุการของคณะกรรมการ และ กกม. และให้มีหน้าที่และอำนาจดังต่อไปนี้ด้วย

การจัดตั้ง สกมช. และ คณะกรรมการระดับชาติ (กมช. / กกม.)

NCSA สกมช

โครงสร้างองค์กร อำนาจหน้าที่

Cybersecurity Function Incident Response	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ	สำนักประสานงาน สำนักปฏิบัติการ
Support Function Front Line	สำนักนโยบายและยุทธศาสตร์การรักษาความมั่นคงปลอดภัยไซเบอร์ ศูนย์วิจัยความมั่นคงปลอดภัยไซเบอร์ สำนักบริหารโครงสร้างพื้นฐานสำคัญทางสารสนเทศ สำนักวิชาการความมั่นคงปลอดภัยไซเบอร์แห่งชาติ สำนักกฎหมาย	
Support Function Backoffice	สำนักบริหารกลาง สำนักการเงินและกลยุทธ์องค์กร สำนักเทคโนโลยีสารสนเทศ	ฝ่ายตรวจสอบภายใน ฝ่ายการคุ้มครองข้อมูลส่วนบุคคล ฝ่ายพัฒนาองค์กร ฝ่ายบริหารความเสี่ยงองค์ก

เป้าหมาย ตามแผนปฏิบัติการ 64 65

- G1 มีระบบบริหารจัดการด้านความมั่นคงปลอดภัยไซเบอร์ที่พร้อมรับมือต่อภัยคุกคามในทุกรูปแบบ
- G2 หน่วยงานภาครัฐ และ CII มีการปกป้องและพร้อมตอบสนองต่อภัยคุกคามทางไซเบอร์อย่างมีประสิทธิภาพ
- G3 มีเครือข่ายความร่วมมือที่เข้มแข็ง ทั้งในประเทศและต่างประเทศ
- G4 มีบุคลากรไซเบอร์อย่างเพียงพอ สอดรับกับความต้องการของประเทศ
- G5 หน่วยงานที่เกี่ยวข้องมีความตระหนัก รับรู้ และเข้าใจถึงความสำคัญในการรักษาความมั่นคงปลอดภัยไซเบอร์

อยู่ระหว่างดำเนินการ

จัดหาบุคลากรในระยะแรก
โดยการยืมตัวข้าราชการและเจ้าหน้าที่ของรัฐ

ผลักดันการขอรับการจัดสรรงบประมาณ

NCSA National Cybersecurity Agency

การจัดตั้ง สกมช. และ คณะกรรมการระดับชาติ (กมช. / กกม.)

คณะกรรมการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

กมช.

- กำหนดนโยบาย แผนปฏิบัติการ.
- กำหนดแผนปฏิบัติการ
- กำหนดมาตรการ แนวทาง และประกาศหลักเกณฑ์ต่าง ๆ

กกม.

- กำกับดูแล NationalCERT
- กำหนดประมวลแนวทางปฏิบัติและมาตรฐานหน้าที่ CII
- บริหารจัดการเหตุการณ์ภัยคุกคามทางไซเบอร์

03 กำหนดระบบบริหารจัดการในแต่ละระดับให้ชัดเจน

พระราชบัญญัติ
การรักษาความมั่นคงปลอดภัยไซเบอร์
พ.ศ. ๒๕๖๒

พระบาทสมเด็จพระปรเมนทรรามาธิบดีศรีสินทรมหาวชิราลงกรณ
พระวชิรเกล้าเจ้าอยู่หัว

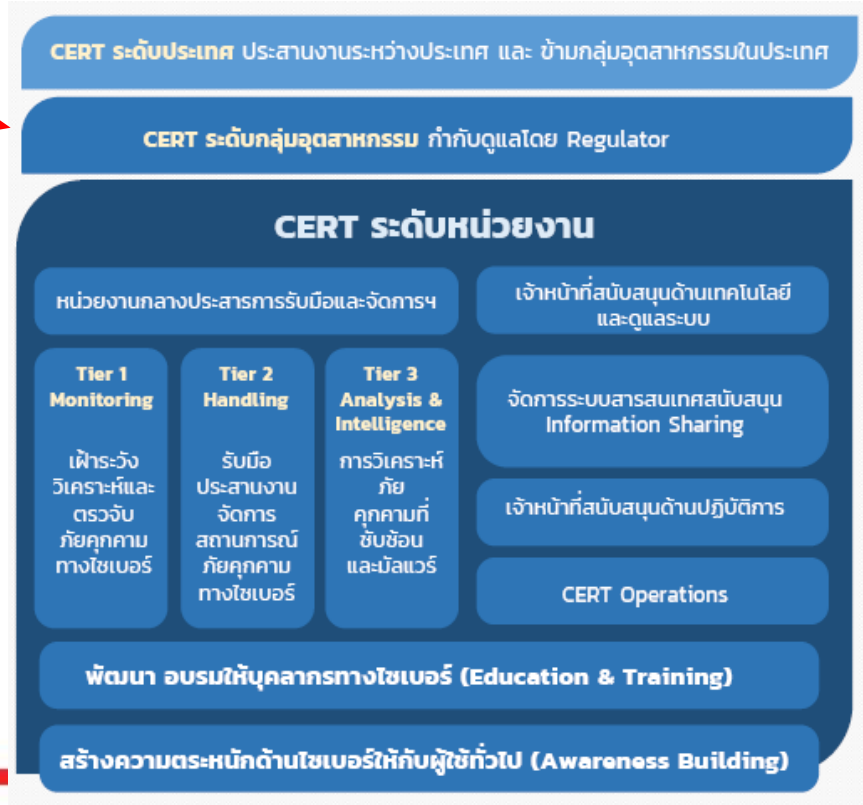
ให้ไว้ ณ วันที่ ๒๔ พฤษภาคม พ.ศ. ๒๕๖๒
เป็นปีที่ ๔ ในรัชกาลปัจจุบัน

ดำเนินงานตามนโยบาย แผนงาน และมติของ กมช. กกม.

บังคับใช้ / ครอบคลุม

- หน่วยงานของรัฐ
- CII
- คณะกรรมการระดับชาติ กมช. กกม.
- จัดตั้งหน่วยงานที่ดูแลเป็นการเฉพาะ

1. นโยบายและแผน
2. ติการ
3. นโยบายบริ ารการ (หน่วยงานของรัฐ และ CII)
4. ประมวลแนวทางปฏิบัติและกรอบมาตรฐานไซเบอร์



ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ

NationalCERT

IDENTIFY / PROTECT / DETECT / RESPONSE / RECOVER

- เฝ้าระวัง วิเคราะห์และตรวจจับภัยคุกคามไซเบอร์ (Monitor)
- รับมือ ประสานงาน และจัดการกับสถานการณ์ภัยคุกคามไซเบอร์
- วิเคราะห์ภัยคุกคามไซเบอร์ที่ซับซ้อนและมัลแวร์
- ตรวจประเมินความมั่นคงปลอดภัยของระบบ
- แลกเปลี่ยนและเผยแพร่ข้อมูลภัยคุกคามทางไซเบอร์
- ประเมินความเสี่ยงและวางแผนความต่อเนื่องของบริการสำคัญ
- พัฒนา อบรมบุคลากรทางไซเบอร์
- สร้างความตระหนักด้านไซเบอร์

04 เสริมสร้างและพัฒนาระบบการรายงานในสถานการณ์ฉุกเฉิน

LOADING...

รอการจัดสรรงบประมาณดำเนินการปี 64

LOADING...

1. ระบบ Help Desk ของ NationalCERT

1 ระบบบริหารจัดการรับแจ้งปัญหา พร้อมติดตั้งระบบเครือข่าย รองรับ 60 คู่สาย

2. การประเมินความเสี่ยงต่อภัยคุกคามไซเบอร์ของประเทศ

1 จำนวนรายงานการวิเคราะห์และประเมินความเสี่ยงฯ และกำหนดแนวทางการบริหารความเสี่ยงฯ ของประเทศ ไม่น้อยกว่า 4 ฉบับ

3. จัดตั้งปฏิบัติการร่วมทางไซเบอร์ (NCSA War room)

1 จัดสร้างห้องปฏิบัติการร่วมทางไซเบอร์ + เครื่องมือเทคนิค 1 ห้อง

2 รองรับการปฏิบัติการร่วมไม่น้อยกว่า 10 หน่วยงาน

64 → 65

ระยะเวลาดำเนินการ 9 เดือน

ดำเนินการต่อเนื่อง

NCSA National Cybersecurity Agency

รอการจัดสรรงบประมาณ
ดำเนินการปี 64

LOADING...

1 การจัดตั้งศูนย์อบรม Cybersecurity Training Center

- 1 ศูนย์ฝึกอบรมแบบ Smart Classroom
- 2 ยกระดับการฝึกอบรมให้มีคุณภาพ มาตรฐานสากล รุ่นละ 40 คน

2 ยกระดับขีดความสามารถ (Cyber Security Self-Assessment)

- 1 จำนวนหน่วยงานที่เข้าร่วมการยกระดับขีดความสามารถการรักษาความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 20 หน่วยงาน

3 ส่งเสริมและสนับสนุนการตรวจประเมินมาตรฐานขั้นต่ำ (Baseline)

- 1 จำนวนหน่วยงานที่ได้รับการส่งเสริมและสนับสนุนการตรวจประเมินมาตรฐานขั้นต่ำด้าน ไม่น้อยกว่า 10 หน่วยงาน

64 → 65

ระยะเวลาดำเนินการ 9 เดือน

ดำเนินการต่อเนื่อง

National Cybersecurity Agency

รอการจัดสรรงบประมาณดำเนินการปี 64

1 สร้างทีมปฏิบัติการป้องกันภัยไซเบอร์ (Cyber Protection Team: CPT)

1. จัดกิจกรรม Cyber League (Cyber Tier1, Tier2, Tier3) เพื่อสรรหาบุคลากรผู้ชำนาญการ เพื่อเป็นชุดปฏิบัติการทำหน้าที่ดำเนินการตอบสนองภัยคุกคาม (Incident Response) (ในระดับมหาวิทยาลัย และ ระดับบุคคลทั่วไป) และชักชวนผู้แข่งขันที่ได้รับรางวัลให้เข้าร่วมทีมป้องกันภัยทางไซเบอร์ จำนวนไม่น้อยกว่า 3 คน
2. จัดฝึกอบรมบุคคลากรทีมปฏิบัติการป้องกันภัย ไซเบอร์ จำนวนไม่น้อยกว่า 8 หัวข้อ
3. ผู้เข้าอบรมสอบได้ประกาศนียบัตรที่ได้มาตรฐานตามที่ NCSA ยอมรับ ได้อย่างน้อย 3 ประกาศนียบัตร

64 → 65

ระยะเวลาดำเนินการ 9 เดือน

ดำเนินการต่อเนื่อง

07 สร้างความตระหนักรู้ให้แก่ประชาชนและหน่วยงาน

LOADING...

1 เผยแพร่และสร้างความเข้าใจในนโยบายและกฎระเบียบที่เกี่ยวข้องฯ

2 การจัดกิจกรรม / นิทรรศการ Cybersecurity Open Forum

LOADING...

รอการจัดสรรงบประมาณดำเนินการปี 64

1 จำนวนผู้เข้าร่วมการประชุม / สัมมนา เผยแพร่และสร้างความเข้าใจในนโยบาย และกฎระเบียบ ไม่น้อยกว่า 640 คน

1 จัดกิจกรรมไม่น้อยกว่า 2 ครั้ง

2 จำนวนหน่วยงานที่เข้าร่วมกิจกรรมไม่น้อยกว่าร้อยละ 80 ของหน่วยงานเป้าหมาย

3 แถลงข่าวจำนวนไม่น้อยกว่า 4 ครั้ง และเผยแพร่สื่อประชาสัมพันธ์จำนวนไม่น้อยกว่า 5 เรื่อง

08 ปรับปรุงแก้ไขกฎหมายที่เกี่ยวข้อง

LOADING...

1 จัดทำนโยบายและแผนตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์

1 จำนวน นโยบาย/แผน/แนวทาง การปฏิบัติ / กฎหมาย กฎระเบียบ / แผนรับมือเหตุการณ์ทางไซเบอร์แห่งชาติ (National Cyber Incident Response Plan) ตาม พ.ร.บ. กำหนด ไม่น้อยกว่า 2 เรื่อง

64 → 65

ระยะเวลาดำเนินการ 9 เดือน

ดำเนินการต่อเนื่อง

National Cybersecurity Agency

พัฒนาศักยภาพบุคลากรและเทคโนโลยี ให้ทันสมัยพร้อมรองรับสถานการณ์

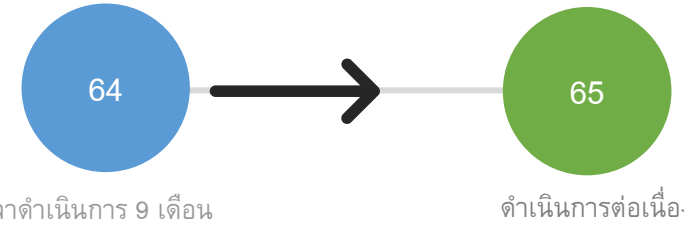
รอการจัดสรรงบประมาณ ดำเนินการปี 64

1 จัดการแข่งขันทักษะทางไซเบอร์ Cyber Top Talent

1. จัดการแข่งขันเพื่อพัฒนาศักยภาพ/เพิ่มทักษะไม่น้อยกว่า 540 คน

2 พัฒนาหลักสูตรและส่งเสริมการศึกษาร่วมกับสถาบันการศึกษา

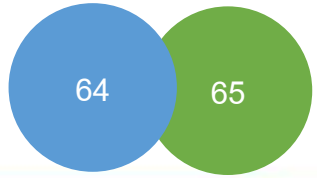
1. จำนวนสถาบันการศึกษาที่เข้าร่วมพัฒนาหลักสูตรและส่งเสริมการศึกษาด้านความมั่นคงปลอดภัยไซเบอร์ ไม่น้อยกว่า 5 หน่วยงาน
2. จำนวนนักศึกษาที่ได้รับทุนการศึกษาไม่น้อยกว่า 25 คน



3 เร่งรัดการพัฒนาบุคลากรด้านความมั่นคงปลอดภัยไซเบอร์

จำนวนบุคลากรจากหน่วยงานของรัฐและ CII ได้รับการพัฒนา

1. ความรู้พื้นฐาน จำนวนไม่น้อยกว่า 1,000 คน และต่อยอดความรู้ในระดับเทคนิค ไม่น้อยกว่า 300 คน
2. ความรู้ระดับผู้เชี่ยวชาญ จำนวนไม่น้อยกว่า 150 คน



โครงสร้างพื้นฐานสำคัญทางสารสนเทศ การรับมือกับภัยคุกคามทางไซเบอร์

ระดับร้ายแรง (มาตรา ๖๓ - ๖๕)

- ในกรณีที่มีความจำเป็นเพื่อการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ให้ กกม. มีคำสั่งให้หน่วยงานของรัฐให้ข้อมูลสนับสนุนบุคลากรในสังกัดหรือใช้เครื่องมือทางอิเล็กทรอนิกส์ที่อยู่ในความครอบครองที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์

- ในกรณีที่เกิดหรือคาดว่าจะเกิดภัยคุกคามทางไซเบอร์ซึ่งอยู่ในระดับร้ายแรง กกม. ดำเนินการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์และดำเนินมาตรการที่จำเป็น

- ในการรับมือและบรรเทาความเสียหายจากภัยคุกคามทางไซเบอร์ในระดับร้ายแรง กกม. มีอำนาจออกคำสั่งเฉพาะเท่าที่จำเป็นให้บุคคลผู้เกี่ยวข้องหรือได้รับผลกระทบ ดำเนินการเฝ้าระวัง ตรวจสอบ ดำเนินมาตรการแก้ไขภัยคุกคามทางไซเบอร์ รักษาสถานะของข้อมูล หรือในกรณีมีความจำต้องเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ กกม. ต้องยื่นคำร้องต่อศาลโดยระบุเหตุอันควรเชื่อได้ว่าบุคคลกำลังกระทำหรือจะกระทำการที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ระดับของภัยคุกคามทางไซเบอร์

ระดับไม่ร้ายแรง

- มีความเสี่ยงอย่างมีนัยสำคัญทำให้ระบบ CII/บริการของรัฐด้อยประสิทธิภาพลง
- ผู้ได้รับคำสั่งที่เกี่ยวข้องสามารถอุทธรณ์ได้

ระดับร้ายแรง

- การโจมตีเพิ่มขึ้นอย่างมีนัยสำคัญ
- มีความเสียหายต่อระบบ CII จนไม่ทำงาน / ความมั่นคงของรัฐ/ความสัมพันธ์ระหว่างประเทศ/การป้องกันประเทศ/เศรษฐกิจ/การสาธารณสุข/ความปลอดภัยสาธารณะ/ความสงบเรียบร้อยของประชาชนเสียหายจนไม่สามารถทำงานหรือให้บริการได้
- การดำเนินการที่กระทบสิทธิต้องขอคำสั่งศาล/สามารถอุทธรณ์ได้ตามกระบวนการปกติของศาล

ระดับวิกฤติ

- การโจมตีระบบ CII ระดับสูงขึ้นส่งผลกระทบรุนแรงเป็นวงกว้างทำให้การบริการล้มเหลวทั้งระบบ/ไม่สามารถแก้ไขด้วยมาตรการเยียวยาตามปกติ
- มีความเสี่ยงที่จะลุกลามไปยัง CII อื่นๆ อาจทำให้คนจำนวนมากเสียชีวิต/ระบบถูกทำลายเป็นวงกว้างระดับประเทศ
- กระทบต่อความสงบเรียบร้อยของประชาชน/เป็นภัยต่อความมั่นคงต่อรัฐอาจทำให้ประเทศอยู่ในภาวะคับขัน
- มีการกระทำความผิดเกี่ยวกับการก่อการร้ายจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตย อันมีพระมหากษัตริย์ทรงเป็นประมุข เอกราช ผลประโยชน์ของชาติ การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย
- การแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

สภาความมั่นคงแห่งชาติ

กมช. อาจมอบหมายให้เลขาฯ ดำเนินการ ได้ทันทีเท่าที่จำเป็น เพื่อเยียวยาความเสียหาล่วงหน้าโดยไม่ต้องขอศาล และต้องรายงานต่อศาลคู่ขนานไป

บทเฉพาะกาล

- ในวาระเริ่มแรก ให้ กมช. ประกอบด้วยประธานกรรมการและกรรมการโดยตำแหน่งและให้เลขาธิการ เป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช. ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้

- ให้ดำเนินการเพื่อให้มี กกม. และ กบส. ภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช.

- ให้ดำเนินการแต่งตั้งเลขาธิการตามระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ

- ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ

บทเฉพาะกาล (ต่อ)

- ระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวงกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ

- ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น

- ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนด

- เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการ เพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่มีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับไปเป็นของสำนักงานตามพระราชบัญญัตินี้

CONTACT US

NCSA Thailand

Line ID : NCSA Thailand

E-Mail: contact@ncsa.or.th

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
120 หมู่ 3 อาคารรัฐประศาสนภักดี ชั้น 7
ศูนย์ราชการเฉลิมพระเกียรติ ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง
เขตหลักสี่ กรุงเทพมหานคร

02-142-6885

CYBERSECURITY KNOWLEDGE SHARING #3

“บทเรียนจาก Hacker ในการรักษาความปลอดภัยเว็บไซต์ ”

23 มีนาคม 2564
13:00 – 15:45 น.

ห้องประชุม Walk the talk ชั้น 15 ETDA
เดอะไนน์ ทาวเวอร์ แกรนด์ พระราม 9

LIVE กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

TOPICS

- **สาธิตการเจาะเว็บไซต์ผ่านช่องโหว่ที่พบบ่อย พร้อมแนวทางป้องกัน**
- **แนะนำการจัดทำเว็บไซต์ปลอดภัย ตามแนวทางมาตรฐานเว็บไซต์ของ ETDA**

SPEAKERS

พลโท ดร.ปรัชญา เฉลิมวัฒน์
เลขาธิการ
กมช.

สุเมธ จิตภัคดีบดินทร์
White Hat Hacker
บริษัท Secure-D Center

อัมฤทธิ์ ทองทั่ว
White Hat Hacker
บริษัท Secure-D Center

พรพรหม ประภากิตติกุล
ผู้เชี่ยวชาญอาวุโส
ThaiCERT

ลงทะเบียนฟรี...ไม่มีค่าใช้จ่าย

ลงทะเบียน
shorturl.at/eqFLW

ขอขอบคุณ

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)
ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี ชั้น 7
ถนนแจ้งวัฒนะ เขตหลักสี่ กรุงเทพฯ 10210 อีเมล contact@ncsa.or.th