



พระราชบัญญัติ

การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

โดย

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

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

การเฝ้าระวัง

การปกป้อง

การรับมือ

ลดความเสี่ยง



รวมจำนวน ๘๓ มาตรา

บททั่วไป

(วันบังคับใช้/นิยาม/ผู้รักษาการ)

บทเฉพาะกาล

หมวด ๑ คณะกรรมการ

กมช.
นรม. เป็นประธานฯ

กม.
รรมว.ตศ.
เป็นประธานฯ

คณะกรรมการ ๓ คน
ดำเนินการรับมือภัยที่
เร่งด่วนได้ทันที

หมวด ๒ สำนักงานคณะกรรมการการรักษา ความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

หมวด ๓ การรักษา ความมั่นคงปลอดภัยไซเบอร์

ส่วนที่ ๑
นโยบาย
และแผน

ส่วนที่ ๒
การบริหาร
จัดการ

ส่วนที่ ๓
โครงสร้าง
พื้นฐานสำคัญ
ทางสารสนเทศ

ส่วนที่ ๔
การรับมือ
ภัยคุกคาม
ทางไซเบอร์

หมวด ๔ บทกำหนดโทษ

หลักการสำคัญของพระราชบัญญัติ

มุ่งที่จะป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เช่น ไวรัส มัลแวร์ อาชญากรคอมพิวเตอร์ ที่ทำให้ระบบคอมพิวเตอร์หรือโครงข่ายของหน่วยงานโครงสร้างพื้นฐานที่สำคัญไม่สามารถทำงานได้เป็นปกติกระทบต่อการให้บริการแก่ประชาชน หรือความสงบเรียบร้อยภายในประเทศ



วันบังคับใช้

ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศในราชกิจจานุเบกษาเป็นต้นไป
(มีผลใช้บังคับ ตั้งแต่วันที่ ๒๘ พฤษภาคม ๒๕๖๒ เป็นต้นไป)

คำนิยามที่สำคัญ

➤ “ภัยคุกคามทางไซเบอร์”

หมายความว่า การกระทำหรือการดำเนินการใดๆ โดยมีขอบโดยใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือโปรแกรมไม่พึงประสงค์ โดยมีมุ่งหมายให้เกิดการ**ประทุษร้าย**ต่อระบบคอมพิวเตอร์ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง และ**เป็นภัยอันตรายที่ใกล้จะถึง**ที่จะก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อการทำงานของคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

➤ “หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ”

หมายความว่า หน่วยงานของรัฐหรือหน่วยงานเอกชนซึ่งมีภารกิจหรือให้บริการโครงสร้างพื้นฐานสำคัญทางสารสนเทศ

➤ “หน่วยงานควบคุมหรือกำกับดูแล”

หมายความว่า หน่วยงานของรัฐ หน่วยงานเอกชนหรือบุคคลซึ่งมีกฎหมายกำหนดให้มีหน้าที่และอำนาจในการควบคุมหรือกำกับดูแลการดำเนินกิจการของหน่วยงานของรัฐหรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ



การรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
(กมช.)

คณะกรรมการบริหารสำนักงานคณะกรรมการ
การรักษาความมั่นคงปลอดภัยไซเบอร์
(กบส.)

คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์
(กกม.)

สำนักงาน

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เลขาธิการ

คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ



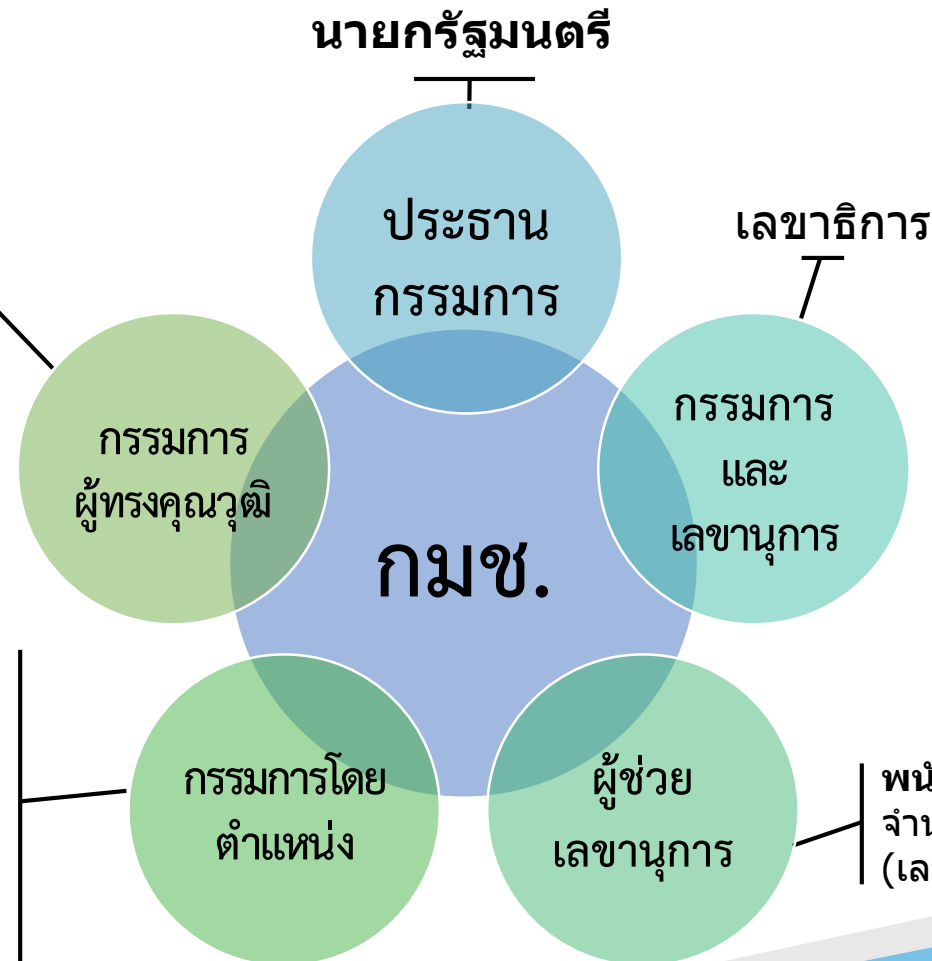
คณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (กมช.)

จำนวนไม่เกิน 7 คน
(คณะรัฐมนตรีเป็นผู้แต่งตั้ง)

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

จำนวน 6 คน

1. รัฐมนตรีว่าการกระทรวงกลาโหม
2. รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม
3. ปลัดกระทรวงการคลัง
4. ปลัดกระทรวงยุติธรรม
5. ผู้บัญชาการตำรวจแห่งชาติ
6. เลขาธิการสภาความมั่นคงแห่งชาติ



- เสนอนโยบาย
- จัดทำแผนปฏิบัติการ
- การกำหนดมาตรการแนวทาง และประกาศหลักเกณฑ์ต่างๆ
- แต่งตั้ง/ถอดถอนเลขาธิการ

พนักงานของสำนักงาน
จำนวนไม่เกิน 2 คน
(เลขาธิการแต่งตั้ง)

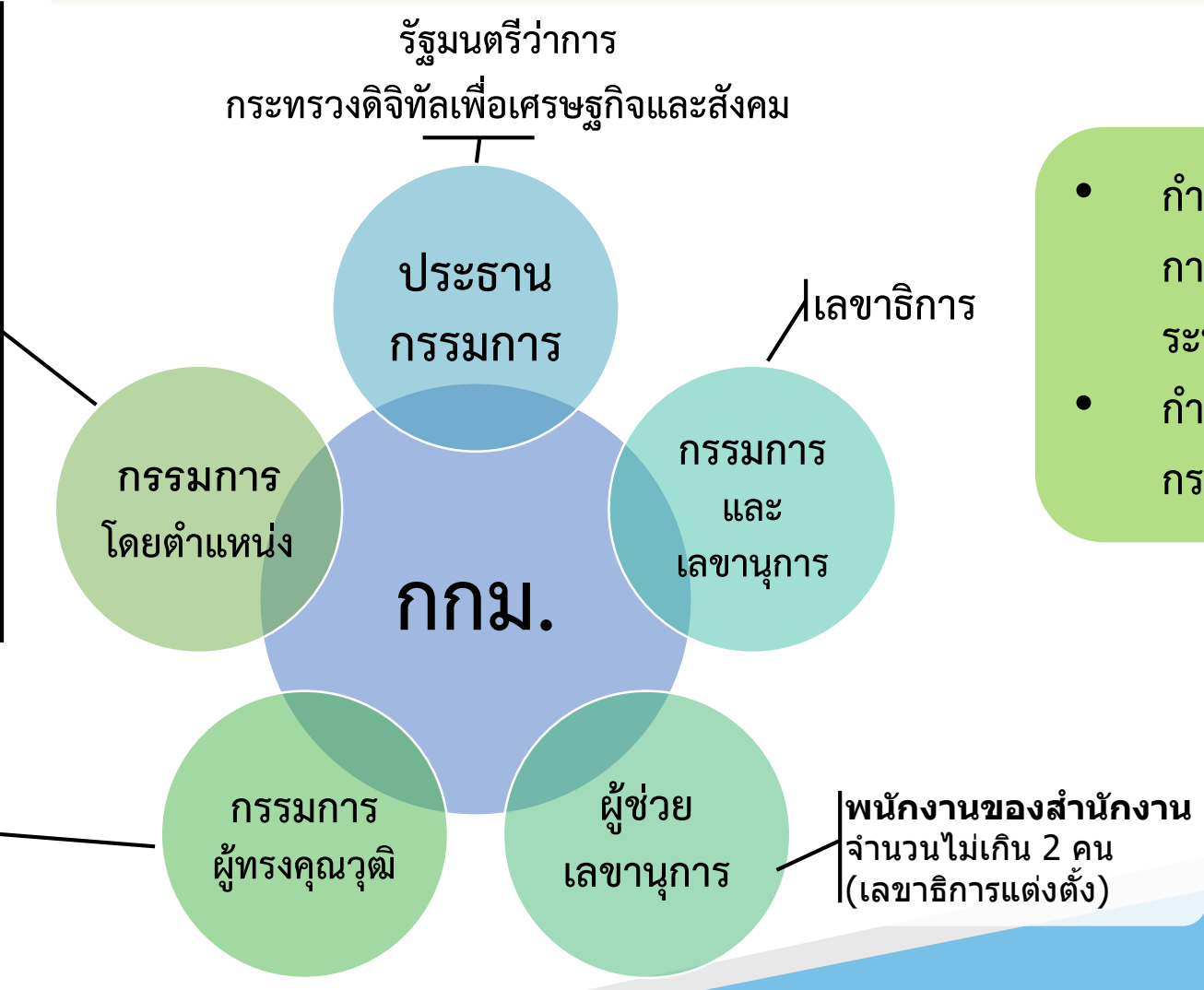
คณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ (กกม.)

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 และประสบการณ์เป็นที่ประจักษ์และเป็นประโยชน์ต่อการรักษาความมั่นคงปลอดภัยไซเบอร์



- กำกับดูแลศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ
- กำหนดประมวลผลทางปฏิบัติ กรอบมาตรฐานหน้าที่ CII

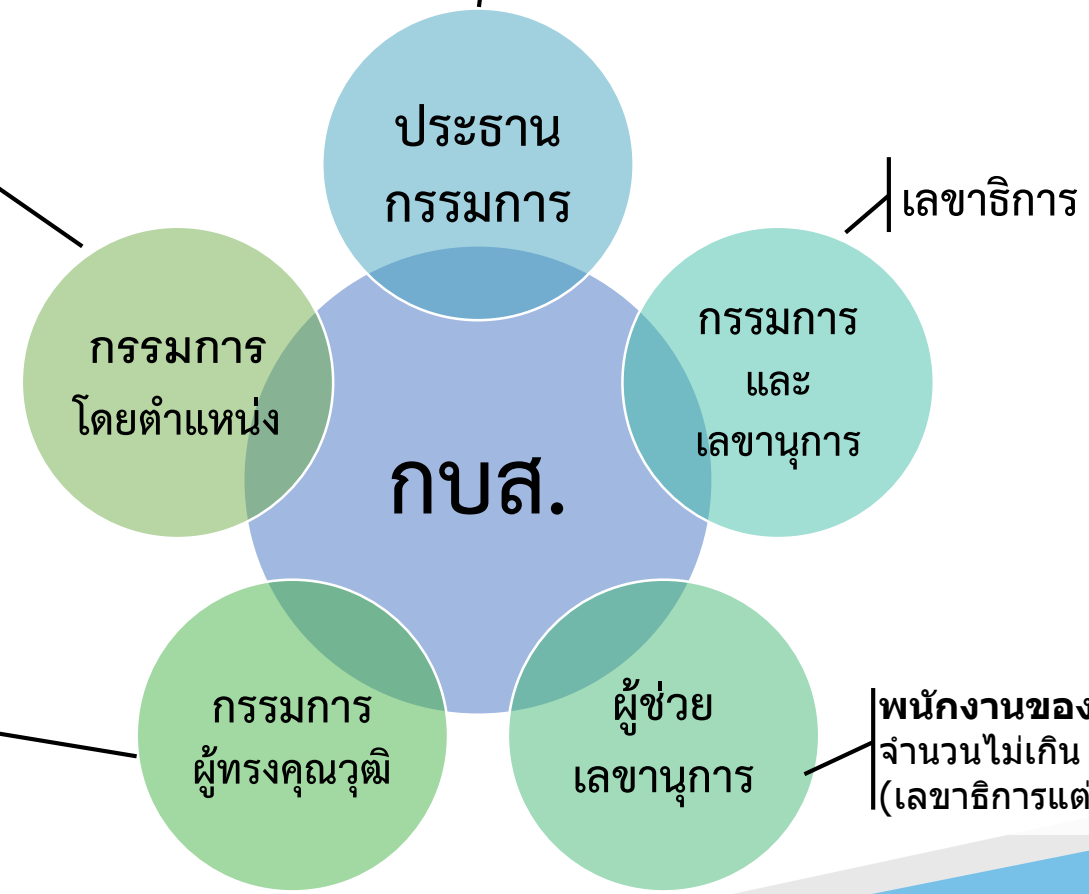
พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒

คณะกรรมการบริหารสำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์ (กบส.)

จำนวนไม่เกิน 6 คน
วาระการดำรงตำแหน่งคราวละ 4 ปี
(คณะรัฐมนตรีเป็นผู้แต่งตั้ง)

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

รัฐมนตรีว่าการ
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม



- บริหารงานและแผนการดำเนินงานของสำนักงาน

จำนวน 4 คน

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

พนักงานของสำนักงาน
จำนวนไม่เกิน 2 คน
(เลขาธิการแต่งตั้ง)

สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

- เป็นหน่วยงานธุรการของ กกก. 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

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

การรักษาความมั่นคงปลอดภัยไซเบอร์



นโยบายและแผน (มาตรา ๔๑ - ๔๔)

- คณะกรรมการฯ จัดทำนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์เพื่อเสนอคณะรัฐมนตรีเห็นชอบ
- ในการจัดทำนโยบายและแผนตามวรรคหนึ่ง ให้สำนักงานจัดให้มีการรับฟังความเห็นหรือประชุมร่วมกับหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ
- หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องดำเนินการให้เป็นไปตามนโยบายและแผน

การเฝ้า
ระวัง

การ
ปกป้อง

การรับมือ

ลดความ
เสี่ยง

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

การรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายและแผน (มาตรา ๔๑ - ๔๔)

- กกม. จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานขั้นต่ำสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานนั้น โดยคำนึงถึงหลักการบริหารความเสี่ยง ดังต่อไปนี้



- (๑) การระบุความเสี่ยงที่อาจเกิดขึ้นแก่คอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ระบบคอมพิวเตอร์ ข้อมูลอื่นที่เกี่ยวข้องกับระบบคอมพิวเตอร์ ทรัพย์สิน และชีวิตร่างกายของบุคคล
- (๒) มาตรการป้องกันความเสี่ยงที่อาจเกิดขึ้น
- (๓) มาตรการตรวจสอบและเฝ้าระวังภัยคุกคามทางไซเบอร์
- (๔) มาตรการเผชิญเหตุเมื่อมีการตรวจพบภัยคุกคามทางไซเบอร์
- (๕) มาตรการรักษาและฟื้นฟูความเสียหายที่เกิดจากภัยคุกคามทางไซเบอร์

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

การรักษาความมั่นคงปลอดภัยไซเบอร์

นโยบายและแผน (มาตรา ๔๑ - ๔๔)

- ให้องค์กรของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงานให้สอดคล้องกับนโยบายและแผนว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ และประมวลแนวทางปฏิบัติขั้นต่ำ



- (๑) แผนการตรวจสอบและประเมินความเสี่ยงด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ โดยผู้ตรวจประเมิน ผู้ตรวจสอบภายใน หรือผู้ตรวจสอบอิสระจากภายนอก อย่างน้อยปีละหนึ่งครั้ง
- (๒) แผนการรับมือภัยคุกคามทางไซเบอร์

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

การรักษาความมั่นคงปลอดภัยไซเบอร์



การบริหารจัดการ (มาตรา ๔๕-๔๗)

- หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ มีหน้าที่ป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ ตามประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ของแต่ละหน่วยงาน
- ให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ แจ้งรายชื่อเจ้าหน้าที่ระดับบริหารและระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ไปยังสำนักงาน

การเฝ้า
ระวัง

การ
ปกป้อง

การรับมือ

ลดความ
เสี่ยง

โครงสร้างพื้นฐานสำคัญทางสารสนเทศการเฝ้าระวัง (มาตรา ๕๒ - ๕๖)

- หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ ต้องให้มีการเฝ้าระวังภัยคุกคามทางไซเบอร์หรือเหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยไซเบอร์กับโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตนตามมาตรฐานซึ่งกำหนดโดยหน่วยงานควบคุมหรือกำกับดูแล และตามประมวลแนวทางปฏิบัติ รวมถึงระบบมาตรการที่ใช้แก้ปัญหาเพื่อรักษาความมั่นคงปลอดภัยไซเบอร์ที่คณะกรรมการหรือ กกม. กำหนดและต้องเข้าร่วมการทดสอบสถานะความพร้อมในการรับมือกับภัยคุกคามทางไซเบอร์ที่สำนักงานจัดขึ้น



- เมื่อมีเหตุภัยคุกคามทางไซเบอร์เกิดขึ้นอย่างมีนัยสำคัญต่อระบบของหน่วยงาน โครงสร้างพื้นฐานสำคัญทางสารสนเทศ ให้หน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ รายงานต่อสำนักงานและหน่วยงานควบคุมหรือกำกับดูแลและปฏิบัติกรับมือกับภัยคุกคามทางไซเบอร์ตามที่กำหนดใน ส่วนที่ ๔ ทั้งนี้ กกม. อาจกำหนดหลักเกณฑ์และวิธีการกรายงานด้วยก็ได้

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

การรักษาความมั่นคงปลอดภัยไซเบอร์

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. ต้องยื่นคำร้องต่อศาล โดยระบุเหตุอันควรเชื่อได้ว่าบุคคลกำลังกระทำหรือจะกระทำการที่ก่อให้เกิดภัยคุกคามทางไซเบอร์ในระดับร้ายแรง

ระดับของภัยคุกคามทางไซเบอร์



ระดับ
ไม่ร้ายแรง

- มีความเสี่ยงอย่างมีนัยสำคัญทำให้ระบบ CII/บริการของรัฐด้อยประสิทธิภาพลง
- ผู้ได้รับคำสั่งที่เกี่ยวข้องสามารถอุทธรณ์ได้

ระดับ
ร้ายแรง

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

ระดับ
วิกฤติ

- การโจมตีระบบ CII ระดับสูงซึ่งส่งผลกระทบต่อระบบรุนแรงเป็นวงกว้างทำให้การบริการล้มเหลวทั้งระบบ/ไม่สามารถแก้ไขด้วยมาตรการเยียวยาตามปกติ
- มีความเสี่ยงที่จะลุกลามไปยัง CII อื่นๆ อาจทำให้คนจำนวนมากเสียชีวิต/ระบบถูกทำลายเป็นวงกว้างระดับประเทศ
- กระทบต่อความสงบเรียบร้อยของประชาชน/เป็นภัยต่อความมั่นคงต่อรัฐอาจทำให้ประเทศอยู่ในภาวะคับขัน
- มีการกระทำความผิดเกี่ยวกับการก่อการร้ายจำเป็นต้องมีมาตรการเร่งด่วนเพื่อรักษาไว้ซึ่งการปกครองระบอบประชาธิปไตยอันมีพระมหากษัตริย์ทรงเป็นประมุข เอกราช ผลประโยชน์ของชาติ การคุ้มครองสิทธิเสรีภาพ ความสงบเรียบร้อย
- การแก้ไขเยียวยาความเสียหายจากภัยพิบัติสาธารณะอันมีมาอย่างฉุกเฉินและร้ายแรง

สภาความมั่นคงแห่งชาติ

กมช. อาจมอบหมายให้เลขาฯ ดำเนินการ ได้ทันทีเท่าที่จำเป็น เพื่อเยียวยาความเสียหายล่วงหน้าโดยไม่ต้องขอศาล และต้องรายงานต่อศาลคู่ขนานไป



การใช้อำนาจของเจ้าหน้าที่

พระราชบัญญัตินี้ กำหนดให้มีพนักงานเจ้าหน้าที่ โดยมีหน้าที่และอำนาจ เฉพาะที่กำหนดไว้ในการป้องกัน รับมือและลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ และในการปฏิบัติหน้าที่ต้องอยู่ภายใต้การกำกับดูแลของ กกม. และเลขาธิการ

ทั้งนี้ หากเป็นการใช้อำนาจที่อาจละเมิดสิทธิของประชาชน เช่น การเข้า ตรวจสอบ ยึด อุปกรณ์คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือข้อมูลอื่น ที่เกี่ยวข้องกักระบบคอมพิวเตอร์ที่เกี่ยวข้องจะทำให้เฉพาะเท่าที่จำเป็น เพื่อป้องกันภัยคุกคามทางไซเบอร์เท่านั้น และต้องมีคำสั่งศาลก่อนเสมอ



บทกำหนดโทษ

บทกำหนดโทษ

กำหนดโทษทางอาญาไว้เฉพาะเท่าที่จำเป็นโดยแยกเป็น ๒ ประเภท คือ



โทษสำหรับพนักงานเจ้าหน้าที่



โทษสำหรับองค์กรและหน่วยงานที่มีหน้าที่ดูแลปกป้องระบบที่มีความสำคัญ
หรือองค์กรที่เกี่ยวข้องที่จำเป็นต้องช่วยเหลือดูแลระบบ แต่ละเลยการปฏิบัติหน้าที่
หรือไม่ให้ความร่วมมือในกรณีที่มีภัยคุกคามในระดับร้ายแรง

ตารางสรุปการกำหนดโทษ

<p>accountability ของผู้ใช้อำนาจ ตามกฎหมาย</p>	<ul style="list-style-type: none"> • พนักงานเจ้าหน้าที่ (ม.๗๐ ม. ๗๑) • ผู้ใด (ม.๗๒) 	<ul style="list-style-type: none"> • เปิดเผยหรือส่งมอบข้อมูลให้แก่บุคคลใด • กระทำโดยประมาทเป็นเหตุให้ผู้อื่นล่วงรู้ข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ • ล่วงรู้ข้อมูลฯ ที่พนักงานเจ้าหน้าที่ได้มาแล้วนำไปเปิดเผยต่อผู้หนึ่งผู้ใด 	<ul style="list-style-type: none"> • จำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๖๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ • จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๒๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ • จำคุกไม่เกิน ๒ ปี หรือปรับไม่เกิน ๔๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ
<p>ผิดหน้าที่ทั่วไป</p>	<p>หน่วยงาน CII (ม.๗๓)</p>	<ul style="list-style-type: none"> • ไม่รายงานเหตุภัยคุกคามทางไซเบอร์โดยไม่มีเหตุอันสมควร 	<ul style="list-style-type: none"> • ปรับไม่เกิน ๒๐๐,๐๐๐ บาท
<p>ไม่ให้ความร่วมมือในการรวบรวมข้อมูล</p>	<p>ผู้ใด (ม.๗๔)</p>	<ul style="list-style-type: none"> • ไม่ปฏิบัติตามหนังสือเรียกของพนักงานเจ้าหน้าที่หรือไม่ส่งข้อมูลให้แก่พนักงานเจ้าหน้าที่ โดยไม่มีเหตุอันสมควร 	<ul style="list-style-type: none"> • ปรับไม่เกิน ๑๐๐,๐๐๐ บาท
<p>ไม่ให้ความร่วมมือในการรับมือภัยคุกคามในระดับร้ายแรง</p>	<p>ผู้ใด (ม.๗๕ วรรคหนึ่ง) (ม. ๗๕ วรรคสอง) (ม. ๗๖) นิติบุคคล (ม. ๗๗)</p>	<ul style="list-style-type: none"> • ไม่เฝ้าระวัง/ไม่ตรวจสอบหาข้อบกพร่อง ที่กระทบต่อการรักษาความมั่นคงปลอดภัยฯ ตามคำสั่งของ กกม. โดยไม่มีเหตุอันสมควร • ไม่ดำเนินการแก้ไขภัยคุกคาม/ไม่รักษาสถานะของข้อมูลคอมฯ หรือระบบฯ ตามคำสั่งของ กกม. หรือไม่ปฏิบัติตามคำสั่งศาลเพื่อเข้าถึงข้อมูลเท่าที่จำเป็น • ชัดขวาง ไม่ปฏิบัติตามคำสั่ง ของ กกม. หรือพนักงานเจ้าหน้าที่ซึ่งปฏิบัติตามคำสั่งของ กกม. (ตรวจสอบสถานที่ / เข้าถึงข้อมูล / ทดสอบการทำงาน / ยึดหรืออายัดเพื่อตรวจวิเคราะห์) โดยไม่มีเหตุอันสมควร 	<ul style="list-style-type: none"> • ปรับไม่เกิน ๓๐๐,๐๐๐ บาท หากไม่ปฏิบัติตามคำสั่งที่ให้ปฏิบัติ ปรับเป็นรายวันอีก ไม่เกินวันละ ๑๐,๐๐๐ บาท นับแต่วันที่ครบกำหนดตามคำสั่ง • จำคุกไม่เกิน ๑ ปี หรือปรับไม่เกิน ๒๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ • จำคุกไม่เกิน ๓ ปี หรือปรับไม่เกิน ๖๐,๐๐๐ บาท หรือทั้งจำทั้งปรับ
<p>ถ้าการกระทำความผิดของนิติบุคคลเกิดจากการสั่งการหรือการกระทำของกรรมการหรือผู้จัดการ หรือบุคคลใดซึ่งรับผิดชอบในการดำเนินงานของนิติบุคคลนั้น หรือในกรณีที่บุคคลดังกล่าวมีหน้าที่ต้องสั่งการหรือกระทำการและละเว้นไม่สั่งการหรือไม่กระทำการจนเป็นเหตุให้นิติบุคคลนั้นกระทำความผิด ผู้นั้นต้องรับโทษตามที่บัญญัติไว้สำหรับความผิดนั้น ๆ ด้วย</p>			

บทเฉพาะกาล



- ในวาระเริ่มแรก ให้ กมช. ประกอบด้วยประธานกรรมการและกรรมการโดยตำแหน่งและให้เลขาธิการ เป็นกรรมการและเลขานุการ เพื่อปฏิบัติหน้าที่เท่าที่จำเป็นไปพลางก่อน และให้ดำเนินการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช. ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ ในการแต่งตั้งกรรมการผู้ทรงคุณวุฒิ รัฐมนตรีว่าการกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมอาจเสนอรายชื่อบุคคลต่อคณะรัฐมนตรีเพื่อพิจารณาแต่งตั้งเป็นกรรมการผู้ทรงคุณวุฒิดังกล่าวด้วยได้
- ให้ดำเนินการเพื่อให้มี กกม. และ กบส. ภายในเก้าสิบวันนับแต่วันที่ได้มีการแต่งตั้งกรรมการผู้ทรงคุณวุฒิของ กมช.
- ให้ดำเนินการแต่งตั้งเลขาธิการตามพระราชบัญญัตินี้ให้แล้วเสร็จภายในเก้าสิบวันนับแต่วันที่จัดตั้งสำนักงานแล้วเสร็จ
- ให้ดำเนินการจัดตั้งสำนักงานให้แล้วเสร็จเพื่อปฏิบัติงานตามพระราชบัญญัตินี้ภายในหนึ่งปีนับแต่วันที่พระราชบัญญัตินี้ใช้บังคับ



บทเฉพาะกาล



- ระหว่างที่ดำเนินการจัดตั้งสำนักงานยังไม่แล้วเสร็จ ให้สำนักงานปลัดกระทรวง กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่สำนักงานตามพระราชบัญญัตินี้ และให้ปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคมทำหน้าที่เลขาธิการจนกว่าจะมีการแต่งตั้งเลขาธิการ
- ในวาระเริ่มแรก ให้คณะรัฐมนตรีจัดสรรทุนประเดิมให้แก่สำนักงานตามความจำเป็น
- ให้รัฐมนตรีเสนอต่อคณะรัฐมนตรีเพื่อพิจารณาให้ข้าราชการ พนักงาน เจ้าหน้าที่ หรือ ผู้ปฏิบัติงานอื่นใดในหน่วยงานของรัฐ มาปฏิบัติงานที่สำนักงานเป็นการชั่วคราวภายในระยะเวลาที่คณะรัฐมนตรีกำหนด
- เมื่อพระราชบัญญัตินี้ใช้บังคับ ให้รัฐมนตรีเสนอคณะรัฐมนตรีดำเนินการ เพื่ออนุมัติให้มีการโอนบรรดาอำนาจหน้าที่ กิจการ ทรัพย์สิน สิทธิ หนี้ และงบประมาณของบรรดาภารกิจที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ของสำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ ที่มีอยู่ในวันก่อนวันที่พระราชบัญญัตินี้ใช้บังคับไปเป็นของสำนักงานตามพระราชบัญญัตินี้

