ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

Security Categorization

ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567 | มีผลใช้บังคับ 18 มกราคม 2568 → มีผลบังคับใช้กับ GOV REG และ CII

เพื่อให้ GOV REG และ CII สามารถกำหนดความสำคัญของข้อมูล/ระบบสารสนเทศ นำไปสู่การเลือกมาตรการในการควบคุมความมั่นคงปลอดภัยไซเบอร์ที่เหมาะสม ทำให้ประชาชนได้รับบริการที่มีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์อันจะส่งผลให้ธุรกิจหรือบริการภายในประเทศได้รับความเชื่อมั่นมากยิ่งขึ้น อย่างคุ้มค่า

1 STEP กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์

ให้แก่ข้อมูลหรือระบบสารสนเทศ **โดยพิจารณาวัตถุประสงค์ด้านความมั่นคงปลอดภัยไซเบอร์ (Security objectives)** ดังนี้

2 STEP ประเมินและจัดระดับผลกระทบที่อาจเกิดขึ้น

โดยพิจารณาผลกระทบในแต่ละด้าน ดังนี้

3 STEP จัดระดับผลกระทบที่อาจเกิดขึ้นเป็น 3 ระดับ

ระดับต่ำ | **ระดับกลาง** | **ระดับสูง**

ระดับผลกระทบ	การรักษาความลับ (Confidentiality)	การรักษาความถูกต้องครบถ้วน (Integrity)	สภาพพร้อมใช้งาน (Availability)
ระดับต่ำ	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับ**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **เพียงเล็กน้อยหรืออย่างจำกัด**
ระดับกลาง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับมาก**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรง**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรง**
ระดับสูง	**ข้อมูล**ที่ถูกกำหนดชั้นความลับเป็นชั้น**ลับที่สุด**	**การแก้ไขหรือทำลายข้อมูล** โดยไม่ได้รับอนุญาตอาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**	**กรณีที่ไม่สามารถเข้าถึงและใช้งาน** ได้อาจ**ส่งผลกระทบ** **อย่างร้ายแรงมาก**

หมายเหตุ

- **กรณีระบบสารสนเทศมีข้อมูลหลายประเภทข้อมูล** ให้กำหนดคุณลักษณะ โดย**ใช้ผลกระทบของข้อมูลที่มีระดับมากที่สุด**
- **หน่วยงานต้องพิจารณาทบทวนการกำหนดคุณลักษณะทุก 3 ปีเป็นอย่างน้อย** หรือทบทวนเมื่อข้อมูล ระบบสารสนเทศ หรือหน้าที่ของหน่วยงานเปลี่ยนแปลงอย่างมีนัยสำคัญ

จัดทำโดย : สำนักกฎหมาย สกมช.

ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7826
อีเมล : cii@ncsa.or.th

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

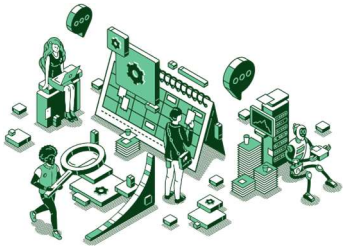
เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

Security Baselines

ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567 | มีผลใช้บังคับ 18 มกราคม 2568 → มีผลบังคับใช้กับ GOV REG และ CII

เพื่อให้ GOV REG และ CII สามารถกำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำได้อย่างเหมาะสมคุ่มค่า ลดมาตรการควบคุมและค่าใช้จ่ายที่เกินความจำเป็น ช่วยประหยัดงบประมาณแผ่นดินของประเทศ



ภายหลังจากหน่วยงานได้กำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ และได้ระดับผลกระทบที่อาจเกิดขึ้นแก่ข้อมูลหรือระบบสารสนเทศแล้ว

ให้กำหนดมาตรการควบคุมความมั่นคงปลอดภัยไซเบอร์ขั้นต่ำ

สำหรับข้อมูลหรือระบบสารสนเทศในแต่ละระดับ ดังนี้

ผลกระทบระดับต่ำ = SET A

ผลกระทบระดับกลาง = SET A + SET B

ผลกระทบระดับสูง = SET A + SET B + SET C

ประมวลแนวทางปฏิบัติ

กรอบมาตรฐานด้าน Cybersecurity

SET A

- **การประเมินความเสี่ยง** ด้าน Cybersecurity
- **แผนการรับมือ** ภัยคุกคามทางไซเบอร์

- **การระบุความเสี่ยง** (Identify)
  - การจัดการทรัพย์สิน
  - การประเมินความเสี่ยงและกลยุทธ์
- **มาตรการตรวจสอบและเฝ้าระวัง** (Detect)
  - การตรวจสอบและเฝ้าระวัง
- **มาตรการป้องกัน** (Protect)
  - การควบคุมการเข้าถึง
  - การทำให้ระบบมีความแข็งแกร่ง
  - การสร้างความตระหนักรู้
- **มาตรการเผชิญเหตุ** (Respond)
  - แผนการรับมือ
  - แผนการสื่อสารในภาวะวิกฤต
  - การฝึกซ้อม

SET B

- **แผนการตรวจสอบ** ด้าน Cybersecurity

- **มาตรการป้องกัน** (Protect)
  - การเชื่อมต่อระยะไกล
  - สื่อเก็บข้อมูลแบบถอดได้

SET C

- **การระบุความเสี่ยง** (Identify)
  - การประเมินช่องโหว่และการทดสอบเจาะระบบ
  - การจัดการผู้ให้บริการภายนอก
- **มาตรการป้องกัน** (Protect)
  - การแบ่งปันข้อมูล
- **มาตรการรักษาและฟื้นฟูความเสียหาย** (Recover)
  - การรักษาและฟื้นฟูความเสียหายที่เกิด

จัดทำโดย : สำนักกฎหมาย สกมช.

ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7826

อีเมล : cii@ncsa.or.th

ประกาศคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ

เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566

(ฐานอำนาจตามมาตรา 9 (4) แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562)

ประกาศในราชกิจจานุเบกษา 18 มกราคม 2567 | มีผลใช้บังคับ 19 มกราคม 2567

บุคคลธรรมดา คณะบุคคล หรือนิติบุคคล ที่เป็นผู้ให้บริการ Cyber Security

เพื่อส่งเสริมธุรกิจและการให้บริการด้านความมั่นคงปลอดภัยไซเบอร์ของประเทศ ให้มีคุณภาพและได้รับการยอมรับจากผู้ใช้บริการทั้งในและต่างประเทศ ส่งผลให้ประเทศมีอำนาจในการแข่งขันมากยิ่งขึ้น รวมทั้งผู้ใช้บริการสามารถเลือกผู้ให้บริการที่เหมาะสมกับตนและได้มาตรฐาน

เลือกขั้นที่ประสงค์ขอรับรองคุณภาพ

การรับรองคุณภาพของผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์มี 3 ระดับ

	ขั้นต้น	ขั้นก้าวหน้า	ขั้นสูง
ประเภทผู้ได้รับการรับรอง	บุคคลธรรมดา, คณะบุคคล, นิติบุคคล	นิติบุคคล	นิติบุคคล
เอกสาร/หลักฐานในการยื่นคำขอรับรอง	เอกสารแสดงความเชี่ยวชาญของบุคลากรของผู้ยื่นคำขอ เอกสารแสดงประสบการณ์การทำงานในประเภทบริการที่ขอรับการรับรอง		เอกสารการรับรองตนเอง ว่าปฏิบัติตามมาตรฐานที่กำหนดในประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานฯ (เฉพาะผู้ยื่นคำขอเป็นนิติบุคคล)
การตรวจรับรองคุณภาพ	✓ ตรวจเอกสาร/หลักฐาน	✓ ตรวจเอกสาร/หลักฐาน ✓ สัมภาษณ์	✓ ตรวจเอกสาร/หลักฐาน ✓ ตรวจมาตรฐานสากล ✓ สัมภาษณ์ ✓ ตรวจ ณ สถานประกอบการหรือสถานที่ให้บริการ
อายุใบรับรอง	2 ปี	3 ปี	

ขั้นตอนการดำเนินการ

START

ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

→ **ยื่นคำขอ** รับรองคุณภาพ

→ NCSA สกมช. **ตรวจสอบคำขอ** เอกสาร/หลักฐาน

→ **มอบหมายองค์กรที่ทำหน้าที่ตรวจคุณภาพ** ที่ กมช. ให้ความเห็นชอบ **หรือ** **แต่งตั้งคณะทำงานตรวจประเมิน**

→ **ตรวจสอบและประเมิน**

→ **คณะทำงานรับรองคุณภาพ** **พิจารณาผลการตรวจสอบ**

FINISH

ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมฯ

ติดต่อสอบถามเพิ่มเติม

โทร : 0 2502 7825

อีเมล : Research@ncsa.or.th

จัดทำโดย : สำนักกฎหมาย สกมช.