กรอบการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐ

GOV
หน่วยงาน
ของรัฐ

*** ดำเนินการตามนโยบายบริหารจัดการที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับ GOV** *(3 Lines of Defense, ตั้ง CISO/Head of Information Security, ทำกรอบบริหาร-ทะเบียน-ติดตามความเสี่ยง, กำหนดนโยบายจัดการความเสี่ยง, ทบทวนปีละ 1 ครั้ง)*
* ดำเนินการตามนโยบายและแผนฯ ว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ **(ม.43)**
* จัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สอดคล้องกับนโยบายและแผนที่กำหนดโดย สกมช. และป้องกัน รับมือ ลดความเสี่ยง ตามประมวลฯ **(ม.44 – 45)**
* แจ้งรายชื่อ จนท.ระดับบริหาร และระดับปฏิบัติการ เพื่อประสานงานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ไปยัง สกมช. **(ม.46)**
* **กรณีเกิด/คาดว่าจะเกิดภัยคุกคามฯ ให้ตรวจสอบเพื่อประเมินภัยคุกคาม และให้ป้องกัน รับมือ ลดความเสี่ยง ตามประมวลฯ แล้วรายงาน สกมช. และ REG โดยเร็ว (ม.58)**

มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์
* พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562
* ประกาศ กมช. เรื่อง นโยบายและแผนปฏิบัติการว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ (พ.ศ. 2565 – 2570)
* ประกาศ กกม. เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์สำหรับหน่วยงานของรัฐ และหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ. 2564
* ประกาศ กมช. เรื่อง มาตรฐานการกำหนดคุณลักษณะความมั่นคงปลอดภัยไซเบอร์ให้แก่ข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
* ประกาศ กมช. เรื่อง มาตรฐานขั้นต่ำของข้อมูลหรือระบบสารสนเทศ พ.ศ. 2566
* ประกาศ กมช. เรื่อง มาตรฐานและแนวทางส่งเสริมพัฒนาระบบการให้บริการเกี่ยวกับการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2566
* ประกาศ กมช. เรื่อง มาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ระบบคลาวด์ พ.ศ. 2567
* ประกาศ กมช. เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยสำหรับเว็บไซต์ พ.ศ. 2568

เอกสารอ้างอิง https://www.ncsa.or.th/standards/laws
* **เล่มรวมกฎหมายว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์** https://drive.ncsa.or.th/s/FQk8f6My94Brcjc

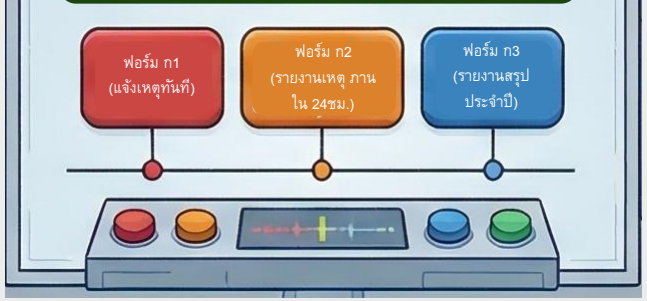
กรอบการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยไซเบอร์
สำหรับหน่วยงานของรัฐ

กระบวนการดำเนินงาน และการรายงานเหตุ (Operations & Incident Reporting)

มาตรฐานเฉพาะด้าน

- มาตรฐานคลาวด์ฯ
- มาตรฐานเว็บไซต์ฯ

การรายงานเหตุภัยคุกคามฯ



การเฝ้าระวังและการเก็บ Log

- มีกลไกตรวจสอบภัยคุกคามฯ และการจัดการ Log

การกำกับดูแล และนโยบาย (Governance & Policy) ตามนโยบายและแผนฯ ว่าด้วยความมั่นคงปลอดภัยไซเบอร์

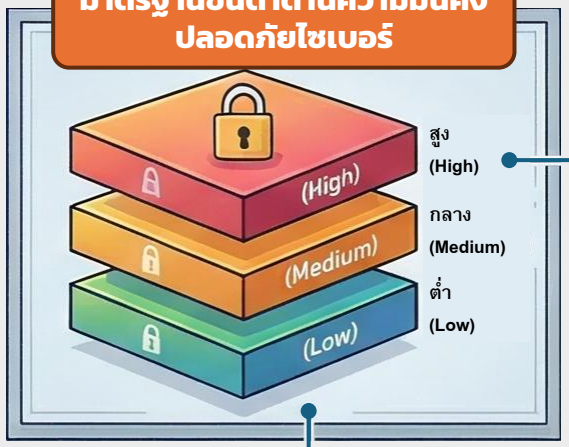
โครงสร้างบุคลากรแบบ 3 Lines of Defense

- แต่งตั้ง CISO และแบ่งหน้าที่เพื่อความโปร่งใส

การจัดทำประมวลแนวทางปฏิบัติฯ

- จัดทำแผนฯ และมีการทบทวนอย่างน้อยปีละ 1 ครั้ง

มาตรฐานขั้นต่ำด้านความมั่นคงปลอดภัยไซเบอร์



- การประเมินระดับผลกระทบ ตามหลัก CIA Triad

CIA Triad:
ความลับ (Confidentiality)
ความถูกต้อง (Integrity)
ความพร้อมใช้งาน (Availability)

เพื่อกำหนด **"มาตรฐานขั้นต่ำ"** ให้แก่ข้อมูลหรือระบบสารสนเทศ