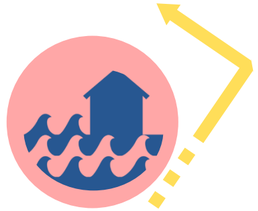
มตช. 27001-2566

ความมั่นคงปลอดภัยด้านสารสนเทศ ความมั่นคงปลอดภัยทางไซเบอร์ และการปกป้องความเป็นส่วนตัว – ระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศ – ข้อกำหนด

รับมาจาก ISO/IEC 27001: 2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements แทน มตช. ฉบับเดิม (มตช. 27001-2563) ซึ่งรับมาจาก ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ระบุข้อกำหนดสำหรับการจัดทำ การนำไปใช้ การรักษาไว้ และการปรับปรุงระบบการจัดการความมั่นคงปลอดภัยด้านสารสนเทศอย่างต่อเนื่องตามบริบทขององค์กร โดยอ้างอิงตามหลักการ 3 ประการ ได้แก่ (1) การรักษาความลับ (Confidentiality) (2) ความครบถ้วนถูกต้อง (Integrity) และ (3) ความพร้อมในการใช้งาน (Availability)

มาตรฐานนี้ใช้ได้กับทุกองค์กร โดยไม่คำนึงถึงประเภท ขนาด หรือลักษณะองค์กร



เนื้อหาของมาตรฐาน

- บริบทองค์กร (Context of the organization)
- ความเป็นผู้นำ (Leadership)
- การวางแผน (Planning)
- การสนับสนุน (Support)
- การดำเนินการ (Operation)
- การประเมินสมรรถนะ (Performance evaluation)
- การปรับปรุง (Improvement)

มตช. 27001-2566 (ต่อ)

การเปลี่ยนแปลง

การเปลี่ยนแปลงสำคัญใน Annex A ได้แก่

1. โครงสร้างโดยรวมได้รับการปรับปรุงเป็น 4 ส่วนหลัก องค์กร บุคคล กายภาพ และเทคโนโลยี แทน 14 ส่วนในฉบับก่อนหน้า

2. มาตรการควบคุม (Controls) ลดลงจาก 114 เหลือ 93 รายการ มีการรวมและลบมาตรการควบคุมบางตัว

3. แนวคิดของแอททริบิวต์ มีความสอดคลองกับคำศัพทเฉพาะที่ใชทั่วไปในระบบความปลอดภัยในโลกดิจิทัล

แอททริบิวต์ทั้ง 5 ได้แก่ (1) ประเภทการควบคุม (2) คุณสมบัติด้านการรักษาความปลอดภัยของสารสนเทศ (3) แนวคิดหลักด้านการรักษาความปลอดภัยทางไซเบอร์ (4) ความสามารถในการปฏิบัติงาน และ (5) กลุ่มการรักษาความปลอดภัย

กลุ่มเป้าหมายผู้ใช้งานมาตรฐานฉบับนี้

องค์กรที่ต้องการสร้างความเชื่อมั่นว่ามีการจัดการสารสนเทศอย่างปลอดภัย **เช่น บริษัทด้านเทคโนโลยี บริษัทการเงิน บริษัทโทรคมนาคม องค์กรที่เกี่ยวข้องกับการดูแลสุขภาพ บริษัทที่ดำเนินธุรกิจ E-commerce เป็นต้น**

จากข้อมูลของ ISO survey 2021 พบว่า มีการออกใบรับรอง ISO 27001 ให้แก่องค์กรในประเทศไทย จำนวน 370 ฉบับ

source: ISO Survey 2021 results - Number of certificates and sites per country and the number of sector overall

วัตถุประสงค์

- **สร้างความเชื่อมั่น**ให้แก่ผู้มีส่วนได้เสีย (เช่น ลูกค้า คู่ค้า) **และเพิ่มขีดความสามารถในการแข่งขันขององค์กร**
- **ปกป้องทรัพย์สินทางปัญญา ตราสินค้า (brand) และชื่อเสียงขององค์กร**
- **ช่วยหลีกเลี่ยง**การเกิดเหตุการณ์ต่าง ๆ เช่น **การละเมิดข้อมูล การเสียค่าใช้จ่ายอันเนื่องมาจากการฟ้องร้องหรือสืบสวน**