มตช. 27002-2566

ความมั่นคงปลอดภัยด้านสารสนเทศ ความมั่นคงปลอดภัยทางไซเบอร์ และการปกป้องความเป็นส่วนตัว - การควบคุมความมั่นคงปลอดภัยด้านสารสนเทศ

รับมาจาก ISO 27002: 2022 Information security, cybersecurity and privacy protection - Information security controls แทน มตช. ฉบับเดิม (มตช. 27002-2563) ซึ่งรับมาจาก ISO 27002:2013 Information technology - Security techniques - Code of practice for information security controls

ระบุชุดอ้างอิงสำหรับการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศทั่วไป ครอบคลุมถึงการประยุกต์ใช้แนวทางในการควบคุมด้านต่าง ๆ เช่น

- **การควบคุมองค์กร (Organizational controls) → ข้อ 5**
- **การควบคุมบุคลากร (People controls) → ข้อ 6**
- **การควบคุมเทคโนโลยี (Technological controls) → ข้อ 7**
- **การควบคุมทางกายภาพ (Physical controls) → ข้อ 8**

โดยมาตรฐานให้ตัวอย่างการนำแต่ละคุณลักษณะไปประยุกต์ใช้กับองค์กร ภาคผนวก A

มตช. 27002-2566 (ต่อ)

การเปลี่ยนแปลง

- **ปรับปรุงโครงสร้างมาตรฐาน**จาก 18 หัวข้อ เหลือ 8 ข้อ (จัดกลุ่มมาตรการควบคุมข้อมูลสารสนเทศออกเป็น 4 ด้าน ได้แก่ การควบคุมองค์กร การควบคุมบุคลากรการควบคุมเทคโนโลยี การควบคุมทางกายภาพ)
- **เพิ่มหัวข้อ** Threat intelligence (5.7) การใช้ cloud services (5.23) ICT readiness for business continuity (5.30) Physical security monitoring (7.4) Configuration management (8.9) Information deletion (8.10) Data masking (8.11) Data leakage prevention (8.12) Monitoring activities (8.16) Web filtering (8.23) Secure coding (8.28)

กลุ่มเป้าหมายผู้ใช้งานมาตรฐานฉบับนี้

องค์กรที่ต้องการขอการรับรอง ISO 27001 **เช่น บริษัทด้านเทคโนโลยี บริษัทการเงิน บริษัทโทรคมนาคม**
องค์กรที่เกี่ยวข้องกับการดูแลสุขภาพ บริษัทที่ดำเนินธุรกิจ E-commerce เป็นต้น

วัตถุประสงค์

เป็นแนวทางในการจัดทำมาตรการควบคุมความมั่นคงปลอดภัยด้านสารสนเทศทั่วไปขององค์กร ซึ่งช่วยให้องค์กรสามารถปกป้องทรัพย์สินทางปัญญา ตราสินค้า (brand) และชื่อเสียงขององค์กร ตลอดจนสร้างความเชื่อมั่นขององค์กร