สารบัญ

ตารางแสดงความหมายของสัญลักษณ์ **10**

1. นโยบายความมั่นคงปลอดภัยขององค์กร (Security policy) 11

1.1 นโยบายความมั่นคงปลอดภัยสำหรับสารสนเทศ (Information security policy) 11

2. โครงสร้างทางด้านความมั่นคงปลอดภัยภายในองค์กร
(Organizational Security) 12

2.1 โครงสร้างทางด้านความมั่นคงปลอดภัยของสารสนเทศภายในองค์กร(Information security infrastructure) 12

2.2 การควบคุมความมั่นคงปลอดภัยแก่หน่วยงานภายนอกที่มีความจำเป็นต้องใช้งานระบบสารสนเทศขององค์กร (Security of third party access) 14

2.3 การมอบหมายงานทางด้านสารสนเทศให้กับหน่วยงานภายนอก (Outsourcing) 15

3. การจัดหมวดหมู่และการควบคุมทรัพย์สินขององค์กร
(Asset classification and control) **15**

3.1 การจัดทำบัญชีทรัพย์สิน (Accountability for assets) 15

3.2 การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information classification) 16

4. ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร
(Personnel Security) **17**

4.1 การสร้างความมั่นคงปลอดภัยในกระบวนการสรรหาบุคลากร (Security in job definition and resourcing) 17

4.2 การอบรมพนักงาน (User training) 18

4.3 การตอบโต้ต่อเหตุการณ์ที่ละเมิดความมั่นคงปลอดภัย
(Responding to security incidents and malfunctions) 18

5. ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร
(Physical and environmental security) **20**

5.1 บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure areas) 20

5.2 ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment security) 21

5.3 การป้องกันทั่วไป (General controls) 23

6. การบริหารจัดการด้านการสื่อสารและการดำเนินงานของเครือข่ายสารสนเทศขององค์กร (Communications and operations management) **23**

6.1 การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational procedures and responsibilities) 23

6.2 การวางแผนและการตรวจรับทรัพยากรระบบสารสนเทศ (System Planning and Acceptance) 25

6.3 การป้องกันซอฟต์แวร์และสารสนเทศขององค์กร(Protection against malicious Software) 26

6.4 การสำรองข้อมูล (Housekeeping) 26

6.5 การบริหารและจัดการเครือข่ายขององค์กร (Network management) 27

6.6 การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media handling and security) 28

6.7 การแลกเปลี่ยนสารสนเทศและซอฟต์แวร์ (Exchange of information and software) 29

7. การควบคุมการเข้าถึง (Access control) **31**

7.1 การควบคุมการเข้าถึงระบบสารสนเทศ (Business requirements for access control) 31

7.2 การจัดการการเข้าถึงระบบของพนักงาน (User access management) 32

7.3 ความรับผิดชอบหน้าที่ของพนักงาน (User responsibilities) 33

7.4 การควบคุมการเข้าถึงเครือข่าย (Network access control) 34

7.5 การควบคุมการใช้งานระบบที่ให้บริการ (Operating system access control) 35

7.6 การควบคุมการใช้งานระบบสารสนเทศ (Application access control) 37

7.7 การเฝ้าดูการใช้งานระบบ (Monitoring system access and use) 38

7.8 คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถาน (Mobile computing and teleworking control) 39

8. การพัฒนาและดูแลระบบสารสนเทศ
(Systems development and maintenance) 40
8.1 การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security requirements of systems) 40
8.2 ความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security in application system) 41
8.3 การใช้การเข้ารหัสกับสารสนเทศ (Cryptographic controls) 42
8.4 ความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบ (Security of system files) 43
8.5 ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in development and support processes) 44
9. การบริหารความต่อเนื่องของการดำเนินงานขององค์กร
(Business continuity management) 46
9.1 การบริหารความต่อเนื่องให้กับการดำเนินงานขององค์กร (Aspects of business continuity) 46
10. การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศขององค์กร(Compliance) 48
10.1 การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย (Compliance with legal requirements) 48
10.2 การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยและรายละเอียดทางเทคนิค (Reviews of security policy and technical compliance) 50
10.3 การพิจารณาการตรวจสอบระบบ (System audit considerations) 51

ภาคผนวก ก 53

เกณฑ์การกำหนดระดับความเสี่ยง 61

ตัวอย่างหน่วยงานที่มีความคาบเกี่ยวกับโครงสร้างพื้นฐานที่สำคัญของประเทศไทยและควรจัดจัดทำมาตรฐานนี้ในระดับความมั่นคงปลอดภัยสูงสุด (1+2+3) 64

รายนามผู้จัดทำคณะอนุกรรมการด้านความมั่นคงภายใต้ คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ 69