



คณะทันตแพทยศาสตร์ มหาวิทยาลัยมหิดล

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้ตรวจสอบ

ผู้ช่วยคณบดีฝ่ายเทคโนโลยีสารสนเทศและสื่อสารองค์กร

ผู้รับรอง

คณบดี วิทยาธร

รองคณบดีฝ่ายเทคโนโลยีสารสนเทศและสื่อสารองค์กร

ผู้อนุมัติ

คณบดี

เลขที่เอกสาร ISMS-EX-006

วันที่อนุมัติใช้ - 1 ก.ย. 2565



### รายละเอียดเอกสาร

ประเภทเอกสาร : เอกสารภายนอก (External Document)	เลขที่เอกสาร : ISMS-EX-๐๐๒
ชื่อหน่วยงาน : คณะกรรมการด้านความมั่นคงปลอดภัยสารสนเทศ (ISMS Core Team)	ระดับชั้นความลับ : ใช้ภายในเท่านั้น
เรื่อง : แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	แก้ไขครั้งที่ : ๐
วันที่อนุมัติใช้ : ๐๑/๐๙/๒๕๖๕	จำนวนหน้า : ๔๘ หน้า

### ประวัติเอกสาร

เวอร์ชัน	วันที่	รายละเอียด	ผู้จัดทำ/ผู้ปรับปรุง
๑.๐	๑๕/๐๘/๒๕๖๕	เวอร์ชันเริ่มต้น	คณะกรรมการ ISMS Core Team



## สารบัญ

แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ .....	๑
ส่วนที่ ๑ การควบคุมการเข้าถึงข้อมูลและสารสนเทศ (Data and Information Access Control).....	๑
ส่วนที่ ๒ การจำแนกประเภทข้อมูลและสารสนเทศ (Data and Information Classification).....	๒
ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management).....	๔
ส่วนที่ ๔ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) .....	๖
ส่วนที่ ๕ การบริหารจัดการสินทรัพย์ (Assets Management) .....	๗
ส่วนที่ ๖ การควบคุมการเข้าถึงเครือข่าย (Network Access Control) .....	๘
ส่วนที่ ๗ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) .....	๙
ส่วนที่ ๘ การควบคุมการเข้าถึงแอปพลิเคชันและสารสนเทศ (Application and Information Access Control).....	๑๐
ส่วนที่ ๙ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malwares).....	๑๑
ส่วนที่ ๑๐ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking).....	๑๓
ส่วนที่ ๑๑ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control) .....	๑๓
ส่วนที่ ๑๒ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control) .....	๑๔
ส่วนที่ ๑๓ การควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail Control) .....	๑๕
ส่วนที่ ๑๔ การควบคุมการใช้อินเทอร์เน็ต (Internet Control).....	๑๖
ส่วนที่ ๑๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer Control).....	๑๗
ส่วนที่ ๑๖ การใช้งานเครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์เคลื่อนที่ (Computer Notebook and Mobile Device Control) .....	๑๘
ส่วนที่ ๑๗ การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration) .....	๒๐
ส่วนที่ ๑๘ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log).....	๒๑
แนวปฏิบัติการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล .....	๒๒
ส่วนที่ ๑ การรักษาความปลอดภัยฐานข้อมูล .....	๒๒
ส่วนที่ ๒ การสำรองข้อมูล.....	๒๔
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ.....	๒๖
ส่วนที่ ๑ การตรวจสอบและประเมินความเสี่ยง.....	๒๖
ส่วนที่ ๒ ความเสี่ยงที่อาจเป็นอันตรายต่อเทคโนโลยีสารสนเทศ .....	๒๗



แนวปฏิบัติการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม.....	๒๙
แนวปฏิบัติการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ.....	๓๓
แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของเทคโนโลยีสารสนเทศ .....	๓๕
แนวปฏิบัติการกำหนดหน้าที่และความรับผิดชอบของบุคคลที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ.....	๓๖
แนวปฏิบัติการการเข้ารหัส และการจัดการกุญแจ (Cryptographic and Key Management).....	๓๘
แนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก (Supplier Management) (อ้างถึงประกาศนโยบายฯ ข้อ ๔.๘).....	๔๐
แนวปฏิบัติการบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management) (อ้างถึงประกาศนโยบายฯ ข้อ ๔.๘).....	๔๓
แนวปฏิบัติการจัดหา ทดสอบและเปลี่ยนแปลงระบบ (System acquisition, testing and change) (อ้างถึงประกาศนโยบายฯ ข้อ ๔.๘).....	๔๕