

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย
ด้านสารสนเทศ ของกระทรวงสาธารณสุข
(Cyber Security)

สารบัญ

	หน้า
คำนิยาม	๑
หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ	๓
ส่วนที่ ๑. การควบคุมการเข้าถึงสารสนเทศ	๓
ส่วนที่ ๒. การบริหารจัดการการเข้าถึงของผู้ใช้	๕
ส่วนที่ ๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๗
ส่วนที่ ๔. การบริหารจัดการสินทรัพย์	๙
ส่วนที่ ๕. การควบคุมการเข้าถึงเครือข่าย	๑๐
ส่วนที่ ๖. การควบคุมการเข้าถึงระบบปฏิบัติการ	๑๓
ส่วนที่ ๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ	๑๕
ส่วนที่ ๘. การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรม ไม่ประสงค์ดี	๑๗
ส่วนที่ ๙. การปฏิบัติงานจากภายนอกสำนักงาน	๑๙
ส่วนที่ ๑๐. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย	๒๐
ส่วนที่ ๑๑. การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย	๒๑
ส่วนที่ ๑๒. การควบคุมการใช้จดหมายอิเล็กทรอนิกส์	๒๒
ส่วนที่ ๑๓. การควบคุมการใช้อินเทอร์เน็ต	๒๔
ส่วนที่ ๑๔. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล	๒๕
ส่วนที่ ๑๕. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา	๒๗
ส่วนที่ ๑๖. การตรวจจับการบุกรุก	๒๙
ส่วนที่ ๑๗. การติดตั้งและกำหนดค่าของระบบ	๓๐
ส่วนที่ ๑๘. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์	๓๒
หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล	๓๓
ส่วนที่ ๑. การรักษาความปลอดภัยฐานข้อมูล	๓๓
ส่วนที่ ๒. การสำรองข้อมูล	๓๕
หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๗
ส่วนที่ ๑. การตรวจสอบและประเมินความเสี่ยง	๓๗
ส่วนที่ ๒. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ	๓๘
หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสภาพแวดล้อม	๔๐
หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ	๔๔
หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของ ระบบเทคโนโลยีสารสนเทศ	๔๕

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

๔๖

ภาคผนวก ๑ การจัดทำประกาศแนวนโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ภาคผนวก ๒ แนวปฏิบัติ เมื่อเกิดฟิชซิง (Phishing) ที่เว็บไซต์ของหน่วยงาน