



นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
(ICT Security Policy)
สถาบันมะเร็งแห่งชาติ
พ.ศ. ๒๕๖๖



ประกาศสถาบันมะเร็งแห่งชาติ
เรื่อง นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy)
พ.ศ. ๒๕๖๖

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๕๙ ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ (PDPA) กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ กลุ่มงานดิจิทัลการแพทย์ สถาบันมะเร็งแห่งชาติ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๑. สถาบันมะเร็งแห่งชาติส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ ตอบสนองต่อพันธกิจและนโยบายขององค์กร
๒. สถาบันมะเร็งแห่งชาติมีหน้าที่จำกัด ระบุ เพิกถอนสิทธิหรือบดบังโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญให้กลุ่มงานดิจิทัลทางการแพทย์รายงานการฝ่าฝืนให้ต้นสังกัดหรือสถาบันมะเร็งแห่งชาติเพื่อพิจารณาลงโทษ
๓. สถาบันมะเร็งแห่งชาติสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ
๔. สถาบันมะเร็งแห่งชาติสนับสนุนนโยบายความมั่นคงปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการป้องกันและรักษาข้อมูลความลับของผู้ใช้บริการและข้อมูลผู้ป่วยอย่างเคร่งครัด

ประกาศ ณ วันที่ ๑๓ กันยายน พ.ศ. ๒๕๖๖

(ว่าที่ร้อยตำรวจโทหญิงนภา ศิริวิวัฒนากุล)
ผู้อำนวยการสถาบันมะเร็งแห่งชาติ

กลุ่มงานดิจิทัลการแพทย์ กลุ่มภารกิจด้านการพัฒนาระบบสุขภาพ
นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร
(ICT Security Policy)
สถาบันมะเร็งแห่งชาติ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้กำหนดให้หน่วยงานรัฐต้องมีการจัดทำนโยบายและระเบียบวิธีปฏิบัติการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ กลุ่มงานดิจิทัลการแพทย์ สถาบันมะเร็งแห่งชาติจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โดยมีวัตถุประสงค์ ดังนี้

๑. สถาบันมะเร็งแห่งชาติส่งเสริมและสนับสนุนรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศตอบสนองต่อพันธกิจและนโยบายขององค์กร
๒. สถาบันมะเร็งแห่งชาติมีหน้าที่จำกัด ระบุ เพิกถอนสิทธิหรือบطلลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนระเบียบปฏิบัติ ในกรณีสำคัญให้กลุ่มงานดิจิทัลการแพทย์รายงานการฝ่าฝืนให้ต้นสังกัดหรือสถาบันมะเร็งแห่งชาติเพื่อพิจารณาลงโทษ
๓. สถาบันมะเร็งแห่งชาติสนับสนุนให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานเสมอ
๔. สถาบันมะเร็งแห่งชาติสนับสนุนความมั่นคงปลอดภัยของข้อมูลตามระเบียบปฏิบัติ เพื่อการป้องกันและรักษาข้อมูลความลับของผู้ใช้บริการและข้อมูลผู้ป่วยอย่างเคร่งครัด

สารบัญ

	หน้า
คำนิยาม	๖
หมวดที่ ๑ นโยบายความมั่นคงปลอดภัย (Security Policy)	๑๐
๑.๑ จัดทำนโยบายความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร (Information Security Policy Document)	๑๐
๑.๒ ทำการทบทวนนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)	๑๑
หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)	๑๑
๒.๑ โครงสร้างภายในด้านความมั่นคงปลอดภัยสารสนเทศ (Internal Organization)	๑๑
๒.๒ อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)	๑๔
หมวดที่ ๓ การรักษาความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)	๑๕
๓.๑ การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)	๑๕
๓.๒ การสร้างความความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)	๑๖
หมวดที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management)	๑๗
๔.๑ ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)	๑๗
๔.๒ การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information Classification)	๒๑
๔.๓ การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handling)	๒๓
หมวดที่ ๕ ความการควบคุมการเข้าถึง (Access Control)	๒๔
๕.๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)	๒๔
๕.๒ การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)	๒๗
๕.๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)	๒๘
๕.๔ การควบคุมการเข้าถึงระบบ (System and Application Access Control)	๓๐
หมวดที่ ๖ การเข้ารหัสข้อมูล (Cryptography)	๓๒
๖.๑ การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)	๓๒

สารบัญ (ต่อ)

	หน้า
หมวดที่ ๗ ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)	๓๓
๗.๑ บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)	๓๓
๗.๒ ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)	๓๖
หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)	๓๘
๘.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)	๓๘
๘.๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)	๔๐
๘.๓ การสำรองข้อมูล (Backup)	๔๒
๘.๔ การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)	๔๔
๘.๕ การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)	๔๕
๘.๖ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)	๔๕
๘.๗ การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)	๔๕
หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)	๔๖
๙.๑ การจัดการระบบรักษาความมั่นคงปลอดภัยระบบเครือข่าย (Network Security Management)	๔๖
๙.๒ การถ่ายโอนข้อมูล (Information Transfer)	๔๗
หมวดที่ ๑๐ การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)	๔๙
๑๐.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)	๔๙
๑๐.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)	๕๐
๑๐.๓ ข้อมูลสำหรับการทดสอบ (Test data)	๕๑
หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)	๕๒
๑๑.๑ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)	๕๒
๑๑.๒ การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)	๕๓

สารบัญ (ต่อ)

	หน้า
หมวดที่ ๑๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)	๕๔
๑๒.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)	๕๔
หมวดที่ ๑๓ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหาร จัดการ เพื่อสร้าง ความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)	๕๗
๑๓.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)	๕๗
๑๓.๒ การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)	๕๘
หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบาย ความมั่นคงปลอดภัยสารสนเทศของสถาบันมะเร็งแห่งชาติ (Compliance)	๕๙
๑๔.๑ การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)	๕๙
๑๔.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)	๖๑

ข้อ ๑ คำนิยาม

“โรงพยาบาล” หมายถึง สถาบันมะเร็งแห่งชาติ

“ระบบเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง ระบบสารสนเทศ ระบบฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบ Security ระบบงาน (ซอฟต์แวร์สำเร็จรูป ซอฟต์แวร์ประยุกต์) และระบบสื่อสารของสถาบันมะเร็งแห่งชาติ

“กลุ่มงานดิจิทัลการแพทย์” หมายถึง กลุ่มงานดิจิทัลการแพทย์ ภายใต้ภารกิจด้านการพัฒนาระบบสุขภาพ สถาบันมะเร็งแห่งชาติ

“เจ้าหน้าที่” หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้าง พนักงานกระทรวงสาธารณสุข ลูกจ้างชั่วคราว

“ผู้รับจ้างให้บริการจากภายนอก” หมายถึง เจ้าหน้าที่หน่วยงานภายนอกที่จ้างมาปฏิบัติงาน (Outsource) ที่มีการใช้งานหรือให้บริการเกี่ยวกับระบบสารสนเทศโรงพยาบาลของสถาบันมะเร็งแห่งชาติ

“สถาบันมะเร็งแห่งชาติ” หมายถึง สถาบันมะเร็งแห่งชาติ รวมถึงสถาบันมะเร็งแห่งชาติที่อยู่ภายใต้สังกัดกรมการแพทย์

“หน่วยงานภายนอก” หมายถึง บริษัท/สถาบันมะเร็งแห่งชาติ ที่สถาบันมะเร็งแห่งชาติ ได้ว่าจ้างหรือมอบหมายให้ดำเนินการในเรื่องระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ ที่ปรึกษา ผู้รับจ้าง ผู้ขาย ผู้ให้บริการ หรือเป็นผู้ให้บริการ และอื่น ๆ ที่เกี่ยวข้อง รวมถึงหน่วยงานภายนอกอื่นที่มาขอใช้บริการด้วย

“ผู้ใช้งาน/ผู้ให้บริการ” หมายถึง ข้าราชการ ลูกจ้าง และพนักงานราชการ ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ

“ผู้บริหาร” หมายถึง ผู้มีอำนาจในการบังคับบัญชาในสถาบันมะเร็งแห่งชาติ ได้แก่ รองผู้อำนวยการสถาบันมะเร็งแห่งชาติ หรือเทียบเท่า หัวหน้ากลุ่มงาน เป็นต้น

“ผู้บริหารระดับสูงสุด” หมายถึง ผู้อำนวยการสถาบันมะเร็งแห่งชาติ หรือเทียบเท่า

“สิทธิ์ของผู้ใช้งาน/สิทธิ์ของผู้ให้บริการ” หมายถึง สิทธิ์ที่ใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ

“ผู้พัฒนาระบบ” หมายถึง เจ้าหน้าที่/หน่วยงานภายนอก ที่สถาบันมะเร็งแห่งชาติ ได้ว่าจ้างหรือมอบหมายให้ดำเนินการในเรื่องการพัฒนาระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ

“ผู้ดูแลระบบ” หมายถึง (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากผู้อำนวยการภารกิจด้านการแพทย์ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

“ISMR” หมายถึง ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative : ISMR)

“ISMS Steering Committee (IMC)” หมายถึง คณะกรรมการอำนวยการระบบบริหารความมั่นคงปลอดภัยสารสนเทศ สถาบันมะเร็งแห่งชาติ

“ISMS Working Team (IWT)” หมายถึง คณะกรรมการเตรียมความพร้อม ISO/IEC ๒๗๐๐๑:๒๐๑๓ สถาบันมะเร็งแห่งชาติ ซึ่งมีองค์ประกอบดังนี้

- หัวหน้าคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Manager: ISM)
- เจ้าหน้าที่ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Staff: ISS)
- เจ้าหน้าที่ควบคุมเอกสาร (Document Controller: DC)

“ทรัพย์สิน” หมายถึง ทรัพย์สินของสถาบันมะเร็งแห่งชาติ ซึ่งแบ่งเป็น ๘ ประเภท

๑. กระบวนการทำงาน (Business Process) หมายถึง กระบวนการ กระบวนการย่อย หรือกิจกรรมที่สำคัญที่หากแก้ไข เสียหาย สูญเสียไปแล้วจะมีผลต่อการปฏิบัติงานตามภารกิจขององค์กร กระบวนการที่มีกระบวนการสำคัญอันเป็นความลับ หรือกระบวนการที่เกี่ยวข้องกับเทคโนโลยีที่มีสิทธิ์ความเป็นเจ้าของ หรือกระบวนการที่สำคัญสำหรับองค์กรที่จำเป็นต้องมี เพื่อปฏิบัติตามกฎหมาย กฎระเบียบ หรือข้อผูกพันตามสัญญา เช่น กระบวนการเก็บความต้องการ และออกแบบระบบงาน กระบวนการติดตั้งระบบงาน กระบวนการบริหารจัดการลิขสิทธิ์ เป็นต้น
๒. ข้อมูล และสารสนเทศ (Information) หมายถึง ข้อมูลสำคัญในระบบสารสนเทศ สารสนเทศที่เป็นข้อมูลบุคคล สารสนเทศที่เป็นข้อมูลเกี่ยวกับยุทธศาสตร์ หรือกลยุทธ์ขององค์กร สารสนเทศที่สำคัญที่มีมูลค่าสูงที่ต้องจัดเก็บรักษา เช่น ข้อมูล Log ของอุปกรณ์ ข้อมูล License ซอร์สโค้ดของระบบงาน ข้อมูลสำรอง ข้อมูลบัญชีผู้ใช้งาน เป็นต้น
๓. ฮาร์ดแวร์ (Hardware) หมายถึง อุปกรณ์ที่เกี่ยวข้องในการให้บริการ เช่น เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์ป้องกันการโจมตีจากผู้บุกรุกทางเครือข่าย อุปกรณ์ป้องกันไวรัสทางระบบเครือข่ายอินเทอร์เน็ต อุปกรณ์ที่จัดเก็บข้อมูล อุปกรณ์สื่อบันทึกข้อมูล/สื่อจัดเก็บข้อมูล สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์แม่ข่ายสำหรับงานเผื่อสำรอง เก็บสำหรับสำรองข้อมูล เป็นต้น
๔. ซอฟต์แวร์ (Software) หมายถึง ระบบปฏิบัติการ ระบบงานทางธุรกิจ Directory Server ที่เกี่ยวข้องกับผู้ดูแลระบบ ซอฟต์แวร์ Antivirus ซอฟต์แวร์สนับสนุนที่ใช้การบริหารจัดการและการบำรุงรักษา (Supporting Software) เช่น ระบบงานทางธุรกิจ ซอฟต์แวร์สำหรับงานเผื่อสำรอง ซอฟต์แวร์สำหรับควบคุม Access Control ระบบปฏิบัติการ Windows เป็นต้น

๕. เครือข่าย (Network) หมายถึง เครือข่าย องค์ประกอบเกี่ยวกับการเชื่อมต่อเครือข่าย เช่น สวิตช์ ไร้เตอร์ สายเคเบิล ประเภทการเชื่อมต่อ อุปกรณ์ Security สายไฟฟ้า และสายสื่อสาร เป็นต้น
๖. บุคลากร (Personnel) หมายถึง บุคลากรที่เกี่ยวข้องกับการดำเนินกิจกรรมความมั่นคงปลอดภัยสารสนเทศ ผู้ดูแลศูนย์ข้อมูล ผู้ดูแลเครื่องแม่ข่ายและระบบเครือข่าย ผู้ดูแลระบบสนับสนุนศูนย์ข้อมูล ผู้สนับสนุนการใช้ระบบสารสนเทศ (Helpdesk) เจ้าหน้าที่ Contractor/ Outsource ที่ปฏิบัติงาน เช่น บุคลากรส่วนบริหารจัดการเทคโนโลยีสารสนเทศ บุคลากรส่วนพัฒนาระบบประมวลผลข้อมูล บุคลากรส่วนวางแผนและส่งเสริมการใช้เทคโนโลยีสารสนเทศ เป็นต้น
๗. สถานที่ (Site) หมายถึง อาคาร สถานที่ตั้ง สิ่งแวดล้อมภายนอก และทางกายภาพ พื้นที่การแบ่งเขตโซนภายในสถานที่ ระบบสนับสนุนในการดูแลอาคารสถานที่ อุปกรณ์เครื่องมือสนับสนุนต่างๆ เช่น อุปกรณ์ Generator อุปกรณ์ UPS ระบบ Access Control ระบบดับเพลิง ระบบปรับอากาศ ระบบกล้องวงจรปิด ศูนย์คอมพิวเตอร์หลัก ศูนย์คอมพิวเตอร์สำรอง ห้องปฏิบัติงานของเจ้าหน้าที่ เป็นต้น
๘. องค์กร (Organization) โครงสร้างขององค์กร (Structure of the organization) เช่น คณะบริหารจัดการรักษาความมั่นคงปลอดภัยสารสนเทศในองค์กร เป็นต้น โครงการที่พัฒนา (Project) เช่น โครงการพัฒนาซอฟต์แวร์ และโครงการปรับปรุงพัฒนาระบบสารสนเทศ เป็นต้น ผู้ให้บริการภายนอก (Supplier) เช่น Supplier ที่เกี่ยวข้องกับการซ่อมบำรุงเครื่องแม่ข่าย, อุปกรณ์ Network, อุปกรณ์ Security, อุปกรณ์ Generator, อุปกรณ์ UPS, ระบบดับเพลิง, ระบบปรับอากาศ และ Vendor ที่พัฒนาซอฟต์แวร์ เป็นต้น

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน/ผู้ใช้บริการ เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำรงไว้ซึ่งความลับ (Confidential) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิดชอบ และความน่าเชื่อถือ

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่ทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ ขาดคุณสมบัติด้านความลับ (Confidential) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) อาทิ การปลอมแปลงหน้าเว็บไซต์ การเจาะระบบ การขโมยข้อมูลทางเว็บไซต์ การแฮกเว็บไซต์ การรั่วไหลของข้อมูล การแพร่ระบาดของไวรัสและหนอนอินเทอร์เน็ต ระบบล่มไม่สามารถให้บริการได้ และการบุกรุกเครือข่าย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เป็นสถานการณ์
ซึ่งอาจทำให้ระบบของสถาบันมะเร็งแห่งชาติ ถูกบุกรุก หรือโจมตี และระบบความมั่นคงปลอดภัยถูกคุกคาม

“สถาบันมะเร็งแห่งชาติ” หมายถึง เป็นพื้นที่การทำงานที่เข้าได้เฉพาะบุคลากรที่เกี่ยวข้องกับงานนั้น ๆ
ใน สถาบันมะเร็งแห่งชาติ

“PDPA” หมายถึง พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

หมวดที่ ๑

นโยบายความมั่นคงปลอดภัย (Security Policy)

๑. นโยบายความมั่นคงปลอดภัย (Security Policy)

วัตถุประสงค์

เพื่อกำหนดทิศทางและให้การสนับสนุนการดำเนินการด้านความมั่นคงปลอดภัยสำหรับสารสนเทศของสถาบันมะเร็งแห่งชาติ เพื่อให้เป็นไปตามหรือสอดคล้องกับข้อกำหนดทางธุรกิจ กฎหมาย และระเบียบปฏิบัติที่เกี่ยวข้อง

นโยบาย

๑.๑ จัดทำนโยบายความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร (Information Security Policy Document)

๑.๑.๑. ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรเพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยนโยบายดังกล่าวจะต้องได้รับ การอนุมัติจากผู้มีอำนาจสูงสุดของสถาบันมะเร็งแห่งชาติ ในการนำไปใช้

๑.๑.๒. กำหนดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่ของสถาบันมะเร็งแห่งชาติ และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

๑.๒ ทำการทบทวนนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)

ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี

หมวดที่ ๒

โครงสร้างทางด้านการมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

๒.๑ โครงสร้างภายในด้านการมั่นคงปลอดภัยสารสนเทศ (Internal Organization)

วัตถุประสงค์

เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของสถาบัน
มะเร็งแห่งชาติ ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

นโยบาย

๒.๑.๑ บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

- ๑) ISMR ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการดำเนินงานทางด้านการมั่นคง
ปลอดภัยสำหรับสารสนเทศของสถาบันมะเร็งแห่งชาติ ไว้อย่างชัดเจน
- ๒) ผู้อำนวยการสถาบันมะเร็งแห่งชาติสถาบันมะเร็งแห่งชาติ ต้องแต่งตั้งคณะ หรือกลุ่มผู้ทำงาน
หลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหารจัดการความมั่นคงปลอดภัยสำหรับ
สารสนเทศของสถาบันมะเร็งแห่งชาติ
- ๓) บทบาทหน้าที่แบ่งได้ดังนี้

๓.๑) ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้อำนวยการสถาบันมะเร็งแห่งชาติ
- รองผู้อำนวยการด้านพัฒนาระบบสุขภาพหรือเทียบเท่า

ความรับผิดชอบ

๓.๑.๑ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน
ติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๓.๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบ
คอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่
สถาบันมะเร็งแห่งชาติ หรือ
ผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒) ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่มงาน/หัวหน้างาน หรือเทียบเท่า

ความรับผิดชอบ

๓.๒.๑) หัวหน้ากลุ่มงานดิจิทัลการแพทย์ รับผิดชอบต่อดูแลการปฏิบัติงานของเจ้าหน้าที่ทุกงาน
ภายใต้กลุ่มงานดิจิทัลการแพทย์

๓.๒.๑.๑ กำกับดูแล ให้คำปรึกษา แนะนำการพัฒนาระบบสารสนเทศ ข้อมูล และโครงสร้าง
ด้านดิจิทัล ของสถาบันมะเร็งแห่งชาติ

๓.๒.๑.๒ กำกับดูแล ติดตามการพัฒนาาระบบดิจิทัลให้เป็นไปตามมาตรฐานความมั่นคงปลอดภัย กำหนดแนวทางการใช้ วางมาตรฐานด้านดิจิทัลของสถาบันมะเร็งแห่งชาติ และวางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความมั่นคงปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๓.๒.๑.๓ วางแผน ปรับปรุงระบบและกำกับดูแลการใช้งานระบบสารสนเทศโรงพยาบาลให้เป็นไปตามกฎหมาย PDPA

๓.๒.๑.๔ เสนอแนะปัญหา เป้าหมายและแนวทางการพัฒนาาระบบดิจิทัลของสถาบันมะเร็งแห่งชาติ รวมทั้งบูรณาการแผนงาน โครงการ งบประมาณและทรัพยากร ด้านดิจิทัลการแพทย์ให้เกิดการใช้ประโยชน์สูงสุด

๓.๒.๑.๕ ประสานงานและพัฒนาความร่วมมือด้านดิจิทัลกับหน่วยงานต่างๆ ทั้งภายในและภายนอกสถาบันมะเร็งแห่งชาติเพื่อเชื่อมโยงการดำเนินงาน การบริการและการเชื่อมต่อข้อมูลระหว่างหน่วยงาน อีกทั้งเป็นผู้แทนสถาบันฯ ในการประชุม สัมมนา แลกเปลี่ยนความรู้ ความร่วมมือในงานด้านดิจิทัล

๓.๒.๒) หัวหน้างานบริหารสารสนเทศโรงพยาบาล รับผิดชอบดูแลการปฏิบัติงานของเจ้าหน้าที่ทุกงานภายใต้งานบริหารสารสนเทศโรงพยาบาล

๓.๒.๒.๑ วางแผน และจัดการ ให้เกิดการใช้นระบบสารสนเทศโรงพยาบาลอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด

๓.๒.๒.๒ กำกับดูแล ให้คำปรึกษา สนับสนุน ส่งเสริมให้มี การใช้งานระบบสารสนเทศโรงพยาบาลและเทคโนโลยีอื่น มาเป็นเครื่องมือในการเพิ่มศักยภาพการดำเนินกิจกรรมภายในสถาบันมะเร็งแห่งชาติ

๓.๒.๒.๓ กำกับดูแล บริหารจัดการ การให้ข้อมูล สนับสนุนการฝึกอบรมการปฏิบัติงานของส่วนงานต่างๆ ให้บุคลากรมีศักยภาพ ระบบข้อมูลมีความถูกต้องและเป็นปัจจุบัน

๓.๒.๒.๔ กำกับดูแล วางแผน การบริหารจัดการความเสี่ยงและความมั่นคงปลอดภัย ระบบสารสนเทศโรงพยาบาลและระบบเชื่อมต่อ

๓.๒.๒.๕ กำหนดแนวทางในการการจัดเก็บ การประมวลผล การใช้ประโยชน์และการพัฒนาระบบข้อมูลสารสนเทศโรงพยาบาล และเป็นศูนย์ข้อมูลกลางของสถาบันมะเร็งแห่งชาติ

๓.๒.๒.๖ กำกับดูแล ระบบสารสนเทศโรงพยาบาล และระบบเชื่อมต่อให้สามารถใช้งานได้ตลอดเวลา (๒๔ ชั่วโมง)

๓.๒.๓) หัวหน้างานอุปกรณ์โครงสร้างดิจิทัลการแพทย์ รับผิดชอบดูแลการปฏิบัติงานของเจ้าหน้าที่ทุกงานภายใต้ งานอุปกรณ์โครงสร้างดิจิทัลการแพทย์

๓.๒.๓.๑ กำกับดูแล การบำรุงรักษาอุปกรณ์ Server อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ทั้งหมดภายในสถาบันมะเร็งแห่งชาติ

๓.๓.๓.๒ กำกับดูแล วางแผนการติดตั้ง เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงทั้งหมด

๓.๓.๓.๓ วางระบบ และดูแลความมั่นคงปลอดภัยทางสารสนเทศ รวมถึงการป้องกันการเกิดการถูกเจาะระบบ การกู้คืนข้อมูลและแก้ไขปัญหาเมื่อเกิดเหตุการณ์ไม่พึงประสงค์ด้านระบบเครือข่ายโดยไม่ได้รับอนุญาตรับผิดชอบดูแลการปฏิบัติงานของเจ้าหน้าที่ทุกงานภายใต้ งานบริหารสารสนเทศโรงพยาบาล

๓.๒.๔) ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการสถาบันมะเร็งแห่งชาติ เช่น นักวิชาการคอมพิวเตอร์ นักจัดการงานทั่วไป

๓.๒.๔.๑ ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๓.๒.๔.๒ ให้บริการแก้ไขปัญหาด้านระบบสารสนเทศโรงพยาบาลและอุปกรณ์ต่อพ่วง แก่เจ้าหน้าที่ทุกส่วนงานภายในสถาบันมะเร็งแห่งชาติ ที่เปิดให้การตรวจรักษา

๓.๒.๔.๓ ตรวจสอบการทำงานของระบบสารสนเทศระบบหลัก ให้ดำเนินงานได้ตลอดเวลา (๒๔ ชั่วโมง)

๓.๒.๔.๔ ให้บริการแก้ไขปัญหาด้าน application แก่ผู้ป่วยและเจ้าหน้าที่

๓.๒.๔.๕ รับผิดชอบควบคุม ดูแล รักษาความมั่นคงปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ระบบเครือข่าย ห้อง Data Center ห้อง NOC และเครื่องคอมพิวเตอร์แม่ข่าย

๓.๒.๔.๖ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๓.๒.๔.๗ ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันมะเร็งแห่งชาติ

๓.๒.๕) เจ้าหน้าที่กลุ่มงานดิจิทัลการแพทย์ที่ปฏิบัติงานนอกเวลาราชการ รับผิดชอบให้ระบบ

สารสนเทศ

โรงพยาบาล สามารถใช้งานได้ตลอด ๒๔ ชั่วโมง

๓.๒.๕.๑ ให้บริการแก้ไขปัญหาด้านระบบสารสนเทศโรงพยาบาลและอุปกรณ์ต่อพ่วง แก่เจ้าหน้าที่ทุกส่วนงานภายในสถาบันมะเร็งแห่งชาติในการให้บริการผู้ป่วย

๓.๒.๕.๒ ตรวจสอบการทำงานของระบบสารสนเทศระบบหลัก ให้ดำเนินงานได้ตลอดเวลา (๒๔ ชั่วโมง)

๓.๒.๕.๓ รายงานเหตุการณ์ไม่พึงประสงค์ทางสารสนเทศและเครือข่ายกับผู้บังคับบัญชา ที่อาจเกิดความเสียหายแก่สถาบันมะเร็งแห่งชาติ เจ้าหน้าที่หรือผู้มารับบริการ

๓.๒.๕.๔ ให้บริการแก้ไขปัญหาด้าน application ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมาย

๒.๑.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

ผู้บริหาร สถาบันมะเร็งแห่งชาติ ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้เกิดการเปลี่ยนแปลงทรัพย์สินของสถาบันมะเร็งแห่งชาติ หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับอนุญาตหรือโดยไม่ได้เจตนาก็ตาม

๒.๑.๓ ข้อมูลสำหรับการติดต่อกับหน่วยงานอื่น (Contact with Authorities)

ISM ต้องกำหนดรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานอื่น ๆ เช่น ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ศูนย์ประสานงานการรักษาความมั่นคงปลอดภัยคอมพิวเตอร์ประเทศไทย (ThaiCERT) เป็นต้น เพื่อใช้สำหรับการติดต่อประสานงานทางด้านความมั่นคงปลอดภัยในกรณีที่มีความจำเป็น

๒.๑.๔ การมีรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน (Contact with Special Interest Groups)

ISM ต้องกำหนดรายชื่อและข้อมูลสำหรับการติดต่อกับกลุ่มต่าง ๆ ที่มีความสนใจเป็นพิเศษในเรื่องเดียวกัน กลุ่มที่มีความสนใจด้านความมั่นคงปลอดภัยสารสนเทศ หรือสมาคมต่าง ๆ ในอุตสาหกรรมที่สถาบันมะเร็งแห่งชาติ มีส่วนร่วมและเอกสารกำหนดให้มีการระบุนวันที่จัดทำเอกสาร

๒.๑.๕ การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

๑) ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

๒) กรณีโครงการที่จ้างบริษัทภายนอก โครงการที่หน่วยงานภายนอกดำเนินการให้ และโครงการที่สถาบันมะเร็งแห่งชาติ จัดทำเองต้องดำเนินการตามระเบียบทางราชการ และปฏิบัติตาม PDPA

๒.๒ อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอกและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

นโยบาย

๒.๑.๖ นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

ต้องมีการกำหนดและปฏิบัติตามนโยบายหรือมาตรการสนับสนุน สำหรับการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่น ๆ) ที่มีการนำมาใช้งาน เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และควรคำนึงถึงความเสี่ยงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกัน

๒.๒.๒ การปฏิบัติงานจากระยะไกล (Teleworking)

๑) ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่สถาบันมะเร็งแห่งชาติกำหนด

๒) ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๓) ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความมั่นคงปลอดภัย เช่น รหัสผ่าน หรือวิธีการเข้ารหัส เป็นต้น

๔) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของสถาบันมะเร็งแห่งชาติ

๕) ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่าง ๆ ของสถาบันมะเร็งแห่งชาติที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

๖) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

หมวดที่ ๓

การรักษาความมั่นคงปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

๓.๑ การจัดทามบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงาน สถาบันมะเร็งแห่งชาติ

นโยบาย

๓.๑.๑ การสรรหามบุคลากร (Screening)

๑) เจ้าหน้าที่ฝ่ายทรัพยากรบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นเจ้าหน้าที่ เจ้าหน้าที่ชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก๊ง ทำลายหรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติมาก่อน

๒) เจ้าหน้าที่ประสานงานฝ่ายทรัพยากรบุคคลต้องจัดให้มีการลงนามในสัญญาระหว่าง

๒.๑ “เจ้าหน้าที่” และสถาบันมะเร็งแห่งชาติ ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) และลงนามในข้อตกลงว่าจะไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA)

๒.๒ “ผู้รับจ้างให้บริการจากภายนอก” และสถาบันมะเร็งแห่งชาติ ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) และลงนามในข้อตกลงว่าจะไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่อง ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

๓) ในการสรรหามบุคลากรนอกจากความเหมาะสมตามตำแหน่งแล้ว กรณีเป็นข้าราชการ ต้องมีการตรวจสอบสารเสพติดในร่างกายก่อนรับเข้าทำงาน และตรวจประวัติอาชญากรรม

๓.๑.๒ ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

๑) เจ้าหน้าที่ประสานงานฝ่ายทรัพยากรบุคคล ต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยเจ้าหน้าที่ฝ่ายทรัพยากรบุคคล ต้องแจ้งให้กลุ่มงานเทคโนโลยีสารสนเทศ ทราบภายใน ๑๕ วัน นับจากวันที่เกิดเหตุดังนี้

- การว่าจ้างงาน
- การเปลี่ยนแปลงสภาพการว่าจ้างงาน
- การลาออกจากงาน หรือการสิ้นสุดการเป็นผู้บริหาร เจ้าหน้าที่และลูกจ้าง หรือการถึงแก่กรรม
- การโยกย้าย
- การพักงาน การลงโทษทางวินัย หรือระงับการปฏิบัติหน้าที่

๓.๒ การสร้างความความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์

เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของสถาบันมะเร็งแห่งชาติ

นโยบาย

๓.๒.๑ หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ISMR ต้องกำหนดให้เจ้าหน้าที่ และผู้รับจ้างให้บริการจากภายนอกรับทราบและปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของสถาบันมะเร็งแห่งชาติ ด้วย

๓.๒.๒ การสร้างความตระหนัก การให้ความรู้และการอบรมให้ความรู้ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness, Education and Training)

๑) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ผู้รับจ้างขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

๒) ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ เกี่ยวกับความตระหนักและวิธีปฏิบัติ เพื่อสร้างความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัย และการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติด้วย

๓) เจ้าหน้าที่ของสถาบันมะเร็งแห่งชาติ ใหม่ทุกคน ต้องได้รับการอบรม/รับทราบเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และระเบียบปฏิบัติที่เกี่ยวข้องกับสถาบันมะเร็งแห่งชาติก่อนหรืออย่างน้อยภายใน ๙๐ วันนับจากเข้าทำงานในสถาบันมะเร็งแห่งชาติ โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

๔) เจ้าหน้าที่ประสานงานฝ่ายทรัพยากรบุคคล และ ISM มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ ให้แก่บุคลากรด้วย

๓.๒.๓ กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหาร สถาบันมะเร็งแห่งชาติ ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของราชการและ สถาบันมะเร็งแห่งชาติ แต่หากเป็นการละเมิดข้อกำหนด บทลงโทษจะเป็นไปตามฐานความผิดที่ได้กระทำตามที่ระบุในแต่ละข้อกำหนดนั้น ๆ

หมวดที่ ๔

การบริหารจัดการทรัพย์สิน (Asset Management)

๔.๑ ความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์

เพื่อให้ทรัพย์สินของสถาบันมะเร็งแห่งชาติ ได้รับการป้องกันและปกป้องอย่างเหมาะสม

นโยบาย

๔.๑.๑ ทะเบียนทรัพย์สิน (Inventory of assets)

๑) ต้องจัดทำและเก็บทะเบียนทรัพย์สิน ซึ่งรวมถึง ๑. กระบวนการทำงาน (Business Process) ๒. ข้อมูล และสารสนเทศ (Information) ๓. ฮาร์ดแวร์ (Hardware) ๔. ซอฟต์แวร์ (Software) ๕. เครือข่าย (Network) ๖. บุคลากร (Personnel) ๗. สถานที่ (Site) ๘. องค์กร (Organization) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการทรัพย์สินของสถาบันมะเร็งแห่งชาติ

๒) ต้องมีการตรวจสอบทรัพย์สิน (Inventory Check) ต้องจัดให้มีการตรวจสอบบัญชีทรัพย์สินทุกประเภท อย่างน้อยปีละ ๑ ครั้ง หรือตามระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๓) ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของทรัพย์สิน เมื่อมีทรัพย์สินใหม่หรือทรัพย์สินที่มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๔.๑.๒ ความเป็นเจ้าของทรัพย์สิน (Ownership for Assets)

จะต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบข้อมูลและทรัพย์สินทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ อย่างชัดเจน

๔.๑.๓ การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets)

๑) จะต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและทรัพย์สินอย่างเหมาะสม

๒) การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมด ที่สถาบันมะเร็งแห่งชาติ เป็นผู้จัดทำมานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของสถาบันมะเร็งแห่งชาติ การใช้งานระบบและอุปกรณ์ต่าง ๆ เพื่อกิจธุระส่วนตัวนั้น อนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็นอุปสรรคต่อการทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
- เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดย สถาบันมะเร็งแห่งชาติ จะต้องมีความรับผิดชอบต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพย์สินเหล่านี้ให้มีความมั่นคงปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของสถาบันมะเร็งแห่งชาติ

- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของสถาบันมะเร็งแห่งชาติ อย่างระมัดระวัง และให้การปกป้องเสมือนเป็นทรัพย์สินของตน
- เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของสถาบันมะเร็งแห่งชาติ ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้องอัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์ โดยระยะเวลาว่างเว้นจากการใช้งานแล้ว ต้องทำการ Log Off ต้องไม่เกิน ๑๕ นาที
- ผู้ใช้งานต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ของสถาบันมะเร็งแห่งชาติ
- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายใน สถาบันมะเร็งแห่งชาติ อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสถาบันมะเร็งแห่งชาติ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์
- อุปกรณ์คอมพิวเตอร์ของสถาบันมะเร็งแห่งชาติ ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใด ๆ ก่อนได้รับอนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของสถาบันมะเร็งแห่งชาติ อย่างเด็ดขาด

๓) การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของสถาบันมะเร็งแห่งชาติ
- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของสถาบันมะเร็งแห่งชาติ ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อ มา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสมโดยสถาบันมะเร็งแห่งชาติเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ
- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอ เพื่อให้ผู้ใช้งานทั่วไปของสถาบันมะเร็งแห่งชาติ มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้
- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของสถาบันมะเร็งแห่งชาติ เท่านั้น

๔) การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

- สถาบันมะเร็งแห่งชาติ จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในการทำวิจัยการค้นหาค้นหาข้อมูลความรู้ และการติดต่อสื่อสารกับบุคคลภายนอก เพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของสถาบันมะเร็งแห่งชาติ

- ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้สถาบันมะเร็งแห่งชาติ และบุคคลผู้ที่เกี่ยวข้องกับ สถาบันมะเร็งแห่งชาติ เสื่อมเสียชื่อเสียง หรือ เกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย
- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้ สถาบันมะเร็งแห่งชาติ ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม
- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อปอัพ หรือเข้าสู่เว็บไซต์ใด ๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้ อาจมีโปรแกรมมัลแวร์แฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต
- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย
- สถาบันมะเร็งแห่งชาติ ไม่สนับสนุนการแสดงความคิดเห็นส่วนตัว หรือเผยแพร่ข้อมูลส่วนบุคคลในรูปแบบอิเล็กทรอนิกส์ (เช่น ผ่านทางเว็บบอร์ด โซเชียลมีเดีย) ของเจ้าหน้าที่ ที่อาจทำให้สถาบันมะเร็งแห่งชาติ เจ้าหน้าที่ ผู้ป่วยและบุคคลภายนอก เกิดความเสียหาย ทั้งนี้ ความเสียหายใด ๆ ที่อาจเกิดขึ้นจากการกระทำดังกล่าว ถือเป็นความรับผิดชอบของเจ้าหน้าที่ผู้ใช้นั้น

๕) การอนุญาตให้ใช้งานอีเมลมีดังนี้

- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล้วงละเมิดและการนำอีเมลไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น ict@nci.go.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไป โดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
- E-mail Account ทั้งหมด และอีเมลทุกฉบับ (รวมถึงอีเมลส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ ถือเป็นทรัพย์สินของสถาบันมะเร็งแห่งชาติ
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมลของสถาบันมะเร็งแห่งชาติ
- ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงาน และอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของสถาบันมะเร็งแห่งชาติ เพื่อกระทำการใด ๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมายตัวอย่างเช่น เพื่อการโฆษณา ยาสูบ สิ่งมีพิษ สิ้นค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามผู้ใช้งานทำสำเนาข้อความ หรือทำสำเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมลของบุคคลอื่น ก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมลนั้นในนามตัวแทนของสถาบันมะเร็งแห่งชาติ

- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมล หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม
- ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมลพร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่ต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล
- ผู้ใช้งานต้องทำการส่งอีเมลให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมลฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน
- ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมลขยะ (Junk Mail) หรือโฆษณาสินค้าต่าง ๆ (Spam Mail) เป็นต้น
- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใด ๆ กับการส่ง อีเมลหลอกลวง หรือการส่งอีเมลในลักษณะ ลुकโซ่โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ช่มชู้ ลามกอนาจาร การยั่วยู่ทางเพศ หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อ สถาบันมะเร็งแห่งชาติ
- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์ หรือโปรแกรมแฝง (โทรจัน)

กรณีนี้ที่เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ไม่ปฏิบัติตามที่ สถาบันมะเร็งแห่งชาติ กำหนด

- สำหรับข้าราชการ ให้ดำเนินการตามระเบียบข้าราชการพลเรือน พ.ศ. ๒๕๕๑
- สำหรับพนักงานราชการ ให้ดำเนินการตามระเบียบสำนักนายกรัฐมนตรีว่าด้วยพนักงานราชการ พ.ศ. ๒๕๔๗

๔.๑.๔ การคืนทรัพย์สิน (Return on Assets)

เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์ รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่าง ๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน

๔.๒ การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information Classification)

วัตถุประสงค์

เพื่อให้แน่ใจว่าสารสนเทศของสถาบันมะเร็งแห่งชาติ ได้รับการปกป้องในระดับที่เหมาะสม

นโยบาย

๔.๒.๑ การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)

๑) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความมั่นคงปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข สาธารณสุข เป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ป่วย ประวัติผู้ป่วย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล ซึ่งตาม PDPA ถือว่า เป็นข้อมูลที่มีความอ่อนไหว

๑.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด (Top Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ใช้ภายใน (Internal Use) หรือ เอกสารควบคุม หมายถึง เอกสารที่ใช้สำหรับบุคลากรภายในสถาบันมะเร็งแห่งชาติเท่านั้น
- ข้อมูลทั่วไป หรือ เผยแพร่ต่อสาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นในบังคับบัญชาในสถาบันมะเร็งแห่งชาตินั้น

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป ไม่สามารถเข้าถึงข้อมูลผู้ป่วยได้
- ระดับชั้นสำหรับบุคลากรทางการแพทย์ สามารถเข้าถึงข้อมูลผู้ป่วยได้ตามสิทธิที่ได้รับมอบหมาย
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับมอบหมายตามอำนาจหน้าที่

๑.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๔.๒.๒ การจัดทำป้ายชื่อ ของข้อมูล (Labeling of Information)

๑) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความมั่นคงปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสำเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความมั่นคงปลอดภัย

๔.๒.๓ การจัดการทรัพย์สิน (Handling of Asset)

๑) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

๒) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

๓) ผู้ใช้งานควรเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อกได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อที่ไวโดยไม่อยู่ที่โต๊ะทำงาน

๔) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ โดยทันที

๕) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่มีการเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๖) เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของสถาบันมะเร็งแห่งชาติ หรือข้อมูลผู้ป่วยที่สามารถระบุตัวตนได้ ในพื้นที่สาธารณะ เช่น ลิฟท์ ร้านอาหาร ฯลฯ

๗) สื่อบันทึกข้อมูล และอุปกรณ์คอมพิวเตอร์พกพาต่าง ๆ (เช่น PDA, USB-Drive, CD-Rom เป็นต้น) ที่มีข้อมูลลับของสถาบันมะเร็งแห่งชาติ บันทึกอยู่ ต้องได้รับการดูแลรักษาและใช้งานอย่างระมัดระวัง

๔.๓ การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มีความมั่นคงปลอดภัย (Media Handling)

วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของสถาบันมะเร็งแห่งชาติ โดยการถูกเปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

นโยบาย

๔.๑.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

๑) การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์ หรือความเสียหายในระหว่างนี้ที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูล โดยปฏิบัติตามเอกสารขั้นตอนปฏิบัติในการจัดระดับชั้นความลับของข้อมูล (Information Classification and Media Handling Procedure) (WP-ACA-IFT-๕๐๐๖-๐๐)

๔.๑.๒ การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

๑) สถาบันมะเร็งแห่งชาติ จัดทำระเบียบวิธีปฏิบัติงานสำหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๔.๑.๓ การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย โดยปฏิบัติตามขั้นตอนปฏิบัติในการเข้าถึงพื้นที่ควบคุม (Physical Entry Control Procedure) (WP-ACA-IFT-๕๐๐๕-๐๐)

หมวดที่ ๕

ความการควบคุมการเข้าถึง (Access Control)

๕.๑ การควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirement for Access Control)

วัตถุประสงค์

เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย

นโยบาย

๕.๑.๑ นโยบายควบคุมการเข้าถึง (Access Control Policy)

๑) มีการกำหนดให้มีการควบคุมการใช้งานข้อมูลและระบบสารสนเทศ เพื่อควบคุมการเข้าถึง ให้เข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๒) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานและหน้าที่ความรับผิดชอบของผู้ใช้งานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ โดยปฏิบัติตามขั้นตอนปฏิบัติในการบริหารจัดการบัญชีผู้ใช้งาน (User Access Management Procedure) (WP-ACA-IFT-๕๐๐๗-๐๐) ทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

๓) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

๔) ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ และเฝ้าระวังการละเมิดความมั่นคงปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๕) ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๖) ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ

๗) การเข้าถึงข้อมูล และระบบสารสนเทศของสถาบันมะเร็งแห่งชาติ จะกระทำได้อีกต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความมั่นคงปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอนการทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสำรองข้อมูลและการกู้ข้อมูลที่เสียหายกลับคืนมา

๕.๑.๒ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) ผู้ใช้งานต้องได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๑) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ ต้องได้รับอนุญาตจากหัวหน้ากลุ่มงานดิจิทัลการแพทย์และต้องปฏิบัติตามนโยบาย

นี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “แบบคำขอรหัสเข้าระบบสารสนเทศโรงพยาบาล”(FM-HSD-IFT-๐๘๐๑๖-๐๐)

๒) การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่สถาบันมะเร็งแห่งชาติรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการภารกิจด้านการแพทย์และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งานอื่น ๆ

๓) ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๔) ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- ระบบเครือข่ายทั้งหมดของสถาบันมะเร็งแห่งชาติที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบันมะเร็งแห่งชาติต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
- ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบันมะเร็งแห่งชาติในลักษณะที่ผิดปกติ
- การเข้าสู่ระบบเครือข่ายภายในสถาบันมะเร็งแห่งชาติ โดยผ่านทางระบบอินเทอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใส่รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
- ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของสถาบันมะเร็งแห่งชาติ
- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- การระบุอุปกรณ์บนเครือข่าย
 - ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียด เครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
 - อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
 - ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
 - กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
 - อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

- การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์
- ๕) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ
 - เว้นว่างจากการใช้งานไม่เกินกว่า ๒ ชั่วโมง
- ๖) ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)
- ๗) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อนดำเนินการ
- ๘) กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย
- ๙) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ พ.ศ. ๒๕๕๐
- ๑๐) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกสถาบันมะเร็งแห่งชาติ เพื่อดูแลรักษาความมั่นคงปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้
 - บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสถาบันมะเร็งแห่งชาติจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้ากลุ่มงานหรือผู้ดูแลที่ได้รับอนุญาต
 - มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม
 - วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้ากลุ่มงานหรือผู้ดูแลที่ได้รับอนุญาต
 - การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันมะเร็งแห่งชาติอย่างเพียงพอ
 - การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในสถาบันมะเร็งแห่งชาติจากระยะไกล ต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการเข้ารหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
- ๑๑) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้
 - Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต
 - Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศภายใน
- ๑๒) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
- ๑๓) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกสถาบันมะเร็งแห่งชาติ ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑๔) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันมิให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๑๕) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๒ การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์

เพื่อป้องกันมิให้ผู้ที่ไม่มียสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

๕.๒.๑ การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)

การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายใน สถาบันมะเร็งแห่งชาติ เป็นต้น โดยปฏิบัติตามขั้นตอนปฏิบัติในการบริหารจัดการบัญชีผู้ใช้งาน (User Access Management Procedure) (WP-ACA-IFT-๕๐๐๗-๐๐) โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนของสถาบันมะเร็งแห่งชาติ อย่างเคร่งครัด

๕.๒.๒ การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท

๕.๒.๓ การบริหารจัดการสิทธิ์ตามระดับสิทธิ์การเข้าถึง (Management of Privileged Access Right)

๑) ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

๒) ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log-on เข้าสู่ระบบสารสนเทศ

๕.๒.๔ การบริหารจัดการข้อมูลความลับสำหรับการพิสูจน์ตัวตนของผู้ใช้งาน (Management of Secret Authentication Information of User)

๑) ต้องมีกระบวนการจัดการที่ช่วยป้องกันข้อมูลในการส่งมอบให้แก่ผู้ใช้งานเพื่อพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นความลับ และการเก็บรักษาข้อมูลความลับของตัวเอง การส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งานซึ่งเป็นข้อมูลลับ

๒) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ต้องปฏิบัติตามวิธีปฏิบัติงานเรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ

๕.๒.๕ การทบทวนสิทธิ์ในการเข้าถึงระบบของผู้ใช้งาน (Review of User Access Rights)

ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๕.๒.๖ การถอนหรือการจัดการสิทธิ์การเข้าถึง (Removal or Adjustment of Access Rights)

๑) สิทธิ์การเข้าถึงของพนักงานและลูกจ้างของหน่วยงานภายนอกต่อสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศต้องได้รับการถอดถอนเมื่อสิ้นสุดการจ้างงาน หมดสัญญา หรือสิ้นสุดข้อตกลงการจ้าง และต้องได้รับการปรับปรุงให้ถูกต้องอย่างสม่ำเสมอ โดยปฏิบัติงานแบบฟอร์มการทบทวนสิทธิ์ (User Right Review Form) (FM-ACA-IFT-๕๐๐๙-๐๐)

๒) ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ตามขั้นตอนปฏิบัติการในการบริหารจัดการบัญชีผู้ใช้งาน (User Access Management Procedure) (WP-ACA-IFT-๕๐๐๗-๐๐)

๕.๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

วัตถุประสงค์

เพื่อให้ผู้ใช้งานมีความรับผิดชอบในการป้องกันข้อมูลที่ใช้ในการพิสูจน์ตัวตน

นโยบาย

๕.๓.๑ การใช้ข้อมูลการพิสูจน์ตัวตนซึ่งเป็นข้อมูลลับ (Use of Secret Authentication Information)

๑) การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

- ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) ตัวเล็ก ตัวใหญ่ และตัวอักษรพิเศษ (Special character)
- หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเอง หรือตรงกับคำในพจนานุกรม
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้เพิ่มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

๒) การนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เหมาะสมและเป็นมาตรฐานสากล

- ๓) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าจะการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง
- ๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของสถาบันมะเร็งแห่งชาติ และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านล้าสมัย หรือเกิดจากความผิดพลาดใด ๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้
- คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
 - การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
 - การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
 - เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
 - เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที
- ๕) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าจะข้อมูลนั้นจะเป็นของสถาบันมะเร็งแห่งชาติ หรือเป็นข้อมูลของบุคคลภายนอก
- ๖) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของสถาบันมะเร็งแห่งชาติ ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากรองผู้อำนวยการด้านการแพทย์
- ๗) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสถาบันมะเร็งแห่งชาติ และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย
- ๘) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์
- ๙) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สถาบันมะเร็งแห่งชาติ จะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่สถาบันมะเร็งแห่งชาติ ต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับสถาบันมะเร็งแห่งชาติ ซึ่งสถาบันมะเร็งแห่งชาติ อาจแต่งตั้งให้ผู้ที่ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๕.๔ การควบคุมการเข้าถึงระบบ (System and Application Access Control)

วัตถุประสงค์

เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

นโยบาย

๕.๔.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๑) ต้องมีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบ ได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่ต้องจำเป็นต้องใช้งาน

๒) บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของสถาบันมะเร็งแห่งชาติ อย่างเคร่งครัด ก่อนที่จะได้รับอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ

๕.๔.๒ ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)

ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบมีการหน่วงเวลาการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๕ ครั้ง และต้องวิเคราะห์บททวนว่าเป็นการโจมตีหรือไม่ อย่างน้อยไตรมาสละ ๑ ครั้ง

๕.๔.๓ ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้ระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด (๙๐ วัน)

๕.๔.๔ การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

๑) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๒) ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการใช้งานโปรแกรมยูทิลิตี้ เช่น ผู้ใช้งานระบบ เป็นต้น

๕.๔.๕ การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code)

ผู้พัฒนาระบบสารสนเทศต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ใช้งานจริงหรือให้บริการ เช่น

- ไม่ควรเก็บ Source Code ไว้ในเครื่องที่ใช้งานจริงและต้องเก็บ Source Code ไว้ในที่ที่ปลอดภัย
- ต้องไม่เก็บ Source Code ที่อยู่ในระหว่างทำการทดสอบรวมไว้กับ Source Code ที่ใช้งานได้จริงแล้ว

หมวดที่ ๖ การเข้ารหัสข้อมูล (Cryptography)

๖.๑ การกำหนดการควบคุมการเข้ารหัสข้อมูล (Cryptographic controls)

วัตถุประสงค์

เพื่อให้มีการเข้ารหัสข้อมูลอย่างเหมาะสมและได้ผล และเพื่อป้องกันความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

นโยบาย

๖.๑.๑ นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

สถาบันมะเร็งแห่งชาติ ต้องมีวิธีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง อย่างเหมาะสม

๖.๑.๒ การบริหารจัดการกุญแจในการเข้ารหัสข้อมูล (Key Management)

การใช้งาน การป้องกัน และอายุการใช้งานของกุญแจต้องมีการจัดทำและปฏิบัติตามตลอดวงจรชีวิตของกุญแจ โดยองค์กรควรมีการกำหนดมาตรการในการเก็บ Key ที่เป็นข้อมูลลับอย่างเหมาะสม

หมวดที่ ๗

ความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อมขององค์กร (Physical and Environmental Security)

๗.๑ บริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย (Secure Areas)

วัตถุประสงค์

เพื่อเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยทางกายภาพที่เกี่ยวกับสถานที่ซึ่งเป็นที่ตั้งและพื้นที่ใช้งานของระบบเทคโนโลยีสารสนเทศ ตลอดจนอุปกรณ์คอมพิวเตอร์ ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สินสถาบันมะเร็งแห่งชาติ

นโยบาย

๗.๑.๑ การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

1) สถาบันมะเร็งแห่งชาติจะต้องมีการจำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุมการเข้าออก

2) สถาบันมะเร็งแห่งชาติจะต้องจำแนก กำหนด และแบ่งบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)” รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และประกาศให้ทราบทั่วกัน (สถาบันมะเร็งแห่งชาติควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศประเภทใดบ้าง และมีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศใดที่อาจจำแนกได้มากกว่า ๑ ประเภท)

3) สถาบันมะเร็งแห่งชาติต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

4) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

๗.๑.๒ การควบคุมการเข้าออก (Physical Entry Controls)

สถาบันมะเร็งแห่งชาติที่เกี่ยวข้องกับการบริหารจัดการอาคารและสถานที่ ต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ” ที่มีสิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

๑) ต้องกำหนด “เจ้าหน้าที่ กลุ่มงานเทคโนโลยีสารสนเทศ” ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

๒) “เจ้าหน้าที่ กลุ่มงานเทคโนโลยีสารสนเทศ” จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้ เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๓) หากมีบุคคลอื่นใดที่ไม่ใช่ “เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้า สถาบันมะเร็งแห่งชาติต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้าพื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดยสถาบันมะเร็งแห่งชาติ เจ้าของพื้นที่ต้องจัดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่ยินยอมและไม่อนุญาตให้เข้าพื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกห้อง Data Center ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บบันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๔) บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนเองที่ออกให้โดยสถาบันมะเร็งแห่งชาติของรัฐ ตัวอย่างเช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของสถาบันมะเร็งแห่งชาติ ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่สถาบันมะเร็งแห่งชาติ

๕) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ และบุคคลภายนอกต้องติดบัตรเจ้าหน้าที่ หรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ในพื้นที่สถาบันมะเร็งแห่งชาติ ทั้งนี้ บัตรประจำตัวและบัตรผู้มาติดต่อ ไม่อนุญาตให้ออนกรรรมสิทธิ์หรือหิบบิยืมกันใช้งาน

๖) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ต้องไม่เปิดประตูห้อง Data Center ทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่สถาบันมะเร็งแห่งชาติ โดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สถาบันมะเร็งแห่งชาติ และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๗) ผู้ใช้งานต้องแจ้งเจ้าหน้าที่รักษาความมั่นคงปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่แขวนบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อในพื้นที่สถาบันมะเร็งแห่งชาติ

๘) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มาติดต่อนั้นอยู่ในพื้นที่สถาบันมะเร็งแห่งชาติ

๗.๑.๓ การรักษาความมั่นคงปลอดภัยสถาบันมะเร็งแห่งชาติ ห้องทำงาน และเครื่องมือต่าง ๆ (Securing Offices, Rooms and Facilities)

๑) ISMR ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่น ๆ ให้กับสถาบันมะเร็งแห่งชาติ ห้องทำงานและเครื่องมือต่าง ๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก สถาบันมะเร็งแห่งชาติ หรือห้องจะต้อง ไม่มีป้าย หรือสัญลักษณ์ ที่บ่งบอกถึงการมีระบบสำคัญอยู่ในสถานที่ดังกล่าว ประตู หน้าต่างของสถาบันมะเร็งแห่งชาติ หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๒) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเองเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อก อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลำพังบนโต๊ะทำงาน ในห้องประชุม หรือในตู้ที่ไม่ได้ล็อกกุญแจโดยเด็ดขาด

๔) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้โดยปฏิบัติตามแบบฟอร์มคำร้องขอทำลายสื่อบันทึกข้อมูล (Disposal of media Form) (FM-ACA-IFT-๕๐๐๘-๐๐) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตนเองโดยนโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร สถาบันมะเร็งแห่งชาติ

เด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าของพื้นที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่างถูกต้องของสถาบันมะเร็งแห่งชาติเท่านั้น

๗.๑.๔ การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ (Protecting against External and Environmental Threats)

สถาบันมะเร็งแห่งชาติต้องมีการป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น ซึ่งเป็นภัยคุกคามจากภายนอกต้องมีการเตรียมการป้องกันเหตุที่อาจเกิดขึ้น

๗.๑.๕ การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

1) หัวหน้าของแต่ละสถาบันมะเร็งแห่งชาติ ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวิดีโอในบริเวณนั้น เป็นต้น

2) สถาบันมะเร็งแห่งชาติต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวิดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๗.๑.๖ การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งของ (Delivery and Loading Areas)

1) สถาบันมะเร็งแห่งชาติต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควรแบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้าจะต้องไม่อยู่ในพื้นที่ ๆ บุคคลภายนอกเข้าถึงได้

2) เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวตลอดเวลาขณะปฏิบัติหน้าที่ในบริเวณ กลุ่มงานเทคโนโลยีสารสนเทศ และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัว ถือเป็นหน้าที่ที่จะต้องแจ้งเจ้าหน้าที่รักษาความมั่นคงปลอดภัยโดยทันที

๗.๒ ความมั่นคงปลอดภัยของอุปกรณ์ (Equipment)

วัตถุประสงค์

เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่น ๆ

นโยบาย

๗.๒.๑ การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

- ๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- ๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- ๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- ๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- ๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในสถาบันมะเร็งแห่งชาติ
- ๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๒.๒ การดูแลอุปกรณ์ต่าง ๆ (Supporting Utilities)

- 1) เจ้าหน้าที่ต้องกำหนดให้มีการดูแลรักษาอุปกรณ์ Utilities ที่เกี่ยวข้อง เช่น Uninterruptible Power Supply (UPS) อุปกรณ์ตรวจจับความชื้น อุปกรณ์ตรวจจับควัน เป็นต้น
- 2) เจ้าหน้าที่ต้องมีการตรวจสอบการให้บริการของอุปกรณ์ อย่างน้อยปีละ ๒ ครั้ง

๗.๒.๓ การเดินสายไฟและสายเคเบิล (Cabling Security)

- 1) ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้า หรือสายเคเบิลเข้ามาภายในอาคารสถาบันมะเร็งแห่งชาติ
- 2) บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสถาบันมะเร็งแห่งชาติ และมีการติดตั้งตู้พักสาย ต้องล็อกไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิ์เท่านั้น

๗.๒.๔ การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ ๑ ครั้ง หรือตามที่เจ้าของผลิตภัณฑ์แนะนำ เป็นต้น

๗.๒.๕ การนำทรัพย์สินขององค์กรออกนอกสถาบันมะเร็งแห่งชาติ (Removal of Asset)

อุปกรณ์สารสนเทศหรือซอฟต์แวร์ ต้องไม่มีการนำออกนอก สถาบันมะเร็งแห่งชาติ โดยไม่ได้รับอนุญาต

๗.๒.๖ การป้องกันอุปกรณ์และทรัพย์สินสารสนเทศที่ใช้งานอยู่นอกสถาบันมะเร็งแห่งชาติ (Security of Equipment and asset Off-Premises)

สถาบันมะเร็งแห่งชาติต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของสถาบันมะเร็งแห่งชาติ เช่น เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ เป็นต้น เมื่อถูกนำไปใช้งานนอกสถาบันมะเร็งแห่งชาติ จะต้องปฏิบัติตามระเบียบในการใช้งานการยืม-คืน

๗.๒.๗ การจัดการอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้ใหม่ (Secure Disposal or Re-use of Equipment)

สถาบันมะเร็งแห่งชาติต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าวก่อนนำอุปกรณ์ไปแจกจ่าย

๗.๒.๘ การป้องกันอุปกรณ์ของผู้ใช้งานที่ไม่มีผู้ดูแล (Unattended User Equipment)

ผู้ใช้งานต้องป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์ ระบบสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายที่ไม่มีผู้ดูแล

๗.๒.๙ การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศที่สำคัญไว้ในที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy)

เจ้าหน้าที่ต้องกำหนดการควบคุมเอกสาร ข้อมูล หรือสื่อต่าง ๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ที่ไม่ปลอดภัยในขณะที่ไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญ ปรากฏในขณะที่ไม่ได้ใช้งาน

หมวดที่ ๘

ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

๘.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์

เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

นโยบาย

๘.๑.๑ การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

๑) ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในสถาบันมะเร็งแห่งชาติ เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วย รายละเอียดขั้นตอนการปฏิบัติ และเจ้าหน้าที่หรือสถาบันมะเร็งแห่งชาติผู้รับผิดชอบ

๒) คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้น ๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง

๓) มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๘.๑.๒ การจัดการการเปลี่ยนแปลง (Change Management)

๑) ต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้ง โดยปฏิบัติตามขั้นตอนปฏิบัติในการบริหารการเปลี่ยนแปลง (Change Management Procedure) (WP-ACA-IFT-๕๐๐๓-๐๐) เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานหรือรายงานกับ ISS (จัดการการเปลี่ยนแปลง)

๒) เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวข้องกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง

๓) ISS (จัดการการเปลี่ยนแปลง) ต้องจัดให้มีการประชุมเป็นประจำเพื่อตรวจสอบคำร้องขอการเปลี่ยนแปลง (Change Request) และพิจารณาตรวจสอบ การเปลี่ยนแปลงต่าง ๆ ให้เป็นที่พอใจและยอมรับได้

๔) ตาราง และ/หรือ แผนการเปลี่ยนแปลงทุกครั้งต้องได้รับความเห็นชอบจาก ISS (จัดการการเปลี่ยนแปลง) ก่อนจะทำการเปลี่ยนแปลง

๕) บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้สถาบันมะเร็งแห่งชาติที่เกี่ยวข้องได้รับทราบโดยทันทีฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

- วันที่รับเรื่อง และวันที่ทำการเปลี่ยนแปลง
- เจ้าของข้อมูล และผู้ดูแลระบบ
- วิธีการเปลี่ยนแปลง
- ผลของการเปลี่ยนแปลง (สำเร็จ หรือ ล้มเหลว)

๘.๑.๓ การจัดการขีดความสามารถ (Capacity Management)

๑) ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่าง ๆ โดยปฏิบัติตามเอกสารขั้นตอนปฏิบัติในการบริหารจัดการสมรรถนะของอุปกรณ์ (Capacity Management Procedure) (WP-ACA-IFT-๕๐๐๙-๐๐) ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน ๑ ปีที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

๒) แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิ การ Tuning การจัดหาเพิ่มเติม

๘.๑.๔ การแยกเครื่องมือในการประมวลผลสารสนเทศในการพัฒนา ทดสอบและสภาพแวดล้อมในการปฏิบัติงาน (Separation of Development, Testing and Operational Environment)

ต้องมีการแยกเครื่องมือในการประมวลผลสารสนเทศ (ระบบคอมพิวเตอร์และเครือข่าย) ในการพัฒนาและทดสอบ อาทิ การพัฒนาซอฟต์แวร์ควรมีการแยกเครื่องที่ใช้ในการพัฒนาและทดสอบ ออกจากกับเครื่องที่ใช้งานจริง หากจำเป็นระบบเครือข่ายของการพัฒนาควรแยกออกจากระบบที่ใช้งานจริงด้วย

๘.๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Protection from Malware)

วัตถุประสงค์

เพื่อให้สารสนเทศและอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและมั่นคงปลอดภัย

นโยบาย

๘.๒.๑ มาตรการป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

๑) สถาบันมะเร็งแห่งชาติ ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้น ซอฟต์แวร์ที่สถาบันมะเร็งแห่งชาติอนุญาตให้ใช้งานหรือที่สถาบันมะเร็งแห่งชาติมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๒) ซอฟต์แวร์ (Software) ที่สถาบันมะเร็งแห่งชาติได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากรองผู้อำนวยการด้านการแพทย์หรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

๓) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus) ตามที่สถาบันมะเร็งแห่งชาติได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากรองผู้อำนวยการด้านการแพทย์

๔) บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๕) ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๖) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๗) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

๘) ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของสถาบันมะเร็งแห่งชาติ หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากรองผู้อำนวยการด้านการแพทย์

๙) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของสถาบันมะเร็งแห่งชาติ สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการดังนี้

๙.๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความมั่นคงปลอดภัยระบบ รวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกระหัสผ่านของบุคคลอื่น

๙.๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

- ๙.๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์
- ๙.๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์
- ๙.๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์
- ๑๐) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)
 - ๑๐.๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก
 - ๑๐.๒) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น
 - ๑๐.๓) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง
 - ๑๐.๔) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากหน่วยงานภายนอก สถาบันมะเร็งแห่งชาติ ต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ
 - ๑๐.๕) ผู้พัฒนาระบบจากภายนอก (outsourcer) ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) และลงนามในข้อตกลงว่าจะไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA) ก่อนดำเนินการ
 - ๑๐.๖) ผู้พัฒนาระบบจากภายนอก (Outsourcer) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสถาบันมะเร็งแห่งชาติ

๘.๓ การสำรองข้อมูล (Backup)

วัตถุประสงค์

เพื่อเป็นแนวทางในกำหนดการสำรองข้อมูล เพื่อใช้ในการกู้ระบบในกรณีที่เกิดเหตุต่าง ๆ เช่น ภัยธรรมชาติ ระบบเสียหาย ฯลฯ

นโยบาย

๘.๓.๑ การสำรองข้อมูล (Information Backup)

- ๑) พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นมากไปน้อย
- ๒) กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล
- ๓) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสถาบันมะเร็งแห่งชาติ พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง
- ๔) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้
 - กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
 - กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
 - บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
 - ตรวจสอบค่าคอนฟิกูเรชันต่าง ๆ ของระบบการสำรองข้อมูล
 - จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลได้อย่างชัดเจน
 - จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับสถาบันมะเร็งแห่งชาติต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับสถาบันมะเร็งแห่งชาติ
 - ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
 - ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
 - จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้
 - ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น
 - กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

- ๕) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย
- มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
 - มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
 - มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
 - มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
 - มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
 - การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น
- ๖) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง
- ๗) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- ๘) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมีสภาพพร้อมใช้งานอยู่เสมอ
- ๙) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละสถาบันมะเร็งแห่งชาติ อย่างน้อยปีละ ๑ ครั้ง

๘.๔ การบันทึกข้อมูลล็อกและการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์

เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

นโยบาย

๘.๔.๑ การบันทึกข้อมูลเหตุการณ์ (Event logging)

ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิบัติการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้

๘.๔.๒ การป้องกันข้อมูลล็อก (Protection of Log Information)

ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

๘.๔.๓ ข้อมูลล็อกของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Admin/WTerator and Operator Logs)

ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

๘.๔.๔ การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในสถาบันมะเร็งแห่งชาติให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของสถาบันมะเร็งแห่งชาติ ถูกบุกรุกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

๘.๕ การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์

เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

นโยบาย

๘.๕.๑ การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบรารี ซอฟต์แวร์ชุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่าไม่ก่อให้เกิดปัญหาให้กับเครื่องที่ให้บริการอยู่

๘.๖ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วย เพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

๘.๖.๑ การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

๘.๖.๒ การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

๑) สถาบันมะเร็งแห่งชาติ ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่สถาบันมะเร็งแห่งชาติจัดหาเข้ามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๒) ซอฟต์แวร์ (Software) ที่สถาบันมะเร็งแห่งชาติได้จัดเตรียมไว้ให้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากรองผู้อำนวยการด้านการแพทย์หรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

๘.๗ การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์

เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของสถาบันมะเร็งแห่งชาติ

นโยบาย

๘.๗.๑ การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

ISS ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของสถาบันมะเร็งแห่งชาติน้อยที่สุด

หมวดที่ ๙

ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

๙.๑ การจัดการระบบรักษาความมั่นคงปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์

เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ

นโยบาย

๙.๑.๑ การควบคุมการเข้าถึงเครือข่าย (Network Control)

๑) ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๒) การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในสถาบันมะเร็งแห่งชาติ ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๓) ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ และเครือข่ายที่สถาบันมะเร็งชาตินั้นรับผิดชอบ

๔) ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

๕) บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของสถาบันมะเร็งแห่งชาติ ด้วย

๙.๑.๒ ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

๑) ระบบเครือข่ายทั้งหมดของสถาบันมะเร็งแห่งชาติ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องมีการใช้อุปกรณ์หรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ ฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับไวรัสด้วย

๒) ต้องจำกัดจำนวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของสถาบันมะเร็งแห่งชาติ ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่าย สถาบันมะเร็งแห่งชาติ ได้

๓) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์บริการเชื่อมต่อจากภายนอก (Remote Access Service) บนเครื่องคอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ โดยไม่ได้รับอนุญาต

๔) ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใด ๆ จากภายนอกเข้ากับระบบคอมพิวเตอร์และระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขออนุมัติอย่างเหมาะสมก่อนทุกครั้ง

๕) ห้ามผู้ใช้งานติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการเครือข่าย ตัวอย่างเช่น Router, Switch, Hub และ Wireless Access Point ฯลฯ โดยไม่ได้รับอนุญาตเด็ดขาด

๖) ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของสถาบันมะเร็งแห่งชาติ ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอก ผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายใน สถาบันมะเร็งแห่งชาติ โดยเด็ดขาด

๙.๑.๓ การจัดแบ่งเครือข่ายภายใน สถาบันมะเร็งแห่งชาติ (Segregation in Network)

๑) ต้องออกแบบระบบเครือข่ายตามกลุ่มของการบริการระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีการใช้งาน โดยแบ่งตามกลุ่มของผู้ใช้และกลุ่มของระบบสารสนเทศ โดยแบ่งเป็นโซนภายใน (Internal Zone) และ โซนภายนอก (External Zone) เพื่อให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

๒) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙.๒ การถ่ายโอนข้อมูล (Information Transfer)

วัตถุประสงค์

เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กร และถ่ายโอนข้อมูลกับภายนอกสถาบันมะเร็งแห่งชาติ

นโยบาย

๙.๒.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ

(Information Transfer Policies and Procedures)

1) ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติ หรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการและมีการปฏิบัติตามเพื่อป้องกันสารสนเทศที่มีการถ่ายโอนกับหน่วยงานภายนอก

2) ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามขั้นตอนปฏิบัติในการจัดระดับชั้นความลับของข้อมูล (Information Classification and Media Handling Procedure)

3) ในการแลกเปลี่ยน ถ่ายโอนข้อมูลส่วนบุคคล ต้องปฏิบัติตาม PDPA อย่างเคร่งครัด

๙.๒.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

ต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล โดยปฏิบัติตามเอกสารสัญญาการรักษาความลับ (Non-disclosure Agreement) และหากมีการแลกเปลี่ยนข้อมูลส่วนบุคคลต้องมีการจัดทำข้อตกลงการ

ประมวลผลข้อมูล data processing agreement) หรือ ข้อตกลงการแลกเปลี่ยนข้อมูล (data sharing agreement)

๙.๒.๓ การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

๙.๒.๔ การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล (Confidentiality or Non-Disclosure Agreements)

๑) ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล หรือสัญญาไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA) ซึ่งเป็นไปตามความต้องการด้านการป้องกันข้อมูลของสถาบันมะเร็งแห่งชาติ และมีการทบทวนอย่างสม่ำเสมอ

๒) พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของสถาบันมะเร็งแห่งชาติ ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) และต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ในข้อตกลงว่าจะไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA)

หมวดที่ ๑๐

การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

๑๐.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์

เพื่อให้แน่ใจว่ามีการสร้างความมั่นคงปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดจนวงจรการพัฒนา ระบบ ซึ่งรวมถึงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

นโยบาย

๑๐.๑.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัย (Information Security Requirements Analysis and Specification)

ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือชื่อการใช้งานสถาบันมะเร็งแห่งชาติดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยงใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสำรองข้อมูล ระบบเครือข่ายสำรอง เป็นต้น
- มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

๑๐.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ (Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกัน และการเปิดเผย หรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๑.๓ การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดพลาด การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

๑๐.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์

เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศที่มีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (development lifecycle)

นโยบาย

๑๐.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อกำหนดที่องค์กรกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความมั่นคงปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developer) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนามีช่องโหว่ที่รู้จักกัน (Common Vulnerabilities and Exposures (CVE)) และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

๑๐.๒.๒ กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบสารสนเทศที่ใช้จริง หรือให้บริการอยู่แล้ว เช่น

- คำขอให้แก้ไขต้องมาจากผู้มีสิทธิ์
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

โดยดำเนินการตามขั้นตอนปฏิบัติในการบริหารการเปลี่ยนแปลง (Change Management Procedure) (WP-ACA-IFT-๕๐๐๓-๐๐)

๑๐.๒.๓ การตรวจสอบซอฟต์แวร์หลังจากการเปลี่ยนแปลงระบบปฏิบัติการ (Technical Review of Applications After Operating Platform Changes)

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่าง ๆ ที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

๑๐.๒.๔ การควบคุมการเปลี่ยนแปลงของซอฟต์แวร์สำเร็จรูป (Restrictions on Changes to Software Packages)

เมื่อมีการใช้งานซอฟต์แวร์สำเร็จรูปต้องมีการควบคุมการเปลี่ยนแปลงเท่าที่จำเป็น และการเปลี่ยนแปลงทั้งหมดจะต้องถูกทดสอบและจัดทำเป็นเอกสารเพื่อให้สามารถนำมาใช้งานได้เมื่อมีการปรับปรุงซอฟต์แวร์ในอนาคต

๑๐.๒.๕ หลักการวิศวกรรมระบบด้านความมั่นคงปลอดภัย (Secure system engineering principles)

เพื่อให้เกิดความมั่นคงปลอดภัยทางด้านวิศวกรรมระบบ ต้องมีการกำหนดขึ้นมาเป็นลายลักษณ์อักษร โดยมีการปรับปรุงอย่างต่อเนื่อง และมีการประยุกต์ใช้กับงานพัฒนาระบบ

๑๐.๒.๖ สภาพแวดล้อมของการพัฒนาระบบที่มีความมั่นคงปลอดภัย (Secure development environment)

สถาบันมะเร็งแห่งชาติต้องมีการจัดทำหรือป้องกันสภาพแวดล้อมในการทำงานต่าง ๆ ให้มีความเหมาะสมและปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

๑๐.๒.๗ การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

ในการทำสัญญาว่าจ้างการพัฒนาระบบของสถาบันมะเร็งแห่งชาติ ต้องมีความชัดเจนและครอบคลุมถึงสัญญาทางด้านลิขสิทธิ์ซอฟต์แวร์ การใช้ระบบ การตรวจสอบระบบ โดยละเอียดก่อนติดตั้งใช้งานจริง รวมถึงการรับรองคุณภาพของระบบ และการกำหนดขอบเขตในการจ้างพัฒนาระบบ

๑๐.๒.๘ การทดสอบด้านความมั่นคงปลอดภัยของระบบ (System security testing)

โปรแกรมหรือระบบที่พัฒนาขึ้นมา ควรมีการทดสอบคุณสมบัติด้านความมั่นคงปลอดภัย โดยต้องมีการทดสอบอยู่ในช่วงระหว่างการพัฒนา

๑๐.๒.๙ การทดสอบเพื่อรับรองระบบ (System acceptance testing)

๑) มีการจัดทำแผนการทดสอบหรือเกณฑ์ที่เกี่ยวข้องเพื่อรับรองระบบ โดยต้องมีการจัดทำทั้งสำหรับระบบใหม่ และระบบที่ปรับปรุง

๒) ต้องจัดให้มีเกณฑ์ในการยอมรับระบบใหม่ ระบบที่จัดซื้อเข้ามาใช้งาน หรือทรัพยากรสารสนเทศอื่น ๆ ก่อนการใช้งาน รวมทั้งต้องจัดทำเอกสาร Checklist หัวข้อที่ทำการทดสอบระบบก่อนที่จะตรวจรับระบบนั้น และให้มีการเซ็นชื่อเจ้าหน้าที่ทำการทดสอบและลายเซ็นผู้ส่งมอบ

๑๐.๓ ข้อมูลสำหรับการทดสอบ (Test data)

วัตถุประสงค์

เพื่อให้มีการป้องกันข้อมูลที่นำมาใช้ในการทดสอบ

นโยบาย

๑๐.๓.๑ การป้องกันข้อมูลสำหรับการทดสอบ (Protection of Test Data)

ข้อมูลจริงที่จะนำไปใช้ในการทดสอบระบบ จะต้องได้รับอนุญาตจากผู้รับผิดชอบในการรักษาข้อมูลนั้น ๆ ก่อน เมื่อใช้งานเสร็จจะต้องทำการลบข้อมูลจริงออกจากระบบทดสอบทันที และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริงไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และสถาบันมะเร็งแห่งชาติที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ ๑๑

ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑๑.๑ ความมั่นคงปลอดภัยสารสนเทศกับความสัมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์

เพื่อให้มีการป้องกันทรัพย์สินขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

๑๑.๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

สถาบันมะเร็งแห่งชาติจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างสถาบันมะเร็งแห่งชาติกับผู้ให้บริการภายนอก

๑๑.๑.๒ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

๑) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่างสถาบันมะเร็งแห่งชาติกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความปลอดภัยสำหรับสารสนเทศ

๒) ผู้ดูแลระบบต้องให้สิทธิการเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

๓) การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของสถาบันมะเร็งแห่งชาติจากหน่วยงานภายนอก ต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากรองผู้อำนวยการด้านการแพทย์หรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

๔) ผู้ให้บริการภายนอกต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายและสารสนเทศที่ยอมรับได้ (Acceptable Use Policy: AUP) และลงนามในข้อตกลงว่าจะไม่เปิดเผยความลับของสถาบันมะเร็งแห่งชาติ (Non Disclosure Agreement: NDA)

๕) สัญญาระหว่างสถาบันมะเร็งแห่งชาติ และ หน่วยงานภายนอก ในการให้บริการ ต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้

- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- ระดับการให้บริการ (Service Level)
- หน้าที่และความรับผิดชอบขององค์กรและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้
- ราคา และเงื่อนไขการชำระเงิน

- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์กร

๑๑.๑.๓ ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

๑) ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๒) ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

๑๑.๒ การบริหารจัดการ การให้บริการโดยผู้ให้บริการภายนอก (Supplier service delivery management)

วัตถุประสงค์

เพื่อให้มีการรักษาไว้ซึ่งระดับความมั่นคงปลอดภัย และระบบการให้บริการตามที่ตกลงกันไว้ในข้อตกลงการให้บริการ ของผู้ให้บริการภายนอก

นโยบาย

๑๑.๒.๑ การติดตามและทบทวนบริการของผู้ให้บริการภายนอก (Monitoring and review of Supplier Services)

๑) สถาบันมะเร็งแห่งชาติ ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับ สถาบันมะเร็งแห่งชาติ ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

๒) ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๓) การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของสถาบันมะเร็งแห่งชาติ

๑๑.๒.๒ การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

๑) การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของสถาบันมะเร็งแห่งชาติ

๒) การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติและมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนำระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

หมวดที่ ๑๒

การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๑๒.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์

เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสถาบันมะเร็งแห่งชาติ ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

๑๒.๑.๑ หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

ISS ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสถาบันมะเร็งแห่งชาติและขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี

๑๒.๑.๒ การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

๑) ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสถาบันมะเร็งแห่งชาติ โดยผ่านช่องทางรายงานที่กำหนดไว้

๒) ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายใน สถาบันมะเร็งแห่งชาติ ต่อผู้บังคับบัญชา หรือสถาบันมะเร็งแห่งชาติจัดการความมั่นคงปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

๓) ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อ ISS ทันที

๔) ผู้ใช้งานที่พบว่าฮาร์ดแวร์หรืออุปกรณ์ใด ๆ เกิดความเสียหาย หรือทำงานผิดปกติ ต้องรายงานต่อ ISS (บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ) ทันที

๕) ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ใน สถาบันมะเร็งแห่งชาติ ต้องไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา สถาบันมะเร็งแห่งชาติ จัดการความมั่นคงปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

๑๒.๑.๓ การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

ISS ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสถาบันมะเร็งแห่งชาติ ที่สังเกตพบหรือเกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

๑๒.๑.๔ การประเมินและตัดสินใจต่อสถานการณ์ความมั่นคงปลอดภัยสารสนเทศ (Assessment of and decision on information security events)

๑) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

๒) จัดทำเกณฑ์ในการตัดสินเหตุการณ์ที่ถือว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

๑๒.๑.๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ (Response to information security incidents)

๑) ISS ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

๒) เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๓) โดยได้จัดทำแยกประเภทตามระบบต่าง ๆ ดังนี้

๓.๑) ระบบป้องกันผู้บุกรุก

๓.๑.๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำกรตรวจสอบมี ดังต่อไปนี้

- มีการโจมตีอย่างน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
- ระดับความรุนแรงอย่างน้อยเพียงใด
- หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

๓.๒) ระบบไฟร์วอลล์

๓.๒.๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง

๓.๒.๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

- Packet ที่ไฟร์วอลล์ได้ทำการ Block
- ลักษณะของ Packet ที่ถูก Block
- Packet ของหมายเลขไอพี ของเครือข่ายใดถูก Block เป็นจำนวนมาก

๓.๒.๓) กรณีที่ตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้อำนวยการภารกิจด้านการแพทย์เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๓.๓) ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสถาบันมะเร็งแห่งชาติ

๓.๓.๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในสถาบันมะเร็งแห่งชาติ ไปยังภายนอกหรือไม่

๓.๓.๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของสถาบันมะเร็งแห่งชาติ

๓.๓.๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่าย แล้วทำการแก้ไขเครื่องนั้นทันที

๑๒.๑.๖ การเรียนรู้จากเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Learning from Information Security Incidents)

ISS (บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ) ต้องบันทึกเหตุการณ์ละเมิดความมั่นคงปลอดภัย โดยอย่างน้อยจะต้องพิจารณาถึงประเภทของเหตุการณ์ปริมาณที่เกิดขึ้นและค่าใช้จ่ายเกิดขึ้นจากความเสียหาย เพื่อจะได้เรียนรู้จากเหตุการณ์ที่เกิดขึ้นแล้วและเตรียมการป้องกันที่จำเป็นไว้ล่วงหน้า

๑๒.๑.๗ การเก็บรวบรวมหลักฐาน (Collection of Evidence)

ISS (บริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหมาย หรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หมวดที่ ๑๓

ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหาร จัดการ เพื่อสร้างความต่อเนื่องทางธุรกิจ (Information Security Aspects of Business Continuity Management)

๑๓.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์

เพื่อป้องกันการหยุดชะงักในการดำเนินงานของสถาบันมะเร็งแห่งชาติ ที่เป็นผลมาจากความล้มเหลวหรือการหยุดทำงานของระบบ

นโยบาย

๑๓.๒.๑ การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Planning information security continuity)

๑) องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

๒) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแนวทางปฏิบัติ ในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ควรพิจารณา ดังนี้

๓) การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหาย และมีผลกระทบต่อการทำงานของสถาบันมะเร็งแห่งชาติ และการให้บริการด้านเทคโนโลยีสารสนเทศสถาบันมะเร็งแห่งชาติ ฯ

๔) การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น

๕) การดำเนินการเพื่อให้ สถาบันมะเร็งแห่งชาติ สามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น

๖) การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงาน สถาบันมะเร็งแห่งชาติ กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

๑๓.๒.๒ การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Implement information security continuity)

๑) สถาบันมะเร็งแห่งชาติ ต้องจัดตั้ง ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ของระบบเทคโนโลยีสารสนเทศ

๒) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแผนรองรับ เหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับ ประยุกต์แก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบแผนอย่างน้อยปีละ ๑ ครั้ง

๑๓.๒.๓ การตรวจสอบ ทบทวน และการประเมินความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Verify, review and evaluate information security continuity)

๑) ISS (บริหารจัดการแผนสร้างความปลอดภัยให้กับธุรกิจ) ต้องกำหนดเวลาการทดสอบแผน กำหนดการทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนถึงสิ้นสุดกระบวนการทดสอบ

๒) ISS (บริหารจัดการแผนสร้างความปลอดภัยให้กับธุรกิจ) ต้องกำหนดเหตุการณ์จำลองที่จะใช้ทดสอบและรายละเอียด ในการกำหนดรายละเอียดของเหตุการณ์จำลอง ควรระบุวัตถุประสงค์ ขอบเขต ของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอน การทดสอบแผนฉุกเฉิน

๓) ISS (บริหารจัดการแผนสร้างความปลอดภัยให้กับธุรกิจ) ต้องกำหนดทรัพยากรต่าง ๆ ที่ใช้ในการ ทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการ ทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่าง ๆ และงบประมาณที่ต้องใช้ด้วย

๔) ISS (บริหารจัดการแผนสร้างความปลอดภัยให้กับธุรกิจ) ต้องกำหนดแผนงาน แนวทาง และ ระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับ สถานการณ์ปัจจุบัน

๑๓.๒ การเตรียมอุปกรณ์ประมวลผลสำรอง (Redundancies)

วัตถุประสงค์

เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

๑๓.๒.๔ สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ (Availability of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสำรองไว้เพียงพอ เพื่อให้ตรงตามความ ต้องการด้านสภาพความพร้อมใช้ที่กำหนด

หมวดที่ ๑๔

การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิด นโยบายความมั่นคงปลอดภัยสารสนเทศของสถาบันมะเร็งแห่งชาติ (Compliance)

๑๔.๑ การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์

เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

นโยบาย

๑๔.๒.๑ การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ

(Identification of Applicable Legislation and Contractual Requirements)

๑) สถาบันมะเร็งแห่งชาติ ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับกฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของสถาบันมะเร็งแห่งชาติ

๒) เจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด

๓) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ ถือเป็นทรัพย์สินของสถาบันมะเร็งแห่งชาติ (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก รวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร หรือลิขสิทธิ์ของบุคคลภายนอก) ทั้งนี้ สถาบันมะเร็งแห่งชาติ สามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๔) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของสถาบันมะเร็งแห่งชาติ กำหนดไว้

๕) ห้ามเจ้าหน้าที่สถาบันมะเร็งแห่งชาติ ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของสถาบันมะเร็งแห่งชาติ กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

๖) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศไม่ขัดต่อข้อกำหนดใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชี่ยวชาญด้านกฎหมายก่อนดำเนินการส่งออก

๑๔.๒.๒ ทรัพย์สินทางปัญญา (Intellectual Property Rights)

๑) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่สถาบัน
มะเร็งแห่งชาติจัดหาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๒) ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software
Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย

๓) ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสาร
ใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของ
สถาบันมะเร็งแห่งชาติ โดยเด็ดขาด

๑๔.๒.๓ การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือ
ข้อบังคับ ที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบสถาบันมะเร็งแห่งชาติ
ว่าด้วยงานสารบรรณ และกฎหมาย เช่น ระเบียบสำนักนายกรัฐมนตรี

๑๔.๒.๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล

(Privacy and protection of personally identifiable information)

สถาบันมะเร็งแห่งชาติ ต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ
สัญญา ที่เกี่ยวกับ สถาบันมะเร็งแห่งชาติ

๑๔.๒.๕ การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

สถาบันมะเร็งแห่งชาติ ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และ
ระเบียบที่เกี่ยวข้อง

๑๔.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์

เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

นโยบาย

๑๔.๒.๖ การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ (Independent review of information security)

IWT ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย วิธีปฏิบัติงานต่าง ๆ ให้ถูกต้องและเป็นปัจจุบันตามรอบระยะเวลาที่กำหนด อย่างน้อยปีละ ๑ ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

๑๔.๒.๗ การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของสถาบันมะเร็งแห่งชาติ (Compliance with Security Policy and Standards)

๑) IWT ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของสถาบันมะเร็งแห่งชาติตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้

๒) IWT ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีปฏิบัติงานรวมถึงแบบฟอร์มที่เกี่ยวข้องเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

๑๔.๒.๘ การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

IWT ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้ว อย่างน้อยปีละ ๑ ครั้ง ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ/หรือ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อตรวจสอบข้อบกพร่องของระบบด้วย