นโยบายความมั่นคงปลอดภัย

ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ICT Security Policy

โรงพยาบาลปางศิลาทอง จังหวัดกำแพงเพชร

สารบัญ

โรงพยาบาลปางศิลาทอง

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

.....

ข้อ ๑ ผู้ใช้งานเครื่องคอมพิวเตอร์ หรือ คอมพิวเตอร์พกพา ต้องการเปิด-เปิดเครื่องตามวิธีที่กำหนดอย่างเหมาะสม (Shutdown ระบบ โดยไม่ปิดเครื่องที่ปุ่มบนตัวเครื่อง)

ข้อ ๒ ผู้ใช้ต้องป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้ (Username) และ รหัสผ่าน (Password) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้ รหัสผ่าน (Password) และต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีผู้ใช้งาน (Username) ผู้นั้น

ข้อ ๓ ผู้ใช้ห้ามนำเข้าและส่งออกข้อมูล สารสนเทศจากระบบ HOSxP, LAB, X-Ray และ 3Refer ผ่านอุปกรณ์สำรองข้อมูลภายนอก เช่น Flash Drive, External Drive, CD/DVD เป็นต้น ยกเว้นได้รับอนุญาตจากผู้ดูแลระบบ (แบบฟอร์มอนุญาต)

ข้อ ๔ ผู้ใช้ห้ามทำการแก้ไขข้อมูลในระบบซึ่งมิได้เป็นผู้บันทึกข้อมูล หรือไม่มีส่วนเกี่ยวข้องโดยไม่ได้รับอนุญาต หากต้องการแก้ไขข้อมูลให้แจ้งเหตุแก่ผู้ลงบันทึก ผู้ดูแลระบบ หรือผู้ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๕ ผู้ใช้งานห้ามทำการติดตั้งหรือใช้ Software อื่นใดโดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ (หากต้องการติดตั้งให้ลงบันทึกตามแบบฟอร์มขอติดตั้ง)

ข้อ ๖ ผู้ใช้เก็บไฟล์เอกสารหรืองานใดๆ บนหน้า Desktop, Document หรือ โฟลเดอร์ใดๆ ที่เก็บไว้ใน Drive เดียวกับระบบปฏิบัติการ (Drive C:\ ) ถ้ามีการเก็บไฟล์ใดๆไว้บน Drive ดังกล่าวทางผู้ดูแลระบบจะไม่รับผิดชอบในกรณีที่ไฟล์สูญหายหรือไม่สามารถใช้งานได้

ข้อ ๗ ห้ามผู้ใช้งานใช้คอมพิวเตอร์ที่ให้บริการผู้ป่วย เพื่อความบันเทิงขณะปฏิบัติงาน เช่น การดูหนัง ฟังเพลง เล่นเกม อันเป็นการรบกวนการปฏิบัติงาน

ข้อ ๘ ผู้ใช้งานคอมพิวเตอร์ห้ามเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์ออกจากจุดติดตั้งก่อนได้รับอนุญาตจากผู้ดูแลระบบ (แบบฟอร์มอนุญาต)

ข้อ ๙ ผู้ใช้งานห้ามเผยแพร่ข้อมูลผู้ป่วยแก่สาธารณและบุคคลที่ไม่เกียวข้อง ผ่านสื่อสังคมออนไลน์ (Social Media) เช่น Facebook, LINE, Website หรือ โปรแกรมอื่นๆ ที่เชื่อมต่อกับอินเตอร์เน็ต ยกเว้นเพื่อประสานงานตามแนวทางการรักษาผู้ป่วย เฉพาะผู้ที่เกี่ยวข้องหรือได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้ป่วย/ญาติซึ่งยินยอมเผยแพร่ได้เป็นครั้งคราว

ข้อ ๑๐ ผู้ใช้งานห้ามเปิดไฟล์ เอกสารแนบ หรือสื่อโฆษณา ทีส่งมาทาง Email, Facebook, Line, Link อื่นๆ หรือ สื่อ Social ต่างๆ ที่ไม่ทราบแหล่งที่มา และแจ้งงาน IT ทุกครั้งเมื่อพบความผิดปกติ

ข้อ ๑๑ ผู้ใช้งานต้องรับผิดชอบความเสียหาย ที่เกิดขึ้น กับคอมพิวเตอร์, เครื่องพิมพ์, ปลั๊กไฟ หรืออุปกรณ์อิเล็กทรอนิกส์อันเนื่องมากจากความประมาทของผู้ใช้งาน

นิยามคำศัพท์

คำศัพท์	ความหมาย
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร	ระบบสารสนเทศ ระบบฐานข้อมูล ระบบคอมพิวเตอร์ ระบบเครือข่ายระบบ Security ระบบงาน (ซอฟต์แวร์สำเร็จรูป ซอฟต์แวร์ประยุกต์) และระบบสื่อสารของสำนักงาน
เจ้าหน้าที่	ข้าราชการ พนักงานราชการ ลูกจ้าง ของโรงพยาบาลปางศิลาทอง
ผู้รับจ้างให้บริการจากภายนอก	เจ้าหน้าที่หน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน (Outsource) ที่มีการใช้งานหรือให้บริการเกี่ยวกับระบบสารสนเทศของ โรงพยาบาลปางศิลาทอง
หน่วยงาน	โรงพยาบาลปางศิลาทอง จังหวัดกำแพงเพชร รวมถึงหน่วยงานที่อยู่ภายใต้ สังกัด
หน่วยงานภายนอก	บริษัท/หน่วยงาน ที่โรงพยาบาลปางศิลาทอง ได้ว่าจ้างหรือมอบหมายให้ดำเนินการในเรื่อง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ ที่ปรึกษา ผู้รับจ้าง ผู้ขาย ผู้ให้บริการ หรือเป็นผู้ใช้บริการ และอื่นๆ ที่เกี่ยวข้อง รวมถึงหน่วยงานภายนอกอื่นที่มาขอใช้บริการ
ผู้ใช้งาน/ผู้ใช้บริการ	ข้าราชการ ลูกจ้าง พนักงานราชการ และพนักงานกระทรวงสาธารณสุข ผู้ดูแลระบบ ผู้บริหารองค์กร ผู้รับบริการ หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน
ผู้บริหาร	ผู้มีอำนาจในการบังคับบัญชาในหน่วยงาน ได้แก่ ผู้อำนวยการ/หัวหน้าหน่วยงาน หรือเทียบเท่า เป็นต้น
ผู้บริหารระดับสูงสุด	นายแพทย์สาธารณสุขจังหวัด ผู้อำนวยการโรงพยาบาล สาธารณสุขอำเภอ
สิทธิ์ของผู้ใช้งาน/สิทธิ์ของผู้ใช้บริการ	สิทธิ์ที่ใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลปางศิลาทอง
ผู้พัฒนาระบบ	เจ้าหน้าที่/หน่วยงานภายนอก ที่โรงพยาบาลปางศิลาทอง ได้ว่าจ้างหรือมอบหมายให้ ดำเนินการในเรื่องการพัฒนาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปางศิลาทอง
ผู้ดูแลระบบ	(System Administrator) หมายถึง ผู้ที่ได้รับมอบหมายจากหัวหน้าหน่วยงาน ให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
ISMS	ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management System)
ISMR	ผู้บริหารระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Management Representative : ISMR)

นิยามคำศัพท์

คำศัพท์	ความหมาย
IST	คณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Working Team : IST) ซึ่งมีองค์ประกอบดังนี้ - หัวหน้าคณะทำงานระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Manager: ISM) - เจ้าหน้าที่ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (Information Security Staff: ISS) - เจ้าหน้าที่ควบคุมเอกสาร (Document Controller: DC)
ทรัพย์สิน	ทรัพย์สินของโรงพยาบาลปางศิลาทอง ซึ่งแบ่งเป็น 5 ประเภท - ทรัพย์สินข้อมูล (Information and Document Asset) หมายถึง ฐานข้อมูล ไฟล์ข้อมูลเอกสารสัญญา/ข้อตกลง เอกสารระบบ (System Document) เอกสารคู่มือ ผู้ใช้งานเอกสารการอบรม เอกสารขั้นตอนการปฏิบัติงานด้านสารสนเทศแผนดำเนินงานเพื่อความต่อเนื่อง (Business Continuity Plans) หลักฐานการตรวจสอบ (Audit Trials) และข้อมูลArchived และอื่น ๆ - ทรัพย์สินซอฟต์แวร์ (Software Asset) หมายถึง โปรแกรมประยุกต์ (Application Software) ซอฟต์แวร์ระบบ (System Software) โปรแกรมอรรถประโยชน์ (Utilities) และเครื่องมือที่ใช้ในการพัฒนาและบริหารจัดการ (Development Tools) และอื่นๆ - ทรัพย์สินอุปกรณ์ (Hardware Asset) หมายถึง อุปกรณ์คอมพิวเตอร์ อุปกรณ์สื่อสาร สื่อจัดเก็บข้อมูล และ อุปกรณ์หรือเครื่องมืออื่น ๆ - ทรัพย์สินงานบริการ (Service Asset) หมายถึง ทรัพย์สินที่โรงพยาบาลปางศิลาทองใช้บริการ หรือให้บริการ เช่น การให้บริการอินเทอร์เน็ต การใช้ บริการ DR-Site และอื่นๆ - ทรัพย์สินบุคลากร (People Asset) หมายถึง เจ้าหน้าที่ดูแลระบบสารสนเทศ เจ้าหน้าที่ดูแลระบบเครือข่าย เจ้าหน้าที่ดูแลห้องศูนย์ปฏิบัติการ DC-Site เจ้าหน้าที่ธุรการ และอื่น ๆ

นิยามคำศัพท์

คำศัพท์	ความหมาย
ลำดับชั้นความลับของข้อมูล	ลำดับชั้นความลับของข้อมูลแบ่งออกเป็น 4 ชั้น ดังนี้ - ข้อมูลลับที่สุด (Top Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด - ข้อมูลลับมาก (Secret) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง - ข้อมูลลับ หรือ ใช้ภายใน (Internal Use) หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย - ข้อมูลทั่วไป หรือ สาธารณะ (Public) หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้
ใช้ภายใน (Internal Use)	ใช้ภายใน โรงพยาบาลปางศิลาทอง
การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งาน/ผู้ใช้บริการ เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
ความมั่นคงปลอดภัย ด้านสารสนเทศ	การธ รงไว้ซึ่งความลับ (Confidential) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ
เหตุการณ์ด้านความ มั่นคงปลอดภัย	เหตุการณที่ทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลปางศิลาทอง ขาดคุณสมบัติด้านความลับ(Confidential) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability) อาทิการปลอมแปลงหน้าเว็บไซต์ การเจาะระบบ การขมขู่ทางเว็บไซต์ การคุกคามทางเว็บไซต์ การรั่วไหลของข้อมูลการแพร่ระบาดของไวรัสและหนอนอินเทอร์เน็ต ระบบล่มไม่สามารถให้บริการได้ และการบุกรุกเครือขาย
สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคำดคิด	เป็นสถานการณ์ ซึ่งอาจทำให้ระบบของโรงพยาบาลปางศิลาทอง ถูกบุกรุก หรือโจมตี และ ระบบความมั่นคงปลอดภัยถูกคุกคาม

หมวดที่ ๑ นโยบายความมั่นคงปลอดภัย (Security Policy)

๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)

วัตถุประสงค์

๑. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานสารสนเทศของ โรงพยาบาลปางศิลาทอง ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในหน่วยงานสังกัดโรงพยาบาลปางศิลาทองได้รับทราบถือปฏิบัติ ตามนโยบายอย่างเคร่งครัด

๓. เพื่อ กำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับสังกัดโรงพยาบาลปางศิลาทอง ตระหนักถึงความ สำคัญของการรักษาความมั่นคงในการใช้ งานด้านสารสนเทศของสังกัดโรงพยาบาลปางศิลาทองและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการ ทบทวนนโยบายปีละ ๑ ครั้ง

นโยบาย

๑.๑.๑ จัดทำนโยบายความมั่นคงปลอดภัยเป็นลายลักษณ์อักษร (Information Security Policy Document)

๑) ต้องจัดทำนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศเป็นลายลักษณ์อักษร เพื่อให้เกิดความเชื่อมั่น และมีความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยนโยบายดังกล่าวจะต้องได้รับ การอนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ในการนำไปใช้

๒) กำหนดให้มีการเผยแพร่เอกสารนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศให้กับเจ้าหน้าที่และผู้ที่เกี่ยวข้องในขอบเขตรับทราบ

๑.๑.๒ ทำการทบทวนนโยบายความมั่นคงปลอดภัย (Review of the Information Security Policy)

๑) ต้องดำเนินการตรวจสอบ ทบทวน และประเมินนโยบายระบบบริหารความมั่นคงปลอดภัยสารสนเทศตามระยะเวลาที่กำหนดไว้ หรืออย่างน้อย ๑ ครั้งต่อปี

หมวดที่ ๒ โครงสร้างทางด้านความมั่นคงปลอดภัยสารสนเทศ (Organizational of Information Security)

๒.๑ โครงสร้างภายในด้านความมั่นคงปลอดภัยสารสนเทศ (Internal Organization)

วัตถุประสงค์: เพื่อให้มีการกำหนดกรอบการบริหารและจัดการความมั่นคงปลอดภัยสำหรับสารสนเทศของ โรงพยาบาลปางศิลาทอง ตั้งแต่การเริ่มต้นและการควบคุมการปฏิบัติงานเพื่อให้มีความมั่นคงปลอดภัย

นโยบาย

๒.๑.๑ บทบาทและหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Roles and Responsibilities)

๑) ISMR ต้องกำหนดหน้าที่ความรับผิดชอบของเจ้าหน้าที่ ในการดำเนินงานทางด้านความมั่นคง ปลอดภัยสำหรับสารสนเทศของ โรงพยาบาลปางศิลาทอง ไว้อย่างชัดเจน

๒) ผู้บริหาร โรงพยาบาลปางศิลาทอง ต้องแต่งตั้งคณะ หรือกลุ่มผู้ทำงานหลัก ตลอดจนทรัพยากรที่จำเป็น เพื่อบริหาร และจัดการ
ความมั่นคงปลอดภัยสำหรับสารสนเทศของโรงพยาบาลปางศิลาทอง

๓) บทบาทหน้าที่แบ่งได้ดังนี้

๓.๑) ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

- ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO) ของหน่วยงาน
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือเทียบเท่าระดับผู้อำนวยการ

ความรับผิดชอบ

๓.๑.๑ รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ

๓.๑.๒ รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบ คอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒) ระดับบริหาร ผู้รับผิดชอบ ได้แก่ หัวหน้ากลุ่ม/หัวหน้าฝ่าย หรือเทียบเท่า

ความรับผิดชอบ

๓.๒.๑ รับผิดชอบ กำกับ ดูแลการปฏิบัติงานของผู้ปฏิบัติ ตลอดจนศึกษา ทบทวน วางแผน ติดตามการบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๓.๒.๒ รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย ระบบสารสนเทศและระบบฐานข้อมูล

๓.๓) ระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้ที่ได้รับมอบหมายให้ปฏิบัติหน้าที่จากหัวหน้าส่วนราชการ เช่น นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่เครื่องคอมพิวเตอร์มีหน้าที่

- ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของ ฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ
- รับผิดชอบควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่าย ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย
- ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด
- ป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต
- รับผิดชอบในการรักษาความปลอดภัย ระบบอินเทอร์เน็ต
- ปฏิบัติงานอื่น ๆ ตามที่ได้รับมอบหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของ โรงพยาบาลปางศิลาทอง

๒.๑.๒ การแบ่งแยกหน้าที่ความรับผิดชอบ (Segregation of duties)

ผู้บริหาร โรงพยาบาลปางศิลาทอง ต้องแบ่งหน้าที่และกำหนดความรับผิดชอบที่ชัดเจนในการปฏิบัติงาน เพื่อลดโอกาสที่จะทำให้มีการเปลี่ยนแปลงทรัพย์สินของ โรงพยาบาลปางศิลาทอง หรือมีการใช้ทรัพย์สินผิดวัตถุประสงค์ โดยไม่ได้รับ อนุญาตหรือโดยไม่ได้เจตนาก็ตาม

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 ในอุตสาหกรรมที่ โรงพยาบาลปางศิลาทอง มีส่วน ร่วม และเอกสารกำหนดรายชื่อ และข้อมูลสำหรับการติดต่อ จำเป็นจะต้องกำหนดให้มีการระบุวันที่จัดทำเอกสาร

๒.๑.๕ การบริหารจัดการโครงการเพื่อให้มีความมั่นคงปลอดภัย (Information Security in Project Management)

๑) ต้องมีการกำหนดระเบียบ ข้อบังคับ กฎเกณฑ์ต่าง ๆ เกี่ยวกับการดำเนินงานและการเข้าถึงข้อมูลเพื่อให้งานโครงการมีความมั่นคงปลอดภัย เช่น การกำหนดสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน ให้ดำเนินการตามระเบียบปฏิบัติ เรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑)

๒) กรณีโครงการที่จ้างบริษัทภายนอก โครงการที่หน่วยงานภายนอกดำเนินการให้ และโครงการที่โรงพยาบาลปางศิลาทองจัดทำเองต้องดำเนินการตามระเบียบทางราชการที่เกี่ยวข้อง

๒.๒ อุปกรณ์คอมพิวเตอร์แบบพกพาและการปฏิบัติงานจากภายนอก (Mobile Devices and Teleworking)

วัตถุประสงค์: เพื่อรักษาความมั่นคงปลอดภัยสำหรับสารสนเทศของการปฏิบัติการระยะไกลหรือการปฏิบัติงานจากภายนอกและการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา

นโยบาย

๒.๒.๑ นโยบายสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์แบบพกพา (Mobile device policy)

ต้องมีการกำหนดและปฏิบัติตามนโยบายหรือมาตรการสนับสนุนสำหรับการใช้งานของอุปกรณ์คอมพิวเตอร์แบบพกพา (Notebook, Tablet, Smartphone และอุปกรณ์สื่อสารเคลื่อนที่อื่นๆ) ที่มีการนำมาใช้งาน เพื่อบริหารจัดการความเสี่ยงที่มีต่ออุปกรณ์ดังกล่าว และควรคำนึงถึงความเสียงของการทำงานในสภาพแวดล้อมที่ไม่ได้รับการป้องกันโดยให้ดำเนินการตามระเบียบปฏิบัติ เรื่อง การใช้เครื่องคอมพิวเตอร์ประเภทพกพาในการปฏิบัติงานนอกสถานที่ (Mobile Computing and Communications) (P-IT-MO-๐๑)

๒.๒.๒ การปฏิบัติงานจากระยะไกล (Teleworking)

๑) ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

๒) ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ ให้กับผู้ใช้งานจากระยะไกล

๓) ผู้ใช้งานจากระยะไกลทุกคน ต้องผ่านการพิสูจน์ตัวตนก่อนการใช้งาน เพื่อเพิ่มความปลอดภัย เช่น รหัสผ่านหรือวิธีการเข้ารหัส เป็นต้น

๔) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล หากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๕) ต้องกำหนดชนิดของงาน ชั่วโมงการทำงาน ชั้นความลับของข้อมูล ระบบงานและบริการต่างๆ ของ หน่วยงานที่อนุญาตและไม่อนุญาตให้ปฏิบัติงานจากระยะไกล

๖) ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติ การขอยกเลิก การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึง ระบบสารสนเทศและการคืนอุปกรณ์ที่ใช้ปฏิบัติงานจากระยะไกล

หมวดที่ ๓ การรักษาความปลอดภัยด้านทรัพยากรมนุษย์ (Human resource security)

๓.๑ การจัดหาบุคลากรก่อนการจ้างงาน (Prior to Employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างเข้าใจในหน้าที่ความรับผิดชอบของตนเองและมีความเหมาะสมตามบทบาทหน้าที่ที่ได้รับพิจารณาจ้างงาน โรงพยาบาลปางศิลาทอง

นโยบาย

๓.๑.๑ การสรรหาบุคลากร (Screening)

๑) เจ้าหน้าที่กลุ่มบริหารงานบุคคล ต้องทำการตรวจสอบคุณสมบัติของผู้สมัครงานทุกคนก่อนที่จะบรรจุเป็นเจ้าหน้าที่ เจ้าหน้าที่ชั่วคราวหรือนักศึกษาฝึกงาน โดยต้องไม่มีประวัติในการบุกรุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลในระบบเทคโนโลยีสารสนเทศของหน่วยงานใดมาก่อน

๒) เจ้าหน้าที่ประสานงานกลุ่มบริหารงานบุคคล ต้องจัดให้มีการลงนามในสัญญาระหว่าง

- ๒.๑ “เจ้าหน้าที่” และหน่วยงาน ลงนามในหนังสือยอมรับเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use Policy: AUP) (F-IT-AC-๐๒.๐๑) และบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non Disclosure Agreement: NDA) (F-IT-HR-๐๑.๐๑) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว
- ๒.๒ “ผู้รับจ้างให้บริการจากภายนอก” และหน่วยงาน ลงนามในหนังสือยอมรับเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use Policy: AUP) (F-IT-AC-๐๒.๐๑) และบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non Disclosure Agreement: NDA) (F-IT-HR-๐๑.๐๑) โดยการลงนามนี้จะเป็นส่วนหนึ่งของการว่าจ้างเจ้าหน้าที่นั้น ๆ ทั้งนี้ต้องมีผลผูกพันทั้งในขณะที่ทำงานและผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากที่สิ้นสุดการว่าจ้างแล้ว

๓) ปฏิบัติตามระเบียบปฏิบัติ เรื่อง : การบริหารจัดการทรัพยากรบุคคลด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ (Human resources security) (P-IT-HR-๐๑)

๔) ในการสรรหาบุคลากรนอกจากความเหมาะสมตามตำแหน่งแล้ว ต้องมีการตรวจสอบสารเสพติดในร่างการก่อนรับเข้าทำงาน โดยผู้สมัครเพื่อเข้ารับตำแหน่ง จะต้องมีเอกสารการรับรองจากแพทย์แนบมาพร้อมเอกสารในการสมัคร

๓.๑.๒ ข้อกำหนดและเงื่อนไขของการจ้างงาน (Terms and conditions of employment)

๑) เจ้าหน้าที่ประสานงานกลุ่มบริหารงานบุคคล ต้องกำหนดเงื่อนไขการจ้างงานที่รวมถึงหน้าที่ความรับผิดชอบทางด้านความมั่นคงปลอดภัยทางด้านสารสนเทศ โดยเจ้าหน้าที่กลุ่มบริหารงานบุคคล ต้องแจ้งให้โรงพยาบาลปางศิลาทองทราบทันที เมื่อมีเหตุดังนี้

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

๓.๒ การสร้างความความมั่นคงปลอดภัยขณะเป็นเจ้าหน้าที่ (During employment)

วัตถุประสงค์: เพื่อให้พนักงานและผู้ที่ทำสัญญาจ้างตระหนักและปฏิบัติตามหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศของ โรงพยาบาลปางศิลาทอง

นโยบาย

๓.๒.๑ หน้าที่ความรับผิดชอบของผู้บริหาร (Management responsibilities)

ISMR ต้องกำหนดให้เจ้าหน้าที่ พนักงานข้าราชการ และผู้รับจ้างให้บริการจากภายนอกรับทราบและปฏิบัติตามนโยบาย กฎ ระเบียบและขั้นตอนการทำงานที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศของ โรงพยาบาลปางศิลาทอง ด้วย

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

๑) เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง ผู้รับจ้างขององค์กรทุกคนต้องได้รับการอบรมให้ความรู้ โดยเนื้อหาที่แต่ละบุคคลจะได้รับการฝึกอบรมต้องเหมาะสมกับบทบาทหน้าที่ในการปฏิบัติงานของแต่ละบุคคล เพื่อเป็นการสร้างความตระหนัก และฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศ

๒) ต้องจัดอบรมให้ความรู้แก่เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง เกี่ยวกับความตระหนักและวิธีปฏิบัติเพื่อสร้างความ มั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งรวมถึงการแจ้งให้ทราบเกี่ยวกับนโยบายความมั่นคง ปลอดภัยและการเปลี่ยนแปลงที่เกิดขึ้นด้านเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลปางศิลาทองด้วย

๓) เจ้าหน้าที่ของ โรงพยาบาลปางศิลาทอง ใหม่ทุกคน ต้องได้รับการอบรมเกี่ยวกับนโยบายการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และระเบียบปฏิบัติที่เกี่ยวข้องกับหน่วยงานก่อนหรืออย่างน้อยภายใน ๙๐ วันนับจากเข้าทำงานในหน่วยงาน โดยควรเป็นส่วนหนึ่งของการปฐมนิเทศ และต้องมีการลงนามและเก็บรวบรวมไว้ในแฟ้มประวัติของบุคลากรด้วย

๔) เจ้าหน้าที่ประสานงานกลุ่มบริหารงานบุคคล และ ISM มีหน้าที่ในการแจ้งให้ทราบเกี่ยวกับนโยบายความ มั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และการเปลี่ยนแปลงที่เกิดขึ้นทางด้านความมั่นคงปลอดภัยระบบ เทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลปางศิลาทอง ให้แก่บุคลากรด้วย

๓.๒.๓ กระบวนการทางวินัย (Disciplinary Process)

ผู้บริหาร โรงพยาบาลปางศิลาทอง ต้องกำหนดบทลงโทษทางวินัยสำหรับผู้ที่ฝ่าฝืนนโยบาย กฎ และ/หรือระเบียบปฏิบัติของราชการและ โรงพยาบาลปางศิลาทอง แต่หากเป็นการละเมิดข้อกฎหมาย บทลงโทษจะเป็นไปตามฐานความผิดที่ได้ กระทำตามที่ระบุในแต่
ละข้อกฎหมายนั้น ๆ

๓.๓ การสิ้นสุดหรือการเปลี่ยนการจ้างงาน (Termination and change of employment)

วัตถุประสงค์: เพื่อป้องกันผลประโยชน์ขององค์กรซึ่งเป็นส่วนหนึ่งของการเปลี่ยนหน้าที่ หรือสิ้นสุดการจ้างงาน

นโยบาย

๓.๓.๑ การสิ้นสุดหรือการเปลี่ยนหน้าที่ความรับผิดชอบของการจ้างงาน
(Termination or Change of Employment Responsibilities)

๑) ต้องมีการกำหนดและสื่อสารให้พนักงานหรือผู้ทำสัญญาได้รับทราบ รวมทั้งมีการควบคุมให้ปฏิบัติตามข้อกำหนดในสัญญา

๒) เจ้าหน้าที่กลุ่มบริหารงานบุคคลมีหน้าที่ดูแลหากมีการแต่งตั้งโยกย้าย ปลดหรือเปลี่ยนแปลงตำแหน่งใด ๆ ที่เกี่ยวข้องกับความรับผิดชอบใน โรงพยาบาลปางศิลาทอง

๓) เจ้าหน้าที่ผู้เกี่ยวข้องเมื่อได้รับเรื่องของผู้ใช้งานที่สิ้นสุดสภาพการจ้างงานหรือเปลี่ยนหน้าที่ความรับผิดชอบจากกลุ่มบริหารงานบุคคล ให้ปฏิบัติตามระเบียบปฏิบัติ เรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑) เพื่อดำเนินการเพิกถอนสิทธิ์หรือเปลี่ยนแปลงสิทธิ์

หมวดที่ ๔ การบริหารจัดการทรัพย์สิน (Asset Management)

๔.๑ การความรับผิดชอบต่อทรัพย์สิน (Responsibility for Assets)

วัตถุประสงค์: **เพื่อให้ทรัพย์สินของ โรงพยาบาลปางศิลาทอง ได้รับการป้องกันและปกป้องอย่างเหมาะสม**

นโยบาย

๔.๑.๑ ทะเบียนทรัพย์สิน (Inventory of assets)

๑) ต้องจัดทำและเก็บทะเบียนทรัพย์สิน ซึ่งรวมถึงทรัพย์สินข้อมูล และเอกสาร (Information and Document Asset) ทรัพย์สินซอฟต์แวร์ (Software Asset) ทรัพย์สินอุปกรณ์ (Hardware Asset) ทรัพย์สินงานบริการ (Service Asset) และบุคลากร (People Asset) เพื่อเป็นข้อมูลเบื้องต้นสำหรับการนำไปวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงที่มีต่อทรัพย์สินอย่างเหมาะสม รวมถึงเป็นการควบคุมและจัดการทรัพย์สินของ โรงพยาบาลปางศิลาทอง โดยปฏิบัติตามเอกสาร ระเบียบปฏิบัติ เรื่อง การบริหารจัดการทรัพย์สินสารสนเทศของ โรงพยาบาลปางศิลาทอง
(Asset Management) (P-IT-AM-๐๑)

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

๓) ต้องประเมินความเสี่ยงตามแนวทางการจัดการความเสี่ยงของทรัพย์สิน เมื่อมีทรัพย์สินใหม่ หรือทรัพย์สินที่ มีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

๔.๑.๒ ความเป็นเจ้าของทรัพย์สิน (Ownership for Assets)

จะต้องกำหนดบุคคล หรือหน่วยงานผู้รับผิดชอบข้อมูลและทรัพย์สินทั้งหมดด้านเทคโนโลยีสารสนเทศและการสื่อสารของ โรงพยาบาลปางศิลาทอง อย่างชัดเจน

๔.๑.๓ การอนุญาตให้ใช้ทรัพย์สิน (Acceptable Use for Assets)

๑) จะต้องกำหนด แสดง บันทึกเป็นเอกสาร และกฎการอนุญาตให้ใช้ข้อมูลและทรัพย์สินอย่างเหมาะสม

๒) การอนุญาตให้ใช้งานทรัพย์สินด้านอุปกรณ์คอมพิวเตอร์มีดังนี้

- ระบบเทคโนโลยีสารสนเทศและอุปกรณ์การประมวลผลข้อมูลที่เกี่ยวข้องทั้งหมดที่ โรงพยาบาลปางศิลาทอง เป็นผู้จัดหามานั้น มีวัตถุประสงค์เพื่อให้ใช้ในการดำเนินงานของ โรงพยาบาลปางศิลาทอง การใช้งานระบบและอุปกรณ์ต่างเพื่อกิจ ธุระส่วนตัวนั้นอนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม ซึ่งจะต้องไม่รบกวนหรือเป็น อุปสรรคต่อการ ทำงานตามหน้าที่ความรับผิดชอบของเจ้าหน้าที่
- เจ้าหน้าที่ ตลอดจนหน่วยงานภายนอก ที่ได้รับการว่าจ้างโดย โรงพยาบาลปางศิลาทอง จะต้องมีความรับผิดชอบ ต่ออุปกรณ์คอมพิวเตอร์ที่ได้มอบไว้ให้ใช้งาน รวมทั้งสอดส่องดูแลทรัพยากรเหล่านี้ให้มีความปลอดภัย และคงความถูกต้อง โดยหมายรวมถึงข้อมูล และระบบสารสนเทศของโรงพยาบาลปางศิลาทอง

- ผู้ใช้งานต้องรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ และอุปกรณ์ต่าง ๆ ของโรงพยาบาลปางศิลาทอง อย่าง ระมัดระวัง และ ให้การปกป้องเสมือนเป็นทรัพย์สินของตน

- เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์พกพาทั้งหมดของโรงพยาบาลปางศิลาทอง ต้องได้รับการปกป้องด้วยรหัสผ่านของระบบปฏิบัติการทุกครั้งเมื่อต้องการเข้าใช้งาน และต้องได้รับการปกป้อง อัตโนมัติโดยรหัสผ่านของ Screen Saver หรือทำการ Log Off อุปกรณ์ทุกครั้งเมื่อไม่ได้ใช้งานอุปกรณ์โดยระยะเวลาว่างเว้นจากการใช้งานแล้วต้องทำการ Log Off ต้องไม่เกิน ๑๕ นาที

- ผู้ใช้งานต้องไม่ติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ลงในเครื่องคอมพิวเตอร์ของ โรงพยาบาลปางศิลาทอง

- เครื่องคอมพิวเตอร์พกพาที่มีการเก็บข้อมูลลับไว้ ต้องได้รับการปกป้องเทียบเท่ากับเครื่องคอมพิวเตอร์ที่ใช้งานอยู่ภายใน โรงพยาบาลปางศิลาทอง อาทิ การติดตั้งซอฟต์แวร์ป้องกันไวรัส ซอฟต์แวร์ป้องกันสปายแวร์ และมีการปรับปรุง Security Patch อยู่เสมอ ฯลฯ ทั้งนี้ ผู้ใช้งานต้องทำการปกป้องอุปกรณ์และข้อมูลในอุปกรณ์ตามคำแนะนำที่ระบุไว้ใน เอกสารขั้นตอนการปฏิบัติงาน เรื่องการใช้เครื่องคอมพิวเตอร์ประเภทพกพาในการปฏิบัติงานนอกสถานที่ (Mobile Computing and Communications) (P-IT-MO-๐๑)

- อุปกรณ์คอมพิวเตอร์ของ โรงพยาบาลปางศิลาทอง ต้องไม่ถูกดัดแปลง หรือติดตั้งอุปกรณ์เพิ่มเติมใดๆ ก่อนได้รับ อนุญาตจากผู้บริหารของส่วนงานนั้น ๆ และเจ้าหน้าที่ต้องไม่อนุญาตให้ผู้ไม่มีหน้าที่เกี่ยวข้องทำการติดตั้งฮาร์ดแวร์หรือ ซอฟต์แวร์ใด ๆ บนเครื่องคอมพิวเตอร์ของ โรงพยาบาลปางศิลาทอง อย่างเด็ดขาด

๓) การอนุญาตให้ใช้งานทรัพย์สินด้านซอฟต์แวร์มีดังนี้

- ห้ามเจ้าหน้าที่ ทำการติดตั้งหรือเผยแพร่ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์บนระบบคอมพิวเตอร์ของ โรงพยาบาลปางศิลาทอง

- ซอฟต์แวร์ที่นำมาใช้ในการประมวลผลและจัดเก็บข้อมูลลับหรือข้อมูลสำคัญของ โรงพยาบาลปางศิลาทอง ทั้งที่ได้มาจากการพัฒนาขึ้นโดยเจ้าหน้าที่ หรือที่ได้รับการจัดซื้อมา ต้องได้รับการตรวจสอบ ควบคุม และอนุมัติอย่างเหมาะสม โดยหน่วยงานเจ้าของระบบหรือข้อมูล ก่อนนำมาติดตั้งใช้งานบนระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลปางศิลาทอง

- ระบบสารสนเทศทั้งหมดที่ถูกใช้งานโดยผู้ใช้งานทั่วไป ต้องมีเอกสารสนับสนุนการใช้งานอย่างเพียงพอผู้ใช้งานทั่วไปของ โรงพยาบาลปางศิลาทอง มีความเข้าใจและสามารถใช้งานระบบสารสนเทศได้

- รายชื่อซอฟต์แวร์ หรือระบบสารสนเทศ ที่ถูกติดตั้งในเครื่องคอมพิวเตอร์ของผู้ใช้งานต้องได้รับการจัดทำเป็นเอกสาร และได้รับการอนุมัติโดยผู้บริหารของสายงานเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าซอฟต์แวร์เหล่านี้มีลิขสิทธิ์ถูกต้องครบถ้วน และได้รับการติดตั้งเพื่อวัตถุประสงค์ในการทำงานของ โรงพยาบาลปางศิลาทองเท่านั้น

๔) การอนุญาตให้ใช้งานอินเทอร์เน็ตมีดังนี้

- โรงพยาบาลปางศิลาทอง จัดหาบริการอินเทอร์เน็ตไว้เพื่อสนับสนุนการดำเนินงาน และอำนวยความสะดวกแก่เจ้าหน้าที่ในทำวิจัยการค้นหาข้อมูลความรู้และการติดต่อสื่อสารกับบุคคลภายนอกเพื่อเพิ่มประสิทธิภาพในการทำงานและการให้บริการของ โรงพยาบาลปางศิลาทอง

- ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้โรงพยาบาลปางศิลาทองและ การใช้งานบุคคลผู้ที่เกี่ยวข้องกับโรงพยาบาลปางศิลาทอง เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้ อินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

- การเข้าใช้งานอินเทอร์เน็ตต้องเข้าใช้งานผ่าน Gateway ที่ได้รับอนุญาต หรือผ่านเครื่องคอมพิวเตอร์ลูกข่ายที่ได้รับการจัดเตรียมเพื่อใช้งานเฉพาะกิจเท่านั้น ทั้งนี้โรงพยาบาลปางศิลาทอง ขอสงวนสิทธิ์ในการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งาน เพื่อตรวจสอบการใช้งานในลักษณะที่ไม่เหมาะสม

- ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป็อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

- ห้ามผู้ใช้งานเข้าชม ดาวน์โหลด หรือทำ ซ้ำสื่อลามกอนาจาร และสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

- โรงพยาบาลปางศิลาทอง ไม่สนับสนุนการแสดงความคิดเห็นส่วนตัวในรูปแบบอิเล็กทรอนิกส์ (เช่นผ่านทางเว็บบอร์ด) ของเจ้าหน้าที่ ทั้งนี้ความเสียหายใดๆ ที่อาจเกิดขึ้นจากการแสดงความคิดเห็นดังกล่าว ถือเป็นความรับผิดชอบของ เจ้าหน้าที่ผู้นั้น

๕) การอนุญาตให้ใช้งานอีเมลมีดังนี้

- ผู้ใช้งานอีเมลทั้งหมดของโรงพยาบาลปางศิลาทอง ต้องมี E-mail Account เป็นของตนเอง
- E-mail Account ต้องได้รับการปกป้องด้วยรหัสผ่าน เพื่อป้องกันการถูกล่วงละเมิดและการนำอีเมลไปใช้ในทางที่ผิด
- E-mail Account ที่มีวัตถุประสงค์พิเศษ เช่น ict-moph@health.moph.go.th อาจได้รับการสร้างขึ้นเพื่อเป็น E-mail Account กลางของส่วนงาน และ/หรือ เพื่อใช้งานร่วมกันโดยผู้ใช้งานมากกว่าหนึ่งคนขึ้นไปโดยต้องมีผู้ใช้งานหนึ่งคนที่ได้รับการแต่งตั้งให้ทำหน้าที่เป็นเจ้าของ E-mail Account นั้น
- E-mail Account ทั้งหมด และอีเมลทุกฉบับ (รวมถึงอีเมลส่วนตัว) ที่ถูกสร้าง และเก็บรักษาอยู่บนระบบคอมพิวเตอร์ หรือระบบเครือข่ายของโรงพยาบาลปางศิลาทอง ถือเป็นทรัพย์สินของ โรงพยาบาลปางศิลาทอง
- ผู้ใช้งานต้องใช้งานซอฟต์แวร์ที่ได้รับอนุญาตเท่านั้นในการเข้าถึง และ/หรือ ติดต่อสื่อสารกับระบบอีเมลของ โรงพยาบาลปางศิลาทอง
- พื้นที่เก็บอีเมลบนเครื่องคอมพิวเตอร์แม่ข่ายส่วนกลาง (Mailbox Size) ของผู้ใช้งานมีขนาดที่จำกัด ทั้งนี้เมื่อปริมาณของอีเมลมากจนใกล้เคียงกับขนาดพื้นที่ที่ตั้งค่าไว้ ผู้ใช้งานจะได้รับข้อความแจ้งเตือนจากระบบและถ้าหากปริมาณของอีเมลมากเกินกว่าพื้นที่จัดเก็บแล้ว ผู้ใช้งานจะไม่สามารถรับ-ส่งอีเมลได้ตามปกติอีกต่อไป
- ขนาดของอีเมลและไฟล์แนบได้รับการจำกัดไว้ โดยหากอีเมลและไฟล์แนบมีขนาดใหญ่เกินกว่าที่กำหนด ผู้ใช้งานจะได้รับจดหมายตีกลับแจ้งว่าไม่สามารถส่งอีเมลดังกล่าวได้
- ผู้ใช้งานต้องลบอีเมลที่ไม่จำเป็นออกจาก Mailbox ของตนอยู่เสมอ เพื่อเป็นการรักษาพื้นที่เก็บอีเมลให้ เป็นไปตามขนาดที่โรงพยาบาลปางศิลาทอง กำหนด ทั้งนี้ผู้ใช้งานต้องเก็บรักษาอีเมลที่เกี่ยวข้องกับการทำงาน และอีเมลตามที่กฎหมายกำหนดไว้เท่านั้น
- ห้ามใช้ E-mail Account ของโรงพยาบาลปางศิลาทอง เพื่อกระทำการใดๆ ที่เกี่ยวข้องกับสิ่งผิดกฎหมาย ตัวอย่างเช่น เพื่อการโฆษณายาสูบ สิ่งมึนเมา สินค้าหนีภาษี การเผยแพร่ซอฟต์แวร์ละเมิดลิขสิทธิ์ เป็นต้น
- ห้ามผู้ใช้งานทำสาเนาข้อความ หรือทำสาเนาไฟล์แนบที่เป็นข้อมูลลับจากอีเมลของบุคคลอื่นก่อนได้รับอนุญาตจากเจ้าของข้อมูล
- ผู้ใช้งานต้องร่างเนื้อหาของอีเมลด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งออกอีเมลนั้นในนามตัวแทนของ โรงพยาบาลปางศิลาทอง
- ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมล หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

- ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมลพร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการ ลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล

-ผู้ใช้งานต้องทำการส่งอีเมลให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมลฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

- ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมลขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น

- ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่ง อีเมลหลอกลวง หรือการส่งอีเมลในลักษณะลูกโซ่โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมลที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

- ห้ามผู้ใช้งานส่งอีเมลที่มีไฟล์แนบเกี่ยวกับการพนัน ภาพลามกอนาจาร หรือไฟล์อื่นใดที่ไม่เกี่ยวข้องกับการทำงานและส่งผลเสียต่อ โรงพยาบาลปางศิลาทอง

- ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีไวรัส อีเมลบอมบ์ หรือโปรแกรมแฝง (โทรจัน)

กรณีที่เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ไม่ปฏิบัติตามที่โรงพยาบาลปางศิลาทองกำหนด

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

๔.๑.๔ การคืนทรัพย์สิน (Return on Assets)

เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ซึ่งพ้นสภาพจากการจ้างงานต้องคืนทรัพย์สินทั้งหมดซึ่งเกี่ยวข้องกับระบบงานคอมพิวเตอร์
รวมทั้งกุญแจ บัตรประจำตัวเจ้าหน้าที่ บัตรผ่านเข้า-ออก คอมพิวเตอร์และอุปกรณ์ต่อพ่วง คู่มือ และเอกสารต่างๆ ให้แก่ผู้บังคับบัญชาก่อนวันสุดท้ายของการว่าจ้างงาน โดยปฏิบัติตามระเบียบปฏิบัติ เรื่องการส่งคืนทรัพย์สิน (Return of assets) (P-IT-HR-๐๒)

๔.๒ การจัดหมวดหมู่ข้อมูลและทรัพย์สินสารสนเทศ (Information Classification)

วัตถุประสงค์: เพื่อทำให้แน่ใจว่าสารสนเทศของโรงพยาบาลปางศิลาทอง ได้รับการปกป้องในระดับที่

เหมาะสม **นโยบาย**

๔.๒.๑ การกำหนดชั้นความลับของสารสนเทศ (Classification of Information)

๑) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัย ของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เป็นข้อมูลที่เกี่ยวข้องกับข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี
- ข้อมูลสารสนเทศด้านการแพทย์และการสาธารณสุข สาธารณสุข เป็นข้อมูลที่เกี่ยวข้องกับการรักษาผู้ปุวย ประวัติผู้ปุวย ข้อมูลทางการแพทย์และข้อมูลสถานพยาบาล

๑.๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลทีมีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๑.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

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

๑.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่ที่และลำดับชั้นในบังคับบัญชาในหน่วยงานนั้น
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้หรือได้ทำการเผยแพร่สำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย เข้าถึงข้อมูลหรือระบบได้โดยสิทธิ์ที่ได้รับหมอบหมายตามอำนาจหน้าที่

๑.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์ ให้ถือตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง หลักเกณฑ์และวิธีการในการจัดทำหรือแปลงเอกสารและข้อความให้อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓

๔.๒.๒ การจัดทำป้ายชื่อ ของข้อมูล (Labeling of Information)

๑) ต้องจัดให้มีวิธีการจัดทำและจัดการป้ายชื่อสำหรับปิดฉลากเอกสารข้อมูลและอุปกรณ์ทรัพย์สินสารสนเทศที่เกี่ยวข้องกับการบริหารด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒) ข้อมูลที่อยู่ในรูปแบบของเอกสาร ที่ถูกจัดทำขึ้นจะต้องมีการควบคุมและรักษาความปลอดภัยอย่างเหมาะสมตั้งแต่การเริ่มพิมพ์ การจัดทำป้ายชื่อ การเก็บรักษา การทำสาเนา การแจกจ่าย จนถึงการทำลาย และกำหนดเป็นระเบียบปฏิบัติให้เจ้าหน้าที่ ต้องปฏิบัติตามเพื่อให้มั่นใจว่าข้อมูลได้รับการควบคุมและรักษาความปลอดภัย

๔.๒.๓ การจัดการทรัพย์สิน (Handling of Asset)

๑) ข้อมูลลับต้องไม่ถูกเปิดเผยกับผู้อื่น เว้นแต่มีความจำเป็นในการปฏิบัติงานเท่านั้น

๒) ผู้ใช้งานต้องตระหนักถึงการรักษาข้อมูลที่ถูกเก็บไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้งาน โดยเฉพาะอย่างยิ่ง เครื่องคอมพิวเตอร์ที่มีการใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ข้อมูลลับเหล่านี้ต้องได้รับการปกป้องโดยการเข้ารหัส หรือโดยวิธีการอื่นใดของระบบปฏิบัติการ หรือระบบสารสนเทศอย่างเหมาะสม

๓) ผู้ใช้งานต้องเก็บรักษาเอกสารลับและสื่อบันทึกข้อมูลที่มีข้อมูลลับในตู้ที่สามารถปิดล็อคได้เมื่อไม่ได้ใช้งาน โดยเฉพาะอย่างยิ่งเมื่ออยู่นอกเวลาทำการ หรือเมื่อต้องทิ้งเอกสารหรือสื่อนั้นไว้โดยไม่อยู่ที่โต๊ะทำงาน

๔) ข้อมูลลับต้องถูกเก็บออกจากอุปกรณ์ประมวลผลต่าง ๆ เช่น เครื่องพิมพ์ เครื่องโทรสาร เครื่องถ่ายเอกสาร ฯลฯ โดยทันที

๕) เจ้าหน้าที่ต้องไม่เปิดเผยข้อมูลลับต่อบุคคลภายนอก ยกเว้นในกรณีที่การเปิดเผยนั้นครอบคลุมโดยข้อตกลงการไม่เปิดเผยข้อมูล

๖) เจ้าหน้าที่ต้องไม่พูดคุยหรือใช้งานข้อมูลลับของโรงพยาบาลปางศิลาทอง ในพื้นที่สาธารณะ เช่น ทางเดิน ร้านอาหาร ฯลฯ

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

๔.๓ การจัดการสื่อที่ใช้ในการบันทึกข้อมูลให้มความมั่นคงปลอดภัย (Media Handing)

วัตถุประสงค์: เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับสื่อที่ใช้ในการบันทึกข้อมูลของโรงพยาบาลปางศิลาทอง โดยการถูก เปิดเผยโดยไม่ได้รับอนุญาต การเปลี่ยนแปลง การขนย้าย การลบ หรือการทำลายข้อมูล

นโยบาย

๔.๓.๑ การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ (Management of Removable Media)

๑) การบริหารจัดการสำหรับสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องมีการจัดทำขั้นตอนสำหรับบริหารจัดการสื่อบันทึกข้อมูล โดยต้องมีความสอดคล้องกับวิธีหรือขั้นตอนการจัดชั้นความลับของสารสนเทศที่องค์กรกำหนดไว้ สื่อบันทึกข้อมูลที่มีข้อมูลต้องมีการป้องกันข้อมูลจากการถูกเข้าถึงโดยไม่ได้รับอนุญาต การนำไปใช้ผิดวัตถุประสงค์หรือความเสียหายในระหว่างนี้ที่นำส่งหรือขนย้ายสื่อบันทึกข้อมูลนั้น ต้องกำหนดวิธีปฏิบัติและสิทธิ์สำหรับการใช้งานสื่อบันทึกข้อมูลโดยปฏิบัติตามเอกสารระเบียบปฏิบัติ เรื่อง การจัดการกับสื่อบันทึกข้อมูลที่เคลื่อนย้ายได้ (Management of Removable Media) (P-IT-AM-๐๓)

๔.๓.๒ การทำลายสื่อบันทึกข้อมูล (Disposal of Media)

๑) โรงพยาบาลปางศิลาทอง จัดทำระเบียบระเบียบปฏิบัติ สำหรับการทำลายสื่อที่ใช้ในการบันทึกข้อมูลอย่างเป็นลายลักษณ์อักษร

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** ของกระทรวงกลาโหม สหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๔.๓.๓ การเคลื่อนย้ายสื่อบันทึกข้อมูล (Physical Media Transfer)

ต้องมีวิธีการจัดส่งสื่อบันทึกข้อมูล (สารสนเทศหรือซอฟต์แวร์) ให้มีความมั่นคงปลอดภัย โดยปฏิบัติตามระเบียบปฏิบัติ เรื่อง การจัดระดับชั้นความลับและการจัดการกับระบบสารสนเทศ (Information Classification, Labeling and Handling) (P-IT-AM-๐๒)

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 โดยปฏิบัติตามระเบียบปฏิบัติ เรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑) ทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้บังคับบัญชาตามความจำเป็นในการใช้งาน

๓) ผู้ดูแลระบบเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศได้

๔) ต้องมีการบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลปางศิลาทอง และ เฝ้าระวังการละเมิดความปลอดภัย ที่มีต่อข้อมูลและระบบสารสนเทศที่สำคัญ

๕) ต้องบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ ของทั้งผู้ทีได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๖) ต้องกำหนดกฎเกณฑ์ข้อห้ามและบทลงโทษการเข้าถึงข้อมูลและระบบสารสนเทศ

๗) การเข้าถึงข้อมูล และระบบสารสนเทศของโรงพยาบาลปางศิลาทอง จะกระทำได้ก็ต่อเมื่อได้รับการอนุมัติโดยผู้บังคับบัญชาของบุคคลนั้น ๆ และสามารถเข้าใช้ข้อมูล และระบบเฉพาะที่เกี่ยวข้องกับงานในหน้าที่ของบุคคลนั้น ๆ เท่านั้น ความปลอดภัยของข้อมูล และกระบวนการรักษาความลับของข้อมูลถือว่าเป็นส่วนหนึ่งในการกำหนดนโยบาย และขั้นตอน การทำงานของระบบสารสนเทศ กระบวนการเหล่านี้หมายรวมถึงการให้สิทธิ์ และการบริหารจัดการรหัสในการเข้าใช้งาน การกำหนดขอบเขตในการเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ และอุปกรณ์ที่เก็บข้อมูลประเภทอื่น ๆ การสารอง ข้อมูล และการกู้ข้อมูลที่เสียหายกลับคืนมา

๕.๑.๒ การเข้าถึงเครือข่ายและบริการเครือข่าย (Access to Network and Network Services) ผู้ใช้งานต้อง ได้รับสิทธิ์การเข้าถึงเฉพาะเครือข่ายและบริการของเครือข่ายตามที่ตนได้รับอนุมัติการเข้าถึงเท่านั้น

๑) ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานและต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด โดยผู้ใช้งานต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย”

๒) การขออนุญาตใช้งานพื้นที่ Web Server ชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อหัวหน้าหน่วยงาน และจะต้องไม่ติดตั้งโปรแกรมใด ๆ ที่ส่งผลกระทบต่อการกระทำ ของระบบและผู้ใช้งานอื่น ๆ

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

๔) ผู้ดูแลระบบ ต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

- ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น
- ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน
- ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้
- ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย
- ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานใน ลักษณะที่ผิดปกติ
- การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านเพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง
- ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน
- ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- การระบุอุปกรณ์บนเครือข่าย
  - ■ ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง
  - ■ อุปกรณ์ที่นำมาเชื่อมต่อจะได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
  - ■ ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้
  - ■ กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้
  - ■ อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้
  - ■ ผู้ขอใช้บริการต้องกรอกแบบฟอร์ม “การขอเชื่อมต่อเครือข่าย” โดยดาวน์โหลดผ่าน เว็บไซต์ของโรงพยาบาลปางศิลาทอง หัวข้อ Intranet สาธารณสุข
  - ■ การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๕) กำหนดระยะเวลาผู้ใช้งานที่อยู่ในระบบเครือข่ายให้ออกจากระบบเครือข่ายเมื่อ

- เว้นว่างจากการใช้งานไม่เกินกว่า ๘ ชั่วโมง

๖) ผู้ดูแลระบบ ต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย (Server) และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่าง ๆ ของซอฟต์แวร์ระบบ (Systems Software)

๗) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบงานต้องมีการขออนุมัติจากผู้ดูแลระบบให้ติดตั้งก่อน ดำเนินการ

๘) กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอฟต์แวร์ของระบบงาน ไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๙) การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและ สามารถระบุถึงตัวบุคคลได้ตามแนวทาง พ.ร.บ. คอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑๐) กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) จากผู้ใช้งานภายนอกหน่วยงาน เพื่อดูแลรักษาความปลอดภัยของระบบ ตามแนวทางปฏิบัติ ดังต่อไปนี้

- บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากหัวหน้าหน่วยงาน

- มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

- วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากหัวหน้าหน่วยงาน

- การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

- การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วย การใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๑๑) กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

- Internet แบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

- Intranet แบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศภายใน

๑๒) กำหนดการป้องกันเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่าง ๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๑๓) ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ด้วย

๑๔) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคล ที่เข้าใช้งานระบบเครือข่ายของหน่วยงาน ในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะ ที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๑๕) IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อ สามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้ โดยง่าย

๑๖) การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๒ การจัดการการเข้าถึงระบบของผู้ใช้งาน (User Access Management)

วัตถุประสงค์: เพื่อป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์ใช้งานสามารถเข้าถึงระบบสารสนเทศได้

นโยบาย

๕.๒.๑ การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration)

การลงทะเบียนผู้ใช้งานใหม่ ต้องกำหนดให้มีระเบียบปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนผู้ใช้งานใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งระเบียบปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อลาออกไป หรือเมื่อเปลี่ยนตำแหน่งงานภายในโรงพยาบาลปางศิลาทอง เป็นต้น โดยปฏิบัติตามระเบียบปฏิบัติ เรื่องการลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑) โดยผู้ใช้งานต้องได้รับการทบทวน และพิจารณาอนุมัติตามขั้นตอนของโรงพยาบาลปางศิลาทอง อย่างเคร่งครัด

๕.๒.๒ การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning)

การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึง ทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ 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) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ต้องปฏิบัติตามระเบียบปฏิบัติ เรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑) โดยการส่งมอบข้อมูลการพิสูจน์ตัวตนของผู้ใช้งาน เจ้าหน้าที่จะส่งโดยใช้แบบฟอร์ม F-IT-AC-๐๑.๐๑

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 ตามระเบียบปฏิบัติ เรื่อง การลงทะเบียนใช้งานระบบสารสนเทศ (P-IT-AC-๐๑)

๒) ต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ ตามระเบียบปฏิบัติ เรื่อง การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights Procedure) (P-IT-AC-๐๑)

๕.๓ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibly)

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 รวมทั้งห้ามทำ การเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)
- กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical Character) ตัวอักษร (Alphabet) ตัวเล็ก ตัวใหญ่ และตัวอักษรพิเศษ (Special character)
- หลีกเลี่ยงการตั้งรหัสผ่านที่อยู่บนพื้นฐานที่สามารถเดาได้ง่าย เช่น ชื่อหรือนามสกุลของตนเองหรือตรงกับคำในพจนานุกรม
- ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจารหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่
- ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น
- กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

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

๓) การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้อง รับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้ทรัพย์สินหรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านล็อกก็ดีหรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดยปฏิบัติตามแนวทาง ดังนี้

- คอมพิวเตอร์ทุกประเภท การเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง
- การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง
- การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตน และต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้
- เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ ต้องทำการล็อกหน้าจอทุกครั้ง และต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง
- เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๐ นาที

๕) ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของโรงพยาบาลปางศิลาทอง หรือเป็นข้อมูลของบุคคลภายนอก

๖) ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๗) ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของโรงพยาบาลปางศิลาทอง และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย โดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานต้องมีส่วน ร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๘) ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๙) ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร กระทรวงสาธารณสุขจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการ ละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่กระทรวง สาธารณสุขต้องการตรวจสอบข้อมูล หรือคำดว่าข้อมูลนั้นเกี่ยวข้องกับโรงพยาบาลปางศิลาทอง ซึ่งกระทรวง สาธารณสุขอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ ผู้ใช้งานทราบ

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 ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๒) บัญชีผู้ใช้งานที่มีสิทธิ์การเข้าถึงระบบสารสนเทศในระดับพิเศษ เช่น Root หรือ Administrator ต้องได้รับการพิจารณามอบหมายให้แก่ผู้ใช้งานตามความจำเป็นและมีการกำหนดระยะเวลาในการเข้าถึงอย่างเหมาะสมกับการทำงานเท่านั้น

๓) บุคคลภายนอก ต้องแสดงความยินยอมปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy) ของโรงพยาบาลปางศิลาทอง อย่างเคร่งครัด ก่อนที่จะได้รับ อนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลปางศิลาทอง

๕.๔.๒ ขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure)

ต้องกำหนดกระบวนการในการเข้าถึงระบบให้มีความมั่นคงปลอดภัย โดยกำหนดให้ระบบมีการหน่วงเวลาการให้บริการเป็นเวลา ๕ นาที หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง และต้องวิเคราะห์ทบทวนว่าเป็นการโจมตีหรือไม่ อย่างน้อยเดือนละ ๑ ครั้ง

๕.๔.๓ ระบบบริหารจัดการรหัสผ่าน (Password Management System)

ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้งานระบบเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

๕.๔.๔ การใช้โปรแกรมอรรถประโยชน์ (Use of Privileged Utility Programs)

๑) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

๒) ต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบ เพื่อป้องกันการเข้าถึงโดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

- ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน
- ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน
- จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น
- ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ 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 และเพื่อป้องการความลับ การปลอมแปลง หรือความถูกต้องของสารสนเทศ

นโยบาย

๖.๑.๑ นโยบายการใช้มาตรการเข้ารหัสข้อมูล (Policy on the Use of Cryptographic Controls)

โรงพยาบาลปางศิลาทอง ต้องมีวิธีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้องอย่าง เหมาะสม

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 ข้อมูลและสารสนเทศซึ่งเป็นทรัพย์สิน โรงพยาบาลปางศิลาทอง

นโยบาย

๗.๑.๑ การกำหนดพื้นที่มั่นคงปลอดภัย (Physical Security Perimeter)

๑) หน่วยงานจะต้องมีการจำแนก และกำหนดพื้นที่ในการใช้งานระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม และรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้ เมื่อมีการกำหนดพื้นที่แล้วให้มีการควบคุมการเข้าออก

๒) หน่วยงานจะต้องจำแนก กำหนด และแบ่งบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspaces)” รวมทั้งจัดทำแผนผังแสดงตำแหน่ง และชนิดของพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และประกาศให้ทราบทั่วกัน (หน่วยงานควรระบุให้ชัดเจนว่ามีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศประเภทใดบ้าง และมีพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศใดที่อาจจำแนกได้มากกว่า ๑ ประเภท)

๓) หน่วยงานต้องกำหนดการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศใน “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” ให้สอดคล้องกับหมวดหมู่และความสำคัญของข้อมูลหรือสารสนเทศที่มีอยู่ในระบบ

๔) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ต้องดูแลรักษาสภาพแวดล้อมในการทำงานเสมือนดูแลบ้านของตน

๗.๑.๒ การควบคุมการเข้าออก (Physical Entry Controls)

หน่วยงานที่เกี่ยวข้องกับการบริหารจัดการอาคารและสถานที่ ต้องจัดให้มีการควบคุมการเข้าออกในบริเวณ “พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” โดยให้ผ่านเข้าออกได้เฉพาะ “เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง”ที่มีสิทธิ์เท่านั้น และมีแนวทางปฏิบัติ ดังนี้

๑) ต้องกำหนด “เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง” ที่มีสิทธิ์ผ่านเข้าออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออก ในแต่ละ“พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ” อย่างชัดเจน

๒) “เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง” จะได้รับสิทธิ์ให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๓) หากมีบุคคลอื่นใดที่ไม่ใช่ “เจ้าหน้าที่ โรงพยาบาลปางศิลาทอง” ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้ เป็นการล่วงหน้า หน่วยงานต้องตรวจสอบเหตุผลและความจำเป็น ก่อนที่จะอนุญาต หรือไม่อนุญาตให้บุคคลเข้า พื้นที่เป็นการชั่วคราว ทั้งนี้บุคคลจะต้องแสดงบัตรประจำตัวประชาชน หรือบัตรประจำตัวอื่นที่ราชการออกให้ โดย หน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้าออกไว้เป็นหลักฐาน (ทั้งในกรณีที่อนุญาต และไม่ อนุญาตให้เข้า พื้นที่) และต้องมีการบันทึกข้อมูลการเข้าออกศูนย์ปฏิบัติการ MOPH IDC ของบุคคลภายนอกทุกครั้ง พร้อมทั้งจัดเก็บ บันทึกดังกล่าวไว้อย่างน้อย ๑ ปี

๔) บุคคลภายนอกต้องทำการแลกบัตรประจำตัวของตนที่ออกให้โดยหน่วยงานของรัฐ ตัวอย่างเช่น บัตรประชาชน ใบขับขี่ พาสปอร์ต ฯลฯ กับบัตรผู้มาติดต่อของหน่วยงาน ก่อนได้รับอนุญาตให้เข้าถึงพื้นที่สำนักงาน

๕) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง และบุคคลภายนอกต้องติดบัตรเจ้าหน้าที่ หรือบัตรผู้มาติดต่อตลอดเวลาที่อยู่ใน พื้นที่สำนักงาน ทั้งนี้ บัตรประจำตัวและบัตรผู้มาติดต่อ ไม่อนุญาตให้โอนกรรมสิทธิ์หรือหยิบยืมกันใช้งาน

๖) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ต้องไม่เปิดประตูสำนักงานทิ้งไว้ หรือยินยอมให้บุคคลอื่นติดตามเข้าภายในพื้นที่ สำนักงานโดยเด็ดขาด เว้นแต่บุคคลอื่นนั้นสามารถแสดงบัตรประจำตัวหรือบัตรผู้มาติดต่อได้ เพื่อเป็นการป้องกันการเข้าถึงพื้นที่สำนักงาน และพื้นที่ควบคุมความมั่นคงปลอดภัยโดยบุคคลที่ไม่ได้รับอนุญาต

๗) ผู้ใช้งานต้องแจ้งเจ้าหน้าที่รักษาความปลอดภัยทันที เมื่อพบเห็นบุคคลแปลกหน้าหรือบุคคลที่ไม่ แขวนบัตรเจ้าหน้าที่หรือบัตรผู้มาติดต่อในพื้นที่สำนักงาน

๘) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ควรติดตาม ควบคุมดูแล และให้คำแนะนำผู้ที่มาติดต่อกับตนตลอดเวลาที่ผู้มา ติดต่อนั้นอยู่ในพื้นที่สำนักงาน

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

๑) ISMR ต้องจัดให้มีมาตรการในการรักษาความมั่นคงปลอดภัยอื่นๆ ให้กับสำนักงาน ห้องทำงานและเครื่องมือต่างๆ เช่น เครื่องคอมพิวเตอร์หรือระบบที่มีความสำคัญสูง ต้องไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็น จานวนมาก สำนักงานหรือห้องจะต้อง ไม่มีป้าย หรือ สัญลักษณ์ ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว ประตูหน้าต่างของสำนักงาน หรือห้องต้องใส่กุญแจเสมอ เมื่อไม่มีคนอยู่ ต้องตั้งเครื่องโทรสารหรือเครื่องถ่ายเอกสารแยกออกมาจากบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย เป็นต้น

๒) เจ้าหน้าที่ควรตรวจสอบความมั่นคงปลอดภัยของพื้นทีทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

๓) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งไว้โดยลาพังบนโต๊ะทำงาน ในห้องประชุมหรือในตู้ที่ไม่ได้ล็อคกุญแจโดยเด็ดขาด

๔) ข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์ที่จัดเก็บข้อมูลลับต้องไม่ถูกทิ้งลงในถังขยะโดยไม่ได้รับการทำลายอย่างเหมาะสม วิธีการทำลายข้อมูล สื่อบันทึก วัสดุ และอุปกรณ์เหล่านี้โดยปฏิบัติตามเอกสารระเบียบปฏิบัติ เรื่องการทำลายสื่อบันทึกข้อมูลและข้อมูลบนสื่อบันทึกข้อมูล (Disposal of Media Procedure) (P-IT-CO-๐๓)

๕) เจ้าหน้าที่ต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงาน ของตนโดยเด็ดขาด เว้นแต่บุคคลผู้นั้นเป็นเจ้าหน้าที่ที่ได้รับอนุญาตให้ดำเนินการ และเป็นการดำเนินการที่มีคำสั่งอย่าง ถูกต้องของหน่วยงานเท่านั้น

๗.๑.๔ การป้องกันภัยคุกคามจากภายนอกและสิ่งแวดล้อมอื่น ๆ
(Protecting against External and Environmental Threats)

หน่วยงานต้องมีการป้องกันจากการทำลายของธรรมชาติหรือคนที่อาจจะเกิดขึ้น ซึ่งเป็นภัยคุกคามจาก ภายนอกต้องมีการเตรียมการป้องกันเหตุที่อาจเกิดขึ้น

๗.๑.๕ การปฏิบัติงานในพื้นที่มั่นคงปลอดภัย (Working in Secure Areas)

๑) หัวหน้าของแต่ละหน่วยงาน ต้องมีการควบคุมการปฏิบัติงานของหน่วยงานภายนอกในบริเวณพื้นที่ควบคุม ได้แก่ การไม่อนุญาตให้ถ่ายภาพหรือวีดีโอในบริเวณนั้น เป็นต้น

๒) หน่วยงานต้องมีป้ายประกาศข้อความ “ห้ามเข้าก่อนได้รับอนุญาต” “ห้ามถ่ายภาพหรือวีดีโอ” และ “ห้ามสูบบุหรี่” บริเวณภายในพื้นที่ควบคุมการปฏิบัติงาน

๗.๑.๖ การกำหนดพื้นที่สำหรับบุคคลภายนอกใช้รับส่งสิ่งของ (Delivery and Loading Areas)

๑) หน่วยงานต้องมีการจำกัดพื้นที่การเข้าถึงของบุคคลภายนอกที่อาจเข้ามาในพื้นที่ได้ หากเป็นไปได้ควร แบ่งแยกพื้นที่ที่เกี่ยวข้องกับการทำงานออกจากพื้นที่ที่บุคคลภายนอกเข้ามาได้ เช่น บริเวณเก็บและจัดส่งสินค้า จะต้องไม่อยู่ในพื้นที่ๆ บุคคลภายนอกเข้าถึงได้

๒) เจ้าหน้าที่และเจ้าหน้าที่ของหน่วยงานภายนอก (Third Party) ต้องติดบัตรประจำตัวตลอดเวลาขณะปฏิบัติหน้าที่ในบริเวณโรงพยาบาลปางศิลาทอง และหากผู้ใดพบเห็นผู้ที่ไม่ติดบัตรประจำตัวถือเป็นหน้าที่ที่จะต้องแจ้งเจ้าหน้าที่รักษา ความปลอดภัยโดยทันที

๗.๒ ความมั่นคงปลอดภยของอุปกรณ์ (Equipment)

วัตถุประสงค์: เพื่อป้องกันการใช้อุปกรณ์คอมพิวเตอร์โดยไม่ได้รับอนุญาต และเพื่อให้มั่นใจได้ว่าอุปกรณ์คอมพิวเตอร์ได้มีการป้องกันอย่างเพียงพอจากภัยธรรมชาติ การโจรกรรม และความเสียหายอื่นๆ

นโยบาย

๗.๒.๑ การจัดตั้งและการป้องกันอุปกรณ์ (Equipment Setting and Protection)

๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือ ประเมินในภายหลัง

๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๗.๒.๒ การดูแลอุปกรณ์ต่างๆ (Supporting Utilities)

๑) เจ้าหน้าที่ต้องกำหนดให้มีการดูแลรักษาอุปกรณ์ Utilities ที่เกี่ยวข้อง เช่น Uninterruptible Power Supply (UPS) อุปกรณ์ตรวจจับความชื้น อุปกรณ์ตรวจจับควัน เป็นต้น

๒) เจ้าหน้าที่ต้องมีการตรวจสอบการให้บริการของอุปกรณ์ อย่างน้อยปีละ ๒ ครั้ง

๗.๒.๓ การเดินสายไฟและสายเคเบิล (Cabling Security)

๑) ต้องกำหนดให้มีการป้องกันการเดินสายไฟฟ้า หรือสายเคเบิ้ลเข้ามาภายในอาคารสำนักงาน

๒) บริเวณที่มีการเดินสายไฟฟ้าหรือสายเคเบิลเข้ามาภายในอาคารสำนักงาน และมีการติดตั้งตู้พักสาย ต้องล็อคไว้ตลอดเวลาและจำกัดการเข้าใช้งานได้เฉพาะเจ้าหน้าที่หรือบุคคลที่มีสิทธิ์เท่านั้น

๗.๒.๔ การดูแลรักษาอุปกรณ์ (Equipment Maintenance)

ต้องกำหนดให้มีการดูแลและบำรุงรักษาอุปกรณ์อย่างถูกต้องและสม่ำเสมอ เช่น จัดให้มีการซ่อมบำรุงอย่างน้อยปีละ ๑ ครั้ง หรือตามที่เจ้าของผลิตภัณฑ์แนะนำ เป็นต้น

๗.๒.๕ การนำทรัพย์สินขององค์กรออกนอกสำนักงาน (Removal of Asset)

อุปกรณ์สารสนเทศหรือซอฟต์แวร์ ต้องไม่มีการนำออกนอกโรงพยาบาลปางศิลาทอง โดยไม่ได้รับอนุญาต หากมีความ ประสงค์จะนำออกจากสำนักงานโดยต้องปฏิบัติตามระเบียบปฏิบัติ เรื่อง การขอนำทรัพย์สินขององค์กรออกนอกสำนักงาน (P-IT-PE-๐๕)

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

หน่วยงานต้องกำหนดให้มีการป้องกันทรัพย์สินและอุปกรณ์ของหน่วยงาน เช่น เครื่องคอมพิวเตอร์พกพา โทรศัพท์มือถือ เป็นต้น เมื่อถูกนำไปใช้งานนอกหน่วยงาน จะต้องปฏิบัติตามระเบียบในการใช้งาน การยืม-คืน

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

หน่วยงานต้องกำหนดให้มีวิธีการในการตรวจสอบอุปกรณ์ซึ่งมีข้อมูลสำคัญเก็บไว้ 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 หรือสื่อต่างๆ ที่มีข้อมูลสำคัญจัดเก็บ หรือบันทึกอยู่ ไม่ให้วางทิ้งไว้บนโต๊ะทำงานหรือในสถานที่ไม่ปลอดภัยในขณะไม่ได้นำมาใช้งาน ตลอดจนการควบคุมหน้าจอคอมพิวเตอร์ (Desktop) ไม่ให้มีข้อมูลสำคัญ ปรากฏในขณะไม่ได้ใช้งาน

หมวดที่ ๘ ความมั่นคงปลอดภัยสำหรับการดำเนินงาน (Operation Security)

๘.๑ ขั้นตอนการปฏิบัติงานและหน้าที่ความรับผิดชอบ (Operation Procedures and Responsibilities)

วัตถุประสงค์: เพื่อให้การปฏิบัติงานกับอุปกรณ์ประมวลสารสนเทศเป็นไปอย่างถูกต้องและมีความมั่นคงปลอดภัย

นโยบาย

๘.๑.๑ การกำหนดขั้นตอนการปฏิบัติงานให้เป็นลายลักษณ์อักษร (Document Operating Procedures)

๑) ต้องจัดทำคู่มือ และ/หรือ ขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน เช่น ขั้นตอนการแจ้งเหตุขัดข้อง ขั้นตอนการกู้คืน ขั้นตอนการบำรุงรักษาและดูแลระบบ ซึ่งประกอบไปด้วยรายละเอียดขั้นตอนการปฏิบัติ และ เจ้าหน้าที่หรือหน่วยงานผู้รับผิดชอบ

๒) คู่มือและขั้นตอนการปฏิบัติงานต้องได้รับการปรับปรุงเมื่อมีการปรับเปลี่ยนขั้นตอนและผู้รับผิดชอบการปฏิบัติงานนั้นๆ โดยคู่มือและขั้นตอนการปฏิบัติงานทุกฉบับต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง

๓) มีการกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติหรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๘.๑.๒ การจัดการการเปลี่ยนแปลง (Change Management)

๑) ต้องมีการจัดการการเปลี่ยนแปลงระบบเครือข่าย ระบบคอมพิวเตอร์ อุปกรณ์ ซอฟต์แวร์ ทุกครั้ง โดยปฏิบัติตามวิธีการปฏิบัติงาน เรื่อง การจัดการการเปลี่ยนแปลงสารสนเทศ (Change Management) (P-IT-CO-๐๖)

๒) เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ เช่น ระบบปรับอากาศ น้ำ ไฟฟ้า สัญญาณเตือนภัย อุปกรณ์ตรวจจับ ฯลฯ เจ้าหน้าที่ต้องประสานงานหรือรายงานกับ ISS (จัดการการเปลี่ยนแปลง)

๓) เมื่อมีการเปลี่ยนแปลงสภาพแวดล้อมที่เกี่ยวกับระบบสารสนเทศ ต้องมีเอกสารเป็นทางการในการร้องขอการเปลี่ยนแปลงทุกครั้ง

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

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

๖) บันทึกการเปลี่ยนแปลงทุกครั้งจะต้องแจ้งให้หน่วยงานที่เกี่ยวข้องได้รับทราบโดยบันทึกฯ ต้องประกอบด้วยข้อมูลอย่างน้อยดังต่อไปนี้

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

๘.๑.๓ การจัดการขีดความสามารถ (Capacity Management)

๑) ต้องมีการติดตามสภาพการใช้งาน และวิเคราะห์ขีดความสามารถของทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารปัจจุบันอย่างสม่ำเสมอ ตามความเหมาะสมของทรัพยากรชนิดต่างๆ โดยปฏิบัติตามเอกสารระเบียบปฏิบัติ เรื่อง การจัดการขีดความสามารถระบบ (Capacity Management) (P-IT-CO-๐๒)

๒) ต้องมีการวางแผนจัดการขีดความสามารถของระบบ อย่างน้อยปีละ ๑ ครั้ง โดยพิจารณาจากความต้องการใช้งานทรัพยากรด้านเทคโนโลยีสารสนเทศและการสื่อสารในอนาคต (อาทิ ความต้องการใน ๑ ปีที่จะถึง เช่น CPU ที่ความเร็วสูงขึ้น ฮาร์ดดิสก์ที่ความจุมากขึ้น เป็นต้น) สภาพการใช้งานทรัพยากรในปัจจุบัน การเปลี่ยนแปลงของเทคโนโลยี

๓) แผนการจัดการขีดความสามารถของระบบต้องประกอบด้วยวิธีการจัดการขีดความสามารถ อาทิ การ Turning 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) โรงพยาบาลปางศิลาทอง ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา ดังนั้นซอฟต์แวร์ที่หน่วยงานอนุญาตให้ใช้งานหรือที่หน่วยงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๒) ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ ผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสาเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจาก หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

๓) คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าหน่วยงาน

๔) บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัส คอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๕) ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๖) ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๗) เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

๘) ห้ามลักลอบทำสาเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นทรัพย์สินของหน่วยงาน หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน

๙) ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใด ๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ทรัพย์สินของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ สามารถดำเนินการได้ แต่ต้องไม่ดำเนินการ ดังนี้

๙.๑) พัฒนำโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสาเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

๙.๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครอง ทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

๙.๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรม หรือ แฝงตัวโปรแกรมไปกับโปรแกรมอื่น ในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

๙.๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายระบบจำกัดสิทธิการใช้ (License) ซอฟต์แวร์

๙.๕) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม ประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้งานสร้างเว็บเพจ บนเครือข่ายคอมพิวเตอร์

๑๐) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

๑๐.๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๑๐.๒) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

๑๐.๓) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๑๐.๔) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

๑๐.๕) ผู้พัฒนาระบบจากภายนอก (outsource) ต้องลงนามในหนังสือยอมรับเงื่อนไขนโยบายความปลอดภัยระบบสารสนเทศสำหรับผู้ใช้งาน (Acceptable Use Policy: AUP) (F-IT-AC-๐๒.๐๑) และสัญญาไม่เปิดเผยข้อมูล (Non-Disclosure Agreement) ก่อนดำเนินการ

๑๐.๖) ผู้พัฒนาระบบจากภายนอก (Outsource) ต้องถือปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลปางศิลาทอง

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) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๔) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ใน การสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูล
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบค่ากำหนดเบื้องต้นต่าง ๆ ของระบบการสำรองข้อมูล
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สารองข้อมูล และผู้รับผิดชอบในการสารองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สารองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสารองกับหน่วยงานต้องห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สารองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสารองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สารองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สารองเก็บไว้

๕) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดย

- มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามา ใช้ระบบงานได้ เป็นต้น

- มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำ เมื่อเกิดเหตุเร่งด่วน เป็นต้น

๖) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๗) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๘) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น เพื่อให้ระบบมี สภาพพร้อมใช้งานอยู่เสมอ

๙) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๘.๔ การบันทึกข้อมูลการใช้งาน และการเฝ้าระวัง (Logging and Monitoring)

วัตถุประสงค์: เพื่อให้มีการเก็บหลักฐานหรือบันทึกเหตุการณ์ เพื่อใช้เป็นหลักฐานยืนยัน

นโยบาย

๘.๔.๑ การบันทึกข้อมูลเหตุการณ์ (Event logging)

ต้องกำหนดให้ทำการบันทึกกิจกรรมการใช้งานของผู้ใช้ การปฏิเสธการให้บริการของระบบ และเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยอย่างสม่ำเสมอตามระยะเวลาที่กำหนดไว้ โดยปฏิบัติตามเอกสาร ระเบียบปฏิบัติ เรื่อง การเฝ้าระวังการใช้งานระบบ (System Usage Monitoring Procedure) (P-IT-CO-๐๕)

๘.๔.๒ การป้องกันข้อมูลการใช้งาน (Protection of Log Information)

ต้องกำหนดให้มีการป้องกันข้อมูลบันทึกกิจกรรมหรือเหตุการณ์ต่าง ๆ ที่เกี่ยวข้องกับการใช้งานสารสนเทศ เพื่อป้องกันการเปลี่ยนแปลง หรือการแก้ไขโดยไม่ได้รับอนุญาต

๘.๔.๓ ข้อมูลการใช้งานของผู้ดูแลระบบและเจ้าหน้าที่ปฏิบัติการ (Administrator and Operator Logs)

ต้องกำหนดให้มีการบันทึกกิจกรรมการดำเนินงานของผู้ดูแลระบบ หรือเจ้าหน้าที่ที่เกี่ยวข้องกับระบบอื่น ๆ รวมถึงอุปกรณ์คอมพิวเตอร์และเครือข่าย

๘.๔.๔ การตั้งเวลาให้ถูกต้อง (Clock Synchronization)

ต้องตั้งเวลาของเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ในหน่วยงานให้ตรงกัน โดยอ้างอิงจากแหล่งเวลาที่ถูกระบุตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เพื่อช่วยในการตรวจสอบช่วงเวลาหากเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ของโรงพยาบาลปางศิลาทอง ถูกบุกรุกตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับ คอมพิวเตอร์

๘.๕ การควบคุมการติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Control of Operation Software)

วัตถุประสงค์: เพื่อให้ระบบที่ให้บริการ สามารถให้บริการและมีการทำงานที่ถูกต้อง

นโยบาย

๘.๕.๑ การติดตั้งซอฟต์แวร์บนระบบที่ให้บริการ (Installation of Software on Operational Systems)

ผู้พัฒนาระบบสารสนเทศต้องมีการควบคุมการติดตั้งซอฟต์แวร์ใหม่ ซอฟต์แวร์ไลบารี่ ซอฟต์แวร์อุดช่องโหว่ ลงในเครื่องที่ใช้งานหรือเครื่องให้บริการ โดยก่อนการติดตั้งในระบบจริงจะต้องผ่านการทดสอบการใช้งานมาเป็นอย่างดี ว่า ไม่ก่อให้เกิดปัญหากับเครื่องที่ให้บริการอยู่ โดยปฏิบัติตามวิธีการปฏิบัติเรื่องการควบคุมระบบสารสนเทศที่ใช้ในการปฏิบัติงาน (Control of operational software) (P-IT-IS-๐๒)

๘.๖ การบริหารจัดการช่องโหว่ทางเทคนิค (Technical Vulnerability Management)

วัตถุประสงค์: เพื่อสร้างความมั่นคงปลอดภัยให้กับซอฟต์แวร์สำหรับระบบสารสนเทศ รวมทั้งสารสนเทศในระบบด้วยเพื่อลดความเสี่ยงจากการโจมตีโดยอาศัยช่องโหว่ทางเทคนิคที่มีการเผยแพร่หรือตีพิมพ์ในสถานที่ต่าง ๆ

นโยบาย

๘.๖.๑ การบริหารจัดการช่องโหว่ทางเทคนิค (Management of Technical Vulnerabilities)

ต้องมีการติดตามข้อมูลข่าวสารที่เกี่ยวข้องกับช่องโหว่ในระบบต่าง ๆ ที่ใช้งานและประเมินความเสี่ยงของช่องโหว่เหล่านั้นรวมทั้งกำหนดมาตรการรองรับเพื่อลดความเสี่ยงดังกล่าว

๘.๖.๒ การจำกัดการติดตั้งซอฟต์แวร์ (Restrictions on Software Installation)

๑) โรงพยาบาลปางศิลาทอง ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่ หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๒) ซอฟต์แวร์ (Software) ที่หน่วยงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามมิให้ ผู้ใช้งานทำการ ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสาเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจาก หัวหน้าหน่วยงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิ์ในลิขสิทธิ์

๘.๗ การพิจารณาการตรวจสอบระบบสารสนเทศ (Information System Audit Considerations)

วัตถุประสงค์: เพื่อให้กระบวนการตรวจสอบระบบสารสนเทศทั้งหมด มีผลกระทบน้อยที่สุดต่อการดำเนินงานของหน่วยงาน

นโยบาย

๘.๗.๑ การวางแผนการตรวจสอบระบบสารสนเทศทั้งหมด (Information System Audit Controls)

ISS ต้องวางแผนการตรวจสอบระบบ โดยการตรวจสอบที่จะดำเนินการจะต้องมีผลกระทบต่อระบบ และกระบวนการดำเนินงานของหน่วยงานน้อยที่สุด

หมวดที่ ๙ ความมั่นคงปลอดภัยสำหรับการสื่อสารข้อมูล (Communications Security)

๙.๑ การจัดการระบบรักษาความปลอดภัยระบบเครือข่าย (Network Security Management)

วัตถุประสงค์: เพื่อป้องกันข้อมูลในระบบเครือข่าย และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายของโรงพยาบาลปางศิลาทอง

นโยบาย

๙.๑.๑ การควบคุมการเข้าถึงเครือข่าย (Network Control)

๑) ต้องกำหนดหน้าที่ความรับผิดชอบ รวมทั้งวิธีปฏิบัติเมื่อมีเหตุการณ์ผิดปกติ หรือการละเมิดความปลอดภัย และดำเนินการตรวจสอบผู้กระทำการละเมิด

๒) การจัดทำคู่มือและขั้นตอนการปฏิบัติงานสารสนเทศในหน่วยงาน ต้องมีเนื้อหาในส่วนการใช้งานอุปกรณ์เครือข่ายที่สนับสนุนความมั่นคงปลอดภัย

๓) ต้องแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบเทคโนโลยีสารสนเทศและเครือข่ายที่หน่วยงานนั้นรับผิดชอบ

๔) ต้องบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขที่สำคัญและแจ้งให้หน่วยงานอื่นๆ ที่เกี่ยวข้องทราบ กรณีที่มีการเปลี่ยนแปลงแก้ไขระบบเครือข่าย

๕) บริหารจัดการกิจกรรมที่เกี่ยวข้องให้เหมาะสมและต้องมั่นใจว่าสอดคล้องกับการควบคุมข้อมูลสารสนเทศที่ส่งผ่านเครือข่ายตลอดจนโครงสร้างพื้นฐานของโรงพยาบาลปางศิลาทอง ด้วย

๙.๑.๒ ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย (Security of Network Service)

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

๒) ต้องจำกัดจานวนการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายของโรงพยาบาลปางศิลาทอง และต้องกำหนดให้การเชื่อมต่อเข้ามายังเครื่องคอมพิวเตอร์ที่กำหนดไว้เฉพาะและติดต่อกับระบบงานที่กำหนดไว้เฉพาะเท่านั้น และควรกำหนดให้เครื่องคอมพิวเตอร์และระบบงานดังกล่าวแยกออกจากระบบเครือข่ายที่เป็นส่วนที่ใช้งานจริงของโรงพยาบาลปางศิลาทอง ทั้งทางด้านกายภาพและทางด้าน Logical และต้องไม่อนุญาตให้หน่วยงานภายนอกมีสิทธิ์เข้ามาใช้คอมพิวเตอร์หรือระบบงานเครือข่ายโรงพยาบาลปางศิลาทอง ได้

๓) ห้ามผู้ใช้งานติดตั้งซอฟต์แวร์บริการเชื่อมต่อจากภายนอก (Remote Access Service) บนเครื่อง คอมพิวเตอร์ของตน หรือต่อกับจุดใดก็ตามบนระบบเครือข่ายของโรงพยาบาลปางศิลาทอง โดยไม่ได้รับอนุญาต

๔) ห้ามบุคคลภายนอกทำการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ใดๆ จากภายนอกเข้ากับระบบ คอมพิวเตอร์และระบบเครือข่ายของโรงพยาบาลปางศิลาทอง โดยเด็ดขาด หากมีความจำเป็นต้องใช้งานต้องดำเนินการขอ อนุมัติอย่างเหมาะสมก่อนทุกครั้ง

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

๖) ห้ามผู้ใช้งานที่อยู่บนระบบเครือข่ายของโรงพยาบาลปางศิลาทอง ทำการเชื่อมต่อออกไปยังเครือข่ายภายนอกผ่านทางโมเด็มหรืออุปกรณ์เชื่อมต่ออื่นในขณะที่ยังเชื่อมต่ออยู่กับระบบเครือข่ายภายในโรงพยาบาลปางศิลาทองโดยเด็ดขาด

๙.๑.๓ การจัดแบ่งเครือข่ายภายในโรงพยาบาลปางศิลาทอง (Segregation in Network)

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

๒) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ต้องมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๙.๒ การถ่ายโอนข้อมูล (Information Transfer)

วัตถุประสงค์: เพื่อให้มีวิธีการรักษาความมั่นคงปลอดภัยของสารสนเทศ ที่มีการถ่ายโอนข้อมูลกันภายในองค์กร และถ่ายโอนข้อมูลกับภายนอกหน่วยงาน

นโยบาย

๙.๒.๑ นโยบายและขั้นตอนปฏิบัติสำหรับการถ่ายโอนสารสนเทศ
(Information Transfer Policies and Procedures)

๑) ต้องมีการจัดทำนโยบาย ขั้นตอนปฏิบัติ หรือมาตรการสำหรับการถ่ายโอนสารสนเทศอย่างเป็นทางการและมีการปฏิบัติตามเพื่อป้องกันสารสนเทศที่มีการถ่ายโอนกับหน่วยงานภายนอก

๒) ต้องมีการดำเนินการแลกเปลี่ยนสารสนเทศ โดยปฏิบัติตามระเบียบปฏิบัติ เรื่อง การแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure) (P-IT-CO-๐๔)

๙.๒.๒ ข้อตกลงสำหรับการถ่ายโอนสารสนเทศ (Agreements on Information Transfer)

ต้องมีการจัดทำข้อตกลงในการแลกเปลี่ยนข้อมูล โดยปฏิบัติตามระเบียบปฏิบัติ เรื่อง การแลกเปลี่ยนสารสนเทศ (Information Exchange Procedure) (P-IT-CO-๐๔)

๙.๒.๓ การรักษาความมั่นคงปลอดภัยการส่งข้อความอิเล็กทรอนิกส์ (Electronic Messaging)

ต้องมีการกำหนดวิธีการป้องกันการเข้าถึงข้อมูลอิเล็กทรอนิกส์รวมถึงการจัดส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเครือข่าย

๙.๒.๔ การรักษาความลับหรือข้อตกลงการไม่เปิดเผยข้อมูล
(Confidentiality or Non-Disclosure Agreements)

๑) ต้องมีการจัดทำข้อตกลง หรือสัญญาการรักษาความลับ หรือข้อตกลงการไม่เปิดเผยข้อมูล หรือสัญญาไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement : NDA) ซึ่งเป็นไปตามความต้องการด้านการป้องกันข้อมูลของโรงพยาบาลปางศิลาทอง และมีการทบทวนอย่างสม่ำเสมอ

๒) พนักงาน บุคคล หรือผู้ติดต่อจากหน่วยงานอื่น ที่มีส่วนต้องเข้าถึงสารสนเทศของโรงพยาบาลปางศิลาทอง ต้องจัดให้มีการลงนามในสัญญาระหว่าง “เจ้าหน้าที่” และ “ผู้ติดต่อ” ในนโยบายการใช้งานที่ยอมรับได้ (Acceptable Use Policy: AUP) และสัญญาไม่เปิดเผยความลับของหน่วยงาน (Non-Disclosure Agreement: NDA)

หมวดที่ ๑๐ การจัดหา พัฒนา และดูแลระบบสารสนเทศ (Systems Acquisition, Development and Maintenance)

๑๐.๑ การกำหนดความตองการด้านความมั่นคงปลอดภัยสำหรับระบบสารสนเทศ (Security Requirements of Information Systems)

วัตถุประสงค์: เพื่อให้แน่ใจว่ามีการสร้างความปลอดภัยสารสนเทศให้กับระบบสารสนเทศ ตลอดวงจรการพัฒนาระบบ ซึ่งรวมถึงความต้องการด้านความปลอดภัยสารสนเทศที่ให้บริการผ่านเครือข่ายสาธารณะ

นโยบาย

๑๐.๑.๑ การกำหนดความต้องการด้านความมั่นคงปลอดภัย
(Information Security Requirements Analysis and Specification)

ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยไว้อย่างชัดเจนในระบบที่จะพัฒนาขึ้นมาใช้งาน หรือซื้อมาใช้งานหน่วยงานดูแลระบบเทคโนโลยีสารสนเทศ จะต้องทำการวิเคราะห์ระบบเทคโนโลยีสารสนเทศ ว่ามีความเสี่ยง ใดบ้างที่จะทำให้ข้อมูลเกิดความเสียหาย โดยมุ่งเน้นในส่วนต่าง ๆ ดังนี้

- มาตรการปฏิบัติก่อนที่จะเกิดความเสียหาย เช่น การสารองข้อมูล ระบบเครือข่ายสารอง เป็นต้น
- มาตรการปฏิบัติหลังจากเกิดความเสียหาย เช่น แผนการกู้คืนข้อมูล ระยะเวลาในการกู้คืนข้อมูล เป็นต้น

๑๐.๑.๒ ความมั่นคงปลอดภัยของบริการสารสนเทศบนเครือข่ายสาธารณะ
(Securing application services on public networks)

สารสนเทศที่เกี่ยวข้องกับการบริการสารสนเทศที่มีการส่งผ่านเครือข่ายสาธารณะ ต้องได้รับการป้องกัน และการเปิดเผยหรือเปลี่ยนแปลงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๑.๓ การป้องกันธุรกรรมของบริการสารสนเทศ (Protecting application services transactions)

สารสนเทศที่เกี่ยวข้องกับธุรกรรมของบริการสารสนเทศ ต้องได้รับการป้องกันจากการรับส่งข้อมูลที่ไม่สมบูรณ์ การส่งข้อมูลผิดเส้นทาง การเปลี่ยนแปลงข้อความโดยไม่ได้รับอนุญาต การเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต การส่งข้อมูลซ้ำโดยไม่ได้รับอนุญาต

๑๐.๒ ความมั่นคงปลอดภัยสำหรับกระบวนการในการพัฒนาระบบ (Security in Development and Support Processes)

วัตถุประสงค์: เพื่อให้มั่นใจได้ว่ามีระบบสารสนเทศมีความมั่นคงปลอดภัย ครอบคลุมทั้งวงจรการพัฒนาระบบสารสนเทศ (Development lifecycle)

นโยบาย

๑๐.๒.๑ นโยบายการพัฒนาระบบให้มีความมั่นคงปลอดภัย (Secure development policy)

ต้องมีการกำหนดหลักเกณฑ์สำหรับการพัฒนาซอฟต์แวร์ และมีการปฏิบัติตามนโยบายหรือข้อ กำหนดที่องค์กรกำหนดขึ้นมา เช่น การพัฒนาซอฟต์แวร์ควรคำนึงความปลอดภัยในทุกขั้นตอนของการพัฒนา และนักพัฒนา (Developers) ควรมีความสามารถในการหลีกเลี่ยงไม่ให้โปรแกรมที่พัฒนามีช่วงโหว่ที่รู้จักกัน (Common Vulnerabilities and Exposures (CVE)) และต้องสามารถแก้ไขช่องโหว่ที่ตรวจพบได้

๑๐.๒.๒ กระบวนการในการควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์ (System Change Control Procedures)

ผู้พัฒนาระบบสารสนเทศต้องมีกระบวนการเพื่อควบคุมการเปลี่ยนแปลงแก้ไขซอฟต์แวร์สำหรับระบบ สารสนเทศที่ใช้งานจริง หรือให้บริการอยู่แล้ว เช่น

- คำขอให้แก้ไขต้องมาจากผู้ที่มีสิทธิ์
- ต้องมีการอนุมัติคำขอโดยผู้มีอำนาจ
- ต้องมีการควบคุมผลข้างเคียงที่อาจเกิดขึ้นหลังจากมีการแก้ไข
- เมื่อแก้ไขเสร็จแล้วต้องมีการตรวจรับจากผู้มีอำนาจ
- ต้องเก็บรายละเอียดของคำขอไว้ เป็นต้น

โดยดำเนินการตามระเบียบปฏิบัติ เรื่อง การจัดการเปลี่ยนแปลงระบบสารสนเทศ (Change Management) (P-IT-CO-๐๖)

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

เมื่อระบบปฏิบัติการมีการแก้ไขหรือเปลี่ยนแปลง ผู้พัฒนาระบบสารสนเทศจะต้องตรวจสอบและทดสอบซอฟต์แวร์ต่างๆที่ใช้งานว่าไม่มีผลกระทบต่อการทำงานและความมั่นคงปลอดภัย

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)

หน่วยงานต้องมีการจัดทำหรือป้องกันสภาพแวดล้อมในการทำงานต่างๆ ให้มีความเหมาะสมและปลอดภัย ทั้งการพัฒนาและปรับปรุงระบบเพิ่มเติมตลอดวงจรชีวิตของการพัฒนาระบบ

๑๐.๒.๗ การจ้างหน่วยงานภายนอกเพื่อพัฒนาระบบงาน (Outsourced Development)

ในการทำสัญญาว่าจ้างการพัฒนาระบบของโรงพยาบาลปางศิลาทอง ต้องมีความชัดเจนและครอบคลุมถึงสัญญา ทางด้านลิขสิทธิ์ซอฟต์แวร์ 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 และทำการบันทึกไว้เป็นหลักฐานว่าได้นำข้อมูลจริง ไปใช้ในการทดสอบอะไรบ้าง รวมถึงวัน เวลา และหน่วยงานที่ทดสอบ แจ้งไปยังผู้รับผิดชอบในการรักษาข้อมูลนั้นอีกครั้ง

หมวดที่ ๑๑ ความสัมพันธ์กับผู้ให้บริการภายนอก (Supplier relationships)

๑๑.๑ ความมั่นคงปลอดภัยสารสนเทศกับความสมพันธ์กับผู้ให้บริการภายนอก (Information security in supplier relationships)

วัตถุประสงค์: เพื่อให้มีการป้องกันทรัพย์สินขององค์กร ที่มีการเข้าถึงโดยผู้ให้บริการภายนอก

นโยบาย

๑๑.๑.๑ นโยบายความมั่นคงปลอดภัยสารสนเทศด้านความสัมพันธ์กับผู้ให้บริการภายนอก (Information security policy for supplier relationships)

หน่วยงานจะต้องกำหนดให้มีการจัดทำข้อกำหนด หรือสัญญาร่วมกันระหว่างหน่วยงานกับผู้ให้บริการภายนอก และต้องจัดทำเป็นลายลักษณ์อักษร โดยปฏิบัติตาม Procedure เรื่อง การให้บริการของหน่วยงานภายนอก (P-IT-TP-๐๑)

๑๑.๑.๒ การระบุความมั่นคงปลอดภัยในข้อตกลงการให้บริการภายนอก (Assessing security within supplier agreements)

๑) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ต้องระบุและจัดทำข้อกำหนด ข้อตกลง หรือสัญญาร่วมกันระหว่าง หน่วยงานกับผู้ให้บริการภายนอก ที่เกี่ยวข้องกับความมั่นคงปลอดภัยสำหรับสารสนเทศ โดยปฏิบัติตามระเบียบ ปฏิบัติ เรื่อง การให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management) (P-IT-TP-๐๑)

๒) ผู้ดูแลระบบต้องให้สิทธิการเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

๓) การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอก ต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

๔) ผู้ให้บริการภายนอกต้องลงนามในเอกสารนโยบายการใช้งานที่ยอมรับได้ (Acceptable Use Policy: AUP) และบันทึกข้อตกลงการไม่เปิดเผยข้อมูล (Non-Disclosure Agreement : NDA)

๕) สัญญาระหว่างหน่วยงาน และ หน่วยงานภายนอก ในการให้บริการ ต้อง ระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้

- รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ
- ระดับการให้บริการ (Service Level)
- หน้าที่และความรับผิดชอบขององค์การและหน่วยงานภายนอก ในการให้บริการในครั้งนี้
- ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้
- ราคำ และเงื่อนไขการชาระเงิน
- ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)
- การรักษาความลับของข้อมูลทีได้รับจากการให้บริการแก่องค์การ

๑๑.๑.๓ ห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสารโดยผู้ให้บริการภายนอก (Information and communication technology supply chain)

๑) ข้อตกลงกับผู้ให้บริการภายนอก ต้องรวมถึงความต้องการเรื่องการระบุความเสี่ยงอันเกิดจากห่วงโซ่ของการให้บริการเทคโนโลยีสารสนเทศและการสื่อสาร

๒) ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ ใช้ในการประมวลผลโดยหน่วยงานภายนอก 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) โรงพยาบาลปางศิลาทอง ต้องจัดทำข้อตกลง กำหนดสิทธิ์สำหรับโรงพยาบาลปางศิลาทอง ที่จะตรวจสอบสภาพแวดล้อมการทำงาน รวมทั้งการ
ตรวจสอบการทำงานของหน่วยงานภายนอก โดยพิจารณาจากสัญญาจัดซื้อจัดจ้างของหน่วยงานภายนอก

๒) ต้องมีการทบทวนติดตามและตรวจประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอ

๓) การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ของโรงพยาบาลปางศิลาทอง

๑๑.๒.๒ การบริหารจัดการ การเปลี่ยนแปลงบริการของผู้ให้บริการภายนอก (Managing Changes to Supplier Services)

๑) การเปลี่ยนแปลงรายละเอียดการให้บริการของหน่วยงานภายนอก ที่เกี่ยวข้องกับบริการด้านสารสนเทศของโรงพยาบาลปางศิลาทอง ทุกครั้ง ต้องเป็นไปตามเอกสารระเบียบปฏิบัติ เรื่อง การให้บริการของหน่วยงานภายนอก (Third Party Service Delivery Management) (P-IT-TP-๐๑)

๒) การเปลี่ยนแปลงต่อการให้บริการของผู้ให้บริการภายนอกรวมทั้งการปรับปรุงนโยบาย ขั้นตอนการปฏิบัติ และมาตรการที่ใช้อยู่ในปัจจุบันต้องมีการบริหารจัดการ โดยต้องนาระดับความสำคัญของสารสนเทศ และกระบวนการทางธุรกิจที่เกี่ยวข้องมาพิจารณาด้วย และต้องมีการทบทวนการประเมินความเสี่ยงใหม่

หมวดที่ ๑๒ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Incident Management)

๑๒.๑ การบริหารจัดการเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศและการปรับปรุง (Management of information security incidents and improvements)

วัตถุประสงค์: เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของสำนักงาน ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

นโยบาย

๑๒.๑.๑ หน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ (Responsibilities and Procedures)

ISS ต้องกำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ เพื่อรับมือกับเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของหน่วยงานและขั้นตอนดังกล่าวต้องมีความรวดเร็ว ได้ผล และมีความเป็นระบบระเบียบที่ดี (P-IT-IM-๐๑)

๑๒.๑.๒ การรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Events)

๑) ผู้ใช้งานต้องรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลปางศิลาทอง โดยผ่านช่องทางรายงานที่กำหนดไว้

๒) ผู้ใช้งานและบุคคลภายนอกทุกคนมีหน้าที่รายงานเหตุละเมิดความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในโรงพยาบาลปางศิลาทอง ต่อผู้บังคับบัญชา หรือหน่วยงานจัดการความปลอดภัย (Security Management) ทันทีที่พบเหตุ เพื่อให้สามารถดำเนินการแก้ไขปัญหาได้อย่างทันท่วงที

๓) ผู้ใช้งานที่พบหรือรับทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาด หรือจุดอ่อนของซอฟต์แวร์ ต้องรายงานต่อ ISS ทันที

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

๕) ผู้ใช้งานและบุคคลภายนอกที่พบเหตุละเมิดความมั่นคงปลอดภัยหรือจุดอ่อนใด ๆ ในโรงพยาบาลปางศิลาทอง ต้อง ไม่บอกเล่าเหตุการณ์ที่เกิดขึ้นกับผู้อื่น ยกเว้น ผู้บังคับบัญชา หน่วยงานจัดการความปลอดภัย (Security Management) และห้ามทำการพิสูจน์ข้อสงสัยเกี่ยวกับจุดอ่อนด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

๑๒.๑.๓ การรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Reporting Information Security Weaknesses)

ISS ต้องบันทึกและรายงานจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยของโรงพยาบาลปางศิลาทอง ที่สังเกตุพบหรือ เกิดความสงสัยในระบบหรือบริการที่ใช้งานอยู่

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

๑) สถานการณ์ความมั่นคงปลอดภัยสารสนเทศต้องมีการประเมินและต้องมีการตัดสินว่าสถานการณ์นั้นถือเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศหรือไม่

๒) จัดทำเกณฑ์ในการตัดสินเหตุการณ์ที่ถือว่าเป็นเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ

๑๒.๑.๕ การตอบสนองต่อเหตุการณ์ความมั่นคงปลอดภัย
สารสนเทศ (Response to information security incidents)

๑) ISS ต้องมีการกำหนดขั้นตอนไว้รองรับกรณีเกิดเหตุการณ์ที่ประเมินแล้วว่าก่อให้เกิดความไม่มั่นคงปลอดภัย

๒) เมื่อเกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศต้องได้รับการตอบสนองเพื่อจัดการกับปัญหาตามขั้นตอนปฏิบัติที่จัดทำไว้เป็นลายลักษณ์อักษร

๓) โดยได้จัดทำแยกประเภทตามระบบต่าง ๆ ดังนี้

๓.๑) ระบบป้องกันผู้บุกรุก

๓.๑.๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุก สิ่งที่ทำการตรวจสอบมี ดังต่อไปนี้

- มีการโจมตีมากน้อยเพียงใด และเป็นการโจมตีประเภทใดมากที่สุด
- ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคำดเดาได้หรือไม่
- ระดับความรุนแรงมากน้อยเพียงใด
- 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 เป็นจานวนมาก

๓.๒.๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้ แจ้งหัวหน้าหน่วยงาน เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๓.๓) ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

๓.๓.๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัย คุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบมีดังนี้

- มัลแวร์ประเภทใดถูกพบเป็นจานวนมาก
- มัลแวร์ถูกส่งมาจากเครือข่ายใด และถูกส่งไปยังที่ใด
- มีการส่งมัลแวร์จากเครือข่ายภายในโรงพยาบาลปางศิลาทองไปยังภายนอกหรือไม่

๓.๓.๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจาย อยู่ในเครือข่ายของโรงพยาบาลปางศิลาทอง

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) ต้องรวบรวมและจัดเก็บหลักฐานตามกฎหรือหลักเกณฑ์สำหรับการเก็บหลักฐานอ้างอิงในกระบวนการทางศาลที่เกี่ยวข้อง เมื่อพบว่าเหตุการณ์ที่เกิดขึ้นนั้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมายแพ่งหรืออาญา

หมวดที่ ๑๓ ประเด็นด้านความมั่นคงปลอดภัยสารสนเทศของการบริหารจัดการเพื่อสร้างความต่อเนื่องทางธุรกิจ
(Information Security Aspects of Business Continuity Management)

๑๓.๑ ความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ (Information security continuity)

วัตถุประสงค์: เพื่อป้องกันการหยุดชะงักในการดำเนินงานของโรงพยาบาลปางศิลาทอง ที่เป็นผลมาจากความล้มเหลวหรือการ หยุดทำงานของระบบ

นโยบาย

๑๓.๑.๑ การวางแผนความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
(Planning information security continuity)

๑) องค์กรต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ และด้านความต่อเนื่องในสถานการณ์ความเสียหายที่เกิดขึ้น เช่น ในช่วงที่เกิดวิกฤตหรือภัยพิบัติ

๒) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแนวทางปฏิบัติ ในการจัดทำแผนรองรับเหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ควรพิจารณา ดังนี้

๓) การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของโรงพยาบาลปางศิลาทอง และการให้ บริการด้านเทคโนโลยีสารสนเทศ
สำนักงาน ฯ

๔) การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทาง การควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น

๕) การดำเนินการเพื่อให้โรงพยาบาลปางศิลาทอง สามารถดำเนินงานเป็นไปได้อย่างต่อเนื่อง เช่น การสารองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น

๖) การกลับคืนสู่การทางานปกติ เพื่อให้การดำเนินงานโรงพยาบาลปางศิลาทอง กลับสู่สภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น

๑๓.๑.๒ การปฏิบัติเพื่อเตรียมการสร้างความต่อเนื่องด้านความมั่นคงปลอดภัยสารสนเทศ
(Implement information security continuity)

๑) โรงพยาบาลปางศิลาทอง ต้องจัดตั้ง ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ของระบบเทคโนโลย สารสนเทศ

๒) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องจัดทำแผนรองรับ เหตุการณ์ฉุกเฉินของระบบเทคโนโลยีสารสนเทศ ที่เป็นลายลักษณ์อักษร และปรับ ปรุงแก้ไขให้ทันสมัยอยู่เสมอ รวมถึงการจัดให้มีการทดสอบ แผนอย่างน้อยปีละ ๑ ครั้ง โดยปฏิบัติตามเอกสาร ระเบียบปฏิบัติ เรื่อง การจัดทำแผนการบริหารความต่อเนื่องให้กับ ธุรกิจ (Business Continuity Plans Development and Execution Procedure) (P-IT-BC-๐๑)

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

๑) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องกำหนดเวลาการทดสอบแผน กำหนดการ ทดสอบแผนฉุกเฉินที่ชัดเจน รวมถึงกำหนดระยะเวลาที่ใช้ในการทดสอบตั้งแต่เริ่มต้น จนสิ้นสุดกระบวนการทดสอบ

๒) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องกำหนดเหตุการณ์จาลองที่จะใช้ทดสอบและรายละเอียด ในการกำหนดรายละเอียดของเหตุการณ์จาลอง ควรระบุวัตถุประสงค์ ขอบเขตของระบบงาน หรือกระบวนการทำงานที่เกี่ยวข้องกับการทดสอบแผนทั้งหมด รวมถึงการกำหนดขั้นตอนการทดสอบแผนฉุกเฉิน

๓) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องกำหนดทรัพยากรต่างๆ ที่ใช้ในการทดสอบแผนฉุกเฉิน กำหนดผู้รับผิดชอบที่จะทำหน้าที่ควบคุม ประสานงาน และรับผิดชอบในการจัดการทดสอบแผนฉุกเฉิน รวมถึงสถานที่ และอุปกรณ์เครื่องมือต่างๆ และงบประมาณที่ต้องใช้ด้วย

๔) ISS (บริหารจัดการแผนสร้างความต่อเนื่องให้กับธุรกิจ) ต้องกำหนดแผนงาน แนวทาง และระยะเวลาในการทบทวนและปรับปรุงแผนอย่างชัดเจน เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

๑๓.๒ การเตรียมอุปกรณ์ประมวลผลสารอง (Redundancies)

วัตถุประสงค์: เพื่อจัดเตรียมสภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนเทศ

นโยบาย

๑๓.๒.๑ สภาพความพร้อมใช้งานของอุปกรณ์ประมวลผลสารสนทศ
(Availability of information processing facilities)

อุปกรณ์ประมวลผลสารสนเทศต้องมีการเตรียมการสารองไว้อย่างเพียงพอ เพื่อให้ตรงตามความต้องการด้านสภาพความพร้อมใช้ที่กำหนด

หมวดที่ ๑๔ การปฏิบัติตามข้อกำหนดทางด้านกฎหมาย และบทลงโทษของการละเมิดนโยบายความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน (Compliance)

๑๔.๑ การปฏิบัติตามข้อกำหนดด้านกฎหมายและในสัญญาจ้าง (Compliance with Legal and Contractual Requirements)

วัตถุประสงค์: เพื่อหลีกเลี่ยงการฝ่าฝืนกฎหมายทั้งทางอาญาและทางแพ่ง พระราชบัญญัติ ระเบียบข้อบังคับรวมทั้งสัญญาต่าง ๆ

นโยบาย

๑๔.๑.๑ การระบุข้อกำหนดและความต้องการในสัญญาจ้างในการใช้งานระบบสารสนเทศ (Identification of Applicable Legislation and Contractual Requirements)

๑) โรงพยาบาลปางศิลาทอง ต้องมีการศึกษาและกำหนดรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

๒) เจ้าหน้าที่โรงพยาบาลปางศิลาทอง เจ้าหน้าที่โรงพยาบาลปางศิลาทอง ทุกคนต้องรับทราบ ทำความเข้าใจ และปฏิบัติ ตามรายการของนโยบาย กฎ ระเบียบข้อบังคับ กฎหมาย หรือสัญญาที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ และ การสื่อสารที่กำหนดขึ้นอย่างเคร่งครัด

๓) ข้อมูลที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปางศิลาทอง ถือเป็นทรัพย์สิน ของ โรงพยาบาลปางศิลาทอง (ยกเว้น ข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอกรวมถึงซอฟต์แวร์ หรือวัสดุอื่น ๆ ที่ ได้รับการคุ้มครองโดย สิทธิบัตร หรือลิขสิทธ์ของบุคคลภายนอก) ทั้งนี้โรงพยาบาลปางศิลาทอง สามารถเปิดเผยหรือใช้งาน ข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

๔) เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลปางศิลาทอง และขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์และระบบ เครือข่ายของผู้ใช้งานเพื่อให้มั่นใจว่ามีการใช้งานตรงตามที่นโยบายต่าง ๆ ของโรงพยาบาลปางศิลาทองกำหนดไว้

๕) ห้ามเจ้าหน้าที่โรงพยาบาลปางศิลาทอง ใช้งานทรัพย์สินและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปางศิลาทอง กระทำการใด ๆ ที่ขัดแย้งต่อกฎหมายแห่งราชอาณาจักรไทย และกฎหมายระหว่างประเทศ ไม่ว่าโดยกรณีใดก็ตาม

๖) การส่งซอฟต์แวร์ ข้อมูลลับ ซอฟต์แวร์การเข้ารหัส หรือเทคโนโลยีใด ๆ ออกนอกประเทศไม่ขัดต่อข้อกฎหมายใด ๆ ทั้งของราชอาณาจักรไทย ระหว่างประเทศ และของประเทศปลายทาง ทั้งนี้ผู้ใช้งานต้องปรึกษาผู้บังคับบัญชา และผู้เชียวชาญด้านกฎหมายก่อนดำเนินการส่งออก

๑๔.๑.๒ ทรัพย์สินทางปัญญา (Intellectual Property Rights)

๑) ต้องปฏิบัติตามข้อกำหนดทางลิขสิทธิ์ (Copyright) ในการใช้งานทรัพย์สินทางปัญญาที่หน่วยงานจัดหามาใช้งานและต้องระมัดระวังที่จะไม่ละเมิด

๒) ต้องปฏิบัติตามข้อกำหนดที่ระบุไว้ในลิขสิทธิ์การใช้งานซอฟต์แวร์อย่างเคร่งครัด (Software Copyright) รวมทั้งต้องมีการควบคุมการใช้งานซอฟต์แวร์ตามลิขสิทธิ์ที่ได้รับด้วย

๓) ห้ามผู้ใช้งานทำการใช้งาน ทำซ้ำ หรือเผยแพร่ รูปภาพ บทเพลง บทความ หนังสือ หรือเอกสารใด ๆ ที่เป็นการละเมิดลิขสิทธิ์ หรือติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์บนระบบเทคโนโลยีสารสนเทศของโรงพยาบาลปางศิลาทอง โดยเด็ดขาด

๑๔.๑.๓ การป้องกันข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงในการปฏิบัติตามข้อกำหนด (Protection of Records)

ต้องจัดเก็บข้อมูลเพื่อใช้เป็นหลักฐานอ้างอิงว่าได้ปฏิบัติตามข้อกำหนดทางด้านกฎ ระเบียบ หรือข้อบังคับ ที่ได้กำหนดไว้ โดยมีระยะเวลาจัดเก็บตามความสำคัญของข้อมูล ระเบียบหน่วยงานว่าด้วยงานสารบรรณ และกฎหมาย เช่น ระเบียบสำนักนายกรัฐมนตรี

๑๔.๑.๔ ความเป็นส่วนตัวและการป้องกันข้อมูลส่วนบุคคล
(Privacy and protection of personally identifiable information)

โรงพยาบาลปางศิลาทอง ต้องมีการการป้องกันข้อมูลและความเป็นส่วนตัวตามกฎหมาย ระเบียบ สัญญาที่เกี่ยวกับ โรงพยาบาลปางศิลาทอง

๑๔.๑.๕ การควบคุมการเข้ารหัส (Regulation of cryptographic controls)

โรงพยาบาลปางศิลาทอง ต้องมีการควบคุมการเข้ารหัสข้อมูล ตามข้อตกลง กฎหมาย และระเบียบที่เกี่ยวข้อง

๑๔.๒ การทบทวนความมั่นคงปลอดภัยสารสนเทศ (Information Security Reviews)

วัตถุประสงค์: เพื่อให้มีการปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ อย่างสอดคล้องกับนโยบายและขั้นตอนปฏิบัติขององค์กร

นโยบาย

๑๔.๒.๑ การทบทวนอย่างอิสระด้านความมั่นคงปลอดภัยสารสนเทศ
(Independent review of information security)

IST ต้องมีการทบทวน วิธีการในการบริหารจัดการความมั่นคงปลอดภัยสารสนเทศและการปฏิบัติขององค์กร เช่น ทบทวนวัตถุประสงค์ มาตรการ นโยบาย ระเบียบปฏิบัติ ต่างๆ ให้ถูกต้องและเป็นปัจจุบันตามรอบระยะเวลาที่กำหนด อย่างน้อยปีละ ๑ ครั้ง หรือทบทวนเมื่อมีการเปลี่ยนแปลง

๑๔.๒.๒ การตรวจสอบความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของหน่วยงาน (Compliance with Security Policy and Standards)

๑) IST ต้องจัดให้มีการตรวจสอบระบบทั้งหมดของหน่วยงานตามนโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศและระยะเวลาที่กำหนดไว้

๒) IST ต้องมีการตรวจสอบและทบทวนเอกสารนโยบาย มาตรการ วิธีการปฏิบัติงานรวมถึงแบบฟอร์มที่ เกี่ยวเนื่องกันตามระยะเวลาที่กำหนดหรือเมื่อมีการเปลี่ยนแปลง

๑๔.๒.๓ การทบทวนความสอดคล้องทางเทคนิค (Technical Compliance Review)

IST ต้องจัดให้มีการตรวจสอบรายละเอียดทางเทคนิคของระบบที่ใช้งาน หรือให้บริการอยู่แล้วอย่างน้อยปีละ ๑ ครั้ง ว่ามีความมั่นคงปลอดภัยสารสนเทศอย่างพอเพียงหรือไม่ ได้แก่ การตรวจดูว่าระบบสามารถถูกบุกรุกได้หรือไม่ การปรับแต่งค่าพารามิเตอร์ที่ระบบใช้งานเป็นไปอย่างปลอดภัยหรือไม่ รวมทั้งมีการตรวจสอบระบบโดยทำการใช้ ซอฟต์แวร์ค้นหาช่องโหว่ (Vulnerability Scanning) และ/หรือ ทดสอบการโจมตีระบบ (Penetration Test) เพื่อ ตรวจสอบข้อบกพร่องของระบบด้วย