นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
โรงพยาบาลป่าพะยอม

PAPHAYOM HOSPITAL โรงพยาบาลป่าพะยอม	นโยบาย เรื่อง: นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	หน้า : ๑/๒๐
ชื่อหน่วยงาน : งานสุขภาพดิจิทัล		วันที่เริ่มใช้ : ๔ สิงหาคม ๒๕๖๘
ผู้ตรวจสอบ : (นางสาวพรทิพย์ ชูแป้น) พยาบาลวิชาชีพชำนาญการ		ผู้อนุมัติ : (นางสาวธัญลักษณ์ คงฤทธิ์) นายแพทย์ชำนาญการ รักษาการในตำแหน่ง ผู้อำนวยการโรงพยาบาลป่าพะยอม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล (Information Access Control)
๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
๕. การใช้งานอินเทอร์เน็ต (Use of the Internet)
๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย
๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๑๐. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ให้งานร่วมกัน
๑๑. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)
๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)
๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)
๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ส่วนที่ ๒ นโยบายการจัดการ ระบบสำรองสารสนเทศ

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness)

ความเป็นมา

๑.หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทางธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆมีความมั่นคงปลอดภัยเชื่อถือโรงพยาบาลป่าพะยอม ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลป่าพะยอมเป็นไปอย่างเหมาะสมมีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่องและป้องกันภัยคุกคามต่างๆและการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆที่เกี่ยวข้องและการป้องกันปัญหาที่อาจจะเกิดขึ้น จากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องตลอดจนการถูกคุกคามจากภัยต่างๆ

๒.วัตถุประสงค์

โรงพยาบาลป่าพะยอม ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลป่าพะยอมเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลป่าพะยอมและทำให้ดำเนินงานต่างๆเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลป่าพะยอม มีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนอง ต่อพันธ กิจและนโยบายของโรงพยาบาล

๓.๒ เน้นกำกับดูแล การดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความ ถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับทั้งของโรงพยาบาลเองและหน่วยงานที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษา ความมั่นคง ปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของโรงพยาบาลเพื่อให้ผู้ใช้งานผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชีผู้ใช้สารสนเทศของโรงพยาบาลโดยเคร่งครัด

ผู้รับผิดชอบ

๑. งานสารสนเทศ กลุ่มงานสุขภาพดิจิทัล
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย อ้างอิงมาตรฐาน มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบ ธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล(Information Access Control)

๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

๑.๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดสิทธิการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล ดังนี้

๑.๒.๑ ไม่มีสิทธิ
๑.๒.๒ อ่านได้อย่างเดียว
๑.๒.๓ สร้างข้อมูล
๑.๒.๔ ป้อนข้อมูล
๑.๒.๕ แก้ไขข้อมูล
๑.๒.๖ ลบข้อมูล
๑.๒.๗ อนุมัติการใช้ข้อมูล

๑.๓ กำหนดประเภทข้อมูลของโรงพยาบาลเป็น ๖ ประเภทหลักๆ ดังนี้

๑.๓.๑ ข้อมูลผู้ป่วย
๑.๓.๒ ข้อมูลบุคลากร
๑.๓.๓ ข้อมูลการเงินและบัญชี
๑.๓.๔. ข้อมูลทางการแพทย์
๑.๓.๔. ข้อมูลทางการบริหาร
๑.๓.๖. ข้อมูลการจราจรทางคอมพิวเตอร์

๑.๔ กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของโรงพยาบาลเป็น ๔ ระดับดังนี้

๑.๔.๑ ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๔.๒ ใช้ภายในเท่านั้นเป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างหน่วยงานหรือข้อมูลที่เผยแพร่เฉพาะภายในโรงพยาบาล

๑.๔.๓ ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น

๑.๔.๔ เปิดเผยได้เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกโรงพยาบาล

๑.๕ เกณฑ์ในการกำหนดชั้นความลับของข้อมูล

๑.๕.๑ ประเภทลับ หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๕.๒ ประเภทใช้ภายในเท่านั้น หมายถึง ข้อมูลที่สื่อสารกันในฝ่ายงานหรื หน่วยงาน หรือข้อมูล ที่เผยแพร่เฉพาะภายในโรงพยาบาล

๑.๕.๓ ประเภทส่วนบุคคล หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแล ข้อมูลนั้น

๑.๕.๔ ประเภทเปิดเผยได้หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกโรงพยาบาล

๑.๖ กำหนดระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาลดังนี้

๑.๖.๑ การเข้าถึงสำหรับผู้บริหาร

๑.๖.๒ การเข้าถึงสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

๑.๖.๓ การเข้าถึงสำหรับผู้ดูแลระบบ

๑.๖.๔ การเข้าถึงระดับบุคคล

๑.๖.๕ การเข้าถึงระดับผู้ใช้งานทั่วไป

๑.๗ เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล

๑.๗.๑ ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๑.๗.๒ ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

๑.๗.๓ ผู้ดูแลระบบ มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตาม อำนาจหน้าที่

๑.๗.๔ บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

๑.๗.๕ ผู้ใช้”งานทั่วไป” เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แกไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

๑.๗.๖ การกำหนดสิทธิพิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

๑.๗.๗ การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิหรือหน่วยงานหลักเท่านั้น

๑.๘ กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศ ของโรงพยาบาลในแต่ละประเภทดังนั้น

๑.๘.๑ ข้อมูลผู้ป่วยหน่วยงานหลักคือเวชระเบียนและงานสารสนเทศ

๑.๘.๒ ข้อมูลบุคลากร หน่วยงานหลักคืองานการเจ้าหน้าที่

๑.๘.๓ ข้อมูลการเงินและบัญชีหน่วยงานหลักคือการเงินและบัญชี

๑.๘.๔ ข้อมูลทางการแพทย์ขึ้นอยู่กับหน่วยงานที่โรงพยาบาลมอบหมายเป็นหน่วยงานหลัก

๑.๘.๕ ข้อมูลทางการบริหารขึ้นอยู่กับหน่วยงานที่โรงพยาบาลมอบหมายเป็นหน่วยงานหลัก

๑.๘.๖ ข้อมูลการจราจรทางคอมพิวเตอร์ศูนย์คอมพิวเตอร์และหน่วยงานที่ให้บริการระบบสารสนเทศ

๑.๘.๗ การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจของโรงพยาบาล

๑.๙ การควบคุมการเปลี่ยนแปลง

๑.๙.๑ การเปลี่ยนแปลงใดๆที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการ ดังนี้

(๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงรวมทั้งวางแผนด้านงบประมาณที่ จำเป็นต้องใช้ในการเปลี่ยนแปลง

(๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคลเหล่านั้นมี เวลา เพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

(๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

๑.๙.๒ ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ ในสถานที่ที่มีความมั่นคงปลอดภัยเพื่อให้สามารถน่ากลับมาใช้ได้เมื่อจำเป็น

๑.๑๐ การกำหนดการใช้งานตามภารกิจ

๑.๑๐.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) บุคลากร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิเมื่อพ้นสภาพการเป็นบุคลากรและเปลี่ยนรหัสผ่านใหม่ทุก ๙๐ วัน (๒) ผู้บริหารจะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิเมื่อพ้นสภาพการเป็นผู้บริหาร

(๒) บุคคลภายนอกได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

๑.๑๐.๒ ข้อจำกัดในการเข้าถึง

(๑) บุคลากร เข้าถึงได้ตามสิทธิเบื้องต้นและภารกิจที่ได้รับมอบหมาย

(๒) ผู้บริหาร เข้าถึงตามสิทธิและภารกิจที่ได้รับมอบหมาย

(๓) บุคคลภายนอก เข้าถึงได้ตามที่ได้รับอนุญาต

๑.๑๑ ระยะเวลาการใช้งาน

๑.๑๑.๑ ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานจะเข้าถึงและใช้งานได้ดังนี้ (๑) การเข้าถึงในเวลาราชการ ๐๘.๐๐-๑๖.๐๐ น.

(๒) การเข้าถึงนอกเวลาราชการ หลัง ๑๖.๓๐ น. เป็นต้นไป (๓) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนักขัตฤกษ์

๑.๑๑.๒ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(๑) กำหนดให้ระบบสารสนเทศที่มีความเลี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ ต้องตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต (๒) ต้องจากัดช่วงระยะเวลาการเชื่อมต่อสาหรับระบบสารสนเทศความเลี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ

๑.๑๒ การหมดสิทธิการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๒.๑ บัญชีผู้ใช้หมดอายุ

๑.๑๒.๒ เมื่อมีการเปลี่ยนแปลงสิทธิการเข้าถึง

๑.๑๒.๓ ถูกระงับสิทธิ

๑.๑๓ การทบทวนและตรวจสอบสิทธิการเข้าถึงและการใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๓.๑ ทบทวนและตรวจสอบสิทธิการเข้าถึงและใช้งานระบบสารสนเทศปีละ ๑ ครั้ง โดย ผู้ดูแลระบบพิมพ์ราย'ชื่อ'ของผู้ที่ยังมีสิทธิในระบบแยกตามคณะ/หน่วยงาน,ที่ขอสิทธิ จัดส่งรายชื่อนั้นให้กับหน่วยงานที่ขอสิทธิเพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือไม่หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๑.๑๓.๒ หน่วยงานผู้ขอสิทธิแจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

๑.๑๓.๓ หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิของผู้ใช้ อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับขั้นการเข้าถึงและการใช้งานระบบทันที

๑.๑๔ ช่องทางการเข้าถึง

๑.๑๔.๑ เครือข่ายภายในโรงพยาบาล

๑.๑๔.๒ เครือข่ายภายนอกโรงพยาบาล

๑.๑๔.๓ เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑.๑ การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานต้องจัดทาหลักสูตรการฝึกกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้าน สารสนเทศ

๒.๑.๒ อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่างถูกต้องรวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง

๒.๑.๓ ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวัง ในรูปแบบที่สามารถเข้าใจและนาไปปฏิบัติได้ง่าย

๒.๒ การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบสารสนเทศของโรงพยาบาล จัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศของโรงพยาบาล ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้งาน ออกเป็น ๓ กลุ่มคือ

๒.๒.๑ บุคลากรของโรงพยาบาล

๒.๒.๒ บุคคลภายนอก ที่มาประชุมร่วมที่โรงพยาบาล แขกของหน่วยงาน

๒.๒.๓ หน่วยงานภายนอก (outsource) เชื่อมระบบงานภายในหน่วยงานที่โรงพยาบาลมอบสิทธิให้

๒.๓ การลงทะเบียนผู้ใช้งาน

๒.๓.๑ บุคลากรของโรงพยาบาล บุคลากรดาวน์โหลดแบบฟอร์มที่เว็บไซต์โรงพยาบาลหรือจากงานสารสนเทศ กลุ่มงานสุขภาพดิจิทัล กรองข้อมูลให้ครบพร้อมแนบสำเนาบัตรประชาชน ส่งที่งานสารสนเทศ กลุ่มงานสุขภาพดิจิทัลและงานสารสนเทศ กลุ่มงานสุขภาพดิจิทัลลงทะเบียนในระบบให้

๒.๒.๒ บุคคลภายนอก ที่มาประชุมร่วมที่โรงพยาบาล แขกของหน่วยงาน งานสารสนเทศลงทะเบียน ใช้งานให้เป็นครั้งคราวและจะยกเลิกสิทธิการใช้งานภายใน๒๔ ชั่วโมง

๒.๒.๓ หน่วยงานภายนอก(outsource)เชื่อมระบบงานภายในหน่วยงานที่โรงพยาบาลมอบสิทธิให้ งานสารสนเทศจะกำหนดสิทธิให้บางโมดูลของงาน

๒.๔ การจัดการบัญชีผู้ใช้ของโรงพยาบาล

๒.๕. การจัดการสิทธิของผู้ใช้งาน

๒.๖ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๖.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านมีความมั่นคงปลอดภัย

๒.๖.๒ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๒.๖.๓ ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง

๒.๖.๔. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราวและต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๒.๖.๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยนรหัสผ่านจาก ผู้ดูแลระบบ

๒.๖.๖ ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็นเวลานาน

๒.๖.๗ กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนาไปใช้ โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธการใช้งานขั้วคราวจนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๒.๗ การทบทวนสิทธิการเข้าถึง

๒.๗.๑ ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๒.๗.๒ บัญชีผู้ใช้จะหมดอายุ ดังนี้

(๑) กรณีบุคลากร หมดอายุเมื่อย้ายหรือลาออกจากโรงพยาบาล

(๒) กรณีบุคคลภายนอก สิทธิการเข้าใช้งานระบบสารสนเทศจะหมดตามระยะเวลาที่กำหนดในการเข้าใช้งานระบบ

(๓) กรณีที่ไม่ใช่บุคลากรหน่วยงานภายนอก (outsource) เชื่อมระบบงานภายในหน่วยงานที่ โรงพยาบาลมอบสิทธิให้หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี หรือ เมื่อไม่มีการเข้าใช้งาน ติดต่อกันเกิน ๓ เดือน

๓. การกำหนดหน้าที่ความรับผิดขอบของผู้ใช้งาน (User Responsibilities)

๓.๑. การใช้งานบัญชีผู้ใช้และรหัสผ่าน

๓.๑.๑ ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมี บัญชีชื่อผู้ใช้ของตนเองและห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๓.๑.๒. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๓.๒ การใช้งานรหัสผ่าน

๓.๒.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่โรงพยาบาลกำหนด

๓.๒.๒ ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น วันเดือน ปีเกิด เป็นต้น ต้องประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน

๓.๒.๓ ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๓.๒.๔ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๓.๒.๕ หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิใช้งาน

๓.๒.๖. เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๓.๓ การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

๓.๓.๑ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพ เมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๓.๓.๒ ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแล

๓.๓.๓ ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๓.๔ การจัดวางและการป้องกันอุปกรณ์

๓.๔.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับ อนุญาต

๓.๔.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๓.๔.๓ ดำเนินการตรวจสอบ สอดล่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๕ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๕.๑ จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๓.๕.๒ ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของ หรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

๓.๕.๓ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึง ข้อมูลสำคัญได้

๓.๕.๔ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการ สูญหายหรือการ

เข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๕.๕ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๔๔๔

๓.๕.๖ จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสาร ตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่โรงพยาบาลต้องปฏิบัติตาม

๓.๕.๗ ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลาย หรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๓.๕.๘ สำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสารอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือ ทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อ บันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๓.๖ การป้องกันโปรแกรมไม่ประสงค์ดี

๓.๖.๑ ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ ประสงค์ดีรวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๓.๖.๒ ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๓.๖.๓ ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศผ่านทางระบบเครือข่ายและผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดีก่อนการรับส่งทุกครั้ง

๓.๖.๔ ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดีก่อนการเปิดใช้สามารถประมวลผลได้ (Executable file) เช่นไฟล์นามสกุล .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑ การเข้าใช้งานระบบเครือข่ายของโรงพยาบาล

๔.๑.๑ การเข้าถึงระบบเครือข่ายของโรงพยาบาลจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่โรงพยาบาล ออกให้

๔.๑.๒ ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่ายสามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตาม สิทธิที่ได้รับอนุญาตเท่านั้น

๔.๑.๓ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับงานสารสนเทศ

๔.๑.๔ จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกันรวมทั้งตรวจสอบเปิด-ปิดพอร์ตอุปกรณ์เครือข่ายตามความจำเป็น

๔.๑.๕ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๔.๑.๖ การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของโรงพยาบาล ต้องขออนุญาตใช้บัญชีชั่วคราวจากโรงพยาบาล ซึ่งจะเข้าถึงได้ตามสิทธิที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

๔.๒.การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๔.๒.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในโรงพยาบาล จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและได้รับการพิจารณาอนุญาตจากงานสารสนเทศ

๔.๒.๒ ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานและป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นาอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสาหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณและต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณด้วยวิธีที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูลและทำให้ปลอดภัยมากขึ้น

(๗) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในโรงพยาบาล

(๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการทราบโดยทันที

๔.๓ การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๔.๓.๑ อุปกรณ์ที่นามาเชื่อมต่อได้รับหมายเลข IP Address ตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๔.๓.๒ เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลข IP Address (DHCP Server)

๔.๔ การป้องกันพอร์ตที่ใช้สาหรับตรวจสอบและปรับแต่งระบบ

๔.๔.๑ ต้องควบคุมพอร์ตและหมายเลข IP Address ที่ใช้สาหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๔.๔.๒ ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่ายเมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๔.๔.๓ ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกโรงพยาบาลแต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่โรงพยาบาล กำหนด เช่น VPN เป็นต้น

๔.๔.๔ อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๔.๔.๕ ต้องปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔.๔.๖ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง

๔.๕ การแบ่งแยกเครือข่าย (segregation in networks)

๔.๕.๑ ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔.๕.๒ แบ่งแยกเครือข่ายตามกลุ่มของบริการกลุ่มผู้ใช้และระบบงานต่างๆของโรงพยาบาล

๔.๕.๓ ต้องใช้ไฟร์วอลล์ (Firewall) กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๔.๕.๔ ต้องใช้เกตเวย์ เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงานซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๔.๖ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

๔.๖.๑ อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลข IP Address ที่กำหนด

๔.๖.๒ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๔.๖.๓ ต้องตรวจสอบหมายเลข IP Address ของต้นทางและปลายทาง

๔.๖.๔ ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๔.๖.๕ ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๔.๖.๖ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

๔.๗. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกโรงพยาบาล (User Authentication for External Connections)

๔.๗.๑ ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๔.๗.๒ ผู้ใช้งานที่อยู่ภายนอกหน่วยงานต้องเป็นผู้ที่ได้รับสิทธิในการเข้าใช้บริการแล้วเท่านั้น

๔.๗.๓ ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของโรงพยาบาลโดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่านเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๕. การใช้งานอินเทอร์เน็ต (use of the Internet)

๕.๑ ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่โรงพยาบาลจัดสรรไว้ตามสิทธิที่ได้รับ

๕.๒ ห้ามใช้อินเทอร์เน็ตของโรงพยาบาลเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๕.๓ ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับโรงพยาบาล เป็นต้น

๕.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึงการดาวนโหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิหรือทรัพย์สินทางปัญญา

๕.๕ ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิธ)Bandwidth) จำนวนมากหรือเป็นเวลานาน

๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

๖.๑ กำหนดผู้ดูแลระบบสาหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๖.๒ มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือ เปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๖.๓ ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (time.psu.ac.th) ที่โรงพยาบาลใช้อ้างอิง

๖.๔ เปิดใช้บริการเท่าที่จาเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสาหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัยด้วย

๖.๕ ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอเพื่ออุดช่องโหว่ต่างๆ

๖.๖ ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๗ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

๗. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System access control)

๗.๑ ผู้ดูแลระบบ (System Administrator)

๗.๑.๑ ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์โรงพยาบาล

๗.๒ กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๗.๒.๑ ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๗.๒.๒ ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๗.๒.๓ จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๗.๒.๔ จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจาก อาจสร้างความเสียหายให้กับระบบได้

๗.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๗.๓.๑ ผู้ใช้งานต้องมีบัญชีผู้ใช้ และรหัสผ่านสำหรับเข้าใช้งานระบบสารสนเทศของโรงพยาบาล

๗.๔ การบริหารจัดการรหัสผ่าน (Password Management System)

๗.๔.๑ ต้องจำกัดระยะเวลาในการป้อนรหัสผ่านหากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้ง ที่ กำหนดระบบจะทำการล็อกสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

๗.๔.๒ ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๗.๔.๓ มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๗.๔.๔ ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๗.๔.๕ ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเองแต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๗.๔.๖ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๗.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System utilities)

๗.๕.๑ จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๗.๕.๒ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอกถ้าไม่ต้องใช้งานเป็นประจำ

๗.๕.๓ ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๗.๕.๔ ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๗.๕.๕ โปรแกรมที่ติดตั้งต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิถูกต้องตามกฎหมาย

๗.๕.๖ ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆแล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗.๖ การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

๗.๖.๑ ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่ เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูงให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๗.๖.๒ ถ้าไม่มีการใช้งานระบบ ต้องทาการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๗.๖.๓ เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิด เครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๘. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๘.๑ หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องแต่งตั้งผู้มีสิทธิและกำหนดจำนวนผู้มีสิทธิในการเข้าถึงระบบปฏิบัติการ

๘.๒ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านชองตัวเอง

๘.๓ ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๘.๔ ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๘.๕ ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติหรือไม่ปลอดภัย

๘.๖ ห้ามการติดตั้งซอฟต์แวร์อื่นๆหรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอกรวมทั้งการใช้ไฟล์อื่นโดยไม่อนุญาต

๘.๗ ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงาน สำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๘.๘ ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

๘.๙ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติสำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืน ระบบจากความเสียหายที่พบ เป็นต้น

๘.๑๐ ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๘.๑๑ ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมีความรู้ ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๙. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน

๙.๑ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๙.๒ ระบบต้องไม่แสดงรายละเอียดสำคัญก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๙.๓ ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อเมื่อพบว่ามีความพยายามคาดเดารหัสผ่าน

๙.๔ ระบบจะต้องจำกัดสิทธิผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

๑๐. การเข้าถึงโปรแกรม Hospital OS ระบบบันทึกบริการผู้ป่วยและระบบสารสนเทศ (application and information access control)

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ

๑๐.๑.๑ การจำกัดการเข้าถึงของผู้ใช้งาน

(๑) เข้าได้ตามสิทธิที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

(๓) ต้องบันทึกการออกจากระบบงานโดยทันที ที่ไข้งานเสร็จ

๑๐.๑.๒ แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของโรงพยาบาล ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่าง ชัดเจนเป็นลายลักษณ์อักษร

๑๐.๑.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศต้องบันทึกข้อมูล พฤติกรรมการใช้งาน การเข้าถึง

(๑) ระบบสารสนเทศที่สำคัญ ดังนี้

(๒) ชื่อบัญชีผู้ใช้

(๓) วันเวลาที่เข้าถึงระบบ

(๔) วันเวลาที่ออกจากระบบ

(๕) เหตุการณ์สำคัญที่เกิดขึ้น

(๖) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

(๗) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๘) แสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ

(๙) แสดงการเข้าถึงไฟล์และการกระทากับไฟล์ เช่น เปิด-ปิด เขียน-อ่านไฟล์เป็นต้น

(๑๐) หมายเลขไอพีแอดเดรสที่เข้าถึง

(๑๑) แสดงการหยุดการทางานของระบบป้องกันการบุกรุก

(๑๒) แสดงการหยุดการทางานของระบบงานที่สำคัญๆ

๑๐.๑.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๑๐.๑.๕. การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และ พัฒนาระบบสารสนเทศ

(๑) มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะและต้องกำหนดคุณสมบัติของ รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์มีลูกค้าอ้างอิงน่าเชื่อถือ เป็นต้น

(๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนด ขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องน่าเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

(๓) หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้หรือการลุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณา กระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงานและเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของหน่วยงาน

(๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูลและการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญ

(๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๑๐.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๒.๑ แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัว และอุปกรณ์ของทางราชการ

(๑) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีที่น่าเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณ ที่มีความเสี่ยงต่อการสูญหาย

(๒) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ไดใช่งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเช่าใช้งานคอมพิวเตอร์แบบพกพา

(๔) ไม่ใช่อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

(๕) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัสก่อนการใช่งานสื่อบันทึกข้อมูลพกพาต่างๆ

(๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บช่อมูลบนอุปกรณ์ดังกล่าวจะต้องเช่ารหัสข้อมูลทุกครั้ง

(๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพาเป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในโรงพยาบาล

(๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้ง ซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(๙) มีกระบวนการจัดการอุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อก ติดตั้งโปรแกรม ติดตามเครื่อง ฯลฯ

๑๐.๓.๒. การสำรองข้อมูลและการคู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก ข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการคู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๐.๓ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๐.๓.๑ ผู้ใช้งานงานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเช่าใช้งาน

๑๐.๓.๒ ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารช่อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆภายในองค์กร

๑๐.๓.๓ มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะ ไม่การปฏิบัติงานของผู้ใช่งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์การเช่าถึงข้อมูลโดย ไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๑๐.๓.๔ ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศ ขององค์กรในสถานที่ดังกล่าว

๑๐.๓.๕ ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศของ องค์กรจากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟล์วอลอย่างเหมาะสม

๑๐.๓.๖ ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกลชั่วโมงการทำงานในสถานที่ดังกล่าว ขั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๑. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (traffic log management)

๑๑.๑ ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงานและมี Log server ของหน่วยงาน สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของ โรงพยาบาลเมื่อมีการร้องขอ

๑๑.๒ กำหนดวิธีการในการน่าส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

๑๑.๓ บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของ ผู้ใช้งานและบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้าออกระบบ ซึ่ง ประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โปรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๑.๔ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๑.๕ กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่างๆ และ จำกัดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๒. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (system administrator responsibilities)

๑๒.๑ ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

๑๒.๑.๑ ผู้ดูแลระบบเครือข่าย (system administrator)

๑๒.๑.๒ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (network administrator)

๑๒.๑.๓ ผู้ดูแลระบบสารสนเทศ (application administrator)

๑๒.๒ ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดขอบดังนี้

๑๒.๒.๑ ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอและปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑๒.๒.๒ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งาน นับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนด นับตั้งแต่การใช้บริการสิ้นสุดลงและการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

(๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดขั้นความลับในการเข้าถึงข้อมูลดังกล่าวเพื่อรักษาความครบถ้วนถูกต้องและความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงานหรือบุคคลที่หน่วยงานมอบหมาย

(๒) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๓) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ time.psu.ac.th

๑๒.๓ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๒.๓.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการ

แก้ไขรวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันทีและในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

๑๒.๓.๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่ายให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๑๒.๓.๓ ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่างๆให้เหมาะสม

๑๒.๓.๔ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๑๒.๓.๕ ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๒.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

๑๒.๔.๑ ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๒.๔.๒ ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๒.๕ หลักธรรมมาภิบาลของผู้ดูแลระบบ

๑๒.๕.๑ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

๑๒.๕.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑๒.๕.๓ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (social network)

๑๓.๑ การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๑๓.๒ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาล

๑๓.๓ ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เสนอความคิดเห็นหรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาล

๑๓.๔ หากผู้ใช้งานทราบหรือรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับโรงพยาบาล ผู้ใช้งานต้องงานสารสนเทศ กลุ่มงานสุขภาพดิจิทัลโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๔. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

๑๔.๑ การจัดการบริเวณแวดล้อมทางกายภาพ

๑๔.๑.๑ กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๑๔.๑.๒ กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๑.๓. ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ

๑๔.๒ การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

๑๔.๒.๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๒.๒ ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๔.๒.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว

๑๔.๒.๔ ต้องพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องศูนย์กลางข้อมูล (data center)

๑๔.๒.๕ ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๑๔.๒.๖ มีบันทึกรายการอุปกรณ์ที่น่าเข้า-ออก

๑๔.๒.๗ ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจเพื่อป้องกันการสูญหายของทรัพย์สินและป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

๑๔.๒.๘ ต้องควบคุมหน่วยงานภายนอกในการน่าอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๒.๙ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๒.๑๐ เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง/ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอด ระยะเวลาการปฏิบัติงาน

๑๔.๒.๑๑ ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔.๒.๑๒ ต้องทบทวนหรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๔.๓ การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๑๔.๓.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการ เข้าถึงโดยไม่ได้รับอนุญาต

๑๔.๓.๒ จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๑๔.๓.๓ จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลียงการเข้าถึงพื้นที่อื่นๆ ภายในโรงพยาบาล

๑๔.๓.๔ ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน

๑๔.๓.๔. ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกใหม่สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของโรงพยาบาล

๑๔.๔ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

๑๔.๔.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๑๔.๔.๒ ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น

๑๔.๔.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตเพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๑๔.๕ การนำทรัพย์สินของโรงพยาบาลออกนอกสำนักงาน

๑๔.๕.๑ ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกโรงพยาบาล

๑๔.๕.๒ บันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาลออกนอกสำนักงานเพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อน่าอุปกรณ์ส่งคืน

๑๔.๕.๓ ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของโรงพยาบาลเสมือนเป็นทรัพย์สินของตนเอง

๑๔.๖ ระบบและอุปกรณ์สนับสนุนการทำงาน

๑๔.๖.๑ ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลที่เพียงพอต่อความต้องการใช้งานโดยให้มี (๑) ระบบสำรองกระแสไฟฟ้า (๒)เครื่องกำเนิดกระแสไฟฟ้าสำรอง (๓) ระบบระบายอากาศ (๔)ระบบปรับอากาศและควบคุมความชื้น (๔) ระบบป้องกันอัคคีภัย

๑๔.๖.๒ ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑๔.๖.๓ ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติ หรือหยุดทำงาน จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบ เครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหาต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑.งานสารสนเทศ กลุ่มงานสุขภาพดิจิทัล

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ที่ได้รับมอบหมาย อ้างอิงมาตรฐาน มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบ ธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑.ระบบสำรอง (disaster recovery site: DR site)

๑.๑ จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรองและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๑.๒ ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

๑.๒.๑ มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๑.๒.๒ มีระบบไฟฟ้าสำรอง

๑.๒.๓ มีระบบปรับอากาศและความชื้นที่เหมาะสม

๑.๒.๔ มีระบบป้องกันอัคคีภัย

๑.๒.๕ มีระบบส่องสว่างที่เหมาะสม

๑.๒.๖ มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

๑.๒.๗ มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๑.๒.๘ มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒.การสำรองข้อมูล (Data Backup)

๒.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูลและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๒.๒ กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๒.๓ กำหนดความถี่ในการสำรองข้อมูลระบบที่มีความสำคัญสูงหรือระบบที่มีการเปลี่ยนแปลงบ่อยต้องกำหนดให้มีความถี่ในการรองข้อมูลมากขึ้น

๒.๔ บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูลได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่ สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๒.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆที่เกี่ยวข้องกับระบบสารสนเทศข้อมูลในฐานข้อมูลและข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆเป็นต้น

๒.๖ จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

๒.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๒.๘ มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๘.๑ ต้องกำหนดหน้าที่ และความรับผิดขอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๘.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒.๘.๓ ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๘.๔ ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๘.๕ ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล (Data Recovery)

๓.๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของ ขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๓.๒ ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูล ได้ตามปกติ

๓.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๔ ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑ ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศระบบสำรอง ระบบสำรองข้อมูลและแผน เตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่๓

นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ความรับผิดชอบและความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่างๆ ซึ่งทำให้ระบบสารสนเทศของโรงพยาบาลหรือของหน่วยงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

๑.งานสารสนเทศ กลุ่มงานสุขภาพดิจิทัล

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. หน่วยงานตรวจสอบภายใน

แนวปฏิบัติ

๑.หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

๑.๑ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๒.ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้นดังต่อไปนี้

๒.๑ ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๒.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศหรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๒.๔ ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๒.๕ ความเสี่ยงที่เกิดจากการลักลอบไข้บัญชีผู้ใช้และรหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๖ ความเสี่ยงที่เกิดจากความเสียหายทางกายภาพ เช่น ไฟไหม้ น้ำท่วม อุปกรณ์สูญหาย เป็นต้น

๓.กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔.การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔.๑ ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ

๔.๒ ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๔.๓ ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๔.๔ จุดอ่อนหรือช่องโหว่ที่อาจถูกไข้ในการก่อให้เกิดเหตุการณ์ที่ระบบ

๕. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(Information Security Awareness Policy)

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและผู้เกี่ยวข้องได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑.งานสารสนเทศ กลุ่มงานสุขภาพดิจิทัล

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบ ธุรกรรมทาง อิเล็กทรอนิกส์

แนวปฏิบัติ

๑.ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัย สารสนเทศ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตาม แผนการฝึกอบรมของหน่วยงาน

๒.ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่ เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มี มาตรการเชิง'ป้องกันตามความเหมาะสม

๓.จัดฝึกอบรมการใช้งานสารสนเทศของโรงพยาบาลอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือ เปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๔.จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๕.ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และ นำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่าน เว็บไซต์ฯลฯ

๖.ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้