



โรงพยาบาลท่าวังผา
Thawangpha Hospital

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

โรงพยาบาลท่าวังผา

อำเภอท่าวังผา จังหวัดน่าน

จัดทำโดย

กลุ่มงานสุขภาพดิจิทัล

สารบัญ

	หน้า
ความเป็นมา	๑
ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการทำงานของระบบสารสนเทศ	๔
๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล (Information Access Control)	๔
๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๘
๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	๑๑
๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)	๑๔
๕. การใช้งานอินเทอร์เน็ต (Use of the Internet)	๑๗
๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย	๑๗
๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์	๑๘
๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๑๘
๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย	๒๐
๑๐. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ให้ใช้งานร่วมกัน	๒๑
๑๑. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ(Application and Information Access Control)	๒๑
๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)	๒๕
๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)	๒๖
๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)	๒๗
๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)	๒๘
ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองสารสนเทศ	๓๑
๑. ระบบสำรอง (disaster recovery site: DR site)	๓๑
๒. การสำรองข้อมูล (Data Backup)	๓๒
๓. การกู้คืนข้อมูล (Data Recovery)	๓๒
๔. การทดสอบสภาพพร้อมใช้งาน	๓๓

สารบัญ (ต่อ)

	หน้า
ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ	๓๔
๑. หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้น กับระบบสารสนเทศ	๓๔
๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยง ของหน่วยงานเพื่อการ ประเมินความเสี่ยงนั้น	๓๔
๓. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจาก ความเสี่ยงนั้น	๓๕
๔. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบ	๓๕
๕. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการ รายงานผลการติดตาม ตรวจสอบ และประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร	๓๕
ส่วนที่ ๔ นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)	๓๖

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ ภาครัฐ พ.ศ. ๒๕๕๔ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัย เชื่อถือได้ โรงพยาบาลท่าม่วงฯ ได้กำหนด แนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลท่าม่วงฯ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้ สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศใน ลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ ด้วย

๒. วัตถุประสงค์

โรงพยาบาลท่าม่วงฯ ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยี สารสนเทศและการสื่อสารของโรงพยาบาลท่าม่วงฯ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลท่าม่วงฯ และทำให้ดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและ ประสิทธิภาพและ ประสิทธิผล

๒.๓. เพื่อเผยแพร่ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร และเจ้าหน้าที่ทุกระดับ พร้อมทั้งบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ความเข้าใจและ ตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบ เทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลท่าวังผา มีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและ นโยบายของโรงพยาบาล

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับ ทั้งของ โรงพยาบาล และหน่วยงานที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลท่าวังผา จัดทำขึ้นเพื่อกำหนด แนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่ กำหนดไว้โดยมีรายละเอียดดังต่อไปนี้

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. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ให้ใช้งานร่วมกัน
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 นโยบายการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๔ นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบ สารสนเทศของโรงพยาบาล

๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการ บัญชีผู้ใช้สารสนเทศของโรงพยาบาล โดยเคร่งครัด

ผู้รับผิดชอบ

๑. กลุ่มงานสุขภาพดิจิทัล
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล(Information Access Control)

๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

๑.๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒. กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล ดังนี้

- ๑.๒.๑. ไม่มีสิทธิ์
- 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. ข้อมูลบุคลากรโรงพยาบาล
- ๑.๓.๓. ข้อมูลการเงินและบัญชี
- ๑.๓.๔. ข้อมูลทางการรักษาโรค
- ๑.๓.๕. ข้อมูลทางการบริหาร
- ๑.๓.๖. ข้อมูลการจราจรทางคอมพิวเตอร์

๑.๔. กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของโรงพยาบาลเป็น ๔ ระดับ ดังนี้

- ๑.๔.๑. ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง
- ๑.๔.๒. ใช้ภายในเท่านั้น เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างกลุ่มงาน / หน่วยงาน หรือข้อมูล ที่เผยแพร่เฉพาะภายในโรงพยาบาล
- 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 ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างกลุ่มงาน / 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 มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตาม อำนาจหน้าที่
- ๑.๗.๔. บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้
- ๑.๗.๕. ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดูเขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น
- ๑.๗.๖. การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูล เท่านั้น
- ๑.๗.๗. การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์ หรือหน่วยงานหลักเท่านั้น

๑.๘. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศ ของโรงพยาบาลในแต่ละประเภทดังนี้

- ๑.๘.๑. ข้อมูลผู้ป่วย หน่วยงานหลักคือ ห้องบัตรและเวชระเบียน
- ๑.๘.๒. ข้อมูลบุคลากร หน่วยงานหลักคือ ฝ่ายบริหารงาน (บุคลากร)
- ๑.๘.๓. ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ ฝ่ายบริหารงาน (การเงินและบัญชี)
- ๑.๘.๔. ข้อมูลทางการแพทย์โรค หน่วยงานหลักคือ แพทย์ พยาบาล และ เวชระเบียน
- ๑.๘.๕. ข้อมูลทางการบริหาร หน่วยงานหลักคือ ฝ่ายบริหารโรงพยาบาลเป็นหน่วยงานหลัก
- ๑.๘.๖. ข้อมูลการจราจรทางคอมพิวเตอร์ หน่วยงานหลักคือ ศูนย์คอมพิวเตอร์
- ๑.๘.๗. การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับ การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจของโรงพยาบาล

๑.๙. การควบคุมการเปลี่ยนแปลง

๑.๙.๑. การเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ ให้ดำเนินการ ดังนี้

- (๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง
- (๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคลเหล่านั้นมี เวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง
- (๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการ เปลี่ยนแปลง

๑.๙.๒. ต้องจัดเก็บซอร์สโค้ดและไลบรารีของระบบสารสนเทศทั้งเวอร์ชันปัจจุบันและเวอร์ชันเก่าไว้ ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๑๐. การกำหนดการใช้งานตามภารกิจ

๑.๑๐.๑. การควบคุมการเข้าถึงระบบสารสนเทศ

- (๑) บุคลากร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้น สภาพการเป็นบุคลากรของโรงพยาบาล
- (๒) ผู้บริหาร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้น สภาพการเป็นผู้บริหาร

๑.๑๐.๒. ข้อจำกัดในการเข้าถึง

- (๑) บุคลากร เข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย
- (๒) ผู้บริหาร เข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

๑.๑๑. ระยะเวลาการใช้งาน

๑.๑๑.๑. ระยะเวลาการเข้าถึงและการทำงานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งาน จะเข้าถึงและใช้งานได้ดังนี้

- (๑) การเข้าถึงในเวลาราชการ ๐๘.๓๐-๑๖.๓๐ น.
- (๒) การเข้าถึงนอกเวลาราชการ หลัง ๑๖.๓๐ น. เป็นต้นไป
- (๓) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนขัตฤกษ์

๑.๑๑.๒. การจำกัดระยะเวลาการเชื่อมต่อบริษัทสารสนเทศ

- (๑) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญต้องตัดและ หมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความ
เสียงสูงหรือระบบ ที่มีข้อมูลสำคัญ

๑.๑๒. การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

- ๑.๑๒.๑. บัญชีผู้ใช้หมดอายุ
- ๑.๑๒.๒. เมื่อมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง
- ๑.๑๒.๓. ถูกระงับสิทธิ์

๑.๑๓. การทบทวนและตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

- ๑.๑๓.๑. ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ ปีละ ๑ ครั้ง โดย ผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามกลุ่มงาน / หน่วยงานที่ขอสิทธิ์ จัดส่ง รายชื่อนั้นให้กับหน่วยงานที่ขอสิทธิ์เพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่
- ๑.๑๓.๒. หน่วยงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง
- ๑.๑๓.๓. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับ ระดับชั้นการเข้าถึงและการใช้งานระบบทันที

๑.๑๔. ช่องทางการเข้าถึง

- ๑.๑๔.๑. เครือข่ายภายในโรงพยาบาล
- ๑.๑๔.๒. เครือข่ายภายนอกโรงพยาบาล
- ๑.๑๔.๓. เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

- ๒.๑.๑. ต้องจัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัย ด้านสารสนเทศ
- ๒.๑.๒. อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่าง ถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและ สารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง
- ๒.๑.๓. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควร ระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๒. การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบสารสนเทศของโรงพยาบาลจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศของโรงพยาบาล ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น ๔ กลุ่มคือ

๒.๒.๑. แพทย์ พยาบาล และบุคลากรของโรงพยาบาล

๒.๒.๒. บุคคลอื่น ๆ ที่ โรงพยาบาลมอบสิทธิ์ให้

๒.๓. การลงทะเบียนผู้ใช้งาน

๒.๓.๑. แพทย์ พยาบาล และบุคลากรของโรงพยาบาล จะสร้างบัญชีบุคลากรใหม่ที่เจ้าหน้าที่กลุ่มงาน / หน่วยงาน ป้อนข้อมูล แพทย์ พยาบาล และบุคลากรของโรงพยาบาล เข้าระบบสารสนเทศ

๒.๓.๒. บุคคลอื่นๆที่ โรงพยาบาลมอบสิทธิ์ให้ เช่น บุคคลที่ทำงานในหน่วยงานอิสระ บุคคลที่ โรงพยาบาลมอบสิทธิ์ให้ สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อที่ศูนย์คอมพิวเตอร์โดยมีหนังสือรับรองจากผู้บริหารระดับกลุ่มงาน / หน่วยงานขึ้นไป และแสดงบัตรประจำตัวประชาชน พร้อมสำเนาที่รับรองสำเนาถูกต้อง ๑ ฉบับ

๒.๔. การจัดการบัญชีผู้ใช้ของโรงพยาบาล

๒.๔.๑. การบริหารจัดการบัญชีผู้ใช้สำหรับบุคลากรของโรงพยาบาล โดยผู้บริหารของหน่วยงานแจ้งชื่อผู้แทนที่จะรับผิดชอบในการดูแลบัญชีผู้ใช้ของ บุคลากรในสังกัด โดยมีรายละเอียด ดังนี้

- (๑) ชื่อหน่วยงาน
- (๒) ชื่อ-สกุลของผู้แทน
- (๓) ชื่อบัญชีผู้ใช้ของผู้แทน
- (๔) อีเมลของผู้แทน
- (๕) หมายเลขโทรศัพท์ของผู้แทน

๒.๔.๒. การเปลี่ยนแปลงผู้แทนของหน่วยงาน ให้แจ้งศูนย์คอมพิวเตอร์เป็นลายลักษณ์อักษร ลงนามโดยผู้บริหารของหน่วยงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมอีเมล และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

๒.๕. การจัดการสิทธิ์ของผู้ใช้งาน

๒.๕.๑. เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคย ขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

๒.๕.๒. การแจ้งขอใช้สิทธิ์ / เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบ สารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(๑) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของหน่วยงานหลัก

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๒.๕.๓. ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีผลกระทบ ความผิดตาม นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒.๕.๔. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์ พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา โดยต้องได้รับความ เห็นชอบและอนุมัติจากผู้อำนวยการโรงพยาบาล หรือผู้ที่ได้รับมอบอำนาจจากผู้อำนวยการโรงพยาบาล

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งาน เฉพาะกรณี จำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา ดังกล่าว

(๓) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้อง เปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๒.๖. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๖.๑. ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคง ปลอดภัย

๒.๖.๒. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดย ผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๒.๖.๓. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมลเป็นช่องทางในการส่ง

๒.๖.๔. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๒.๖.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยน รหัสผ่านจากผู้ดูแลระบบ

๒.๖.๖. ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็น เวลานาน

๒.๖.๗. กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิ์การใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยน รหัสผ่านเป็นที่เรียบร้อยแล้ว

๒.๗. การทบทวนสิทธิ์การเข้าถึง

๒.๗.๑. ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชี ผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๒.๗.๒. บัญชีผู้ใช้จะหมดอายุ ดังนี้

(๑) กรณี แพทย์ พยาบาล และบุคลากรของโรงพยาบาล หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของโรงพยาบาล

(๒) กรณีที่ไม่ใช่บุคลากรของโรงพยาบาล หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี หรือ เมื่อไม่มีการเข้าใช้งานติดต่อกันเกิน ๑ เดือน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑. การใช้งานบัญชีผู้ใช้และรหัสผ่าน

๓.๑.๑. ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคน ต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่ แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๓.๑.๒. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๓.๒. การใช้งานรหัสผ่าน

๓.๒.๑. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่โรงพยาบาลกำหนด

๓.๒.๒. ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่มีชื่อถึงตัวผู้ใช้งาน เช่น ชื่อ นามสกุล ชื่อเล่น ชื่อ บิดา ชื่อมารดา ชื่อหน่วยงาน หรือคำศัพท์ที่มีใช้ในพจนานุกรม เป็นต้น ต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า ๖ ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และ ตัวอักษรพิเศษเข้าด้วยกัน

๓.๒.๓. ไม่ใช่โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๓.๒.๔. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๓.๒.๕. หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิ์ใช้งาน

๓.๒.๖. เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๓.๓. การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

- ๓.๓.๑. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อก หน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน
- ๓.๓.๒. ผู้ใช้งานต้องล๊อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแล
- ๓.๓.๓. ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๓.๔. การจัดวางและการป้องกันอุปกรณ์

- ๓.๔.๑. จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้ รับบอนุญาต
- ๓.๔.๒. อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย
- ๓.๔.๓. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๕. การควบคุมสินทรัพย์สารสนเทศและการทำงานของระบบคอมพิวเตอร์

- ๓.๕.๑. จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคง ปลอดภัย
- ๓.๕.๒. ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็น เจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น
- ๓.๕.๓. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ที่ใช้ ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้ เข้าถึงข้อมูลสำคัญได้
- ๓.๕.๔. สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อ ป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับบอนุญาต
- ๓.๕.๕. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษา ความลับทางราชการ พ.ศ. ๒๕๔๔ และแก้ไขเพิ่มเติม ฉบับที่ ๒ พ.ศ. ๒๕๖๑

- ๓.๕.๖. จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับ ข้อมูลหรือ เอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนด อื่นๆ ที่โรงพยาบาลต้องปฏิบัติตาม
- ๓.๕.๗. โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของโรงพยาบาล เป็นโปรแกรมที่ โรงพยาบาลได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งาน คัดลอกโปรแกรม และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็น การกระทำที่ผิดกฎหมาย
- ๓.๕.๘. ไม่เก็บข้อมูลสำคัญของโรงพยาบาลไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึก ข้อมูลที่เป็น สมบัติส่วนบุคคล
- ๓.๕.๙. ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำ การเปลี่ยน หรือทดแทนอุปกรณ์
- ๓.๕.๑๐. ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการ บันทึกข้อมูล ก่อน ทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์
- ๓.๕.๑๑. ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรอง ข้อมูลลง ฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และ จัดเก็บ ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหล ของข้อมูล ทั้งนี้ การลบหรือทำลาย ข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อ บันทึกข้อมูล หรือลบข้อมูล อิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๓.๖. การป้องกันโปรแกรมไม่ประสงค์ดี

- ๓.๖.๑. ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัด โปรแกรมไม่ ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ
- ๓.๖.๒. ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ
- ๓.๖.๓. ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และ ผ่านทางสื่อ บันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกัน และกำจัดโปรแกรมไม่ ประสงค์ดีก่อนการรับส่งทุกครั้ง
- ๓.๖.๔. ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี ก่อน การเปิดใช้ ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่นไฟล์ที่มี นามสกุล .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑. การใช้งานระบบเครือข่ายของโรงพยาบาล

- ๔.๑.๑. การเข้าถึงระบบเครือข่ายของโรงพยาบาลจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วย บัญชีผู้ใช้ที่ โรงพยาบาลออกให้
- ๔.๑.๒. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการ ในระบบ เครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น
- ๔.๑.๓. การเข้าถึงระบบเครือข่ายของโรงพยาบาลจากภายนอกต้องอยู่บนพื้นฐาน ของความจำเป็น เท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่ เพิ่มขึ้นเป็นพิเศษจากมาตรฐานการ เข้าถึงระบบเครือข่ายโรงพยาบาลจาก ภายใน
- ๔.๑.๔. เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ต จะต้องลงทะเบียน กับศูนย์คอมพิวเตอร์
- ๔.๑.๕. จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ต อุปกรณ์เครือข่าย ตามความจำเป็น
- ๔.๑.๖. การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการ อนุมัติจากผู้ดูแล ระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น
- ๔.๑.๗. การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของโรงพยาบาล ต้องขอ อนุญาตใช้บัญชี ชั่วคราวจากโรงพยาบาล ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับ อนุญาตและจะต้องพิสูจน์ตัวตน ด้วยบัญชีชั่วคราวนั้น

๔.๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

- ๔.๒.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในโรงพยาบาลจะต้องทำการ ลงทะเบียน กับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการ ศูนย์คอมพิวเตอร์ หรือ ผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สาย นั้น
- ๔.๒.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้
 - (๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานระบบเครือข่ายไร้สายให้ เหมาะสมกับหน้าที่ ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์ การเข้าถึงอย่างสม่ำเสมอ
 - (๒) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ ในระบบ เครือข่ายไร้สาย

- (๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์ รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจาก ภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้
- (๔) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นำอุปกรณ์ กระจายสัญญาณมาใช้งาน
- (๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงาน ของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ ยาก เพื่อป้องกันผู้โจมตีไม่ไม่สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย
- (๖) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณ ด้วยวิธี ที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA๒ (Wi-Fi Protected Access) เพื่อให้ยากต่อ การดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น
- (๗) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่าย ภายในโรงพยาบาล
- (๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย อย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบ เครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ รายงานต่อหัวหน้าฝ่ายศูนย์คอมพิวเตอร์ทราบโดยทันที

๔.๓. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

- ๔.๓.๑. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย
- ๔.๓.๒. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิตช์L๓

๔.๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

- ๔.๔.๑. ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม
- ๔.๔.๒. ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อ โดยตรงบนตัวอุปกรณ์

- ๔.๔.๓. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกโรงพยาบาล แต่ให้เชื่อมต่อผ่าน ช่องทางที่ปลอดภัยที่โรงพยาบาลกำหนด เช่น VPN เป็นต้น
- ๔.๔.๔. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความ ปลอดภัย
- ๔.๔.๕. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน
- ๔.๔.๖. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่าง สม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔.๕. การแบ่งแยกเครือข่าย (segregation in networks)

- ๔.๕.๑. ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่าย ภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- ๔.๕.๒. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่าง ๆ ของโรงพยาบาล
- ๔.๕.๓. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ
- ๔.๕.๔. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของ หน่วยงาน

๔.๖. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

- ๔.๖.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น
- ๔.๖.๒. ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอกโรงพยาบาล ต้องติดตั้งระบบ ตรวจสอบการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี

๔.๗. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

- ๔.๗.๑. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด
- ๔.๗.๒. มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย
- ๔.๗.๓. ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง
- ๔.๗.๔. ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย
- ๔.๗.๕. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและ การใช้งานบริการเครือข่าย
- ๔.๗.๖. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อระงับการใช้จากเส้นทางอื่น

๔.๘. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกโรงพยาบาล (User Authentication for External Connections)

- ๔.๘.๑. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง
- ๔.๘.๒. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น
- ๔.๘.๓. ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของ โรงพยาบาล โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อ แสดงว่าเป็นผู้ใช้งานตัวจริง

๕. การใช้งานอินเทอร์เน็ต (use of the Internet)

- ๕.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่ โรงพยาบาลจัดสรรไว้ตามสิทธิ์ที่ได้รับ
- ๕.๒. ห้ามใช้อินเทอร์เน็ตของโรงพยาบาลเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล
- ๕.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจ กระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัย ต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับโรงพยาบาล เป็นต้น
- ๕.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการ ปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา
- ๕.๕. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

- ๖.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร
- ๖.๒. มีขั้นตอน / กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่มีพบว่ามี การใช้งานหรือ เปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที
- ๖.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ ให้บริการทุกชนิดให้ตรง กับเวลาอ้างอิงมาตรฐาน (time.psu.ac.th) ที่โรงพยาบาลใช้อ้างอิง
- ๖.๔. เปิดให้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อ ระบบรักษาความปลอดภัยด้วย

- ๖.๕. ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่างๆ
- ๖.๖. ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อน ติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา
- ๖.๗. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

- ๗.๑. แพทย์ พยาบาล และบุคลากรของโรงพยาบาล ไปลงทะเบียนเพื่อใช้บริการระบบจดหมายอิเล็กทรอนิกส์ ได้ที่ศูนย์คอมพิวเตอร์
- ๗.๒. ผู้ใช้งานต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ
- ๗.๓. กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงบนหัวข้อจดหมาย อิเล็กทรอนิกส์
- ๗.๕. ผู้ใช้งานมีหน้าที่จะต้องรักษาบัญชีผู้ใช้ และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง เพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี
- ๗.๖. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุกครั้ง เพื่อ ป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน
- ๗.๗. ในการตรวจสอบความผิดปกติของการใช้งานจดหมายอิเล็กทรอนิกส์ หากพบว่า ผู้ใช้งานรายใดส่ง จดหมายอิเล็กทรอนิกส์มากกว่าจำนวนที่ควรจะเป็น ระบบจะทำการเปลี่ยนรหัสผ่านอัตโนมัติ เพื่อ ป้องกันความเสียหายที่จะเกิดกับระบบของโรงพยาบาล
- ๗.๘. ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิงค์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง
- ๗.๙. ต้องไม่ส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน บัญชีผู้ใช้ หมายเลขบัตรประชาชน หมายเลขบัตร เครดิต ฯลฯ ผ่านจดหมายอิเล็กทรอนิกส์

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System access control)

๘.๑. ผู้ดูแลระบบ (System Administrator)

- ๘.๑.๑. ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ ของโรงพยาบาล

๘.๒. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

- ๘.๒.๑. ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ๘.๒.๒. ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้เมื่อพบว่ามีภัยคุกคามเดาหารหัสผ่าน จากเครื่องปลายทาง
- ๘.๒.๓. จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๘.๒.๔. จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line
เนื่องจาก อาจสร้างความเสียหายให้กับระบบได้

๘.๓. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๘.๓.๑. ผู้ใช้งานต้องมีบัญชีผู้ใช้และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของ
โรงพยาบาล

๘.๓.๒. สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม โดยใช้สมาร์ทการ์ด RFID
หรือ เครื่องอ่านลายพิมพ์นิ้วมือ หรือวิธีการอื่นที่มีความปลอดภัย

๘.๔. การบริหารจัดการรหัสผ่าน (Password Management System)

๘.๔.๑. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกิน
จำนวนครั้ง ที่กำหนด ระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่
สามารถใช้งานได้จนกว่า ผู้ดูแลระบบจะปลดล็อกให้

๘.๔.๒. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามี ความ
พยายามในการเดา รหัสผ่านจากเครื่องปลายทาง

๘.๔.๓. มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๘.๔.๔. ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของ
ระบบงาน

๘.๔.๕. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูล
รหัสผ่านของ ตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๘.๔.๖. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่าน
ของทุกชื่อผู้ใช้ที่ ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๘.๕. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๘.๕.๑. จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรม
อรรถประโยชน์

๘.๕.๒. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๘.๕.๓. ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๘.๕.๔. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๘.๕.๕. โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

๘.๕.๖. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๘.๖. การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

- ๘.๖.๑. ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลา ไม่เกิน ๓๐ นาทีหากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติ การใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลง หรือเป็นเวลาไม่เกิน ๑๕ นาทีตามความ เหมาะสม เพื่อป้องกันการเข้าถึงข้อมูล สำคัญโดยไม่ได้รับอนุญาต
- ๘.๖.๒. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการ เชื่อมต่อเข้าสู่ ระบบโดยอัตโนมัติ
- ๘.๖.๓. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำ การปิด เครื่อง โดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่ กำหนด

๘.๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

- ๘.๗.๑. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบ สารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อ การเชื่อมต่อหนึ่งครั้ง เป็นต้น และ กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติ ของโรงพยาบาล เท่านั้น
- ๘.๗.๒. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณา ถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย
- ๘.๗.๓. กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ /หรือ ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ ภายนอกสำนักงาน มีการจำกัดช่วง ระยะเวลาการเชื่อมต่อ

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

- ๙.๑. หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องแต่งตั้งผู้มีสิทธิ์ และ กำหนดจำนวนผู้มี สิทธิ์ในการเข้าถึงระบบปฏิบัติการ
- ๙.๒. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของ ตัวเอง
- ๙.๓. ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ๙.๔. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการ พยายามคาดเดา รหัสผ่านจากเครื่องปลายทาง

- ๙.๕. ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย
- ๙.๖. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่ โรงพยาบาลไม่อนุญาต
- ๙.๗. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญ อย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต
- ๙.๘. ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง
- ๙.๙. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น
- ๙.๑๐. ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ
- ๙.๑๑. ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดี ว่าต้องดำเนินการอย่างไร

๑๐. การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งานร่วมกัน

- ๑๐.๑. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง
- ๑๐.๒. ระบบต้องไม่แสดงรายละเอียดสำคัญก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- ๑๐.๓. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อเมื่อพบว่ามีคามพยายามคาดเดารหัสผ่าน
- ๑๐.๔. ระบบจะต้องจำกัดสิทธิ์ผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

๑๑. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (application and information access control)

๑๑.๑. การจำกัดการเข้าถึงสารสนเทศ

- ๑๑.๑.๑. การจำกัดการเข้าถึงของผู้ใช้งาน
- (๑) เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น
 - (๒) กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล
 - (๓) ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

- ๑๑.๑.๒. แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของโรงพยาบาลออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่าง ชัดเจนเป็นลายลักษณ์อักษร
- ๑๑.๑.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูล พฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้
- (๑) ชื่อบัญชีผู้ใช้
 - (๒) วันเวลาที่เข้าถึงระบบ
 - (๓) วันเวลาที่ออกจากระบบ
 - (๔) เหตุการณ์สำคัญที่เกิดขึ้น
 - (๕) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ
 - (๖) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
 - (๗) แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ
 - (๘) แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่าน ไฟล์เป็นต้น
 - (๙) หมายเลขไอพีแอดเดรสที่เข้าถึง
 - (๑๐) แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก
 - (๑๑) แสดงการหยุดการทำงานของระบบงานที่สำคัญๆ
- ๑๑.๑.๔. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็น มาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น
- ๑๑.๑.๕. การควบคุมผู้รับเหมาช่วง (outsourc) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และ พัฒนาระบบสารสนเทศ
- (๑) มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของ ผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์มีลูกค้าอ้างอิงน่าเชื่อถือ หรือ ใบรับรองทางด้านทักษะวิชาชีพตาม มาตรฐานสากล มีความพร้อมด้านเทคโนโลยี ของการรับเหมาช่วงทั้ง ในส่วนของ ฮาร์ดแวร์และซอฟต์แวร์รวมถึงระบบสนับสนุน อื่นๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงาน ต้องการ
 - (๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้อง กำหนด ขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมา ช่วงต้องนำเสนอ รายละเอียดงานขอบเขตงานอย่างครบถ้วน

- (๓) หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็น ระยะ ๆ ตามที่กำหนดไว้หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อ พิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความ สม่่าเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของหน่วยงาน
- (๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกชั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญ หรือให้ใช้ข้อมูลจากชุดจำลอง แทนข้อมูลจริง
- (๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๑๑.๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงาน จะต้องดำเนินการดังนี้

- ๑๑.๒.๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ได้แก่ ระบบสารสนเทศ ระบบเวชระเบียนของผู้ป่วย ระบบสารสนเทศ แพทย์พยาบาล และบุคลากรของโรงพยาบาล ระบบสารสนเทศทางการแพทย์ และระบบสารสนเทศทางการเงิน ต้องแยกออกจาก ระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อโรงพยาบาล
- ๑๑.๒.๒. ต้องควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวนโดยเฉพาะ
 - (๑) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับ มอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว
 - (๒) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น
 - (๓) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ
 - (๔) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต
- ๑๑.๒.๓. ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอก องค์กร

๑๑.๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

- ๑๑.๓.๑. แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและ อุปกรณ์ของทางราชการ
 - (๑) ต้องล็อคหรือยึดเครื่องให้อยู่กับที่กรณีที่น่าเครื่องไปใช้ในที่สาธารณะหรือในบริเวณ ที่มีความเสี่ยงต่อการสูญหาย

- (๒) ต้องเปิดใช้ระบบล็อกหน้าจอตโนมติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และใน กรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอบุคคลครั้ง
- (๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา
- (๔) ไม่ใช่อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น
- (๕) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งาน สื่อบันทึก ข้อมูลพกพาต่าง ๆ
- (๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่ ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูล ทุกครั้ง
- (๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจาย สัญญาณ เครือข่ายไร้สายภายในโรงพยาบาล
- (๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภท พกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการ ให้ทันสมัย ไม่ติดตั้ง ซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่ รู้จัก ฯลฯ
- (๙) มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญ หายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรม ติดตามเครื่อง ฯลฯ

๑๑.๓.๒. การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้ บนสื่อบันทึก ข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น
- (๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่ เหมาะสม ไม่เสี่ยงต่อ การรั่วไหลของข้อมูล และทดสอบการกู้คืน ข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

- ๑๑.๔.๑. ผู้ใช้งานงานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน
- ๑๑.๔.๒. ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมี การปฏิบัติงาน จากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร

- ๑๑.๔.๓. มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงาน ของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับ อนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี
- ๑๑.๔.๔. ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบ เทคโนโลยีสารสนเทศ ขององค์กรในสถานที่ดังกล่าว
- ๑๑.๔.๕. ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบ สารสนเทศขององค์กร จากระยะไกลมีระบบป้องกันไวรัสและการใช้งาน ไฟร์วอลล์อย่างเหมาะสม
- ๑๑.๔.๖. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการ ปฏิบัติงานจาก ระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้น ความลับของข้อมูลที่อนุญาตให้ใช้งาน ได้และระบบงานและบริการต่าง ๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์(traffic log management)

- ๑๒.๑. ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงาน และมี Log server ของหน่วยงาน สำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษา ข้อมูลจราจรคอมพิวเตอร์ของ โรงพยาบาลเมื่อมีการร้องขอ
- ๑๒.๒. กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน
- ๑๒.๓. บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการ ปฏิบัติงานของ ผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้าออกระบบ ซึ่ง ประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โพรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ใน การใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่ กำหนดไว้ในพระราชบัญญัติว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์
- ๑๒.๔. ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- ๑๒.๕. กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ ต่างๆ และจำกัด สิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้อง เท่านั้น

๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (system administrator responsibilities)

๑๓.๑. ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

๑๓.๑.๑. ผู้ดูแลระบบเครือข่าย (system administrator)

๑๓.๑.๒. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (network administrator)

๑๓.๑.๓. ผู้ดูแลระบบสารสนเทศ (application administrator)

๑๓.๒. ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๒.๑. ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่ เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑๓.๒.๒. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งาน นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่ การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่ มั่นคงปลอดภัย ดังต่อไปนี้

- (๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการ เข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนถูกต้อง และความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้แล้วแต่ ได้มีการกำหนดผู้ที่ สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย
- (๒) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้
- (๓) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ time.psu.ac.th

๑๓.๓. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๓.๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วย ความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่อง คอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่ อาจเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้ที่ไม่ เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ ผู้ดูแลระบบพิจารณา ระงับการใช้งานของผู้ใช้งานทันที

- ๑๓.๓.๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์ แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ
- ๑๓.๓.๓. ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่างๆ ให้เหมาะสม
- ๑๓.๓.๔. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย
- ๑๓.๓.๕. ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็น ปัจจุบันอยู่เสมอ

๑๓.๔. ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

- ๑๓.๔.๑. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ
- ๑๓.๔.๒. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้น ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑๓.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

- ๑๓.๕.๑. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร
- ๑๓.๕.๒. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมี ข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร
- ๑๓.๕.๓. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้ บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (social network)

- ๑๔.๑. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการ เป็นสำคัญ
- ๑๔.๒. ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของโรงพยาบาล
- ๑๔.๓. ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่ว ุให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของโรงพยาบาล
- ๑๔.๔. หากผู้ใช้งานทราบหรือรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบ กับโรงพยาบาล ผู้ใช้งานต้องแจ้งศูนย์คอมพิวเตอร์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๕.การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

๑๕.๑. การจัดการบริเวณแวดล้อมทางกายภาพ

- ๑๕.๑.๑. กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน
- ๑๕.๑.๒. กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ
- ๑๕.๑.๓. ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่า ยังใช้งานได้ตามปกติ

๑๕.๒. การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

- ๑๕.๒.๑. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ
- ๑๕.๒.๒. ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่
- ๑๕.๒.๓. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมี เหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว
- ๑๕.๒.๔. ต้องพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือ บริเวณที่มีความสำคัญ เช่น ห้องศูนย์กลางข้อมูล (data center)
- ๑๕.๒.๕. ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการ ตรวจสอบในภายหลังเมื่อมีความจำเป็น
- ๑๕.๒.๖. มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก
- ๑๕.๒.๗. ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน และ ป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต
- ๑๕.๒.๘. ต้องควบคุมหน่วยงานภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการ ปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ
- ๑๕.๒.๙. สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ
- ๑๕.๒.๑๐. เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง / ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดเจนตลอดเวลา การปฏิบัติงาน
- ๑๕.๒.๑๑. ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือ บริเวณที่มีความสำคัญ
- ๑๕.๒.๑๒. ต้องทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๕.๓. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

- ๑๕.๓.๑. จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต
- ๑๕.๓.๒. จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น
- ๑๕.๓.๓. จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในโรงพยาบาล
- ๑๕.๓.๔. ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน
- ๑๕.๓.๕. ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้ สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของ โรงพยาบาล

๑๕.๔. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

- ๑๕.๔.๑. จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย
- ๑๕.๔.๒. ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น
- ๑๕.๔.๓. ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บน เครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไข เอกสารนั้น

๑๕.๕. การนำทรัพย์สินของโรงพยาบาลออกนอกสำนักงาน

- ๑๕.๕.๑. ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกโรงพยาบาล
- ๑๕.๕.๒. บันทึกข้อมูลการนำอุปกรณ์ของโรงพยาบาลออกนอกสำนักงาน เพื่อใช้เป็นหลักฐาน ป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน
- ๑๕.๕.๓. ให้เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของโรงพยาบาล เสมือนเป็น ทรัพย์สินของตนเอง

๑๕.๖. ระบบและอุปกรณ์สนับสนุนการทำงาน

- ๑๕.๖.๑. ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาล ที่เพียงพอต่อความต้องการใช้งาน โดยให้มี
 - (๑) ระบบสำรองกระแสไฟฟ้า
 - (๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง
 - (๓) ระบบระบายอากาศ
 - (๔) ระบบปรับอากาศและควบคุมความชื้น
 - (๕) ระบบป้องกันอัคคีภัย

- ๑๕.๖.๒. ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบ ทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- ๑๕.๖.๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติหรือ หยุดทำงาน
- ๑๕.๖.๔. จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้ผู้เกี่ยวข้อง รับทราบ

ส่วนที่ ๒

นโยบายการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของโรงพยาบาลมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง
๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแล เครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่ จำเป็น

ผู้รับผิดชอบ

๑. กลุ่มงานสุขภาพดิจิทัล
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของกลุ่มงาน / หน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ระบบสำรอง (disaster recovery site: DR site)

- ๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชี อย่างน้อยปีละ 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
- ๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล(Data Backup)

- ๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูลและทบทวน บัญชีอย่างน้อยปีละ ๑ ครั้ง
- ๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ
- ๒.๓. กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น
- ๒.๔. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์ทำงานสำเร็จ / ไม่สำเร็จ เป็นต้น
- ๒.๕. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น
- ๒.๖. จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง
- ๒.๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง
- ๒.๘. มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้
 - ๒.๘.๑. ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
 - ๒.๘.๒. ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อ ลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลาานาน ไฟไหม้ แผ่นดินไหว การชุมนุม ประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
 - ๒.๘.๓. ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
 - ๒.๘.๔. ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
 - ๒.๘.๕. ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล(Data Recovery)

- ๓.๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอน ปฏิบัติอย่างสม่ำเสมอ
- ๓.๒. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ ตามปกติ
- ๓.๓. ให้ใช้ข้อมูลทันสมัยที่สุด(Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๔. ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑. ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยง สารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่างๆ ซึ่งทำให้ระบบสารสนเทศของโรงพยาบาลหรือของหน่วยงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

1. กลุ่มงานสุขภาพดิจิทัล
2. ผู้ดูแลระบบที่ได้รับมอบหมาย
3. หน่วยตรวจสอบภายใน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

๑.๑. ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการ ประเมินความเสี่ยงนั้น ดังต่อไปนี้

- ๒.๑. ความเสี่ยงที่เกิดจากการลักลอบเข้าถึงทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่าน ระบบอินเทอร์เน็ต
- ๒.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต
- ๒.๓. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการ ใช้งาน
- ๒.๔. ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกัน มากกว่าหนึ่งจุด
- ๒.๕. ความเสี่ยงที่เกิดจากการลักลอบใช้บัญชีผู้ใช้และรหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๖. ความเสี่ยงที่เกิดจากความเสียหายทางกายภาพ เช่น ไฟไหม้ น้ำท่วม อุปกรณ์สูญหาย เป็นต้น

๓. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

- ๔.๑. ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ
- ๔.๒. ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
- ๔.๓. ภัยคุกคามหรือสิ่งนี้อาจก่อให้เกิดเหตุการณ์ที่ระบุ
- ๔.๔. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๕. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของการ รายงานผลการติดตาม ตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔

นโยบายการสร้างตระหนักรู้ในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

วัตถุประสงค์

เพื่อเผยแพร่ นโยบายและแนวปฏิบัติให้กับบุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึง ความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

- กลุ่มงานสุขภาพดิจิทัล
- หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
- ผู้ดูแลระบบที่ได้รับมอบหมาย
- เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

- ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักรู้เรื่องความมั่นคงปลอดภัยสารสนเทศ โดยอาจ ใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน
- ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักรู้ ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตาม ความเหมาะสม
- จัดฝึกอบรมการใช้งานสารสนเทศของโรงพยาบาลอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลง การใช้งานของระบบสารสนเทศ
- จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และเผยแพร่ทางเว็บไซต์ของหน่วยงาน
- ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติ ได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ ประชาสัมพันธ์แผ่นพับ เผยแพร่ผ่าน เว็บไซต์ฯลฯ
- ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้