[redacted]

มาตรฐานควบคุมการเข้าถึงและการใช้ด้านเทคโนโลยีสารสนเทศโรงพยาบาล

อ้างอิงจาก : มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

1. มาตรฐานข้อมูล(Data)
2. มาตรฐานรหัสข้อมูล
3. มาตรฐานความปลอดภัยและความลับของผู้ป่วย
4. มาตรฐานระบบเครือข่ายคอมพิวเตอร์
5. มาตรฐานทางกายภาพและสภาพแวดล้อม
6. มาตรฐานการปฏิบัติงาน

มาตรฐานข้อมูล(Data)

แนวทางปฏิบัติ

1. ระบบสำรอง (disaster recovery site: DR site)

1.1 จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

1.2 ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

- มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง
- มีระบบไฟฟ้าสำรอง
- มีระบบปรับอากาศและความชื้นที่เหมาะสม
- มีระบบป้องกันอัคคีภัย
- มีระบบส่องสว่างที่เหมาะสม
- มีระบบสื่อสารหรือระบบเครือข่ายสำรอง
- มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

1.3 มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

2. การสำรองข้อมูล (Data Backup)

2.1. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการส ารองข้อมูลและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

2.2 กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

2.3 กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

2.4 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรองสถานการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

2.5 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆเป็นต้น

มาตรฐานข้อมูล(Data) (ต่อ)

แนวทางปฏิบัติ

2.6 จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

2.7 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูลสำรอง

2.8 มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

- ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
- ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

3. การกู้คืนข้อมูล(Data Recovery)

3.1 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของ ขั้นตอนปฏิบัติอย่างสม่ำเสมอ

3.2 ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

3.3 ให้ใช้ข้อมูลทันสมัยที่สุด(Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

3.4 ทดสอบการกู้คืนข้อมูลที่ได้ทำการส ารองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

4. การทดสอบสภาพพร้อมใช้งานต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

มาตรฐานรหัสข้อมูล

1.การควบคุมการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล(Information Access Control)

จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบ หรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

2. กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล ดังนี้

- 2.1. ไม่มีสิทธิ์
- 2.2. อ่านได้อย่างเดียว
- 2.3. สร้างข้อมูล
- 2.4 ป้อนข้อมูล
- 2.5 แก้ไขข้อมูล
- 2.6 ลบข้อมูล
- 2.7. อนุมัติการใช้ข้อมูล

3. กำหนดประเภทข้อมูลของโรงพยาบาลเป็น ๖ ประเภทหลักๆ ดังนี้

- 3.1. ข้อมูลผู้ป่วย
- 3.2 ข้อมูลบุคลากร
- 3.3 ข้อมูลการเงินและบัญชี
- 3.4 ข้อมูลทางการแพทย์
- 3.5 ข้อมูลทางการบริหาร
- 3.6 ข้อมูลการจราจรทางคอมพิวเตอร์

มาตรฐานรหัสข้อมูล (ต่อ)

4. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

4.1 การใช้งานบัญชีผู้ใช้และรหัสผ่าน

4.2 ผู้ใช้งานต้องทาการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมี บัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทาให้ผู้อื่นล่วงรู้รหัสผ่าน

4.3 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

5. การใช้งานรหัสผ่าน

5.1 ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่โรงพยาบาลกำหนด

5.2 ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น วันเดือน ปีเกิด เป็นต้น ต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า 8 ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน

5.3 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

5.4 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

5.5 หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิ์ใช้งาน

5.6 เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

6.การทบทวนและตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

6.1 ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ ปีละ 1 ครั้ง โดย ผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามคณะ/หน่วยงานที่ขอสิทธิ์ จัดส่งรายชื่อนั้นให้กับหน่วยงานที่ขอสิทธิ์เพื่อดาเนินการทบทวนว่ามีรายชื่อที่ลาออกหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่

6.2 หน่วยงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

6.3 หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้ อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบทันที

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

8. มีระบบAuthentication ระบบการยืนยันตัวตนที่เมื่อเราจะเข้าใช้งานระบบอินเตอร์เน็ตเข้าเว็บไซต์ แอปพลิเคชั่นหรืออะไรก็ตามบนโลกออนไลน์

มาตรฐานความปลอดภัยและความลับของผู้ป่วย

1. กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของโรงพยาบาลเป็น ๔ ระดับดังนี้
   1.1 ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง
   1.2 ใช้ภายในเท่านั้น เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างหน่วยงาน หรือข้อมูล ที่เผยแพร่เฉพาะภายในโรงพยาบาล
   1.3.ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น
   1.4 เปิดเผยได้เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกโรงพยาบาล
2. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศ ของโรงพยาบาลในแต่ละประเภทดังนี้
   2.1 ข้อมูลผู้ป่วยหน่วยงานหลักคือ เวชระเบียน และงานสารสนเทศ
   2.2 ข้อมูลบุคลากร หน่วยงานหลักคือ งานการเจ้าหน้าที่
   2.3. ข้อมูลการเงินและบัญชีหน่วยงานหลักคือ การเงินและบัญชี
   2.4 ข้อมูลทางการแพทย์ ขึ้นอยู่กับหน่วยงานที่โรงพยาบาลมอบหมายเป็นหน่วยงานหลัก
   2.5. ข้อมูลทางการบริหาร ขึ้นอยู่กับหน่วยงานที่โรงพยาบาลมอบหมายเป็นหน่วยงานหลัก
   2.6 ข้อมูลการจราจรทางคอมพิวเตอร์ศูนย์คอมพิวเตอร์และหน่วยงานที่ให้บริการระบบ สารสนเทศ
   2.7 การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับ การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจของโรงพยาบาล
3. เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของโรงพยาบาล
   3.1 ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
   3.2 ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
   3.3 ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตาม อำนาจหน้าที่
   3.4 บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้
   3.5 ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น
   3.6 การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูล เท่านั้น
   3.7 การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์ หรือหน่วยงานหลักเท่านั้น

มาตรฐานระบบเครือข่ายคอมพิวเตอร์

การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

1. การเข้าใช้งานระบบเครือข่ายของโรงพยาบาล

1.1 การเข้าถึงระบบเครือข่ายของโรงพยาบาลจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่โรงพยาบาลออกให้

1.2 ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

1.3 เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับ ศูนย์คอมพิวเตอร์

1.4 จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ตอุปกรณ์เครือข่ายตามความจำเป็น

1.5 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จาเป็น

1.6 การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของโรงพยาบาล ต้องขออนุญาตใช้บัญชีชั่วคราวจากโรงพยาบาล ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

2. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

2.1 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในโรงพยาบาล จะต้องทาการลงทะเบียนกับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากศูนย์

2.2 ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(1) ต้องทาการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(2) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นามาใช้ในระบบเครือข่ายไร้สาย

(3) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(4) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นาอุปกรณ์กระจายสัญญาณมาใช้งาน

(5) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสาหรับการตั้งค่าการทางานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(6) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณ ด้วยวิธีที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูล และทาให้ปลอดภัยมากขึ้น

มาตรฐานระบบเครือข่ายคอมพิวเตอร์ (ต่อ)

(7) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในโรงพยาบาล

(8) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย

3. การระบุอุปกรณ์ที่นามาเชื่อมต่อบนเครือข่าย

3.1 อุปกรณ์ที่นามาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

3.1 เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L๓

มาตรฐานทางกายภาพและสภาพแวดล้อม

1. การจัดการบริเวณแวดล้อมทางกายภาพ

1.1. กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

1.2 กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

1.3 ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบ ว่ายังใช้งานได้ตามปกติ

2.การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

2.1 ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

2.2 ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

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

2.5 ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

2.6 มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก

2.7 ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน และป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

2.8 ต้องควบคุมหน่วยงานภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

2.9 สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

2.10 เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง/ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอดระยะเวลาการปฏิบัติงาน

2.11 ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือบริเวณที่มีความสำคัญ

2.12 ต้องทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

มาตรฐานทางกายภาพและสภาพแวดล้อม (ต่อ)

3. ระบบและอุปกรณ์สนับสนุนการทำงาน

3.1 ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของโรงพยาบาลที่เพียงพอต่อความต้องการใช้งาน โดยให้มี

- ระบบสำรองกระแสไฟฟ้า
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง
- ระบบระบายอากาศ
- ระบบปรับอากาศและควบคุมความชื้น
- ระบบป้องกันอัคคีภัย

3.2 ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

3.3 ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติหรือหยุดทำงาน

3.4 จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

มาตรฐานการปฏิบัติงานงานคอมพิวเตอร์ โรงพยาบาลสมเด็จพระยุพราชเลิงนกทา

ข้อตกลงระยะเวลาการให้บริการ SLA (Service Level Agreement)

ลำดับ	กระบวนการทำงาน	ระยะเวลา	หน่วยเวลา	หมายเหตุ
1	ตอบปัญหาทางโทรศัพท์	5 - 10	นาที	ตามความเหมาะสม
2	**Hardware**			
	ติดตั้งระบบปฏิบัติการ + Format	1	ซ.ม.	
	ติดตั้งควบคุม ดูแล server (เครื่อง)	4	ซ.ม.	
	ติดตั้งเครื่องปริ้นเตอร์และ Driver (เครื่อง)	20	นาที	เมื่อมี Driver พร้อมติดตั้ง
	ติดตั้งเครื่องสำรองไฟฟ้า (เครื่อง)	10	นาที	
	ติดตั้งอุปกรณ์คอมพิวเตอร์	15	นาที	
	ซ่อมเครื่องคอมพิวเตอร์	30	นาที	เมื่อมีอุปกรณ์พร้อม
	ซ่อมเครื่องพิมพ์	20	นาที	เมื่อมีอุปกรณ์พร้อม
	เติมหมึก/เปลี่ยนเครื่องพิมพ์	20	นาที	เมื่อมีหมึกพร้อม
	ซ่อมจอคอมพิวเตอร์	15	นาที	เมื่อมีอุปกรณ์พร้อม
	ซ่อมอุปกรณ์ต่อพ่วง	15	นาที	เมื่อมีอุปกรณ์พร้อม
	การบำรุงรักษาคอมพิวเตอร์	30	นาที	
3	**Software**			
	ติดตั้ง Microsoft office	40	นาที	
	ติดตั้ง antivirus	25	นาที	
	ติดตั้ง PACs X-Ray	20	นาที	
	ติดตั้งโปรแกรม HOSxP	35	นาที	
	ติดตั้ง Utility Program	30	นาที	
4	**Network**			
	เพิ่มบัญชีผู้ใช้งานระบบ Internet	15	นาที	
	แก้ไขระบบ Internet ล่มทั้งระบบ	1	ซ.ม.	แล้วแต่ระดับความซับซ้อนของปัญหา
	แก้ไขระบบ Internet ล่มบางจุด	20	นาที	แล้วแต่ระดับความซับซ้อนของปัญหา
	ติดตั้ง Wireless พร้อมเดินสายสัญญาณ (เครื่อง)	1	วัน	เมื่อมีอุปกรณ์พร้อม
5	**HOSxP**			
	เพิ่มบัญชีผู้ใช้งานระบบ HOSxP	15	นาที	
	แก้ไขระบบ HOSxP ล่ม (ทั้งระบบ)	5	ซ.ม.	แล้วแต่ระดับความซับซ้อนของการแสดงผล

	แก้ไขระบบ HOSxP Nonrosponse (ครั้ง)	1	ซ.ม.	แล้วแต่ระดับความซับซ้อนของการแสดงผล
6	**Website**			
	การนำเข้าข้อมูล	1	วัน	เมื่อมีข้อมูลพร้อมนำเข้า
	การแก้ไขการแสดงผล	1-2	วัน	แล้วแต่ระดับความซับซ้อนของการแสดงผล

<u>หมายเหตุ</u>

1. SLA (Service Level Agreement) หมายถึง ข้อตกลงเพื่อรับประกันการบริการระหว่างผู้ให้บริการกับผู้รับบริการ เพื่อเพิ่มความมั่นใจแก่ผู้รับบริการว่าเจ้าหน้าที่จะสามารถให้บริการได้ตามระยะเวลาแต่ละกระบวนงานที่กำหนดไว้ ไม่ถือเป็นข้อผูกพัน อาจมีการเปลี่ยนแปลงได้

2. ระยะเวลาตาม SLA หมายถึง ระยะเวลาการให้บริการ กรณีพื้นฐานปกติของปัญหาในแต่ละด้านทางนิค โดยดุลยพินิจของเจ้าหน้าที่เท่านั้น

<u>เงื่อนไขการดำเนินงาน</u>

หลังจากได้รับแจ้งจะจัดส่งเจ้าหน้าที่ดำเนินการให้ภายในทันที ในกรณีที่เจ้าหน้าที่ พร้อมให้บริการแต่หาก เจ้าหน้าที่ ติดงานให้บริการอื่นอยู่คาดว่าจะเข้าดำเนินการภายใน 30-60 นาทีเป็นอย่างน้อย

ขั้นตอนการติดตั้งโปรแกรมที่จำเป็น

ขั้นตอนการติดตั้งโปรแกรมที่จำเป็น พร้อมระยะเวลาปฏิบัติงาน

ลำดับ	รายชื่อโปรแกรม	ระยะเวลา	หน่วยเวลา	หมายเหตุ
1	ระบบปฏิบัติการ Windows 10	30	นาที	พร้อมอัพเดทระบบ
2	โปรแกรม HOSxP	15-20	นาที	พร้อมอัพเดทระบบ
	- ติดตั้ง Font ที่ระบบจำเป็น			
	- ติดตั้ง From			ตามคำร้องขอแต่ระแผนก
3	โปรแกรม microsoft office 2010	20	นาที	
4	โปรแกรม Smart Refer	5	นาที	
5	โปรแกรม Synapse	5	นาที	
6	โปรแกรม WinRAR	5	นาที	
7	โปรแกรม Adobe Reader	10	นาที	
8	เว็บเบราว์เซอร์ Google Chrome	10	นาที	
9	ติดตั้งไดร์เวอร์ปริ้นเตอร์	15	นาที	ตามรุ่นแต่ละแผนกใช้งาน
10	โปรแกรมอื่นๆ	15	นาที	ตามคำร้องขอแต่ระแผนก
รวมระยะเวลาปฏิบัติงาน		2.25	ซ.ม.	

<u>หมายเหตุ</u>

การติดตั้งระบบปฏิบัติการ Windows และ Program อาจใช้ระยะเวลาที่มีความแตกต่างกัน ขึ้นอยู่กับสเปกจองเครื่องคอมพิวเตอร์นั้น ๆด้วย