เป้าหมายการดำเนินงานสารสนเทศ
โรงพยาบาลบ้านธิ

1. ด้านการวางแผนและออกแบบระบบ

การวางแผนและออกแบบระบบสารสนเทศที่เหมาะสม และตอบสนองความต้องการของผู้ใช้

1. การวางแผนการใช้สารสนเทศในการดูแลรักษาผู้ป่วย การพัฒนาคุณภาพ การบริหาร หรือการศึกษา หรือการวิจัย
2. การออกแบบระบบสารสนเทศให้สอดคล้องกับเป้าหมายของแผน
3. การออกแบบระบบสารสนเทศโดยใช้เทคโนโลยีที่เหมาะสม
4. บุคคลที่เกี่ยวข้องมีส่วนให้ความเห็นที่เป็นประโยชน์ต่อการวางแผนและออกแบบระบบสารสนเทศ
5. การจัดทำและทบทวนแผนบริหารระบบสารสนเทศ ประกอบด้วย
    - มาตรฐานเทคโนโลยี
    - มาตรฐานด้านไอทีของบุคลากร
    - แนวทางปฏิบัติ
    - ระเบียบปฏิบัติ

2. ด้านการดำเนินงานระบบสารสนเทศ

การเชื่อมโยงข้อมูลและสารสนเทศเพื่อใช้ในการบริหาร การดูแลผู้ป่วย และการพัฒนาคุณภาพ

1. การเชื่อมโยงข้อมูล/สารสนเทศจากแหล่งข้อมูลต่างๆ เพื่อประสิทธิภาพของการกระจายข้อมูล/สารสนเทศ หรือ เพื่อลดความขัดแย้งกันของข้อมูลที่เกิดขึ้นจากหลายฐานข้อมูล
2. การสังเคราะห์ แปลผลข้อมูล/สารสนเทศเพื่อประโยชน์ในการบริหาร การดูแลผู้ป่วย การพัฒนาคุณภาพ และการรายงานต่อส่วนราชการ
3. การกระจายข้อมูลและสารสนเทศที่เหมาะสมแก่ผู้ใช้อย่างถูกต้อง ทันเวลา โดยมีรูปแบบและวิธีการที่เป็นมาตรฐานและง่ายต่อการใช้
4. การสนับสนุนทางเทคนิค โดยให้คำปรึกษา และ/หรือให้ความรู้/ฝึกอบรม แก่ผู้ใช้เทคโนโลยีสารสนเทศตามความเหมาะสม

3. ด้านการบริการเวชระเบียน

การจัดระบบบริการเวชระเบียนเพื่อตอบสนองความต้องการของผู้ป่วยและผู้ให้บริการ

1. ระบบดัชนีและระบบการจัดเก็บซึ่งเอื้อต่อการค้นหาเวชระเบียนได้อย่างรวดเร็ว ทันความต้องการของผู้ใช้
2. บริการค้นหาเวชระเบียนตลอด 24 ชั่วโมง
3. เวชระเบียนผู้ป่วยในทุกฉบับได้รับการบันทึกรหัสและทำดัชนีภายในเวลาที่กำหนดไว้
4. ระบบบันทึกเพื่อให้สามารถสืบหาเวชระเบียนที่ถูกยืมออกไปจากหน่วยงานได้

4. ด้านมาตรฐานการบันทึกเวชเวชระเบียน

การจัดทำเวชระเบียนสำหรับผู้ป่วยทุกรายเพื่อให้เกิดการสื่อสารที่ดีระหว่างทีมงานผู้ให้บริการ เกิดความต่อเนื่องในการดูแลรักษา และประเมินคุณภาพการดูแลรักษาได้

1. การจัดทำเวชระเบียนสำหรับผู้ป่วยทุกรายที่เข้ารับบริการของโรงพยาบาล โดยมีข้อมูลและรายละเอียดเพียงพอสำหรับวัตถุประสงค์ต่อไปนี้
    - ทราบว่าผู้ป่วยเป็นใคร
    - ทราบเหตุผลของการรับไว้นอนโรงพยาบาล
    - มีข้อมูลสนับสนุนการวินิจฉัยโรค
    - ประเมินความเหมาะสมของการดูแลรักษาผู้ป่วย
    - ทราบผลลัพธ์และการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ป่วย
    - เอื้ออำนวยต่อการดูแลอย่างต่อเนื่องของผู้ให้บริการ
    - ให้รหัสได้อย่างถูกต้อง
2. นโยบายและวิธีปฏิบัติเป็นลายลักษณ์อักษรสำหรับการบันทึกและการเก็บรายงานผลใน เวชระเบียน

มาตรฐานเทคโนโลยีสารสนเทศ โรงพยาบาลตัวอย่าง

นิยาม

มาตรฐานเทคโนโลยีสารสนเทศ (ICT Standard) หมายถึง แนวทางกรอบกติกาและการจัดการเพื่อใช้อ้างอิงในงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศของโรงพยาบาลตัวอย่าง ทั้งทางด้านซอฟท์แวร์ เครื่องมือ และเทคโนโลยีเพื่อให้การใช้เทคโนโลยีในองค์กรมีทิศทางเดียวกันและตรงกับความต้องการขององค์กร ที่จะนำไปสู่การลดต้นทุนและลดระดับความซับซ้อนในการใช้งานรวมทั้งเกิดความต่อเนื่องของการใช้สารสนเทศในองค์กร ผู้เกี่ยวข้องกับการจัดทำและใช้มาตรฐานเทคโนโลยีสารสนเทศได้แก่ ผู้จัดหา ผู้ดูแล ผู้บริหารจัดการและผู้ใช้อุปกรณ์สารสนเทศ โดยมีฝ่ายวางแผนเทคโนโลยีสารสนเทศขององค์กรเป็นผู้รับผิดชอบปรับปรุงความทันสมัยของมาตรฐานดังกล่าว

วัตถุประสงค์ของการจัดทำมาตรฐานเทคโนโลยีสารสนเทศ

1. เพื่อเป็นแนวทางในการให้บริการและจัดอุปกรณ์ต่างๆให้กับบุคลากรในองค์กร
2. เพื่อให้บุคลากรในองค์กรมีทักษะ ความสามารถไปในทิศทางเดียวกัน สามารถโยกย้ายงานหรือทำการถ่ายโอนความรู้ (Knowledge Transfer) กันได้ง่าย
3. เพื่อเป็นแนวทางในการจัดทำงบประมาณด้าน ICT ของโรงพยาบาลตัวอย่าง

กรรมการสารสนเทศได้แบ่งมาตรฐานเทคโนโลยีสารสนเทศเป็นหมวดใหญ่ๆ 9 หมวดดังนี้

หมวดที่ 1 มาตรฐานสิทธิ์การเบิก/ยืมอุปกรณ์
หมวดที่ 2 มาตรฐาน Hardware
หมวดที่ 3 มาตรฐานโปรแกรมที่ติดตั้งใน PC และ Notebook
หมวดที่ 4 มาตรฐาน e-mail ที่ใช้ในสำนักงาน
หมวดที่ 5 มาตรฐานการจัดเก็บเอกสารแบบอิเลคทรอนิกส์
หมวดที่ 6 มาตรฐานการรักษาความปลอดภัย
หมวดที่ 7 มาตรฐานเกี่ยวกับการพัฒนา Website
หมวดที่ 8 มาตรฐาน Presentation Slide
หมวดที่ 9 มาตรฐานของเครือข่ายคอมพิวเตอร์

ในแต่ละหมวดแบ่งเป็นรายการต่างๆซึ่งสอดคล้องกับนโยบายยุทธศาสตร์ ระเบียบของโรงพยาบาล และเทคโนโลยีด้าน ICT ในปัจจุบัน รายการต่างๆ ที่นำเสนอในคู่มือนี้เป็นเพียงส่วนหนึ่งซึ่งยังไม่ ครอบคลุมถึงรายการอื่นที่อาจมีขึ้นตามความจำเป็นขององค์กรและเทคโนโลยีในอนาคต เนื่องจากเทคโนโลยีสารสนเทศมีการเปลี่ยนแปลงเร็วมาก ดังนั้นคณะกรรมการสารสนเทศจะดำเนินการทบทวนและปรับปรุงรายการต่างๆ เป็นระยะๆ เพื่อให้มีความทันสมัยตามการเปลี่ยนแปลงของเทคโนโลยี

Service Profile

คณะกรรมการสารสนเทศ (IM)

1. บริบท (Context)

โรงพยาบาลบ้านธิ มีระบบบริหารจัดการข้อมูล/สารสนเทศ และได้นำระบบบริการผู้ป่วยโดยใช้ฐานข้อมูลใน ปี 2537 โดยเริ่มต้นด้วยโปรแกรม Mrecord Version Dos ซึ่งเป็นโปรแกรมที่พัฒนาโดย บริษัทเอกชน ต่อมาใน ปี 2551 ได้มีการปรับปรุงระบบโปรแกรม Mrecord จาก Version Dos มาเป็น Version ที่ทำงานบน Windows มาใช้ในการบริหารจัดการข้อมูลตรวจรักษาผู้ป่วย

ปี 2556 ได้นำระบบโปรแกรม HOSxP มาใช้ในการให้บริการโดยสามารถเชื่อมโยงข้อมูลทุกจุดบริการ และเริ่มใช้งานระบบบริหารจัดการข้อมูลตรวจรักษาผู้ป่วย ระบบโปรแกรม Inventory ที่บริหารจัดการงานพัสดุ รวมถึงมีการเชื่อมโยงข้อมูลกับหน่วยงานภายนอกด้วยระบบอินเตอร์เน็ตความเร็วสูง ADSL Fiber Optic และ Leased line

ก.หน้าที่ โครงสร้าง และเป้าหมาย

หน้าที่

1. กำหนดนโยบาย มาตรฐานทางด้านเทคโนโลยีสารสนเทศและเวชระเบียน
2. วางแผนการพัฒนาและออกแบบระบบสารสนเทศให้เชื่อมโยงสอดคล้องกับเป้าหมายการใช้ สารสนเทศขององค์กร
3. รวบรวมข้อมูล วิเคราะห์ สังเคราะห์ และกระจายให้หน่วยงานที่เกี่ยวข้องเพื่อหาโอกาสพัฒนา
4. ส่งเสริมและสนับสนุนให้ทีมและหน่วยงานเข้าใจและสามารถใช้ประโยชน์จากข้อมูลสารสนเทศ
5. ประเมินผลระบบสารสนเทศ การนำข้อมูลไปใช้และวางแผนปรับปรุงระบบ กำหนดมาตรฐานและแนวทางปฏิบัติเกี่ยวกับเวชระเบียนผู้ป่วย
6. สุ่มตรวจสอบความสมบูรณ์ของเวชระเบียนและกำหนดมาตรการเพื่อปรับปรุง
7. สำรวจ ติดตาม ควบคุมกำกับและติดตามการปฏิบัติตามนโยบายและแนวทางปฏิบัติการดำเนินงานด้านระบบสารสนเทศของหน่วยงานต่างๆ
8. ดูแล ควบคุมกำกับและติดตามการจัดเก็บข้อมูล การเผยแพร่ การรักษาความปลอดภัยความลับของผู้ป่วยและการสำรองข้อมูลสำคัญขององค์กร
9. รวบรวมและจัดสรุปผลงานประจำปี

โครงสร้าง

1. นายอนันต์ ครัวอัดเถิง นักวิชาการสาธารณสุข หัวฝ่ายยุทธศาสตร์และและสารสนเทศทางการแพทย์ ประธานกรรมการ
2. นายณรงค์ ปัญญาศรีเลิศ เภสัชกร รองประธานกรรมการ
3. นายวินัย กล่อมแก้ว พยาบาลวิชาชีพ รองประธานกรรมการ
4. นางสุภมาศ ปาระมีแจ้ พยาบาลวิชาชีพ กรรมการ
5. นางสาวนฤภัค ชัยวงศ์ พยาบาลวิชาชีพ กรรมการ
6. นายจตุรงค์ สุริยโต้ นักวิชาการคอมพิวเตอร์ปฏิบัติการ เลขานุการ
7. นายเทพกร โพธาตุ เจ้าพนักงานเวชสถิติ กรรมการ
8. นายจักรกฤษณ์ อโนต๊ะ นักวิชาการสาธารณสุข กรรรมการ

เป้าหมาย

1. ด้านการวางแผนและออกแบบระบบ

1. การวางแผนการใช้สารสนเทศในการดูแลรักษาผู้ป่วย การพัฒนาคุณภาพ การบริหาร หรือการศึกษา หรือการวิจัย
    - การออกแบบระบบสารสนเทศให้สอดคล้องกับเป้าหมายของแผน
    - การออกแบบระบบสารสนเทศโดยใช้เทคโนโลยีที่เหมาะสม
    - บุคคลที่เกี่ยวข้องมีส่วนให้ความเห็นที่เป็นประโยชน์ต่อการวางแผนและออกแบบระบบสารสนเทศ
    - การจัดทำและทบทวนแผนบริหารระบบสารสนเทศ ประกอบด้วย
        - มาตรฐานเทคโนโลยีสารสนเทศ
        - มาตรฐานด้านเวชระเบียน
        - มาตรฐานด้านไอทีของบุคลากร
        - แนวทางปฏิบัติ
        - ระเบียบปฏิบัติ

2. ด้านการดำเนินงานระบบสารสนเทศ การเชื่อมโยงข้อมูลและสารสนเทศเพื่อใช้ในการบริหาร การดูแลผู้ป่วย และการพัฒนาคุณภาพ

1. การเชื่อมโยงข้อมูล/สารสนเทศจากแหล่งข้อมูลต่าง ๆ เพื่อประสิทธิภาพของการกระจายข้อมูล/สารสนเทศ หรือ เพื่อลดความขัดแย้งกันของข้อมูลที่เกิดขึ้นจากหลายฐานข้อมูล
2. การสังเคราะห์ แปลผลข้อมูล/สารสนเทศเพื่อประโยชน์ในการบริหาร การดูแลผู้ป่วยการพัฒนาคุณภาพ และการรายงานต่อส่วนราชการ
3. การกระจายข้อมูลและสารสนเทศที่เหมาะสมแก่ผู้ใช้อย่างถูกต้อง ทันเวลา โดยมีรูป แบบและวิธีการที่เป็นมาตรฐานและง่ายต่อการใช้
4. การสนับสนุนทางเทคนิค โดยให้คำปรึกษา และ/หรือให้ความรู้/ฝึกอบรม แก่ผู้ใช้ เทคโนโลยีสารสนเทศตามความเหมาะสม

3. ด้านการบริการเวชระเบียน การจัดระบบบริการเวชระเบียน เพื่อตอบสนองความต้องการของ ผู้ป่วยและผู้ให้บริการ

1. ระบบดัชนีและระบบการจัดเก็บซึ่งเอื้อต่อการค้นหาเวชระเบียนได้อย่างรวดเร็ว ทัน ความต้องการของผู้ใช้
2. บริการค้นหาเวชระเบียนตลอด 24 ชั่วโมง
3. เวชระเบียนผู้ป่วยในทุกฉบับได้รับการบันทึกรหัสและทำดัชนีภายในเวลาที่กำหนดไว้
4. ระบบบันทึกเพื่อให้สามารถสืบหาเวชระเบียนที่ถูกยืมออกไปจากหน่วยงานได้

4. ด้านมาตรฐานการบันทึกเวชเวชระเบียน การจัดทำเวชระเบียนสำหรับผู้ป่วยทุกรายเพื่อให้เกิดการ สื่อสารที่ดีระหว่างทีมงานผู้ให้บริการ เกิดความต่อเนื่องในการดูแลรักษา และประเมินคุณภาพการ ดูแลรักษาได้

1. การจัดทำเวชระเบียนสำหรับผู้ป่วยทุกรายที่เข้ารับบริการของโรงพยาบาล โดยมีข้อมูลและรายละเอียดเพียงพอสำหรับวัตถุประสงค์ต่อไปนี้

    - ทราบว่าผู้ป่วยเป็นใคร
    - ทราบเหตุผลของการรับไว้นอนในโรงพยาบาล
    - มีข้อมูลสนับสนุนการวินิจฉัยโรค
    - ประเมินความเหมาะสมของการดูแลรักษาผู้ป่วย
    - ทราบผลลัพธ์และการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ป่วย
    - เอื้ออำนวยต่อการดูแลอย่างต่อเนื่องของผู้ให้บริการ
    - ให้รหัสโรคได้อย่างถูกต้อง
    - นโยบายและวิธีปฏิบัติเป็นลายลักษณ์อักษรสำหรับการบันทึกและการเก็บรายงานผลในเวชระเบียน

ข.ขอบเขตหน้าที่ ศักยภาพ ข้อจำกัด

ขอบเขตหน้าที่

1. วางแผนยุทธศาสตร์ แผนการพัฒนา และออกแบบระบบเทคโนโลยีสารสนเทศ
2. กำหนดมาตรฐานเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชด่านซ้าย ทั้งทางด้าน Hardware Software และ People ware เพื่อให้มีทิศทางเดียวกันและสอดคล้องกับแผนยุทธศาสตร์ขององค์กร
3. วางแผนการพัฒนาทักษะด้านไอทีของบุคลากรของโรงพยาบาลทั้งผู้บริหารจัดการ ผู้ดูแลระบบ และผู้ใช้อุปกรณ์สารสนเทศ
4. วางแผนรองรับภัยพิบัติระบบสารสนเทศล่ม แนวทางการแก้ไขปัญหา
5. กำหนดนโยบายการบริหารเวชระเบียน พัฒนาคุณภาพ ประเมิน ทบทวน ตรวจสอบความสมบูรณ์ของเวชระเบียน
6. การรักษาความปลอดภัย ความลับ และการสำรองข้อมูล
7. บริการข้อมูลข่าวสาร และเผยแพร่ข้อมูลทางเว็ปไซต์ของโรงพยาบาล

ศักยภาพ

โรงพยาบาลบ้านธิ เป็นโรงพยาบาลชุมชนขนาด 30 เตียง มีการสนับสนุนระบบไอทีอย่างเพียงพอ เชื่อมโยงระบบข้อมูลโดยระบบเครือข่าย และเชื่อมต่อข้อมูลกับหน่วยงานภายนอกโดยใช้ Internet ความเร็วสูง ADSL , Fiber Optic และ Leased line มีกรรมการสารสนเทศ ,ศูนย์คอมพิวเตอร์ เป็นหน่วยงานรับผิดชอบงานสารสนเทศโดยตรง มีนักวิชาการคอมพิวเตอร์ ที่มีความรู้ความสามารถในการดูแลโปรแกรม และสามารถดูแล ซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์เครือข่าย

ข้อจำกัด

เนื่องจากอำเภอบ้านธิ มีพื้นที่ที่เป็นภูเขาส่วนใหญ่ ทำให้การใช้งานระบบ Internet มีข้อจำกัดในการเชื่อมต่อระบบเครือข่ายกับ โรงพยาบาลส่งเสริมสุขภาพระดับตำบล

ค. ความต้องการของผู้รับผลงานสำคัญ

ผู้รับผลงาน	ความต้องการ
ผู้อำนวยการ	- มีระบบข้อมูลสารสนเทศที่มีประสิทธิภาพเพื่อการบริหาร การจัดบริการ - ระบบคอมพิวเตอร์และระบบเครือข่ายทำงานได้อย่างมีประสิทธิภาพ
กรรมการทีมประสาน	QMT - ข้อมูลข่าวสาร สถิติ ตัวชี้วัดที่สำคัญของโรงพยาบาล - ระบบการจัดการเอกสาร electronic PCT - สถิติข้อมูลที่สำคัญ รายงาน ข้อมูลตัวชี้วัดในเชิงคุณภาพ - มีระบบการรักษาความลับของผู้มารับบริการ - การจัดระบบไอทีเพื่อให้บริการกลุ่มโรคเรื้อรัง เบาหวาน,ความดันโลหิตสูง ของโรงพยาบาล - ระบบข้อมูลงานส่งเสริมป้องกันโรค CT - รพ.สต.มีการใช้โปรแกรม HOSxP PCU ครบทุกแห่ง - สรุปผลการใช้ยาของ รพ.สต.เพื่อบริหารจัดการเรื่องการเบิกจ่ายยา RM - โปรแกรมเก็บข้อมูลและประมวลผลรายงานอุบัติการณ์ความเสี่ยง AIT - รายงานข้อมูลการเงินเพื่อจัดทำระบบบัญชี Winspeed - ระบบงานพัสดุ และรายงาน Ds_Asset - ระบบงานซ่อมบำรุง และรายงาน Ds_Asset - โปรแกรมพิมพ์เช็ค HRD - โปรแกรมบริหารงานบุคลากร การฝึกอบรม การลา
หน่วยงานต่างๆ ใน รพ.	- ข้อมูลที่จัดเก็บในคอมพิวเตอร์ มีความปลอดภัย รวดเร็ว ถูกต้อง - คอมพิวเตอร์ที่ใช้งานในระบบ LAN โปรแกรม HOSxP ที่มีประสิทธิภาพตลอด 24ชม. - บุคลากรมีความรู้ ความสามารถในการแก้ไขปัญหาเกี่ยวกับสารสนเทศ - มีระบบป้องกันการระบุตัวผู้ป่วยผิดคน การเตือนการแพ้ยา หรือระบบข้อความเตือนอื่นๆเพื่อสื่อสารในการให้บริการ - ข้อมูลรายงานต่างๆ มีความถูกต้อง ครบถ้วน และทันเวลา - ข้อมูลการรักษาพยาบาล ถูกต้อง ครบถ้วน - มีการปรับปรุงสิทธิผู้มารับบริการให้ถูกต้องและเป็นปัจจุบัน - ข้อมูลรายงานค่าใช้จ่ายผู้รับบริการมีความถูกต้อง ครบถ้วน
ผู้มารับบริการและญาติ	- ข้อมูลที่จัดเก็บในคอมพิวเตอร์ จัดเก็บได้อย่างถูกต้อง ปลอดภัย และเป็นความลับ - มีระบบบริการที่รวดเร็ว มีประสิทธิภาพ
สสจ.ลำพูน	- การจัดส่งรายงานครบถ้วน ถูกต้อง ทันเวลา
บุคคลภายนอก	- มีเว็ปไซด์เพื่อประชาสัมพันธ์ แจ้งข่าวสารข้อมูลที่เป็นปัจจุบัน

	- มีช่องทางการติดต่อสื่อสารข้อมูลและตอบข้อสงสัย หรือนัดหมายกับแพทย์
สปสช./กระทรวง	- มีการส่งข้อมูลที่ถูกต้อง ครบถ้วน ทันเวลา

ง. ประเด็นคุณภาพที่สำคัญ

1. ข้อมูลสารสนเทศมีความถูกต้อง น่าเชื่อถือ ทันเวลาและตอบสนองต่อการนำไปใช้งาน
2. มีการรักษาความลับอย่างเหมาะสม
3. มีระบบคอมพิวเตอร์ใช้งานได้อย่างมีประสิทธิภาพ มีการสำรองข้อมูล และมีแผนรองรับในการแก้ไขปัญหาป้องกันระบบล่ม

จ. ความท้าทาย ความเสี่ยงสำคัญ

ความท้าทาย

1. พัฒนาระบบข้อมูลข่าวสารเพื่อนำสารสนเทศมาใช้ในการพัฒนาองค์กร
2. พัฒนาระบบเทคโนโลยีที่เอื้อต่อการทำงานและส่งเสริมคุณภาพชีวิตที่ดีของบุคลากร
3. ข้อมูลเวชระเบียนผู้ป่วยมีความสมบูรณ์
4. พัฒนาระบบการเชื่อมโยงข้อมูลผู้ป่วยระหว่างโรงพยาบาล และโรงพยาบาลส่งเสริมสุขภาพตำบล

ความเสี่ยงที่สำคัญ

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลตัวเอย่างพบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

1. **เจ้าหน้าที่หรือบุคลากรของหน่วยงาน(Human error)** เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้ประชุมชี้แจงและจัดให้เจ้าหน้าที่เข้ารับการอบรม ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด
2. **ไวรัสคอมพิวเตอร์ (Computer Virus)**สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้
3. **ระบบไฟฟ้าขัดข้องหรือความเสียหายจากเพลิงไหม้** โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า(UPS)เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย(server) กรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์ จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคาร และทำป้ายบอกจุดติดตั้งเพื่อดับเพลิง

4. **โจรกรรมการขโมยอุปกรณ์คอมพิวเตอร์**ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ล็อคประตูทุกครั้งและติดตั้งกล้องวงจรปิดเพื่อตรวจสอบและจำกัดทางเข้าออกในช่วงนอกเวลาราชการ

2. กระบวนการสำคัญ (Key Process)

กระบวนการสำคัญ	สิ่งที่คาดหวัง	ตัวชี้วัดที่สำคัญ
1.วางแผนยุทธศาสตร์ แผนการพัฒนาและออกแบบระบบเทคโนโลยีสารสนเทศ	• ข้อมูล สารสนเทศมีคุณภาพสามารถมานำใช้ในการบริหาร บริการ และพัฒนาคุณภาพได้ • ข้อมูลมีความถูกต้อง ครบถ้วน ตรงตามความต้องการของหน่วยงาน	ร้อยละความสำเสร็จของ การดำเนินงานปรับปรุงพัฒนาระบบเครือข่ายตามแผน
2.กำหนดมาตรฐานเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระยุพราชด่านซ้าย ทั้งทางด้านHardware Software People wareเพื่อให้มีทิศทางเดียวกันและสอดคล้องกับแผนยุทธศาสตร์ขององค์กร	• ระบบ IT ที่มีคุณภาพและเพียงพอต่อการให้บริการในหน่วยงาน • Hardware software มีมาตรฐาน	ร้อยละความสำเร็จของ การดำเนินงานพัฒนา Software ตามแผน
3.วางแผนการพัฒนาทักษะด้านไอทีของบุคลากรของโรงพยาบาลทั้งผู้บริหาร จัดการ ผู้ดูแลระบบ และผู้ใช้อุปกรณ์สารสนเทศ	• บุคลากรที่มีความรู้ด้านเทคโนโลยีสารสนเทศที่เหมาะสม	ร้อยละของบุคลากรกลุ่มเป้าหมายผ่านการอบรมทักษะความรู้ตามเกณฑ์ที่กำหนด
4.วางแผนรองรับภัยพิบัติระบบสารสนเทศล่ม แนวทางการแก้ไขปัญหา	• มีแนวทางป้องกัน และแก้ไขปัญหากรณีระบบเครือข่ายล่ม	
5. กำหนดนโยบายการบริหารเวชระเบียน พัฒนาคุณภาพ ประเมิน ทบทวน ตรวจสอบความสมบูรณ์ของเวชระเบียน	• การลงบันทึกข้อมูลในเวชระเบียนมีความสมบูรณ์ • เพื่อให้เกิดการสื่อสารระหว่างทีมสหวิชาชีพ • มีข้อมูลในการดูแลรักษาผู้ป่วยอย่างต่อเนื่องประเมินผลคุณภาพการรักษาได้	อัตราความสมบูรณ์ของเวชระเบียน
6. การรักษาความปลอดภัย ความลับและการสำรองข้อมูล	• ข้อมูลมีความปลอดภัย และมีระบบสำรองข้อมูลที่มีประสิทธิภาพ	
7. บริการข้อมูลข่าวสาร และเผยแพร่		

ข้อมูลทางเว็ปไซด์ของโรงพยาบาล		

3. ผลการดำเนินงานตามตัวชี้วัดคุณภาพ

ลำดับ	ตัวชี้วัด	เป้า	ปี2557	หมายเหตุ
1.				
2.				
3.				
4.				
5.				

4. ผลงานและความภาคภูมิใจ

1. จัดทำ Datacenter โดยเชื่อมโยงข้อมูลระหว่างโรงพยาบาลและ รพ.สต.ทุกแห่ง ทำให้สามารถตรวจสอบและส่งต่อข้อมูลการเข้ารับบริการของสถานบริการแต่ละแห่งในเขตอำเภอบ้านธิ
2. พัฒนา Software เพื่อใช้ในงานของโรงพยาบาล ทำให้ลดค่าใช้จ่ายในการจัดซื้อโปรแกรม
    1. โปรแกรม DSHOSxP
    2. โปรแกรม พิมพ์เช็ค
    3. โปรแกรม เยี่ยมบ้าน/รายงาน
    4. โปรแกรม บริหารความเสี่ยง (Risk Management)
    5. โปรแกรม DSDENT
3. พัฒนาการลงบันทึก การตรวจสอบข้อมูล ทำให้ข้อมูล 18 จากการประมวลผลของ สปสช. มีความสมบูรณ์ร้อยละ 99.99
4. พัฒนาระบบงานพัสดุ ทำให้สามารถบริหารจัดการพัสดุต่างๆ ได้อย่างมีประสิทธิภาพ
5. การจัดทำศูนย์ข้อมูลเอกสารโดยใช้ Dropbox ทำให้สามารถเชื่อมโยงเอกสารต่างๆ ลดความซ้ำซ้อนในการจัดทำเอกสาร มีความสะดวก รวดเร็วมากขึ้น
6. พัฒนาระบบออกหน่วยบริการคลินิกพิเศษที่ รพ.สต. โดยมีระบบบันทึกข้อมูลที่เชื่อมโยงกับฐานข้อมูลของโรงพยาบาล ทำให้ลดความซ้ำซ้อนของการลงบันทึกข้อมูล
7. โรงพยาบาลสมเด็จพระยุพราชด่านซ้าย ศูนย์ฝึกอบรมและศึกษาดูงานการพัฒนาระบบสารสนเทศโดยโปรแกรม HOSxP ให้กับเจ้าหน้าที่ของโรงพยาบาล

5.แผนพัฒนาต่อเนื่อง

1. พัฒนาระบบ Datacenter ให้สามารถนำไปใช้ประโยชน์ในการบริการผ่านโปรแกรม HOSxP และ JHCIS รวมถึงการจัดทำระบบรายงานต่างๆ ให้ครบถ้วน ถูกต้อง สมบูรณ์และเป็นปัจจุบัน
2. ฝึกอบรมบุคลากรในการใช้ Software Open source ให้ได้ตามแผน

3. ปรับเปลี่ยน Software ที่ใช้งานให้เป็น Free Software และ Softwareที่ถูกต้องตามลิขสิทธิ์
4. พัฒนาระบบ Internet โดยแยกออกจากระบบงานปกติ และให้ครอบคลุมการใช้งานในส่วนของโรงพยาบาลและบ้านพัก
5. พัฒนาการ Web blogs เพื่อเผยแพร่ผลงานสำหรับทีมประสานและหน่วยงาน

6. SP-IMT-ระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสำหรับสารสนเทศ
7. SP-IMT-ระเบียบปฏิบัติเมื่อระบบเครือข่ายใช้งานไม่ได้
8. SP-IMT-ระเบียบปฏิบัติเมื่อเกิดปัญหาบุคลากรที่ดูแลระบบคอมพิวเตอร์
9. SP-IMT-ระเบียบปฏิบัติการประเมินและการปรับปรุงเวชระเบียน
10. SP-IMT-ระเบียบปฏิบัติการรักษาความลับและความปลอดภัยของข้อมูล
11. SP-IMT-ระเบียบปฏิบัติการปฐมนิเทศบุคลากรใหม่เกี่ยวกับระบบเทคโนโลยีสารสนเทศ
12. SP-IMT-ระเบียบปฏิบัติการบันทึกและการตรวจประเมินคุณภาพการบันทึกเวชระเบียน

แผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

โรงพยาบาลบ้านธิ ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการประชาชนได้รับความสะดวก ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัยหรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศส่งผล กระทบต่อการดำเนินงานของโรงพยาบาล เพื่อป้องกันและแก้ไขปัญหาดังกล่าวกรรมการสารสนเทศโรงพยาบาลตัวอย่าง ได้เล็งเห็นความจำเป็นที่จะต้องมีแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาล

การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลตัวอย่างพบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

1. เจ้าหน้าที่หรือบุคลากรของหน่วยงาน(Human error)เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้ประชุมชี้แจงและจัดให้เจ้าหน้าที่เข้ารับการอบรมให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด
2. ไวรัสคอมพิวเตอร์ (Computer Virus)สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้ มีการดำเนินการดังนี้
3. ระบบไฟฟ้าขัดข้องหรือความเสียหายจากเพลิงไหม้ โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS)เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย(server) กรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์ จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่าง

ปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุม ป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคารและทำป้ายบอกจุดติดตั้งเพื่อดับเพลิง

4. โจรกรรมการขโมยอุปกรณ์คอมพิวเตอร์ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้ามผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ล็อคประตูทุกครั้งและติดตั้งกล้องวงจรปิดเพื่อตรวจสอบและจำกัดทางเข้าออกในช่วงนอกเวลาราชกา

การสำรองข้อมูล

การสำรองข้อมูล(Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย โจรกรรม หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ มีแนวทางโดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลดังนี้ (WI-IMT-027)

1. จัดเก็บข้อมูลใน Server หลัก จัดทำเป็น RAID-5 โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน 5 ลูก
2. จัดเก็บข้อมูลใน Server รอง ตัวที่ 1 จัดทำเป็น RAIDS-5 โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน 5 ลูก
3. จัดเก็บข้อมูลใน Server รอง ตัวที่ 2 โดยใช้การทำ Auto Back up แบบ Full วันละ 1 ครั้งเวลา 00.00 น. และมีการทดสอบข้อมูลสำรองเดือนละ 1 ครั้งโดยการนำข้อมูลไปใช้ในการออกหน่วยให้บริการผู้ป่วยที่ รพ.สต.
4. จัดเก็บข้อมูลสำรองเก็บไว้ในเครื่อง Personal computer ที่เป็นเครื่องลูกข่าย โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time
5. การ Copy ข้อมูล Back up เก็บไว้ใน Hard disk External
6. การจัดพิมพ์เอกสารรายงานการใช้บริการของผู้ป่วยนอกและผู้ป่วยในเพื่อเก็บเป็นหลักฐานการเข้ารับบริการทุกวัน

การเตรียมการป้องกัน

1. การป้องกันไวรัสคอมพิวเตอร์ มีการติดตั้งซอฟท์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งระบบปฏิบัติการเป็น Linux และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายติดตั้ง Software ป้องกันไวรัส และป้องกันการใช้อุปกรณ์สื่อพกพาอื่นๆ เช่น Flash drive , Harddisk Ext. การกำจัดการใช้งาน Internet เช่นการ download การป้องกันการถอดถอนหรือติดตั้งโปรแกรมเพิ่ม เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้
2. การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ
3. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ 20-30 นาที
4. เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

5. เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้ทำการบันทึกข้อมูลที่ยังค้างอยู่ทันที ปิดเครื่องคอมพิวเตอร์ และอุปกรณ์ต่อพ่วงต่างๆ
6. มีระบบป้องกันไฟไหม้ เนื่องจากยังขาดงบประมาณในการสนับสนุนการปรับปรุงห้องคอมพิวเตอร์แม่ข่าย จึงยังไม่มีระบบป้องกันไฟไหม้ที่เหมาะสม แต่ในเบื้องต้น มีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น
7. การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้
8. มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก
9. มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยจะเปิดใช้งานFirewall ตลอดเวลา
10. มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
11. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป
12. การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ

การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัย คุกคามคอมพิวเตอร์

การจัดเตรียมอุปกรณ์ที่จำเป็น ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์คอมพิวเตอร์ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ ดังนี้

1. แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ ข้อมูลสำรองระบบงานที่สำคัญ
2. แผ่นโปรแกรม antivirus/spyware
3. แผ่น driver อุปกรณ์ต่างๆ
4. ระบบสำรองไฟฉุกเฉิน
5. อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์
6. การรักษาความปลอดภัยด้วยรหัสผ่าน เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องสามารถเข้าถึง แก้ไข,เปลี่ยนแปลงข้อมูลหรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดยกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความ

ปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละระดับฐานข้อมูล ดังนี้

7. บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลในส่วนนี้ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบเป็นผู้อนุมัติให้ดำเนินการได้โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

8. กำหนดระยะเวลาการใช้งานระบบสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า6 ตัวอักษรและควรใช้ตัวเลข,อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ 3 เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันทีเพื่อป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

ระเบียบปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติต่างๆ ดังนี้

WI-IMT-020-เรื่อง การปฏิบัติกรณีไฟฟ้าดับ

WI-IMT-021-เรื่อง การปฏิบัติกรณีเครื่องคอมพิวเตอร์ลูกข่าย/อุปกรณ์เครือข่ายขัดข้อง

WI-IMT-022-เรื่อง การปฏิบัติกรณีเครื่อง Server /Database มีปัญหา

WI-IMT-023-เรื่อง การปฏิบัติกรณีเกิดอัคคีภัย

แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 24 ชั่วโมง
4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5. นำ BACKUP / DVD/ HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบผู้ดูแลระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 28 ชั่วโมง
6. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง