โรงพยาบาลบ้านไร่ จ.อุทัยธานี Banrai Hospital,Uthaithani	**แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ปีงบประมาณ ๒๕๖๖** **(Information Technology Plan)**	ฉบับที่ : ..... แก้ไขครั้งที่ : ..... วันที่มีผลบังคับใช้ : .....

หน่วยงาน : โรงพยาบาลบ้านไร่

หน่วยงานที่จัดทำ : ประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์

ผู้จัดทำ :

๑. นางสาวแอนนา แก้วการไร่

๒. นางสาวอรอุมา โพธิ์ประจันทร์

(นางสาวแอนนา แก้วการไร่)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๓ / ม.ค. / ๒๕๖๖

ผู้เห็นชอบ

(นางวลัยพร เฮ้งบริบูรณ์พงศ์)
นักวิชาการสาธารณสุขปฏิบัติการ
๓ / ม.ค. / ๒๕๖๖

ผู้อนุมัติ

(นายวิชาญ แป้นทอง)
ผู้อำนวยการโรงพยาบาลบ้านไร่
๓ / ม.ค. / ๒๕๖๖

บันทึกการปรับปรุงแก้ไขแผน

วันที่แก้ไข	เนื้อหา	ผู้แก้ไข

สารบัญ

โรงพยาบาลบ้านไร่ จ.อุทัยธานี
Banrai Hospital,Uthaithani

แผนการบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ

ประจำปีงบประมาณ ๒๕๖๖

โรงพยาบาลบ้านไร่
๓ มกราคม พ.ศ. ๒๕๖๖

บทที่ ๑ บทนำ

ยุทธศาสตร์กระทรวงสาธารณสุข พ.ศ.๒๕๖๑ - ๒๕๘๐ เป้าหมายให้ประชาชนทุกคนในเขตเครือข่ายบริการได้รับบริการที่มีคุณภาพมาตรฐานทุกระดับและเข้าถึงเทคโนโลยีที่ทันสมัยในเขตเครือข่ายบริการ สำนักงานสาธารณสุขจังหวัดอุทัยธานี จึงได้จัดทำแผนบริหารความเสี่ยงขึ้นเพื่อใช้เป็นแนวทางปฏิบัติในการลดความเสียหายต่างๆที่อาจเกิดขึ้นและส่งผลต่อกระบวนการบริหารงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร การบริหารงานจึงต้องมีการดำเนินการตาม IT Governance เพื่อให้เกิดการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศที่ส่งผลต่อการพัฒนาองค์กร

IT Governance คือหน้าที่และความรับผิดชอบในการจัดการที่ดีทางด้านเทคโนโลยีสารสนเทศควบคู่กับความสามารถด้านอื่นๆ ของคณะกรรมการและผู้บริหารระดับสูงที่ใช้เป็นกรอบ ในกระบวนการบริหารงานภายใน การปฏิบัติตามนโยบาย กลยุทธ์เพื่อสร้างศักยภาพ เพิ่มคุณค่าและการเติบโตอย่างยั่งยืนให้กับองค์กร โดยดำเนินการควบคู่ไปกับการกำกับดูแลกิจการที่ดี การบริหารความเสี่ยงตามองค์ประกอบของการจัดการด้าน IT เริ่มตั้งแต่การวางแผน การจัดองค์กร พนักงาน การดำเนินการและการควบคุม

IT Governance ทำให้เกิดการบริหารและบูรณาการที่เป็นระบบระเบียบเป็นขั้นตอนลดความซ้ำซ้อน ลดความเสี่ยง เพิ่มศักยภาพ โดยสามารถทำงานข้ามสายงานและประสานงานระหว่างองค์กรได้อย่างรวดเร็ว ทันเวลา มีประสิทธิภาพ สอดประสานกับการดำเนินงานระดับต่างๆ จากการใช้ความสามารถและศักยภาพของเทคโนโลยีสารสนเทศ และทรัพยากรต่างๆ เพื่อผลักดันความสำเร็จของการจัดการองค์กรอย่างทั่วถึงเป็นกระบวนการ

โรงพยาบาลบ้านไร่ ได้ประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประจำปีงบประมาณ ๒๕๖๔ มุ่งเน้นนำเทคโนโลยีสารสนเทศเข้ามาใช้การปฏิบัติงานหลายด้าน ให้ตระหนักถึงความสำคัญของการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ซึ่งอาจเกิดขึ้นในระบบบริหารงาน การสั่งการและการปฏิบัติงานตามนโยบายรัฐบาล การดำเนินงานดังกล่าวทำให้ข้อมูลและสารสนเทศต่างๆ ที่ใช้ในการบริหารงานมีปริมาณที่มากมาย มีความเคลื่อนไหวตลอดเวลา โดยเฉพาะอย่างยิ่งข้อมูลสารสนเทศที่ให้บริการประชาชนด้านสาธารณสุข รวมทั้งข้อมูลและสารสนเทศที่หน่วยงานต้องรับผิดชอบตามกระบวนการประมวลผลข้อมูลตามนโยบายสำคัญต่าง ๆ จึงจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาที่อาจเกิดขึ้น และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานนั้นเกิดประโยชน์สูงสุด โรงพยาบาลบ้านไร่จึงได้จัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศขึ้น

/วัตถุประสงค์...

๑. วัตถุประสงค์

๑.๑ เพื่อให้ฝ่ายบริหาร/ฝ่ายปฏิบัติการของทุกหน่วยงานในสังกัดเข้าใจหลักการและกระบวนการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑.๒ เพื่อให้ผู้ปฏิบัติได้ตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นได้และดำเนินการจัดการความเสี่ยงที่เกี่ยวข้อง

๑.๓ เพื่อให้มีการปฏิบัติตามกระบวนการบริหารความเสี่ยงอย่างเป็นระบบและต่อเนื่อง

๑.๔ เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๒. สภาพแวดล้อมด้านเทคโนโลยีสารสนเทศ

จากเหตุการณ์ ไวรัสเรียกค่าไถ่ Ransom ware ของโรงพยาบาลสระบุรี เมื่อวันที่ ๙ กันยายน ๒๕๖๓ ทำให้ระบบคอมพิวเตอร์ของโรงพยาบาลสระบุรี ไม่สามารถเข้าถึงข้อมูลผู้ป่วยที่อยู่ในเซิร์ฟเวอร์ได้ ซึ่งข้อมูลที่โดนเข้ารหัสนั้น เป็นข้อมูลคนไข้ในระบบซึ่งเป็นข้อมูลที่จำเป็นต่อการรักษา และวินิจฉัยโรคเป็นอย่างมาก แม้ว่าทางโรงพยาบาลได้มีการ Backup ข้อมูลบางส่วนเอาไว้บ้าง แต่ข้อมูลเหล่านั้นเป็นข้อมูลเก่าตั้งแต่ปี ๒๕๕๘ ทำให้ไม่สามารถหยิบเอามาใช้ได้เลย ในส่วนของโรงพยาบาลบ้านไร่ ก็มีระบบข้อมูลสารสนเทศและอุปกรณ์ด้านฮาร์ดแวร์ที่เกี่ยวข้องกับการรวบรวมประมวลผล จัดทำรายงานและเผยแพร่ข้อมูลสารสนเทศเช่นเดียวกันที่ต้องจัดการบริหารความเสี่ยงหลายระบบงาน เช่น เว็บเซิร์ฟเวอร์เผยแพร่ข่าวสารโรงพยาบาลบ้านไร่ ประกาศจัดซื้อ/ประกาศจัดจ้าง, ประกาศ ITA ,แผนยุทธศาสตร์และแผนปฏิบัติการต่าง ๆ ,ระบบ HOSxPV๔ ,ระบบ e-claim, ระบบ Threerefer ฯลฯ ในด้านการสื่อสารก็มีการใช้ e-mail, Facebook และ LINE สื่อสารไปยังกลุ่ม เป้าหมายผู้ปฏิบัติและผู้บริหารทุกระดับ หากมีสถานการณ์เร่งด่วนจะใช้ระบบประชุมทางไกล (Web-Conference) และระบบอุปกรณ์ VDO Conference กับส่วนกลาง สื่อสารสองทางได้ชัดเจนและรวดเร็ว ดังเช่น การประชุมทุกสัปดาห์ในการติดตามสถานการณ์ โรคติดเชื้อไวรัสโคโรน่า 2019 ที่ผ่านมาทำให้ผู้บริหารได้ทราบปัญหาและอุปสรรคในการปฏิบัติงานจากหน่วยงานในสังกัดทั่วพื้นที่จังหวัดอุทัยธานี และตัดสินใจแก้ไขปัญหา มอบนโยบายสั่งการได้อย่างทันเหตุการณ์ ในส่วนของการป้องกันการบุกรุกทางเครือข่ายได้ประสานกับ บริษัท กสท โทรคมนาคม จำกัด(มหาชน) ซึ่งเป็นผู้ให้บริการป้องกันการบุกรุกทางเครือข่าย มาวางระบบป้องกันการโจมตีเครือข่ายเทคโนโลยีสารสนเทศภายในโรงพยาบาลทุกแห่ง ในส่วนของระบบคลังข้อมูลสุขภาพ (Data Center) ได้จัดให้มีการเชื่อมโยงกับหน่วยงานในสังกัดทุกแห่ง เพื่อรับส่งข้อมูล ๔๓ แฟ้มเป็นประจำทุกวัน พร้อมทั้งมีระบบ back up ข้อมูลเป็นประจำเพื่อป้องกันความเสี่ยงจากการเสียหายข้อมูลในรูปแบบต่างๆ

/๑.ระบบฐาน...

๑.ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software)

ลำดับ	ชื่อระบบงาน	ผู้รับผิดชอบ	เบอร์โทรศัพท์
๑	เว็บไซต์โรงพยาบาลบ้านไร่	นายภาสกร ป้อมคำ	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๒	ระบบจองห้องประชุมและ Web Conference	นายภาสกร ป้อมคำ	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๓	ระบบจัดการข้อมูล สถานการณ์ COVID-19	น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๔	ระบบ HOSxPV๔	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๕	ระบบรายงานโรงพยาบาลบ้านไร่	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๖	ระบบตัวชี้วัดการดำเนินงานโรงพยาบาลบ้านไร่	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๗	ระบบงบจ่ายตามตัวชี้วัดเกณฑ์คุณภาพและผลงานบริการปฐมภูมิ (QOF)	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๘	ระบบการตรวจสอบคุณภาพข้อมูล OP/PP individual	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๙	ระบบศูนย์ข้อมูลสุขภาพ ๔๓ แฟ้ม HDC	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๐	ระบบคลังข้อมูลสุขภาพ (Data center)	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๑	ระบบ sync คลังข้อมูลสุขภาพ (Data center)	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๒	ระบบ sync Uthai SEPSIS	น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๓	ระบบ Three refer	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๔	ระบบ CH๒U	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๕	ระบบประชุมทางไกล (Cisco Webex Conference)	นายภาสกร ป้อมคำ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๖	ระบบจัดหาคอมพิวเตอร์	น.ส.แอนนา แก้วการไร่	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๗	ระบบตรวจสอบป้องกันการบุกรุกทางเครือข่าย (Firewall)	นายภาสกร ป้อมคำ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๘	ระบบเรียกคิว ตู้ส่งตรวจอัตโนมัติ	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๑๙	ระบบยา RDU	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๒๐	ระบบ X-Ray (DBViewer)	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๒๑	ระบบ LAB (LIS)	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓
๒๒	ระบบ RCM	น.ส.แอนนา แก้วการไร่ น.ส.อรอุมา โพธิ์ประจันทร์	๐-๕๖๕๓๙-๐๐๐-๑๒๓

/๒.ระบบเครือข่าย...

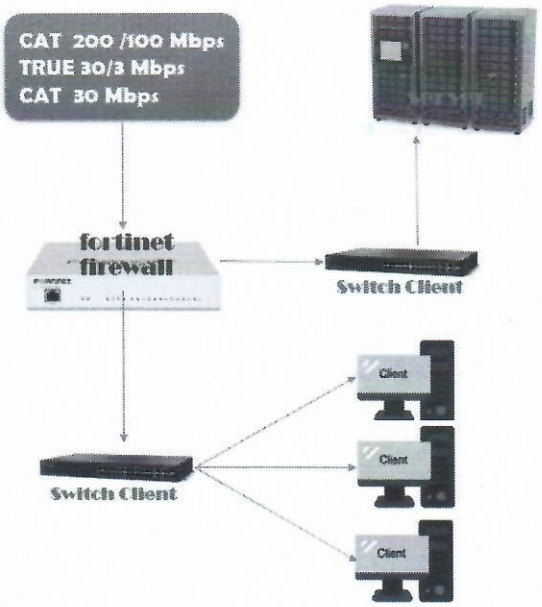
๒.ระบบเครือข่าย

โรงพยาบาลบ้านไร่ ได้มีการจัดทำแผนแม่บทเทคโนโลยีสารสนเทศ มาแล้วหลายฉบับตามแนวทางที่กระทรวงสาธารณสุข วางแนวทางการพัฒนาโครงสร้างพื้นฐานด้านเครือข่ายคอมพิวเตอร์ โดยเน้นให้ทุกหน่วยงานต้องมีระบบเครือข่ายเชื่อมต่อไปยังส่วนกลางเพื่อให้เกิดระบบเครือข่ายอินทราเน็ตกับกระทรวงสาธารณสุข ใช้รับส่งข้อมูล ๔๓ แฟ้ม แต่ในทางปฏิบัติแล้วไม่สามารถดำเนินการได้อย่างมีประสิทธิภาพมากนัก อันเนื่องมาจากโครงการต่างๆในการพัฒนาเครือข่ายคอมพิวเตอร์จำเป็นต้องใช้เงินลงทุนด้าน Hardware Software และโครงข่ายด้านสาธารณูปโภคเป็นจำนวนมาก ปีใดไม่ได้งบ ประมาณเพียงพอ การพัฒนาเครือข่ายก็ขาดประสิทธิภาพเมื่อเทียบกับปริมาณข้อมูลที่เพิ่มขึ้นเรื่อยๆ

อย่างไรก็ตาม การพัฒนาเครือข่ายคอมพิวเตอร์ของโรงพยาบาลบ้านไร่ ก็ได้รับความสำเร็จมาระดับหนึ่ง จากผู้บริหารที่ให้ความสำคัญกับเทคโนโลยีที่ปัจจุบันมีการพัฒนาปรับเปลี่ยนระบบเครือข่ายให้มีความยืดหยุ่น หลายหลายการเชื่อมโยง และเพิ่มปริมาณ Bandwidth ให้มีขนาดใหญ่ขึ้น มีความรวดเร็วในการ Access ข้อมูล รวมทั้งมีอุปกรณ์ป้องกันการบุกรุกทางเครือข่ายอินเตอร์เน็ตที่มีประสิทธิภาพมากขึ้น รองรับการขยายเครือข่ายคอมพิวเตอร์ของโรงพยาบาลบ้านไร่ได้ในอนาคต

การออกแบบสถาปัตยกรรมของระบบเครือข่ายภายในคำนึงถึงหลักการออกแบบ ดังนี้

- Reliability ต้องการให้ระบบเครือข่ายมีความน่าเชื่อถือได้มากที่สุด โดยพยายามลดจุดที่เสี่ยงต่อการทำให้ระบบล่มสลาย (Single point of failure)
- Scalability ต้องการให้ระบบสามารถรองรับต่อการขยายขนาดของระบบในอนาคตได้
- Manageability ต้องการให้ระบบง่ายต่อการบริหารและจัดการ คำนึงถึงความปลอดภัยบนระบบเครือข่าย



ผังการเชื่อมต่อระบบเครือข่าย ภายในโรงพยาบาลบ้านไร่

/๓.นโยบายการ...

๓.นโยบายการบริหารความเสี่ยง

เพื่อสร้างความตระหนักกระตุ้นให้เจ้าหน้าที่โรงพยาบาลบ้านไร่เห็นถึงความจำเป็นในการระมัดระวังต่อสถานการณ์ที่คุกคามต่อประสิทธิภาพการปฏิบัติงาน การบริหารงานและอาจทำให้เกิดความเสียหายต่อระบบฐานข้อมูลสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญที่สุดในการให้บริการประชาชนและการตัดสินใจของผู้บริหาร

แผนบริหารความเสี่ยง จะช่วยให้เจ้าหน้าที่ที่เกี่ยวข้องทราบถึงแนวทางในการปฏิบัติ ซึ่งจะถือเป็นส่วนหนึ่งของการดำเนินงาน การปฏิบัติเพื่อหลีกเลี่ยงความเสี่ยงต่างๆ หรือลดความรุนแรงของผลเสียหายที่อาจเกิดขึ้น

๔.ความหมายและคำจำกัดความของการบริหารความเสี่ยง

๑. ความเสี่ยง (Risk) หมายถึง ภาวะคุกคาม ปัญหา อุปสรรค หรือการสูญเสียโอกาส ซึ่งจะมีผลทำให้โรงพยาบาลบ้านไร่ไม่สามารถบรรลุวัตถุประสงค์ที่กำหนดไว้ หรือก่อให้เกิดผลเสียหายต่อหน่วยงาน โดยเฉพาะอย่างยิ่งผลเสียต่อระบบเทคโนโลยีสารสนเทศที่ใช้ในการบริหารงานและปฏิบัติการโดยเฉพาะอย่างยิ่งการบริการประชาชน

๒. การบริหารความเสี่ยง (Risk Management) หมายถึง การกำหนดแนวทางและกระบวนการในการบ่งชี้ วิเคราะห์ ประเมิน จัดการและติดตามความเสี่ยงที่เกี่ยวข้องกับกิจกรรม หน่วยงาน หรือกระบวนการดำเนินงานของโรงพยาบาลบ้านไร่ รวมทั้งการกำหนดวิธีการในการบริหารและควบคุมความเสี่ยงให้อยู่ในระดับที่ผู้บริหารระดับสูงยอมรับได้

๓. ระบบเทคโนโลยีสารสนเทศและการสื่อสารหมายถึง ระบบเครือข่ายคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์ ระบบเครื่องสื่อสาร ระบบฐานข้อมูล และอุปกรณ์ประกอบระบบต่าง ๆ รวมทั้งอาคารสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบประมวลผลฐานข้อมูลทั้งหมด

๔. ผู้ใช้งาน หมายถึง ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารของหน่วยงาน

๕. สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวกับระบบสารสนเทศของหน่วยงาน

๖. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

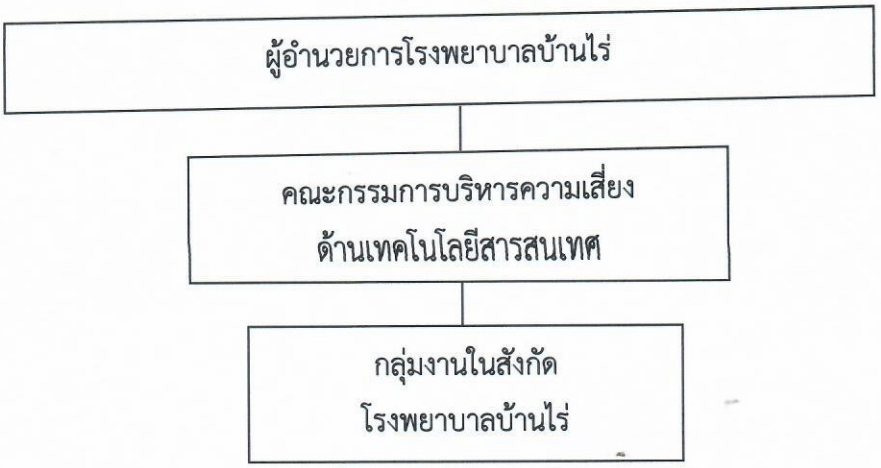
๗. ความมั่นคงปลอดภัยด้านการสารสนเทศ (information security) หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๘. เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

/๙. สถานการณ์...

๙. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected)ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๕. โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านไร่



บทบาทหน้าที่

๑. ถ่ายทอดนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของโรงพยาบาลบ้านไร่ให้บุคลากรในหน่วยงาน มีความรู้ ความเข้าใจ และปฏิบัติตามกฎอย่างเคร่งครัด

๒. ดำเนินการให้หน่วยงานมีระบบฐานข้อมูลที่สนับสนุนการปฏิบัติงานตามภารกิจของหน่วยงานได้อย่างมีประสิทธิภาพ และมีระบบบริหารจัดการเครือข่ายคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

๓. กำหนดมาตรฐานแนวปฏิบัติหรือวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่มาติดต่องานบริการภายในหน่วยงาน ให้ตระหนักถึงความความมั่นคงปลอดภัยด้านสารสนเทศอย่างเคร่งครัด ดังนี้

- ด้านการควบคุมระบบเทคโนโลยีสารสนเทศ การให้บริการอินเตอร์เน็ตเครือข่ายไร้สาย และความปลอดภัยในพื้นที่ห้องควบคุมระบบเครือข่าย
- ด้านการเข้าถึงของผู้ใช้งานสารสนเทศ กำหนดสิทธิการเข้าถึงและยืนยันตัวตนก่อนเข้าใช้งาน
- ด้านการเข้าถึงระบบเครือข่าย ระบบปฏิบัติการ และ โปรแกรมประยุกต์
- ด้านการจัดระบบสำรองฉุกเฉิน

๔. ดูแล ตรวจสอบ ติดตาม เฝ้าระวัง การบุกรุกทางเครือข่ายคอมพิวเตอร์ การบำรุงรักษาซ่อมแซมและจัดหาพัฒนาระบบเทคโนโลยี ให้มีความพร้อมรองรับระบบงานสาธารณสุข

๕. รายงานผลการดำเนินงานและข้อเสนอแนะแนวทางแก้ไขปัญหา

๖. งานอื่นๆ ที่ผู้บังคับบัญชามอบหมาย

/บทที่ ๒ การบริหาร...

บทที่ ๒ การบริหารความเสี่ยง

ขั้นที่ ๑ ขั้นเตรียมการและวางแผน

๑.๑ กำหนดความเสี่ยงที่มีโอกาสเกิดขึ้นต่อวัตถุประสงค์ ภารกิจ ความสำเร็จ

โรงพยาบาลบ้านไร่ ได้พัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อพัฒนาระบบบริการทางแพทย์และสาธารณสุขให้มีคุณภาพและมาตรฐาน สนับสนุนพันธกิจหลักให้ถึงเป้าหมายบริการอย่างมีประสิทธิภาพ

วัตถุประสงค์ ภารกิจ ความสำเร็จด้านเทคโนโลยีสารสนเทศและการสื่อสาร	ความเสียหายที่ยอมรับได้
๑. พัฒนาการเชื่อมโยงเครือข่ายระบบสาธารณสุข	- การเชื่อมโยงเครือข่ายระหว่างหน่วยงานที่เกี่ยวข้องไม่สามารถดำเนินการได้เกิน ๒ ชั่วโมง
๒. ให้ความสำคัญกับระบบความปลอดภัยด้าน ICT	- ระยะเวลา Downtime ของระบบเครือข่ายไม่เกินร้อยละ ๕ ของเวลาทั้งปี
๓. ความมีประสิทธิภาพของระบบเทคโนโลยีสารสนเทศ(ระบบงานและข้อมูล)	- ร้อยละไม่ต่ำกว่า ๘๐ ของหน่วยงานในสังกัดได้ใช้บริการเว็บไซต์ระบบงานและข้อมูลของโรงพยาบาลบ้านไร่พัฒนาขึ้น
๔. ผู้รับบริการมีความพึงพอใจต่อบริการด้าน ICT	- ร้อยละของระดับความพึงพอใจของผู้ใช้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ลดลงจากเดิมไม่เกิน ๒๐ %

สถานะ ชื่อเสียงขององค์กร	ความเสียหายที่ยอมรับได้
๑. ความเชื่อมั่นของประชาชนผู้ใช้บริการฯ	- จำนวนผู้ใช้บริการระบบเทคโนโลยีสารสนเทศ ไม่ลดลงจากเดิม
๒. ความเชื่อมั่นต่อบริการด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานในสังกัด	- การส่งข้อมูล ๔๓ แฟ้ม และรายงานต่างๆ มีความทันเวลา ครบถ้วน ถูกต้อง ไม่ลดลงจากเดิม

๑.๒ วิเคราะห์ปัญหาและโอกาสในองค์กร

วิเคราะห์ปัญหาและโอกาสในองค์กร ในการบริหารความเสี่ยงของโรงพยาบาลบ้านไร่

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
ปัจจัยแห่งความสำเร็จ (Key Success Factors) เพื่อให้การดำเนินการตามกรอบนโยบายเทคโนโลยีสารสนเทศและการสื่อสาร โรงพยาบาลบ้านไร่บรรลุผลตามเป้าหมาย สามารถนำไปปฏิบัติได้อย่างเป็นรูปธรรม คือ ๑. ปัจจัยด้านอุปกรณ์ (Hardware) (๑) พัฒนาโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศและการสื่อสารเพื่อสนับสนุนการพัฒนาระบบสุขภาพของประเทศ

/(๒) มีเครื่องมือ...

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ(ต่อ)

(๒) มีเครื่องมือในการเก็บรวบรวมข้อมูลที่มีประสิทธิภาพ สามารถเก็บรวบรวมข้อมูลได้ครบถ้วนมีคุณภาพตอบสนองความต้องการในการให้บริการสาธารณสุข และด้านบริหารจัดการของผู้บริหาร

๒. ปัจจัยด้านซอฟต์แวร์(Software)

(๑) สร้างเสริมนวัตกรรมบริการและการวิจัยระบบ เครื่องมือและอุปกรณ์เพื่อเพิ่มประสิทธิภาพระบบบริการสาธารณสุข

(๒) ประยุกต์ใช้เทคโนโลยีในการในกระบวนการจัดการและการให้บริการสาธารณสุข

(๓) พัฒนาระบบเทคโนโลยีสารสนเทศการจัดการความรู้ด้านการแพทย์และสุขภาพสำหรับประชาชน

(๔) พัฒนามาตรฐานในด้านการเชื่อมโยงแลกเปลี่ยนข้อมูล (Standard and Interoperability)

๓. ปัจจัยด้านโครงข่ายเทคโนโลยีสารสนเทศ

(๑) เครื่องคอมพิวเตอร์ทุกเครื่องภายในโรงพยาบาลบ้านไร่สามารถเข้าถึงบริการอินเตอร์เน็ตความเร็วสูงหรือการสื่อสารรูปแบบอื่นที่เป็น Broadband ได้อย่างทั่วถึง สะดวกและรวดเร็วโดยปลอดภัย

(๒) ระบบ ICT ของโรงพยาบาลบ้านไร่มีความพร้อม รวดเร็วทันต่อความก้าวหน้าของเทคโนโลยีและความเปลี่ยนแปลงของสังคมโลก รองรับการขยายตัวงานให้บริการประชาชน

(๓) โครงข่าย ICT ของโรงพยาบาลบ้านไร่มีการพัฒนาศักยภาพไปสู่โครงข่ายสมัยใหม่ (Next Generation Network : NGN) ที่สามารถบูรณาการใช้งานร่วมกันได้อย่างทั่วถึง

๔. ปัจจัยด้านบุคลากร

- ผู้บริหารองค์กร

(๑) ผู้บริหารมีวิสัยทัศน์ ให้ความสำคัญ สนับสนุนและส่งเสริมการนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้ในการพัฒนาองค์กร รวมทั้งให้ความสำคัญต่อการบริหารความเสี่ยงของระบบเทคโนโลยี

- ผู้ใช้งาน

(๑) บุคลากรผู้ใช้งานส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้ มีความสนใจและกระตือรือร้นในการใช้เทคโนโลยีมาช่วยในการปฏิบัติงาน

(๒) บุคลากรทุกคนสามารถใช้ E-mail, Internet และการสื่อสารรูปแบบต่างๆ ในการประสานงานและสืบค้นข้อมูลในส่วนที่เกี่ยวข้องเพื่อปฏิบัติงานในภารกิจได้อย่างมีประสิทธิภาพ

(๓) บุคลากรทุกคนเห็นความสำคัญและให้ความร่วมมือในการปฏิบัติตามแผนการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

- ผู้ปฏิบัติงานด้าน ICT

(๑) ผู้ปฏิบัติงานด้าน ICT ส่วนใหญ่มีความรู้พื้นฐานด้านเทคโนโลยีสารสนเทศในระดับที่ใช้งานได้

(๒) ผู้ปฏิบัติงานด้าน ICT มีความสนใจ และกระตือรือร้นในการคิดค้นหารูปแบบการใช้ระบบเทคโนโลยีสารสนเทศช่วยในการปฏิบัติงาน

(๓) ผู้ปฏิบัติงานด้าน ICT ให้ความร่วมมือในการปฏิบัติงานตามแผนบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

/๕. ปัจจัยด้าน...

โอกาส – สิ่งที่จะมีส่วนช่วยให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ(ต่อ)
๕. ปัจจัยด้านข้อมูลสารสนเทศ (๑) พัฒนาระบบฐานข้อมูลโปรแกรม HOSxPV๔ เป็นระบบรวบรวมฐานข้อมูลสุขภาพในโรงพยาบาลบ้านไร่ โดยเป็นข้อมูลที่สามารถนำไปใช้ประโยชน์ได้จริง มีข้อมูลเชื่อมโยงและแลกเปลี่ยนกันได้โดย ระบบการ Sync ข้อมูล Datacenter แพทย์สามารถเข้าถึงข้อมูลสุขภาพของผู้ป่วยได้ทุกที่ทุกเวลา (๒) มีการพัฒนารูปแบบการให้บริการข้อมูลขององค์กรในลักษณะสื่อสารสองทาง (Interactive) และส่งเสริมการมีส่วนร่วมของภาคประชาชน และบุคลากรผู้ปฏิบัติงานผ่านระบบอินเทอร์เน็ต (๓) โรงพยาบาลบ้านไร่ เป็นแหล่งให้บริการในช่องทางการเข้าถึงข้อมูลสารสนเทศสุขภาพและเป็นศูนย์กลางในการสะท้อนความต้องการ ปัญหาและ ข้อเสนอแนะจากภาคประชาชน ๖. ปัจจัยด้านการบริหารจัดการ (๑) มีการจัดตั้งศูนย์คอมพิวเตอร์/งาน IT/บุคลากรด้าน IT เพื่อเป็นหน่วยสนับสนุนและกำกับดูแลงานด้านเทคโนโลยีสารสนเทศภายในหน่วยงาน (๒) มีการแต่งตั้ง คณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านบ้านไร่ เพื่อกำหนดทิศทางการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร (๓) มีการแต่งตั้งคณะกรรมการบริหารและจัดหาระบบคอมพิวเตอร์ประจำโรงพยาบาลบ้านไร่ ทำหน้าที่บริหารการจัดหาระบบคอมพิวเตอร์ของโรงพยาบาลบ้านไร่ เพื่อให้เป็นเกิดความคล่องตัวในการจัดหาอุปกรณ์คอมพิวเตอร์ (๔) มีการแต่งตั้ง คณะกรรมการบริหารและพัฒนาระบบข้อมูลสารสนเทศด้านสุขภาพจังหวัดอุทัยธานี เพื่อพัฒนาและปรับปรุงระบบบริหารจัดการข้อมูล ตามมาตรฐานโครงสร้าง ๔๓ แฟ้ม สู่คลังข้อมูลด้านการแพทย์และสุขภาพ ระดับจังหวัด เขต และกระทรวง (Health Data Center : HDC) ๗. ปัจจัยด้านงบประมาณ (๑) ได้รับการสนับสนุนด้านงบประมาณอย่างต่อเนื่อง

ปัญหา – สิ่งที่จะขัดขวางมิให้กระบวนการบริหารความเสี่ยงประสบผลสำเร็จ
ปัญหา/อุปสรรค ที่พบในระบบงานบริหารจัดการข้อมูล ในภาพรวมของโรงพยาบาลบ้านไร่ ๑. กระบวนการบริหารจัดการและบูรณาการ ด้านการบริหารความเสี่ยงของระบบเทคโนโลยีสารสนเทศภายในองค์กรยังไม่ชัดเจนเท่าที่ควร ๒. กระบวนการบริหารจัดการด้านความปลอดภัยยังไม่ได้รับความร่วมมือในการปฏิบัติเท่าที่ควร
ปัญหา/อุปสรรค ที่พบในความน่าเชื่อถือข้อมูล ๑. ความครบถ้วน ถูกต้อง ทันเวลาของข้อมูลที่ส่งเข้าสู่ระบบคลังข้อมูลสุขภาพ ทางเจ้าหน้าที่มีการบันทึกข้อมูลบางส่วนไม่ครบ มีการบันทึกข้อมูลย้อนหลัง ทำให้ข้อมูลบางส่วน error ๒. กระบวนการบริหารจัดการด้านความปลอดภัย ยังไม่ได้รับความร่วมมือในการปฏิบัติเท่าที่ควร

/๑.๓ กำหนดขอบ...

๑.๓ กำหนดขอบเขต

ขอบเขตของการบริหารความเสี่ยงโรงพยาบาลบ้านไร่ ที่มีความสำคัญต่อวัตถุประสงค์ ภารกิจ สถานะ หรือ ความสำเร็จ

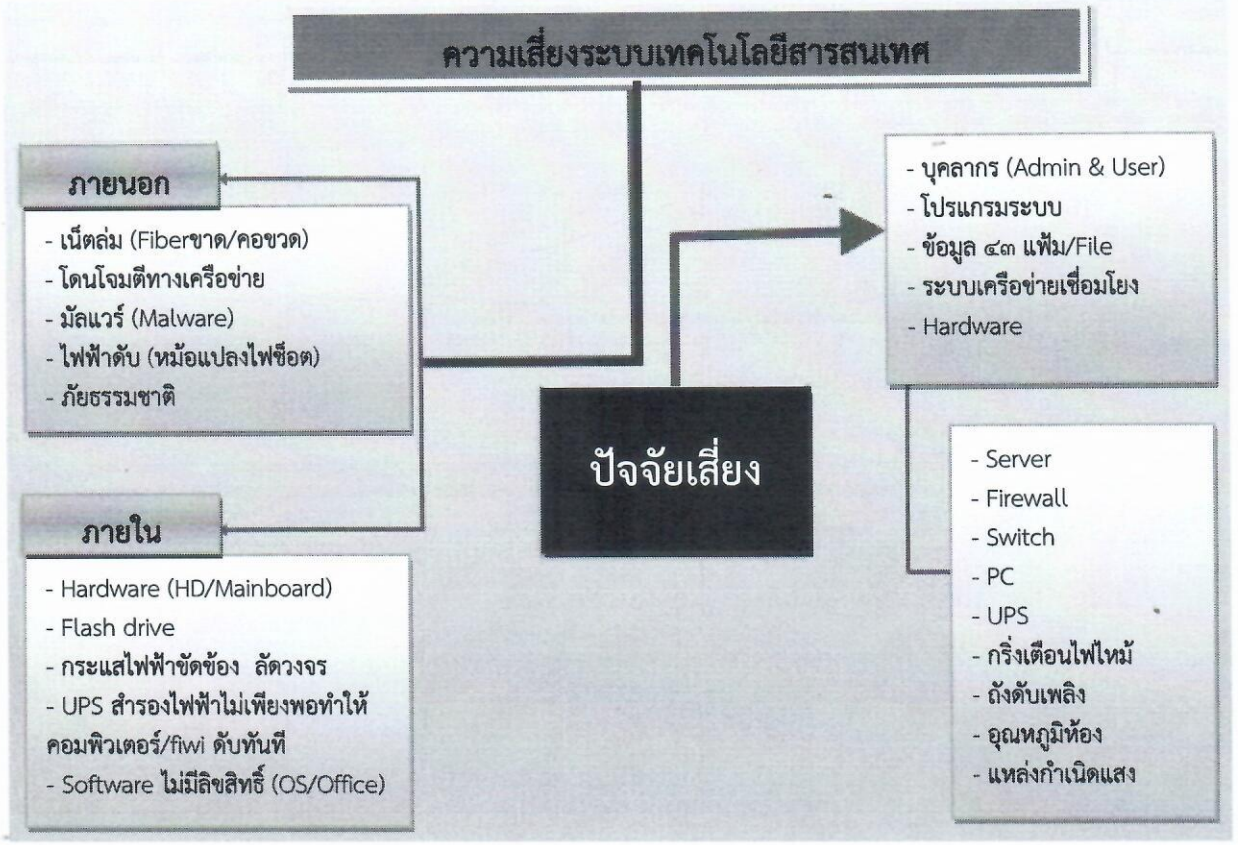
หน่วยงานขององค์กรที่จะจัดให้มีกระบวนการบริหารความเสี่ยง
โรงพยาบาลบ้านไร่

๑.๔ กำหนดตัวบุคลากร

ใช้คำสั่งโรงพยาบาลบ้านไร่ ที่ ๔ /๒๕๖๕ เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านไร่ สั่ง ณ วันที่ ๑๓ มกราคม ๒๕๖๕

ขั้นที่ ๒ บ่งชี้ปัจจัยความเสี่ยง

ผังเหตุการณ์หรือสถานการณ์ที่มีความเสี่ยงต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร



/ขั้นที่ ๓ วิเคราะห์...

ขั้นที่ ๓ วิเคราะห์ความเสี่ยง

ตารางที่ ๑ ระบุความเสี่ยงและผลกระทบด้านต่างๆ ที่จะเกิดขึ้น

กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านไร่				
ที่มาความเสี่ยง/ ปัจจัยเสี่ยง	ผลกระทบด้านต่างๆ			
	ชื่อเสียง	เวลา	การบริการ	บุคลากร
๑.ระบบงานและข้อมูล (System Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	-หน่วยงานถูกวิจารณ์ -จนท.ขาดความเชื่อมั่นระบบเครือข่าย	-เสียเวลากู้คืนระบบ - ใช้เวลาเพิ่มในการหาข้อมูลใหม่	-งานบริการหยุดชะงัก	-บุคลากรที่เกี่ยวข้องถูกตำหนิ
๒.ระบบให้บริการอินเตอร์เน็ต	-งาน IT ถูกกล่าวหา	-ทำให้ระบบเครือข่ายเทคโนโลยีต่างๆทำงานล่าช้า	-ผู้ใช้บริการใช้ระบบเครือข่ายเทคโนโลยีได้ล่าช้า	-บุคลากรที่เกี่ยวข้องถูกตำหนิ/ชี้แจงเหตุ
๓.เครื่อง server ติดไวรัส	-ถูกวิจารณ์ประสิทธิภาพการทำงาน	-ทำให้ระบบสารสนเทศทำงานช้าหรือทำงานไม่ได้	-หน่วยงานที่เกี่ยวข้องใช้งานสารสนเทศล่าช้า	-ถูกตำหนิในเรื่องการดูแลรักษาความปลอดภัย
๔.เครื่อง Client ติดไวรัส	-เสียชื่อระบบป้องกันไวรัส	-เสียเวลาซ่อมเครื่อง -เสียเวลาทำงานราชการ	-ทำให้งานบริหารประชาชนล่าช้า	-เสียเวลาทำงานทุกฝ่าย
๕.การนำเสนอข้อมูลผิดพลาด/ข้อมูลที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือถูกเผยแพร่	-เป็นข่าวลบใน social Media -ถูกประชาชนวิจารณ์	-ต้องใช้เวลาในการกู้ชื่อเสียงคืน	-ขาดความเชื่อในหน่วยงานด้านความปลอดภัย	-บุคลากรที่เกี่ยวข้องถูกตำหนิ
๖.ความเสี่ยงกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่	-ถูกวิจารณ์ประสิทธิภาพระบบสำรองไฟฟ้า	-เสียเวลาทำงานแก้ปัญหา	-ข้อมูลสารสนเทศบางส่วนชำรุด/หยุดให้บริการ	-ผู้ดูแลระบบเสียเวลาซ่อมแซมเครื่อง/หรืออาจต้องกู้คืนระบบ
๗.ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง -ภัยธรรมชาติ	-เป็นข่าวลบใน social Media	-เสียเวลาแก้ปัญหาต้องจัดหาอุปกรณ์ใหม่ทดแทน	-ข้อมูลเสียหายให้บริการไม่ได้	-บุคลากรที่เกี่ยวข้องถูกตำหนิ
๘.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยภายในประเทศ	ผู้บริหารเสียชื่อในการบริหารจัดการความเสี่ยง	เสียเวลาในการซ่อมแซมปรับปรุงระบบใหม่	บุคลากรปฏิบัติงานให้บริการไม่ได้	บุคลากรปฏิบัติงานและให้บริการไม่ได้

/ตารางที่ ๒...

ตารางที่ ๒ แนวทางและกิจกรรมจัดการความเสี่ยง

ปัจจัยเสี่ยง	ความเสียหายที่เกิดขึ้น	แนวทางจัดการ	กิจกรรมในการจัดการ
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านไร่			
๑.ระบบงานและข้อมูล (System Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	-ให้บริการระบบงานและข้อมูลสารสนเทศล่าช้า/ไม่ได้ -เจ้าหน้าที่ถูกตำหนิ	-อัพเดตระบบเทคโนโลยีเครือข่ายความมั่นคงปลอดภัย -สร้างระบบงานสำรองทดแทน	-จัดจ้างบำรุงรักษาอุปกรณ์ป้องกันเครือข่าย -จัดประชุมอบรมบุคลากร IT/เผยแพร่ความรู้ด้านความปลอดภัยระบบเครือข่าย -backup ระบบฐานข้อมูล
๒.ระบบให้บริการอินเตอร์เน็ตล่ม	-ใช้งานอินเตอร์เน็ตไม่ได้ –การสื่อสารรับส่งข้อมูลล่าช้า	-จัดทำอินเตอร์เน็ตโซนแบบ High Availability -เพิ่ม ISP สำรอง	-ทำ load balance และ -ทำแผนจัดการเพิ่มความเร็ว bandwidth อินเตอร์เน็ต
๓.เครื่อง server ติดไวรัส	-ใช้บริการระบบงานและข้อมูลสารสนเทศไม่ได้	-จัดหาระบบป้องกันความปลอดภัยทาง Cyber -พัฒนาความรู้ผู้ดูแลระบบ	-admin ได้รับการอบรมระบบเครือข่ายความปลอดภัยอย่างต่อเนื่อง -ตรวจสอบช่องโหว่ firewall
๔.เครื่อง Client ติดไวรัส	-บุคลากรทำงานล่าช้า -ไฟล์ข้อมูลเสียหาย	-ประกาศใช้/ให้ความรู้ตามนโยบายแนวทางป้องกันระบบรักษาความปลอดภัย -ติดตั้ง update virus signature สม่ำเสมอ	-อบรมให้ความรู้ผู้ใช้งาน -จัดหา ICT support ให้บริการ -ติดตั้งระบบงาน software มีลิขสิทธิ์ เช่น OS/anti-virus
๕.การนำเสนอข้อมูลผิดพลาด/ข้อมูลที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือถูกเผยแพร่	-เป็นข่าวลบใน social Media -ถูกประชาชนวิจารณ์	-ให้มีและใช้ระบบป้องกันความปลอดภัยข้อมูล -กำหนดสิทธิการเข้าถึงข้อมูล	-ตรวจสอบสิทธิผู้ใช้งาน -ตรวจสอบคุณภาพข้อมูล -ตรวจสอบการทำงานของอุปกรณ์คอมพิวเตอร์
๖.ความเสี่ยงจากกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	-ทำให้อุปกรณ์ระบบคอมพิวเตอร์/ข้อมูลเสียหาย	-ติดตั้งเครื่องสำรองไฟฟ้า (UPS) ให้พร้อมใช้งานมีมาตรฐานและสำรองไฟให้มีเวลาพออย่างน้อย ๑๕ นาที	-บำรุงรักษาตรวจสอบความพร้อมใช้งานเครื่องสำรองไฟฟ้า -ประชาสัมพันธ์แนวทางป้องกันคอมพิวเตอร์กรณีไฟดับ
๗.ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน - ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง ภัยธรรมชาติ	-อุปกรณ์คอมพิวเตอร์เสียหาย ใช้งานไม่ได้ -ข้อมูลเสียหาย	-จัดทำแผนป้องกันและแก้ไขภัยพิบัติ (Contingency Plan) -สำรองข้อมูลต่างพื้นที่เสี่ยง	-ซักซ้อมแผนป้องกันภัยฯ -กรณีเกิดเหตุ รีบรายงานผู้บังคับบัญชาทราบทันที -ตรวจสอบความเสียหายเพื่อฟื้นฟูระบบโดยเร็ว
๘.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยภายในประเทศ	-บุคลากรปฏิบัติงานไม่ได้เต็มที่	-จัดให้มีการสำรองข้อมูลระบบ/ฐานข้อมูลสำรองให้พร้อมในสถานที่อื่น	-ซักซ้อมระบบสำรองข้อมูลให้พร้อมในต่างสถานที่

/ขั้นที่ ๔ กิจกรรม...

ขั้นที่ ๔ กิจกรรมและรายงานผลการดำเนินงานตามแผนจัดการความเสี่ยง

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

๑. ระบบงานและข้อมูล (System &Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย

ผู้รับผิดชอบ น.ส.แอนนา แก้วการไร่ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. บำรุงรักษาอุปกรณ์ป้องกันเครือข่าย	firewall ๑ เครื่อง	firewall / ปีละครั้ง	ก.พ. ๖๖	ดำเนินการเรียบร้อย ๑๔ ธ.ค.๖๕	ต้อง update firmwareตอนมีการใช้งานน้อยๆ
๒. อัพเดตโปรแกรม HOSxPXE๔	อัพเดตโปรแกรม HOSxPXE๔ Server ๑ เครื่อง	อัพเดตโปรแกรม HOSxPXE๔ /ปีละ ๔ ครั้ง (รายไตรมาส)	ต.ค.๖๕-ก.ย.๖๖	ดำเนินการเรียบร้อย อัพเดตโปรแกรมทุกเดือน	ต้องอัพเดตโปรแกรมตอนมีการใช้งานน้อยๆ
๓. ทดสอบ Restore ข้อมูล HOSxP๔	Restore ข้อมูลลง Server สำรอง ๑ เครื่อง	ทดสอบ Restore ข้อมูล HOSxPXE๔ / เดือนละ ๑ ครั้ง	ต.ค.๖๕-ก.ย.๖๖	ดำเนินการเรียบร้อย Restore ข้อมูลทุกดือน	ฮาร์ดดิสก์ไม่เพียงพอฐานข้อมูลใหญ่
๔. จัดประชุมอบรม/เผยแพร่ความรู้ด้านความปลอดภัยระบบเครือข่าย	เดือนละครั้ง	การใช้คอมเบื้องต้น	ต.ค๖๕-ก.ย๖๖	ดำเนินการเรียบร้อยผ่านไลน์กลุ่มเจ้าหน้าที่	เจ้าหน้าที่บางท่านไม่ค่อยได้อ่านไลน์กลุ่ม
๕. ทำการ backup ข้อมูล HOSxPXE๔ ทุกวัน	backup ทุกวัน	backup ข้อมูล HOSxPXE๔/ ทุกวัน	ต.ค.๖๕-ก.ย.๖๖	ดำเนินการเรียบร้อยทุกวัน	ฮาร์ดดิสก์ไม่เพียงพอฐานข้อมูลใหญ่

/๒. ระบบให้...

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

๒. ระบบให้บริการอินเตอร์เน็ตล่ม

ผู้รับผิดชอบ นายภาสกร ป้อมคำ ตำแหน่ง นักวิชาการคอมพิวเตอร์

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. ทำ load balance อินเตอร์เน็ตทุกเส้นทาง	Firewall ๑ เครื่อง	เซตค่า/ตรวจสอบระบบปีละ ๑ ครั้ง	ต.ค. ๖๕	ดำเนินการเรียบร้อย	ไม่มี
๒. ทำแผนจัดการเพิ่มความเร็ว bandwidth	Isp ๒ ค่าย	ทำแผน/ปีละ๑ครั้ง	ต.ค. ๖๕	ดำเนินการเรียบร้อย	ไม่มี

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

๓. เครื่อง server ติดไวรัส หรือ ถูกบุรุกทางเครือข่าย

ผู้รับผิดชอบ นายภาสกร ป้อมคำ ตำแหน่ง นักวิชาการคอมพิวเตอร์

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. admin ได้รับการอบรมระบบเครือข่ายความปลอดภัยอย่างต่อเนื่อง	Admin ๒ คน	admin ได้รับการอบรม/ปีละครั้ง	ธ.ค. ๖๕	ดำเนินการเรียบร้อย	ไม่มี
๒. ตรวจสอบช่องโหว่ firewall	firewall ๑ เครื่อง	ตรวจสอบช่องโหว่ firewall/เดือนละครั้ง	ต.ค. ๖๕-ก.ย. ๖๖	ดำเนินการเรียบร้อย	ไม่มี

/๔. เครื่อง Client ...

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
๔. เครื่อง Client ติดไวรัส
ผู้รับผิดชอบ นางสาวอรอุมา โพธิ์ประจันทร์ ตำแหน่ง เจ้าพนักงานเครื่องคอมพิวเตอร์

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. เผยแพร่ประชาสัมพันธ์ให้ความรู้ผู้ใช้งาน	เจ้าหน้าที่ ๒๐๐ ท่าน	เผยแพร่ประชาสัมพันธ์ผ่านกลุ่มไลน์/ปีละ๑ครั้ง	ต.ค. ๖๕ – ก.พ. ๖๖	ดำเนินการเรียบร้อย	เจ้าหน้าที่บางท่านไม่ค่อยได้อ่านไลน์กลุ่ม
๒. ติดตั้งโปรแกรม anti-virus	เครื่องคอมพิวเตอร์ ๑๒๐ เครื่อง	ติดตั้งตรวจสอบโปรแกรม anti-virus/ปีละครั้ง	ต.ค. ๖๕	ดำเนินการเรียบร้อย	anti-virus แบบฟรี ป้องกันไวรัสได้แค่บางส่วน

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
๕. การนำเสนอข้อมูลผิดพลาด/ข้อมูลที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือถูกเผยแพร่
ผู้รับผิดชอบ น.ส.แอนนา แก้วการไร่ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ และ
นายภาสกร ป้อมคำ ตำแหน่ง นักวิชาการคอมพิวเตอร์

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. ตรวจสอบสิทธิผู้ใช้งาน	ผู้ใช้งาน ๒๐๐ ท่าน	ตรวจสอบสิทธิผู้เข้าถึง/ปีละ ๑ ครั้ง	ต.ค. ๖๕ – ก.พ. ๖๖	ดำเนินการเรียบร้อย	ไม่มี
๒. ตรวจสอบคุณภาพข้อมูล	๔๓ แฟ้ม	ตรวจสอบคุณภาพข้อมูล/เดือนละ ๑ ครั้ง	ต.ค. ๖๕ – ก.ย. ๖๖	ดำเนินการเรียบร้อย	ไม่มี
๓. ตรวจสอบเว็บไซต์ของหน่วยงาน	เว็บไซต์ของหน่วยงาน	ตรวจสอบเว็บไซต์/เดือนละ ๑ ครั้ง	ต.ค.๖๕ – ก.ย. ๖๖	ดำเนินการเรียบร้อย	ไม่มี

/๖. ความเสี่ยง...

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
๖. ความเสี่ยงกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่
ผู้รับผิดชอบ นางสาวอรอุมา โพธิ์ประจันทร์ ตำแหน่ง เจ้าพนักงานเครื่องคอมพิวเตอร์

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. ตรวจสอบ บำรุงรักษา พร้อมใช้งานเครื่องสำรองไฟฟ้า	เครื่องสำรองไฟฟ้า ๑๒๐ เครื่อง	ตรวจสอบบำรุงรักษา/ปีละ ๑ ครั้ง	ต.ค.๖๕	ดำเนินการเรียบร้อย	ไม่มี
๒. ประชาสัมพันธ์ให้ความรู้แนวทางแก้ไขคอมพิวเตอร์กรณีไฟดับ	เจ้าหน้าที่ ๒๐๐ ท่าน	ประชาสัมพันธ์ในกลุ่มไลน์เจ้าหน้าที่/ปีละ ๑ ครั้ง	ต.ค. ๖๕	ดำเนินการเรียบร้อย	เจ้าหน้าที่บางท่านไม่ค่อยได้อ่านไลน์กลุ่ม

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี
๗. ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉิน
ผู้รับผิดชอบ น.ส.แอนนา แก้วการไร่ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. ซักซ้อมแผนป้องกันภัย ฯ	เจ้าหน้าที่ ๑๐๐ ท่าน	ซักซ้อมแผน/ปีละครั้ง	ต.ค.-ก.ย. ๖๖	ดำเนินการเรียบร้อย	ไม่มี
๒. กรณีเกิดเหตุ รีบรายงานผู้บังคับบัญชาทราบทันที	เหตุการณ์ที่เกิดขึ้น	กรณีเกิดเหตุ รีบรายงาน/ทุกครั้งที่เกิดเหตุ	ต.ค.-ก.ย. ๖๖	ไม่มี	ไม่มี
๓. ตรวจสอบความเสียหายเพื่อฟื้นฟูระบบโดยเร็ว	ความเสียหาย	ตรวจสอบความเสียหาย/ทุกครั้ง	ต.ค.-ก.ย. ๖๖	ไม่มี	ไม่มี

/๘.ความเสี่ยง...

รายงานการติดตามผลการดำเนินงานตามแผนจัดการความเสี่ยงด้านการใช้เทคโนโลยี

๘. ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยภายในประเทศ

ผู้รับผิดชอบ น.ส.แอนนา แก้วการไร่ ตำแหน่ง นักวิชาการคอมพิวเตอร์ปฏิบัติการ

กิจกรรม	ผลลัพธ์ของกิจกรรม (เป้าหมาย)	เรื่อง/กำหนดการ	ระยะเวลาดำเนินการ	ผลงาน	ปัญหาอุปสรรค/แนวทางแก้ไข
๑. ซักซ้อมระบบสำรองข้อมูลให้พร้อมในต่างสถานที่	Server สำรอง ๑ เครื่อง	ซักซ้อมระบบสำรองข้อมูล/ปีละครั้ง	ต.ค.๖๕ - ก.ย. ๖๖	ดำเนินการเรียบร้อย	ไม่มี

ขั้นที่ ๕ ประเมินและสรุปผลการดำเนินงานตามแผนจัดการความเสี่ยง

ประเมินและสรุปผลการดำเนินงานจัดการความเสี่ยงด้านการใช้เทคโนโลยี

ลำดับความเสี่ยง	เป้าหมายตามกิจกรรมครบถ้วน	ผลการดำเนินการ	% ความเสี่ยงคงเหลือ	สรุปผล ควบคุม หรือยอมรับความเสี่ยง
กิจกรรม / กระบวนงาน : ระบบเทคโนโลยีสารสนเทศ โรงพยาบาลบ้านไร่				
๑.ระบบงานและข้อมูล (System Information) ทำงานไม่ได้ เสียหายหรือถูกทำลาย	๕ กิจกรรม	๕ กิจกรรม	๐%	
๒.ระบบให้บริการอินเตอร์เน็ตล่ม	๒ กิจกรรม	๒ กิจกรรม	๐%	
๓.เครื่อง server ติดไวรัส	๒ กิจกรรม	๒ กิจกรรม	๐%	
๔.เครื่อง Client ติดไวรัส	๒ กิจกรรม	๒ กิจกรรม	๐%	
๕.การนำเสนอข้อมูลผิดพลาด/ข้อมูลที่เป็นความลับรั่วไหล ถูกเปิดเผยหรือถูกเผยแพร่	๓ กิจกรรม	๓ กิจกรรม	๐%	
๖.ความเสี่ยงจากกระแส ไฟฟ้าขัดข้อง ไฟฟ้าดับ/แรงดันไฟฟ้าไม่คงที่	๒ กิจกรรม	๒ กิจกรรม	๐%	
๗.ความเสี่ยงจากภัยหรือสถานการณ์ฉุกเฉินไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิงหรือภัยธรรมชาติ	๓ กิจกรรม	๑ กิจกรรม	๖๖.๖๗%	
๘.ความเสี่ยงจากสถานการณ์ความไม่สงบเรียบร้อยภายในประเทศ	๑ กิจกรรม	๑ กิจกรรม	๐%	

แหล่งอ้างอิง

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ประจำปีงบประมาณ ๒๕๕๗ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

ประกาศกระทรวงสาธารณสุข เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงความปลอดภัยด้านสารสนเทศ ลงวันที่ ๗ มกราคม ๒๕๕๖

สำนักงานคณะกรรมการพัฒนาระบบราชการ. คู่มือเทคนิคและวิธีการบริหารจัดการสมัยใหม่ตามแนวทางการบริหารกิจการบ้านเมืองที่ดีเรื่องการวิเคราะห์และการบริหารความเสี่ยง. พิมพ์ครั้งที่ 2. กรุงเทพฯ : สหมิตรพริ้นติ้ง, 2549