แผนบริหารความเสี่ยง
ด้านเทคโนโลยีสารสนเทศ

พ.ศ. 2567

โรงพยาบาลทุ่งฝน

โรงพยาบาลทุ่งฝน

แผนบริหารความเสี่ยงเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ

ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร วิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ **โรงพยาบาลทุ่งฝน**
2. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
3. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

ศูนย์สารสนเทศและเวชระเบียนอยู่ในกลุ่มงานสารสนเทศทางการแพทย์ เป็นหน่วยงานดูแลระบบ และสนับสนุนพัฒนาระบบเทคโนโลยีสารสนเทศและเวชระเบียน ดูแลระบบคอมพิวเตอร์ทั้งด้าน Hardware Software และฐานข้อมูล ให้ระบบสามารถทำงานได้ตลอด 24 ชั่วโมง มี Server 6 เครื่อง เครื่องคอมพิวเตอร์ตั้งโต๊ะ 130 เครื่อง โดยมีวัตถุประสงค์เพื่อตอบสนองความต้องการของหน่วยงานในโรงพยาบาลและผู้มีส่วนได้เสียเพื่อให้ได้ข้อมูลที่ครบถ้วน ถูกต้อง รวดเร็ว ตรวจสอบได้ และลดขั้นตอนการทำงาน มีการนำข้อมูลที่ได้มาใช้ในการวางแผนการดำเนินงาน การแก้ปัญหาต่าง ๆ เพิ่มช่องทางการสื่อสารและการเรียนรู้ภายในองค์กร โดยด้านโครงสร้างพื้นฐานหรือ Infrastructure มีการเชื่อมโยงเครือข่าย LAN ครอบคลุมหน่วยงานทั้งโรงพยาบาล มีการแบ่งระบบเครือข่ายออกเป็น 2 ระบบ คือ ระบบเครือข่ายการให้บริการผู้ป่วย HOSxP และระบบเครือข่าย Internet

ก. หน้าที่และเป้าหมาย

หน้าที่

เป็นหน่วยงานสนับสนุนที่ตั้งขึ้นมาเพื่อให้บริการระบบเทคโนโลยีสารสนเทศของโรงพยาบาล ในงานดูแลผู้ป่วย งานบริหารและบริการเครือข่ายฯ เพื่อตอบสนองความต้องการของผู้บริหาร ผู้ให้บริการและผู้รับบริการ อย่างถูกต้องทันเวลาและสามารถนำไปใช้ประโยชน์ได้จริง

เป้าหมาย

- โรงพยาบาลมีระบบสารสนเทศและคอมพิวเตอร์ต้องมีความถูกต้อง เพียงพอ พร้อมใช้ ปลอดภัย และได้รับความพึงพอใจ
- มีการจัดเก็บข้อมูลที่สามารถสืบค้นได้ง่าย มีความถูกต้องและทันเวลา
- มีระบบการรักษาความลับและความปลอดภัยของข้อมูล
- มีการเชื่อมโยงข้อมูลเพื่อการบริหาร บริการดูแลผู้ป่วยและการพัฒนาคุณภาพ

ข. ขอบเขตการให้บริการ (Scope of Service)

1. ดูแลระบบให้พร้อมใช้งาน ตลอด 24 ชั่วโมง
2. สำรวจและจัดหาคอมพิวเตอร์และอุปกรณ์ต่อพ่วง
3. บำรุงรักษาดูแลและรักษาความปลอดภัยของระบบเครือข่าย
4. วางแผนและออกแบบระบบรายงานสารสนเทศเพื่อตอบสนองความต้องการตามคำร้องขอข้อมูลของผู้ใช้ กำหนดมาตรฐานและนโยบายสำหรับเวชระเบียน
5. พัฒนาคุณภาพ ประเมิน ทบทวน ความสมบูรณ์ของเวชระเบียนปรับปรุงฐานข้อมูลให้ถูกต้องครบถ้วนก่อนส่งออก
6. เชื่อมโยงข้อมูลสารสนเทศ เพื่อการพัฒนาคุณภาพ
7. ให้คำปรึกษา แนะนำ อบรมงานด้านสารสนเทศและการใช้คอมพิวเตอร์ให้สอดคล้องกับสถานการณ์ปัจจุบัน
8. รวบรวมข้อมูล วิเคราะห์ และนำเสนอข้อมูลต่อทีมนำ หน่วยงาน

นิยามความเสี่ยง

ความเสี่ยง คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และ ความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ

การบริหารความเสี่ยง เป็นการบริหารปัจจัย และควบคุมกิจกรรม หรือ กระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลัก ตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการประจำปี งบประมาณของส่วนราชการ

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

1. **Hardware** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์
2. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน
3. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำ จัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์
4. **ข้อมูลและแฟ้มข้อมูล** หมายถึง ข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง
5. **หน้าที่การปฏิบัติงาน** หมายถึง คำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

- **องค์กร** โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม
- **บุคลากร** บุคลากรที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน
- **เทคโนโลยี** อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

1. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)
2. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)
3. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล
4. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

หลักการตอบสนองความเสี่ยงมี 4 ประการ คือ

1. **การหลีกเลี่ยง (Terminate)** การเลือกที่จะไม่รับความเสี่ยงไว้เลย เช่น หยุดดำเนินการหรือยกเลิกโครงการที่เสี่ยงเกินคุ้ม

2. **การยอมรับ (Take)** การยอมรับความเสี่ยงไว้เองเนื่องจากเห็นว่าโอกาสเกิดต่ำหรือค่าใช้จ่ายในการป้องกันไม่คุ้มค่า เช่น กรณี User/Password ที่หัวหน้างานอาจเปิดเผยให้ลูกน้องทราบ ศูนย์คอมพิวเตอร์ต้องยอมรับและกำหนดมาตรการใหม่เมื่อเกิดปัญหา
3. **การควบคุม (Treat)** การปรับปรุงระบบงานเพื่อป้องกันความเสียหาย
    - การป้องกัน เช่น การติดตั้ง Firewall เพื่อป้องกัน Hacker และไวรัส
    - การควบคุมขนาดความสูญเสีย เช่น การติดตั้งอุปกรณ์ดับเพลิง/ตรวจจับควันในห้อง Server
4. **การถ่ายโอน (Transfer)** การโอนความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น การทำสัญญาบำรุงรักษา (MA) เพิ่มเติม หรือการซื้อประกันภัยอุปกรณ์

ปัจจัยเสี่ยง

1. **ปัจจัยภายนอก** ภัยธรรมชาติ, การขโมยอุปกรณ์ Server, การชำรุดจากการเคลื่อนย้าย, ระบบเครือข่ายหลักขัดข้อง, ไฟฟ้าดับ
2. **ปัจจัยภายใน** ฐานข้อมูลหลักเสียหาย, การติดไวรัสทำลายโปรแกรม, การถูก Hack เข้าสู่ระบบโดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

1. **ความเสียหายร้ายแรงที่สุด** ทำให้ระบบหยุดทั้งระบบ เช่น ภัยธรรมชาติ, Server เสียหาย, ฐานข้อมูลถูกทำลายโดยไวรัส
2. **ความเสียหายชั่วขณะ** ระบบหยุดชั่วคราว เช่น ถูกเจาะระบบฐานข้อมูล, เครือข่ายขัดข้อง, ไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันที

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์**โรงพยาบาลทุ่งฝน** มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ระบบความปลอดภัยอัจฉริยะ (Next-Generation Firewall) ของ **Fortigate** เพื่อทำหน้าที่เป็นปราการด่านหน้าในการบริหารจัดการและควบคุมทราฟฟิกข้อมูลทั้งหมดของโรงพยาบาล

เพื่อให้คอมพิวเตอร์และระบบฐานข้อมูลได้รับความปลอดภัยสูงสุด โรงพยาบาลได้ดำเนินการดังนี้:

1. **Intrusion Prevention & Anti-Virus:** ใช้ Fortigate ในการตรวจจับและป้องกันการบุกรุก (IPS) รวมถึงคัดกรองมัลแวร์และไวรัสในระดับ Gateway ก่อนที่ข้อมูลจะเข้าสู่เครือข่ายภายใน
2. **Web & Content Filtering:** มีการกำหนดนโยบายการเข้าถึงเว็บไซต์และเนื้อหาที่ไม่ปลอดภัย เพื่อลดความเสี่ยงจากการถูกโจมตีผ่านหน้าเว็บ หรือการเผลอดาวน์โหลดไฟล์ที่เป็นอันตราย
3. **Network Segmentation (VLAN):** มีการแบ่งส่วนระบบเครือข่ายภายในออกเป็นกลุ่มงาน (Segmentation) และใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อให้ง่ายต่อการตรวจสอบ ควบคุมทราฟฟิก และจำกัดวงความเสียหายกรณีเกิดความผิดปกติในจุดใดจุดหนึ่ง

4. **Traffic Monitoring:** มีระบบตรวจสอบสถานะการใช้งานเครือข่ายแบบ Real-time เพื่อระบุต้นตอของปัญหาหรือความผิดปกติในระบบได้อย่างรวดเร็ว

ปัจจุบันเครือข่ายของ**โรงพยาบาลทุ่งฝน** เน้นความมั่นคงปลอดภัยของการเชื่อมต่อภายในเป็นหลัก เพื่อให้ระบบ HOSxP และระบบสารสนเทศอื่นๆ สามารถทำงานได้อย่างมีเสถียรภาพตลอด 24 ชั่วโมง

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ประกอบด้วยการวางแผน การประเมินด้านต่างๆ การพัฒนาทางเลือก และการตรวจสอบความเสี่ยงอย่างต่อเนื่องเพื่อรับมือกับการเปลี่ยนแปลง

ลำดับ	ประเภทความเสี่ยง	ปัจจัย/สาเหตุของความเสี่ยง	ผลกระทบที่เกิดขึ้น
1	ด้าน Hardware		
1.1	อุปกรณ์คอมพิวเตอร์และแม่ข่าย (Server) เสียหาย	• อุปกรณ์หมดอายุการใช้งานตามวงรอบ • ภาระงานหนัก (Heavy Load) • สภาพแวดล้อมไม่เหมาะสม (ระบบไฟฟ้าไม่เสถียร/อุณหภูมิห้อง Server สูง)	ระบบหยุดชะงัก ไม่สามารถให้บริการหรือปฏิบัติงานต่อไปได้
1.2	ระบบเครือข่าย (Network) ขัดข้อง	• อุปกรณ์กระจายสัญญาณ (Switch/Router) เสียหาย • ระบบเชื่อมต่อจากผู้ให้บริการภายนอก (ISP) มีปัญหา	ไม่สามารถเชื่อมต่อระบบ HOSxP หรือรับ-ส่งข้อมูลผ่านเครือข่ายได้
2	ด้าน Software		
2.1	ระบบปฏิบัติการหรือแอปพลิเคชันทำงานผิดปกติ	• ระบบปฏิบัติการเสียหาย (OS Crash) • ซอฟต์แวร์ทำงานผิดพลาด (Bug) • การโจมตีจาก Virus, Hacker หรือ Spyware	บริการหยุดชะงัก ข้อมูลอาจถูกล็อคหรือทำลายจนไม่สามารถให้บริการได้
3	ด้านบุคลากร		
3.1	บุคลากรขาดทักษะหรือความชำนาญ	• ไม่เข้าใจขั้นตอนของระบบงานอย่างถ่องแท้ • การปรับเปลี่ยนตำแหน่งงานโดยขาดการถ่ายทอดความรู้ (Knowledge Sharing)	การปฏิบัติงานขาดประสิทธิภาพ และอาจเกิดความล่าช้าในการแก้ไขปัญหา
3.2	การปฏิบัติงานนอกเหนือหน้าที่ความรับผิดชอบ	• เจ้าหน้าที่ทำงานที่ไม่ใช่ความเชี่ยวชาญหรือหน้าที่หลักของตน	เกิดความผิดพลาดในระบบงานเนื่องจากขาดความรู้เฉพาะทาง
4	ด้านข้อมูล (Data)		
4.1	ข้อมูลสูญหายหรือถูกทำลาย	• Hardware เสียหายรุนแรง • ความผิดพลาดจากการปฏิบัติงาน (Human Error) • การบุกรุกจากผู้ไม่หวังดี	สูญเสียข้อมูลสำคัญในการรักษาพยาบาล ไม่มีข้อมูลสำหรับอ้างอิงหรือใช้งาน

4.2	ข้อมูลมีความผิดพลาด (Inaccurate Data)	• บันทึกข้อมูลผิดพลาดจากการปฏิบัติงาน • โปรแกรมประมวลผลค่าผิดพลาด	ข้อมูลขาดความน่าเชื่อถือ ไม่สามารถนำไปใช้ในการตัดสินใจทางการแพทย์หรือบริหารจัดการได้
4.3	ความปลอดภัยและความลับของข้อมูล	• ขาดระบบหรืออุปกรณ์ป้องกันข้อมูลที่มีประสิทธิภาพ • ขาดการตรวจสอบสิทธิ์การเข้าถึง (Access Audit) • ขาดบุคลากรที่มีความเชี่ยวชาญด้าน Security	ข้อมูลผู้ป่วยรั่วไหลสู่ภายนอก หรือถูกแก้ไขโดยไม่ได้รับอนุญาต (กระทบต่อ PDPA)
5	ด้านหน้าที่การปฏิบัติงาน		
5.1	ขั้นตอนการปฏิบัติงานไม่ถูกต้อง	• บุคลากรไม่เข้าใจขั้นตอนมาตรฐาน (SOP) ในการใช้งานระบบ	งานเกิดความผิดพลาด ระบบฐานข้อมูลอาจเกิดความสับสน
5.2	การละเลยหรือขาดการกำกับดูแล	• ขาดความเอาใจใส่ในการตรวจสอบระบบตามวงรอบ	ระบบสะสมปัญหาจนเกิดความเสียหายรุนแรง งานขาดความต่อเนื่องและประสิทธิภาพ