แผนบริหารความเสี่ยงด้านการดำเนินงาน (O)

ด้านเทคโนโลยี

ประจำปีงบประมาณ พ.ศ. ๒๕๖๕

คำนำ

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการจัดการเรื่องราวร้องทุกข์ พ.ศ. ๒๕๕๒ ได้วางหลักเกณฑ์มาตรฐานในการดำเนินการเรื่องราวร้องทุกข์ให้ทุกส่วนราชการมีหลักปฏิบัติในการดำเนินการเรื่องราวร้องทุกข์เป็นแบบแผนและทิศทางเดียวกัน เว้นแต่การจัดการเรื่องราวร้องทุกข์ที่ต้องดำเนินการตามขั้นตอนหรือกระบวนการทางกฎหมายอื่น ในปี พ.ศ. ๒๕๕๗ นี้ สำนักนายกรัฐมนตรีได้จัดทำนโยบายและแผนยุทธศาสตร์การจัดการเรื่องราวร้องทุกข์ เพื่อเป็นกรอบแนวทางในการพัฒนาการจัดการเรื่องราวร้องทุกข์ให้เป็นไปอย่างมีประสิทธิภาพ สอดคล้องกับแผนบริหารราชการแผ่นดิน ตั้งอยู่บนพื้นฐานของหลักธรรมาภิบาล (Good Governance) เพื่อสนองตอบความต้องการของประชาชน เกิดประสิทธิผล คุ้มค่า โปร่งใส และเกิดความเป็นธรรม โรงพยาบาลท่าชนะ ในฐานะหน่วยงานในการให้บริการดูแลสุขภาพของประชาชน โดยรวมในด้านการส่งเสริมสุขภาพ การรักษาพยาบาล การป้องกันโรค และการฟื้นฟูสภาพร่างกาย จำเป็นที่ เจ้าหน้าที่ของรัฐจะต้องอำนวยความสะดวกให้แก่ประชาชน โรงพยาบาลท่าชนะ จึงมีภารกิจสำคัญในการเป็นศูนย์กลางการประสานการแก้ไขปัญหาตามข้อร้องทุกข์/ร้องเรียนของ ประชาชน เพื่อหา แนวทางแก้ไขหรือนำเสนอผู้บริหารพิจารณาสั่งการ ฯลฯ นอกจากนี้ ยังให้ความสำคัญกับกระบวนการและ บุคลากรที่มีขีดความสามารถในการจัดการเรื่องราวร้องทุกข์ ด้วยการจัดทำและกำหนดมาตรฐานการ ปฏิบัติงานที่ชัดเจน สามารถตรวจสอบได้ ลดขั้นตอนที่ไม่จำเป็น โรงพยาบาลท่าชนะ หวังเป็นอย่างยิ่งว่าคู่มือการปฏิบัติงานกระบวนการ จัดการเรื่องราวเรื่องร้องทุกข์/ร้องเรียน โรงพยาบาลท่าชนะ นี้ จะเป็นประโยชน์สำหรับหน่วยงานและบุคลากรผู้ปฏิบัติงานที่จะนำไปเป็นมาตรฐานการปฏิบัติงานการจัดการเรื่องราวร้องทุกข์/ร้องเรียน และสร้างคุณค่าให้แก่ผู้มีส่วนได้เสียอย่างมีคุณภาพ

ดังนั้นเพื่อให้การดำเนินการเกี่ยวกับการจัดการเรื่องร้องเรียนการทุจริตที่อาจเกิดขึ้นในโรงพยาบาลท่าชนะเป็นไปในแนวทางเดียวกัน เกิดประโยชน์ต่อการปฏิบัติราชการและประชาชน และอำนวยความสะดวกต่อเจ้าหน้าที่ผู้ปฏิบัติงาน จึงได้จัดทำคู่มือการปฏิบัติงานเรื่องรับร้องเรียนการทุจริต โดยรวบรวมแนวทางการดำเนินการเรื่องร้องเรียนการทุจริต ทั้งนี้เพื่อให้การจัดการเรื่องร้องเรียนการทุจริตบรรลุผลสัมฤทธิ์ตามภารกิจ

โรงพยาบาลท่าชนะ
๘ พฤศจิกายน ๒๕๖๔

สารบัญ

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดี โดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตาม ควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดการสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กร ทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยง โดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศโรงพยาบาลท่าชนะ

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

ศูนย์สารสนเทศและเวชระเบียนอยู่ในกลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เป็นหน่วยงานดูแลระบบ และสนับสนุนพัฒนาระบบเทคโนโลยีสารสนเทศและเวชระเบียน ดูแลระบบคอมพิวเตอร์ทั้งด้าน Hardware Software และ ฐานข้อมูล ให้ระบบสามารถทำงานได้ตลอด ๒๔ ชั่วโมง มี Server ๒ เครื่อง คอมพิวเตอร์โน๊ตบุ๊ค ๕ เครื่อง เครื่องคอมพิวเตอร์ตั้งโต๊ะ ๑๐๓ เครื่อง โดย มีวัตถุประสงค์เพื่อตอบสนองความต้องการของหน่วยงานในโรงพยาบาลและผู้มีส่วนได้เสียเพื่อให้ได้ข้อมูลที่ครบถ้วน ถูกต้อง รวดเร็ว ตรวจสอบได้ และลดขั้นตอนการทำงาน มีการนำข้อมูลที่ได้มาใช้ในการวางแผนการดำเนินงาน การแก้ปัญหาต่าง ๆ เพิ่มช่องทางการสื่อสารและการเรียนรู้ภายในองค์กร โดยด้านโครงสร้างพื้นฐานหรือ Infrastructure มีการเชื่อมโยงเครือข่าย LAN ครอบคลุมหน่วยงานทั้งโรงพยาบาล มีการแบ่งระบบเครือข่ายออกเป็น ๒ ระบบ คือ ระบบเครือข่ายการให้บริการผู้ป่วย HOSxP และระบบเครือข่าย Internet

ก.หน้าที่และเป้าหมาย

หน้าที่

เป็นหน่วยงานสนับสนุนที่ตั้งขึ้นมาเพื่อให้บริการระบบเทคโนโลยีสารสนเทศของโรงพยาบาลในงานดูแลผู้ป่วย งานบริหารและบริการเครือข่ายฯ เพื่อตอบสนองความต้องการของผู้บริหาร ผู้ให้บริการและผู้รับบริการ อย่างถูกต้องทันเวลาและสามารถนำไปใช้ประโยชน์ได้จริง

เป้าหมาย

- โรงพยาบาลมีระบบสารสนเทศและคอมพิวเตอร์ต้องมีความถูกต้อง เพียงพอ พร้อมใช้ปลอดภัยและได้รับความพึงพอใจ
- มีการจัดเก็บข้อมูลที่สามารถสืบค้นได้ง่าย มีความถูกต้องและทันเวลา
- มีระบบการรักษาความลับและความปลอดภัยของข้อมูล
- มีการเชื่อมโยงข้อมูลเพื่อการบริหาร บริการดูแลผู้ป่วยและการพัฒนาคุณภาพ

ข.ขอบเขตการให้บริการ (Scope of Service)

๑. ดูแลระบบให้พร้อมใช้งาน ตลอด ๒๔ ชั่วโมง

๒. สำรวจและจัดหาคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

๓. บำรุงรักษาดูแลและรักษาความปลอดภัยของระบบเครือข่าย

๔. วางแผนและออกแบบระบบรายงานสารสนเทศเพื่อตอบสนองความต้องการตามคำร้องขอข้อมูลของผู้ใช้กำหนดมาตรฐานและนโยบายสำหรับเวชระเบียน

๕. พัฒนาคุณภาพ ประเมิน ทบทวน ความสมบูรณ์ของเวชระเบียนปรับปรุงฐานข้อมูลให้ถูกต้องครบถ้วนก่อนส่งออก

๖. เชื่อมโยงข้อมูลสารสนเทศ เพื่อการพัฒนาคุณภาพ

๗. ให้คำปรึกษา แนะนำอบรมงานด้านสารสนเทศและการใช้คอมพิวเตอร์ให้สอดคล้องกับสถานการณ์ปัจจุบัน

๘. รวบรวมข้อมูล วิเคราะห์ และนำเสนอข้อมูลต่อทีมนำของหน่วยงาน

นิยามความเสี่ยง

ความเสี่ยง คือ ความไม่แน่นอนที่อาจนำไปสู่ความสูญเสียทั้งที่เป็นตัวเงินและไม่เป็นตัวเงิน ความเสี่ยงมีทั้งประเภทที่เป็นความเสี่ยงที่แท้จริงที่เป็นความเสี่ยงที่มีโดยธรรมชาติ และความเสี่ยงที่เกิดจากการเก็งกำไร ความหมายของความเสี่ยงอาจมีการตีความแตกต่างกันไปหลายอย่างตามแต่ความเชี่ยวชาญ และอาชีพของผู้ให้คำจำกัดความ **การบริหารความเสี่ยง** เป็นการบริหารปัจจัย และควบคุมกิจกรรม หรือกระบวนการต่าง ๆ เพื่อลดโอกาสที่จะทำให้เกิดความเสียหาย หรือล้มเหลว ดังนั้นเพื่อควบคุมให้ระดับความเสียหาย และผลกระทบที่อาจจะเกิดขึ้นในอนาคตอยู่ในระดับที่สามารถรับได้ ประเมินได้ ควบคุมได้ และสามารถตรวจสอบได้อย่างมีระบบ โดยคำนึงถึงการบรรลุเป้าหมายตามภารกิจหลัก ตามกฎหมายจัดตั้งส่วนราชการ และเป้าหมายตามแผนปฏิบัติราชการประจำปีงบประมาณของส่วนราชการและเป้าหมายตามแผนปฏิบัติราชการประจำปีของส่วนราชการ

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กร และการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่างๆ ที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

๓. **บุคลากร** หมายถึง กลุ่มบุคคลที่ปฏิบัติงานกับระบบสารสนเทศ คือ เป็นผู้นำ จัดการข้อมูลและนำผลลัพธ์ออกจากระบบคอมพิวเตอร์

๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. **หน้าที่การปฏิบัติงาน** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กร โดยรวมไม่ว่าจะเป็นฝ่ายต่างๆ ขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกัน หรือลดการเกิดความเสียหายในรูปแบบต่างๆ โดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกัน เพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

๑.การหลีกเลี่ยง (Terminate) เป็นวิธีการที่ง่ายที่สุดในการบริหารความเสี่ยง คือ การเลือกที่จะไม่รับความเสี่ยงไว้เลย อาจหยุดดำเนินการ หรือยกเลิกโครงการ/กิจกรรมที่ก่อให้เกิดความเสียหายได้ การหลีกเลี่ยงความเสี่ยงเมื่อพบว่าผลประโยชน์ที่จะได้รับนั้นไม่คุ้มกับสิ่งที่จะเกิดขึ้น จึงหลีกเลี่ยงที่จะเผชิญกับกิจกรรมความเสี่ยงนั้น หรือการหลีกเลี่ยงความเสี่ยงอาจเกิดขึ้นจากหน่วยงานเลือกที่จะหลีกเลี่ยงกิจกรรมความเสี่ยงนั้น โดยมิได้คิดทบทวนถึงผลที่จะได้รับ นำมาซึ่งการเสียโอกาสของหน่วยงานได้

๒.การยอมรับ (Take) เป็นการยอมรับความเสี่ยง หรือความเสียหายที่อาจจะเกิดขึ้นไว้เองโดยไม่ทำอะไร และยอมรับในผลที่อาจตามมา เนื่องจากเห็นว่าโอกาสหรือความน่าจะเป็นที่จะเกิดความเสียหายอยู่ในวิสัยที่หน่วยงานยอมรับได้ หรือไม่คุ้มค่าสำหรับค่าใช้จ่ายในการสร้างระบบในการจัดการหรือป้องกันความเสี่ยง เช่น การกำหนด User/Password ในการเข้าใช้งานระบบเครือข่ายให้กับหัวหน้างาน เมื่อหัวหน้างานได้ User/Password ที่ทางศูนย์คอมฯ ออกให้แล้ว อาจจะบอกให้ผู้ใต้บังคับบัญชาของตนทราบ User/Password ดังกล่าว และเมื่อผู้ใต้บังคับบัญชาทราบUser/Password ของหัวหน้างาน อาจจะเก็บไว้คนเดียวหรือนำไปบอกให้บุคคลอื่นทราบต่อ ซึ่งในกรณีนี้จะเกิดความเสี่ยงในการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่าย ซึ่งทางศูนย์คอมฯ ต้องยอมรับความเสี่ยงหรือความเสียหายที่อาจเกิดขึ้น และกำหนด User/Password ใหม่ ให้กับหัวหน้างาน เป็นต้น

๓.การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่ เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสียและการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสีย ก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้น การควบคุมขนาดของความสูญเสียเป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิงอุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้องServer ให้มีความเสียหายน้อยที่สุด หรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

๔.การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปีเพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงานองค์กรอาจเลือกซื้อประกันหรือสัญญาการบำรุงรักษาหลังการขายเป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศ ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่อง

ประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การชำรุดเสียหายของตัวเครื่องประมวลผลหลัก หรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้าย หรืออื่นๆ

๑.๔ ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ ขัดข้อง

๑.๕ ระบบกระแสไฟฟ้าขัดข้อง/ ไฟฟ้าดับ

๒. ปัจจัยภายใน ได้แก่

๒.๑ ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒.๒ การถูกไวรัส (Virus) ทำลายฐานข้อมูล และโปรแกรมปฏิบัติการต่างๆ

๒.๓ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

การประเมินความเสียหาย

๑.ความเสียหายที่เกิดผลเสียหายร้ายแรงที่สุด ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลง ได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลายเสียหายจากไวรัส

๒.ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์โรงพยาบาลท่าชนะ มีการกำหนดนโยบายและมาตรการในการรักษาความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้โปรแกรมป้องกันไวรัส และ Firewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายได้รับความปลอดภัยและป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมดปัจจุบันเครือข่ายของ โรงพยาบาลท่าชนะ มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private การใช้งานเพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบกรณีเกิดปัญหา

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๑.	ความเสี่ยงด้าน Hardware		
	๑.๑อุปกรณ์คอมพิวเตอร์เสียหาย	-หมดอายุการใช้งาน -มีการใช้งานหนัก -สภาวะแวดล้อม (ไฟฟ้า,อากาศ)	-ไม่สามารถทำงานต่อไปได้
	๑.๒ระบบเครือข่ายมีปัญหา	-อุปกรณ์เครือข่ายเสียหาย -ผู้ให้บริการเครือข่ายขัดข้อง	-ไม่สามารถใช้บริการผ่านเครือข่ายได้
๒.	ความเสี่ยงด้าน Software		
	๒.๑software ไม่สามารถทำงานได้	-ระบบปฏิบัติการเสียหาย -Software มีการทำงานผิดพลาด -Virus/Hacker/Spyware	-ไม่สามารถให้บริการได้
๓.	ความเสี่ยงด้านบุคลากร		
	๓.๑ ขาดทักษะในการทำงาน	-ไม่เข้าใจระบบงานนั้น ๆ อย่างถี่ถ้วน -ปรับเปลี่ยนตำแหน่งงาน	-งานที่ได้ไม่มีประสิทธิภาพเท่าที่ควร
	๓.๒ ไม่ใช่หน้าที่หลักที่รับผิดชอบ	-ทำงานที่ไม่ใช่หน้าที่ของตน	-งานอาจเกิดผิดพลาด
๔.	ความเสี่ยงด้านข้อมูล		
	๔.๑ข้อมูลถูกทำลาย/สูญหาย	-Hardware เสีย -การปฏิบัติงานผิดพลาด -ผู้ไม่หวังดี	-ไม่มีข้อมูลเพื่อนำไปใช้งาน
	๔.๒ ข้อมูลผิดพลาด	-เนื่องจากการปฏิบัติงานผิดพลาด -โปรแกรมทำงานผิดพลาด	-ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	๔.๓ความปลอดภัยของข้อมูล	-ขาดอุปกรณ์ป้องกันข้อมูลที่ดี -ขาดการตรวจสอบ -ขาดบุคลากรที่มีความรู้อย่างแท้จริง	-อาจทำให้ข้อมูลเสียหาย -ข้อมูลรั่วไหล
๕.	ความเสี่ยงด้านหน้าที่การปฏิบัติ		
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	-ไม่เข้าใจในขั้นตอนปฏิบัติ	-ไม่สามารถทำงานได้หรืองานมีความผิดพลาด
	๕.๒ ละเลยการปฏิบัติหน้าที่	-ไม่เอาใจใส่ในงาน	-งานไม่มีประสิทธิภาพ

แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๑.ความเสี่ยงด้านความเสียหายของระบบสารสนเทศและข้อมูลสารสนเทศ															
๑.๑ระบบฐานข้อมูล/โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ - จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ - ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	-ทุกวัน/ทุกสัปดาห์ -ทุกเดือน -ทุกเดือน	◄	─	─	─	─	─	─	─	─	─	─	►	
๑.๒ข้อมูลเสียหายเกิดจากอุปกรณ์บันทึกข้อมูล (Hard disk) ชำรุด	-จัดทำการสำรองข้อมูลแบบอัตโนมัติ -จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ -ทดสอบการกู้คืนฐานข้อมูลและระบบสารสนเทศ	-ทุกวัน/ทุกสัปดาห์ -ทุกเดือน -ทุกเดือน	◄	─	─	─	─	─	─	─	─	─	─	►	

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๒.ความเสี่ยงด้านภัยพิบัติระบบสารสนเทศ															
๒.๑ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	-ทุกเดือน	←											→	
๒.๒ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง	-ตรวจสอบระบบเครือข่ายสื่อสารหลัก	-ทุกเดือน	←											→	
๓.ความเสี่ยงด้านความมั่นคงและปลอดภัยของระบบข้อมูล															
๓.๑ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	-ทุกเดือน	←											→	
๓.๒การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	-ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	-ทุกเดือน	←											→	
๓.๓การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	-ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	-ทุกเดือน	←											→	

ประเภทความเสี่ยง/กิจกรรม	แนวทางการควบคุม	ระยะเวลาเริ่มต้น/สิ้นสุด	ปีงบประมาณ												หมายเหตุ
			ต.ค.	พ.ย.	ธ.ค.	ม.ค.	ก.พ.	มี.ค.	เม.ย.	พ.ค.	มิ.ย.	ก.ค.	ส.ค.	ก.ย.	
๔.ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
๔.๑การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์กรโดยไม่ได้รับอนุญาต	- กำหนดสิทธิ์ในการเข้าถึงข้อมูล	-เมื่อแต่งตั้ง/โยกย้าย/ลาออก/เกษียณอายุราชการ	←											→	
๕.อุปกรณ์คอมพิวเตอร์เสียหาย															
๕.๑คอมพิวเตอร์ไม่สามารถใช้งานได้	-บำรุงรักษาคอมพิวเตอร์ เช่นเป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	-ทุก ๓ เดือน			✓			✓			✓			✓	