คำสั่งโรงพยาบาลบ้านด่าน

ที่ ๑๕ / ๒๕๖๘

เรื่อง แต่งตั้งคณะกรรมการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศ

เพื่อให้การดำเนินการใดๆ ต่อระบบสารสนเทศโรงพยาบาลบ้านด่าน เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจส่งผลทำให้ระบบสารสนเทศไม่สามารถดำเนินงานต่อไปได้จากภัยคุกคามด้านเครือข่ายต่างๆ ซึ่งอาจส่งผลทำให้เกิดความเสียหายต่อระบบสารสนเทศโรงพยาบาลบ้านด่าน และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และกฎหมายอื่นๆ ที่เกี่ยวข้อง โรงพยาบาลบ้านด่านจึงขอแต่งตั้งคณะกรรมการบริหารความเสี่ยงทางด้านเทคโนโลยีสารสนเทศของโรงพยาบาลบ้านด่าน ดังนี้

๑. นายศาสตรา เข็มบุบผา	นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)	ประธาน
๒. นายวิทธวัช แก้วบุดศา	ทันตแพทย์ชำนาญการ	รองประธาน
๓. นางสาวศศินิภา ประดุจชนม์	นายแพทย์ชำนาญการ	กรรมการ
๔. นางวัลยา ภูทอง	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๕. นางสาวเอื้อมพร สร้อยจิต	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๖. นางอาทิฏญาภรณ์ แก้ววัน	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๗. นางหนึ่งฤทัย ทุมดี	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๘. นางสาวสุภาวดี เดือนประโคน	พยาบาลวิชาชีพชำนาญการ	กรรมการ
๙. นายดุสิต สัตย์ณุชนม์	เภสัชกรปฏิบัติการ	กรรมการ
๑๐. นาวสาวจอมขวัญ ไชยสุวรรณ์	พยาบาลวิชาชีพปฏิบัติการ	กรรมการ
๑๑. นางสาวมนัญญา จันทร	นักเทคนิคการแพทย์ปฏิบัติการ	กรรมการ
๑๒. นายสยาม พรหมเอาะ	นักวิชาการสาธารณสุขปฏิบัติการ	กรรมการ
๑๓. นางสาวสมฤทัย ชูมี	เจ้าพนักงานเวชสถิติปฏิบัติงาน	กรรมการ
๑๔. นางสาวพรตะวัน สุขรอด	เจ้าพนักงานธุรการ	กรรมการ
๑๕. นางสาวดวงจันทร์ ชะงักรัมย์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและเลขานุการ
๑๖. นางสาวบุษรา หงษ์เรืองรัมย์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	กรรมการและผู้ช่วยเลขานุการ

โดยมีหน้าที่ ดังนี้

๑. จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานให้ได้มาตรฐาน

๒. กำหนดแนวปฏิบัติควบคุมการใช้งานระบบสารสนเทศและการสื่อสาร

๓. กำหนดแนวปฏิบัติในการรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

๔. กำหนดแนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๕. กำหนดแนวปฏิบัติในด้านรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อม

๖. กำหนดแนวปฏิบัติในการกำหนดหน้าที่ความรับผิดชอบ

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

สั่ง ณ วันที่ ๑๗ มกราคม พ.ศ. ๒๕๖๘

(นายศาสตรา เข็มบุบผา)
ผู้อำนวยการโรงพยาบาลบ้านด่าน

โรงพยาบาลบ้านด่าน		จำนวนหน้า : ๒
นโยบายและวิธีปฏิบัติ BD-IMIT-๐๑๓		ฉบับที่ ๑
เรื่อง : การปฏิบัติกรณีเครื่อง Server/Database มีปัญหา		วันที่ ๑๘ กุมภาพันธ์ ๒๕๖๔
แผนก : งานสารสนเทศ	แผนกที่เกี่ยวข้อง : จนท.รพ.ที่เกี่ยวข้อง	วันที่ปรับปรุง : ๑๘ กุมภาพันธ์ ๒๕๖๔
ผู้จัดทำ :: งานสารสนเทศ	ผู้อนุมัติ (นายศาสตรา เข็มบุบผา) ผู้อำนวยการโรงพยาบาลบ้านด่าน	

แนวทางปฏิบัติกรณีเครื่อง Server/Database มีปัญหา

๑. กรณีเครื่อง Server /Database มีปัญหา สามารถแก้ไขได้ภายใน ๓๐ นาที

<u>เจ้าหน้าที่ศูนย์คอมพิวเตอร์</u>

- นักวิชาการคอมพิวเตอร์ หรือ เจ้าหน้าที่เครื่องคอมพิวเตอร์ งานสารสนเทศตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากสามารถแก้ไขได้ภายใน ๓๐ นาที แจ้งประกาศให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP ชั่วคราว
- ดำเนินการแก้ไข ตรวจสอบความพร้อมให้เรียบร้อย
- ประกาศให้ทุกหน่วยงานสามารถใช้งาน HOSxP ได้ตามปกติ
- สรุปสาเหตุของปัญหา และลงบันทึกในโปรแกรมความเสี่ยง

<u>เจ้าหน้าที่หน่วยงานต่างๆ</u>

- เมื่อได้รับแจ้งจากงานสารสนเทศ ให้หยุดการใช้งานคอมพิวเตอร์ชั่วคราว
- ประชาสัมพันธ์ให้ประชาชนที่รอรับบริการทราบ และจัดบริการที่สามารถทำได้โดยบันทึกลงในแบบฟอร์ม OPD card พร้อมใบ Slip OPD และเก็บเอกสารเพื่อรอลงบันทึกย้อนหลัง
- เมื่อได้รับแจ้งให้ใช้งานคอมพิวเตอร์ได้ตามปกติ ให้เริ่มนำข้อมูลบริการลงบันทึกในโปรแกรม HOSxP

๒. กรณีเครื่อง Server /Database มีปัญหา ไม่สามารถแก้ไขได้ภายใน ๓๐ นาที

<u>เจ้าหน้าที่งานสารสนเทศ</u>

- นักวิชาการคอมพิวเตอร์ ตรวจสอบสาเหตุของปัญหาและประเมินระยะเวลาในการแก้ไข หากไม่สามารถแก้ไขได้ภายใน ๓๐นาที ให้แจ้งหัวหน้างานสารสนเทศ / ผู้อำนวยการโรงพยาบาลหนองกี่ทราบ
- ผู้อำนวยการโรงพยาบาลหนองกี่ประกาศใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้ โดยใช้มาตรการเดียวกับข้อ **กรณีไฟฟ้าดับ** มากกว่า ๓๐ นาที ให้ทุกหน่วยงานหยุดการใช้งานโปรแกรม HOSxP
- งานสารสนเทศดำเนินการแก้ไขปัญหา Server ให้สามารถใช้งานได้ตามปกติภายใน ๒๔ ชั่วโมง
- ประสานผู้เกี่ยวข้องเพื่อตรวจสอบการลงบันทึกข้อมูลในโปรแกรม HOSxP ย้อนหลัง
- เมื่อเครื่อง Server สามารถทำงานได้ตามปกติ ให้ตรวจสอบความเรียบร้อยของ Server และอุปกรณ์เครือข่าย

- ประกาศแจ้งให้หน่วยงานต่างๆ เปิดคอมพิวเตอร์ใช้งาน HOSxP และเริ่มบันทึกข้อมูลย้อนหลัง
- ติดตามตรวจสอบความเรียบร้อยของการลงบันทึกข้อมูลของหน่วยงานต่างๆ จนกระทั่งระบบข้อมูลเป็นปัจจุบัน และสามารถให้บริการได้ตามปกติ
- ผู้อำนวยการโรงพยาบาลบ้านด่าน ประกาศยกเลิกใช้แผนฉุกเฉินกรณีระบบเครือข่ายใช้งานไม่ได้
- ลงบันทึกในโปรแกรมความเสี่ยงสรุปรายงานนำเสนอผู้อำนวยการและคณะกรรมการบริหารทราบ

หมายเหตุ กรณีเครื่อง Server/Database กำหนดให้ผู้มีรายชื่อดังต่อไปนี้เป็นผู้ตรวจสอบและแก้ไขปัญหา

๑. นางสาวดวงจันทร์ ชะงักรัมย์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ เบอร์ ๐๘๐-๔๘๔๕๙๓๔

๒. นางสาวบุษรา หงษ์เรืองรัมย์ นักวิชาการคอมพิวเตอร์ปฏิบัติการ เบอร์ ๐๖๑-๖๙๑๖๙๖๕

หากไม่สามารถติดต่อได้ ให้ใช้ระเบียบปฏิบัติเช่นเดียวกับ **กรณีไฟฟ้าดับ**

- บันทึกรายงานความเสี่ยงและสรุปปัญหาเสนอ ผู้อำนวยการและคณะกรรมการบริหาร

ผู้รับผิดชอบ : เจ้าหน้าที่งานสารสนเทศโรงพยาบาลบ้านด่าน

แนวปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
โรงพยาบาลบ้านด่าน
อำเภอบ้านด่าน จังหวัดบุรีรัมย์

บทที่ ๑ บทนำ

หลักการและเหตุผล

การบริหารความเสี่ยงเป็นเครื่องมือทางกลยุทธ์ที่สำคัญตามหลักการกำกับดูแลกิจการที่ดีโดยจะช่วยให้การบริหารงานและการตัดสินใจด้านต่างๆ เช่น การวางแผน การกำหนดกลยุทธ์ การติดตามควบคุม และวัดผลการปฏิบัติงาน ตลอดจนการใช้ทรัพยากรต่างๆ อย่างเหมาะสมและมีประสิทธิภาพมากขึ้น ลดกาสูญเสียและโอกาสที่ทำให้เกิดความเสียหายแก่องค์กร โดยเฉพาะอย่างยิ่งในด้านเทคโนโลยีสารสนเทศที่เข้ามามีบทบาทสำคัญในการดำเนินงานของหน่วยงานภายในองค์กรทั้งการจัดเก็บข้อมูล การใช้งานอุปกรณ์คอมพิวเตอร์ การติดต่อสื่อสารผ่านระบบเครือข่าย และวิธีการปฏิบัติงานระบบเทคโนโลยีสารสนเทศต่างๆ ภายใต้สภาวะการดำเนินงานของทุกๆ องค์กรล้วนแต่มีความเสี่ยง ซึ่งก็คือความไม่แน่นอนที่จะส่งผลกระทบต่อการดำเนินงานหรือเป้าหมายขององค์กร จึงจำเป็นต้องมีการจัดการความเสี่ยงเหล่านั้นอย่างเป็นระบบ โดยการระบุความเสี่ยงว่ามีปัจจัยเสี่ยงใดบ้างที่กระทบต่อการดำเนินงานหรือเป้าหมายขององค์กรวิเคราะห์ความเสี่ยงจากโอกาสและผลกระทบที่เกิดขึ้น จัดลำดับความสำคัญของปัจจัยเสี่ยง แล้วกำหนดแนวทางในการจัดการความเสี่ยงโดยต้องคำนึงถึงความคุ้มค่าในการจัดการความเสี่ยงอย่างเหมาะสม

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมและรองรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลสารสนเทศ โรงพยาบาลบ้านด่าน

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

บริบท (Context)

โรงพยาบาลบ้านด่านมีระบบบริหารจัดการข้อมูลสารสนเทศ และได้นำระบบบริการผู้ป่วยโดยใช้ฐานข้อมูลตั้งแต่ปี ๒๕๕๗ โดย เริ่มต้นด้วยโปรแกรม HOSxP ซึ่งเป็นโปรแกรมที่พัฒนาโดยบริษัทบางกอกเมดิคอลซอฟแวร์

นิยาม ความเสี่ยงของระบบสารสนเทศ

คือ เหตุการณ์หรือการกระทำใดๆที่อาจเกิดขึ้นภายในสถานการณ์ที่ไม่แน่นอนและจะส่งผลกระทบหรือสร้างความเสียหายหรือความล้มเหลวหรือลดโอกาสที่จะบรรลุความสำเร็จต่อการบริหารงานของระบบสารสนเทศที่ใช้คอมพิวเตอร์ในการบริหาร

นิยาม ระบบสารสนเทศ

คือ ระบบข้อมูล การจัดเก็บข้อมูล การประมวลผลข้อมูล การไหลข้อมูลทั้งภายในและภายนอกองค์กรและการนำเสนอสารสนเทศ

องค์ประกอบของระบบคอมพิวเตอร์

๑. **Hardware** หมายถึง อุปกรณ์ต่างๆที่กระทำกับข้อมูล เอกสาร ทั้งที่เป็นอุปกรณ์คอมพิวเตอร์และไม่ใช่คอมพิวเตอร์

๒. **Software** หมายถึง ชุดคำสั่งที่สั่งให้คอมพิวเตอร์ทำงาน

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

๔. **ข้อมูลและแฟ้มข้อมูล** หมายถึงข้อมูลและสารสนเทศ ที่ระบบจัดเก็บไว้ในช่วงเวลาหนึ่ง

๕. **หน้าที่การปฏิบัติงาน** หมายถึงคำสั่งหรือกฎเกณฑ์ที่ใช้ในการทำงานของระบบ

องค์ประกอบของระบบสารสนเทศ

องค์กร โครงสร้างขององค์กรระบบสารสนเทศจะทำหน้าที่ในการสนับสนุนการทำงานขององค์กรโดยรวม ไม่ว่าจะเป็นฝ่ายต่างๆขององค์กร

บุคลากร บุคลาการที่ใช้ระบบสารสนเทศจากระบบคอมพิวเตอร์ที่ทำงานร่วมกัน บุคลากรที่ต้องการป้อนข้อมูลไปยังระบบเพื่อส่งต่อไปยังคอมพิวเตอร์

เทคโนโลยี อุปกรณ์ที่ทำหน้าที่ในการจัดการสารสนเทศ เพื่อส่งต่อไปยังบุคลากรที่ใช้ระบบสารสนเทศ

หมายเหตุ องค์ประกอบของระบบสารสนเทศที่ใช้ระบบคอมพิวเตอร์ในการบริหาร จึงประกอบด้วยองค์ประกอบของทั้งสองระบบรวมกัน

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ส่วนราชการต้องมีการวางระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ โดยต้องดำเนินการดังต่อไปนี้

๑. มีการบริหารความเสี่ยงเพื่อกำจัด ป้องกันหรือลดการเกิดความเสียหายในรูปแบบต่างๆโดยสามารถฟื้นฟูระบบสารสนเทศและการสำรองและกู้คืนข้อมูลจากความเสียหาย (Backup andRecovery)

๒. มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๓. มีระบบรักษาความมั่นคงและปลอดภัย (Security) ของระบบฐานข้อมูล

๔. มีการกำหนดสิทธิให้ผู้ใช้ในแต่ละระดับ (Access Rights)

การตอบสนองความเสี่ยง

เมื่อความเสี่ยงได้รับการบ่งชี้และประเมินความสำคัญแล้วผู้บริหารต้องประเมินวิธีการจัดการความเสี่ยงที่สามารถนำไปปฏิบัติได้และผลของการจัดการเหล่านั้น การพิจารณาทางเลือกในการดำเนินการจะต้องคำนึงถึงความเสี่ยงที่ยอมรับได้ และต้นทุนที่เกิดขึ้นเปรียบเทียบกับผลประโยชน์ที่จะได้รับเพื่อให้การบริหารความเสี่ยงมีประสิทธิผล ผู้บริหารอาจต้องเลือกวิธีการจัดการความเสี่ยงอย่างใดอย่างหนึ่ง หรือหลายวิธีรวมกันเพื่อลดระดับโอกาสที่อาจเกิดขึ้นและผลกระทบของเหตุการณ์ให้อยู่ในช่วงที่องค์กรสามารถยอมรับได้ (Risk Tolerance)

หลักการตอบสนองความเสี่ยงมี ๔ ประการ คือ

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

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

๓. การควบคุม (Treat) เป็นการปรับปรุงระบบการทำงาน หรือออกแบบวิธีการทำงานใหม่เพื่อหาทางป้องกันมิให้มีความเสียหายเกิดขึ้น เป็นการลดโอกาสหรือจำนวนครั้งของความเสียหายที่จะเกิด หากเราไม่สามารถป้องกันไม่ให้ความเสี่ยงเกิดขึ้นได้ ก็ควรขจัดให้หมดไป หรือลดความรุนแรงของความเสี่ยงลงโดยมีการจัดทำแผนหรือมาตรการควบคุมขึ้น อาจกำหนดเป็นแนวทางปฏิบัติไว้ล่วงหน้า ทั้งนี้วิธีควบคุมความสูญเสียมีสองวิธีหลัก คือ การป้องกันการเกิดความสูญเสีย และการควบคุมขนาดของความสูญเสียหลังเกิดความสูญเสียขึ้นการป้องกันการเกิดความสูญเสีย เป็นวิธีการที่พยายามจะลดความถี่ของการเกิดความสูญเสียก็คือการหามาตรการหรือวิธีการใด ๆ ในการป้องกันไม่ให้ความสูญเสียเกิดขึ้น เช่น การติดตั้งระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall) เพื่อเป็นการป้องกันการถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบเครือข่ายเป็นการป้องกันบุคคล ไวรัส มิให้เข้าถึงหรือสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ เป็นต้นการควบคุมขนาดของความสูญเสีย เป็นวิธีการที่พยายามจะลดความรุนแรงของความสูญเสียเมื่อเกิดความสูญเสียขึ้นแล้ว เช่น การติดตั้งอุปกรณ์ดับเพลิง อุปกรณ์เตือนไฟไหม้ เช่น เครื่องตรวจจับควันเครื่องตรวจจับความร้อน หรือสัญญาณเตือนภัย เพื่อป้องกันหรือระงับเหตุไฟไหม้ได้ทันเวลา ในกรณีที่เกิดเหตุการณ์ไฟไหม้ห้อง Server เพื่อเป็นการลดความสูญเสียของอุปกรณ์ภายในห้อง Server ให้มีความเสียหายน้อยที่สุดหรือไม่เกิดความเสียหายหรือกระทบต่อการทำงานของระบบเครือข่าย เป็นต้น

๔.การถ่ายโอน (Transfer) การโอนย้ายหรือแบ่งความเสี่ยงไปให้ผู้อื่นช่วยรับผิดชอบ เช่น อุปกรณ์เครือข่ายเมื่อซื้อมาแล้วมีระยะประกันภัยเพียงหนึ่งปี เพื่อเป็นการรับมือในกรณีที่อุปกรณ์เครือข่ายไม่ทำงาน องค์กรอาจเลือกซื้อประกัน หรือสัญญาการบำรุงรักษาหลังการขายเป็นการเพิ่มเติม

ปัจจัยเสี่ยง

ปัจจัยที่จะเกิดความเสียหายกับระบบฐานข้อมูลสารสนเทศของกรมการแพทย์ ได้แก่

๑. ปัจจัยภายนอก ได้แก่

๑.๑ ภัยธรรมชาติ และการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือ เครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล ได้แก่ ไฟไหม้ ภัยพิบัติ

๑.๒ การขโมยอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๑.๓ การขำรุดเสียหายของตัวเครื่องประมวลผลหลัก 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 ซึ่งจะทำให้ต้องหยุดระบบประมวลผลทั้งระบบลงได้แก่ ภัยธรรมชาติ ตัวเครื่องประมวลผลหลักหรือแม่ข่ายเสียหาย (Server) และระบบฐานข้อมูลหลักถูกทำลาย เสียหายจากไวรัส

๒. ความเสียหายที่เกิดผลเสียหายแจะต้องหยุดระบบชั่วขณะ ได้แก่ การถูกเจาะเข้าระบบฐานข้อมูล ระบบสื่อสารของเครือข่ายคอมพิวเตอร์ขัดข้อง และกระแสไฟฟ้าขัดข้อง

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็น ประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุก กรณีตามที่ระบุ

ระบบรักษาความปลอดภัยบนเครือข่าย

ระบบเครือข่ายคอมพิวเตอร์โรงพยาบาลบ้านด่าน มีการกำหนดนโยบายและมาตรการในการรักษา ความปลอดภัยอย่างเข้มงวด โดยใช้ซอฟต์แวร์ เพื่อป้องกันการโจมตีและบุกรุกเข้ามายังเครือข่ายโดยใช้ โปรแกรมป้องกันไวรัสและFirewall เพื่อให้คอมพิวเตอร์ทุกเครื่องที่อยู่ในระบบเครือข่ายของโรงพยาบาล เพื่อให้ได้รับความปลอดภัย และป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบเครือข่ายทั้งหมด ปัจจุบัน เครือข่ายของ โรงพยาบาลบ้านด่าน มีการกำหนดให้ใช้หมายเลข IP Address ประจำหน่วยงานแบบ Private เพื่อเพิ่มความปลอดภัยและสะดวกและรวดเร็วต่อการบริหารจัดการระบบ กรณีเกิดปัญหาการใช้งาน

การบริหารความเสี่ยง (Risk Management)

เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่างๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงเพื่อหาว่าความเสี่ยงได้เปลี่ยนแปลงไปอย่างไร

การประเมินความเสี่ยง

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๑.	**ความเสี่ยงด้าน Hardware**		
	๑.๑ อุปกรณ์คอมพิวเตอร์เสียหาย	- หมดอายุการใช้งาน - มีการใช้งานหนัก - สภาวะแวดล้อม (ไฟฟ้า ,อากาศ)	ไม่สามารถทำงานต่อไปได้
	๑.๒ ระบบเครือข่ายมีปัญหา	- อุปกรณ์เครือข่ายเสียหาย - ผู้ให้บริการเครือข่าขัดข้อง	ไม่สามารถใช้บริการผ่านเครือข่ายได้
๒.	**ความเสี่ยงด้าน Software**		
	๒.๑ Software ไม่สามารถทำงานได้	- ระบบปฏิบัติการเสียหาย - Software มีการทำงานผิดพลาด - Virus /Hacker /Spyware	ไม่สามารถให้บริการได้
๓.	**ความเสี่ยงด้านบุคลากร**		
	๓.๑ ขาดทักษะในการทำงาน	- ไม่เข้าใจระบบงานนั้นๆ อย่างถี่ถ้วน - ปรับเปลี่ยนตำแหน่ง	งานที่ได้ไม่มี ประสิทธิภาพเท่าที่ควร
	๓.๒ ไม่ใช่หน้าที่หลักที่รับผิดชอบ	- ทำงานที่ไม่ใช่หน้าที่ของตน	งานอาจผิดพลาด

ตารางที่ ๑ การประเมินความเสี่ยงแยกตามประเภทความเสี่ยง ๕ ด้าน(ต่อ)

ลำดับ	ความเสี่ยง	สาเหตุ	ผลกระทบ
๔.	**ความเสี่ยงด้านข้อมูล**		
	๔.๑ ข้อมูลถูกทำลาย / สูญหาย	- Hardware เสีย - การปฏิบัติงานผิดพลาด - ผู้ไม่หวังดี	ไม่มีข้อมูลเพื่อนำไปใช้งาน
	๔.๒ ข้อมูลผิดพลาด	- เนื่องจากการปฏิบัติงานผิดพลาด - โปรแกรมทำงานผิดพลาด	ไม่สามารถนำข้อมูลไปใช้เพื่อการตัดสินใจได้
	๔.๓ ความปลอดภัยของข้อมูล	- ขาดอุปกรณ์ป้องกันข้อมูลที่ดี - ขาดการตรวจสอบ - ขาดบุคลากรที่มีความรู้อย่างแท้จริง	อาจทำให้ข้อมูลเสียหาย ข้อมูลรั่วไหล
๕.	**ความเสี่ยงด้านหน้าที่การปฏิบัติ**		
	๕.๑ ปฏิบัติหน้าที่ไม่ถูกต้อง	- ไม่เข้าใจในขั้นตอนปฏิบัติ	ไม่สามารถทำงานได้หรืองานมีความผิดพลาด
	๕.๒ ละเลยการปฏิบัติ	- 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															
๑.๑ ระบบฐานข้อมูล/ โปรแกรมที่ให้บริการเกิดความเสียหาย	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													
๑.๒ ข้อมูลเสียหายเกิดจากอุปกรณ์ บันทึกข้อมูล (Hard disk) ชำรุด	- จัดทำการสำรองข้อมูลแบบอัตโนมัติ	- ทุกวัน/ทุกสัปดาห์													
	- จัดทำการสำรองข้อมูลแบบไม่อัตโนมัติ	- ทุก สัปดาห์เดือนละ ๔ ครั้ง	←											→	
	- ทดสอบการกู้คืนฐานข้อมูล และระบบสารสนเทศ	- ทุก สัปดาห์ เดือนละ ๔ ครั้ง													

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

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															
๒.๑ ไฟไหม้ห้อง Server	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๒.๒ ระบบเครือข่ายสื่อสารหลักเสียหาย/ขัดข้อง	- ตรวจสอบระบบเครือข่ายสื่อสารหลัก	- ทุก ๓ เดือน			√			√			√			√	
๒.๓ ฝนฟ้าคะนอง อุปกรณ์ต่อพ่วงเสียหาย	- ตรวจสอบความพร้อมของระบบป้องกันไฟกรรโชก กราวป้องกันฟ้าผ่า ทำแผนซื้ออุปกรณ์ป้องกันเพิ่ม	- ช่วงฤดูฝน								←	—	—	—	→	
๓. ความเสี่ยงด้านความมั่นคง และปลอดภัยของระบบฐานข้อมูล															
๓.๑ ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ	- ตรวจสอบระบบสำรองไฟฟ้า (UPS)	- ทุกวันที่ ๓๐ ก.ย.ของทุกปี												√	
๓.๒ การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบประมวลผลของเครื่อง Server	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	
๓.๓ การถูกเจาะหรือลักลอบ (Hack) ระบบฐานข้อมูล	- ตรวจสอบระบบป้องกันการบุกรุกระบบเครือข่าย (Firewall)	- ทุกวันที่ ๑ และ ๑๖ ของทุกเดือน	←	—	—	—	—	—	—	—	—	—	—	→	

ตารางที่ ๒ แผนการดูแลจัดการรักษาและแก้ไขปัญหาระบบข้อมูลสารสนเทศ (ต่อ)

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.	
๓.๔ ขาดเครื่องมือป้องกันหรือตรวจจับไวรัส	- มีโปรแกรมป้องกันไวรัสและ Update ฐานข้อมูลไวรัส	- สัปดาห์ละ ๑ ครั้ง	←											→	
๔. ความเสี่ยงด้านสิทธิการใช้งานของผู้ใช้งานในแต่ละระดับ															
๔.๑ การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ภายในองค์การโดยไม่ได้รับอนุญาต	- กำหนดสิทธิในการเข้าถึงข้อมูล	- เมื่อแต่งตั้ง/โยกย้าย /ลาออก / เกษียณอายุราชการ	←											→	
๕. อุปกรณ์คอมพิวเตอร์เสียหาย	- บำรุงรักษาคอมพิวเตอร์ เช่น เป่าฝุ่น สแกนฮาร์ดดิสค์ disk cleanup และ disk defragmenter	- สัปดาห์ละ ๑ ครั้ง													
๕.๑ คอมพิวเตอร์ไม่สามารถใช้งานได้			←											→	