แผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ

หลักการและเหตุผล

โรงพยาบาลเกาะกูด ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานและให้บริการประชาชนได้รับความสะดวก ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศ อาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัยหรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ทำความเสียหายต่อระบบเทคโนโลยีสารสนเทศส่งผล กระทบต่อการดำเนินงานของโรงพยาบาล เพื่อป้องกันและแก้ไขปัญหาดังกล่าวกรรมการสารสนเทศโรงพยาบาลเกาะกูด ได้เล็งเห็นความจำเป็นที่จะต้องมีแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาล

การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลเกาะกูดพบว่าความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๑.เจ้าหน้าที่หรือบุคลากรของหน่วยงาน(Human error) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์ คอมพิวเตอร์ทั้งด้าน Hardware และ software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ ดังนั้นเพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจในการใช้ระบบเทคโนโลยีสารสนเทศ ในเบื้องต้น จึงได้ประชุมชี้แจงและจัดให้เจ้าหน้าที่เข้ารับการอบรม ให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

๒.ไวรัสคอมพิวเตอร์(ComputerVirus)สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ถึงขั้นใช้งานไม่ได้

๓.ระบบไฟฟ้าขัดข้องหรือความเสียหายจากไฟกระชาก โดยได้ติดตั้งอุปกรณ์สำรองไฟฟ้า(UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) กรณีเกิดกระแสไฟฟ้าขัดข้องไฟตกไฟกระชาก ระบบเครือข่ายคอมพิวเตอร์ จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย ส่วนการป้องกันความเสียหายอันเนื่องมาจากเพลิงมีระบบควบคุมป้องกันเพลิงไหม้อย่างเหมาะสม รวมทั้งมีเครื่องดับเพลิงติดตั้งตามจุดต่างๆในอาคารและทำป้ายบอกจุดติดตั้ง เพื่อดับเพลิง

๔.โจรกรรมการขโมยอุปกรณ์คอมพิวเตอร์ในส่วนของห้องคอมพิวเตอร์แม่ข่าย ได้กำหนดห้าม ผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณห้อง ยกเว้นหากจำเป็น จะต้องมีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป สำหรับประตูเข้าออกได้ล๊อคประตูทุกครั้งและติดตั้งกล้องวงจรปิดเพื่อตรวจสอบ และจำกัดทางเข้าออกในช่วงนอกเวลาราชกา

การสำรองข้อมูล

การสำรองข้อมูล(Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลาย โจรกรรม หรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ มีแนวทางโดยมีการตั้งค่าระบบให้มีการสำรองข้อมูลดังนี้

๑. จัดเก็บข้อมูลใน Server หลัก จัดทำเป็น RAID-๓ โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกัน จำนวน ๓ ลูก
๒. จัดเก็บข้อมูลใน Server รอง ตัวที่ ๑ จัดทำเป็น RAIDS-๔ โดยมี Hard disk สำหรับบันทึกข้อมูลที่เหมือนกันจำนวน ๔ ลูก
๓. จัดเก็บข้อมูลใน Server รอง ตัวที่ ๒ โดยใช้การทำ Auto Back up แบบ Full วันละ ๒ ครั้งเวลา ๑๒.๐๐ น.และ ๐๒.๐๐ น.
๔. จัดเก็บข้อมูลสำรองเก็บไว้ในเครื่อง Personal computer ที่เป็นเครื่องลูกข่าย โดยใช้การทำ replication ข้อมูลจากเครื่อง Server หลักแบบ real time
๕. การ Copy ข้อมูล Back up เก็บไว้ใน Hard disk External

การเตรียมการป้องกัน

๑. **การป้องกันไวรัสคอมพิวเตอร์** มีการติดตั้งซอฟแวร์ป้องกันไวรัสคอมพิวเตอร์สำหรับเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งระบบปฏิบัติการเป็น Linux และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่ายติดตั้ง Software ป้องกันไวรัส และป้องกันการใช้อุปกรณ์สื่อพกพาอื่นๆ เช่น Flash drive ,Harddisk Ext. การกำจัดการใช้งาน Internet เช่นการ download การป้องกันการถอดถอนหรือติดตั้งโปรแกรมเพิ่ม เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุก หรือทำลายระบบได้
๒. **การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง** เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ
    - ติด ตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวล ผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าได้ประมาณ ๑๕-๓๐ นาที
    - เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
    - เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้ทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงต่างๆ
    - มีระบบป้องกันไฟไหม้ มีอุปกรณ์ดับเพลิงติดตั้งในทุกอาคาร เพื่อการควบคุมเพลิงในเบื้องต้น

๓. **การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์** เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

- มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก
- มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยจะเปิดใช้ งานFirewall ตลอดเวลา
- มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรอง ข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์
- มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป
- การเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ความรับผิดชอบ
- การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัย คุกคามคอมพิวเตอร์

๔. **การจัดเตรียมอุปกรณ์ที่จำเป็น** ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ศูนย์คอมพิวเตอร์ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัด ข้องใช้งานไม่ได้ ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- ข้อมูลสำรองระบบงานที่สำคัญ
- แผ่นโปรแกรม antivirus/spyware
- แผ่น driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๕. **การรักษาความปลอดภัยด้วยรหัสผ่าน** เพื่อ ป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องสามารถเข้าถึง แก้ไข, เปลี่ยนแปลงข้อมูลหรือไม่สามารถใช้งานระบบสารสนเทศในส่วนที่มิได้มี อำนาจหน้าที่เกี่ยวข้อง โดยกำหนดสิทธิการเข้าถึงข้อมูลและระบบ สารสนเทศ ให้แก้ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้าในระบบได้ตามความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละ ระดับฐานข้อมูล ดังนี้

๑. บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้
๒. บุคคลที่สามารถเรียกดูข้อมูลและแก้ไขปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น
๓. บุคคล ที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูลระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล ผู้รับผิดชอบของหน่วยงานเจ้าของหน่วยงานเป็นผู้ดูแล แก้ไข ข้อมูลใน

ส่วนนี้ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ความรับผิดชอบของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Log in และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิ์เท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลง แก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบเป็นผู้ อนุมัติให้ดำเนินการได้โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขได้และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้เพื่อเป็นการรักษาความปลอดภัยของฐานข้อมูล

๔. กำหนด ระยะเวลาการใช้งานระบบสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้
๕. การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า๖ตัวอักษรและควรใช้ตัวเลข,อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ เดือน โดยการเปลี่ยนรหัสผ่านแต่ละครั้งไม่ควรให้ซ้ำกับรหัสเดิมในครั้งสุดท้าย ซึ่งผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันทีเพื่อ ป้องกันความปลอดภัยของการใช้ระบบสารสนเทศ

ระเบียบปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติต่างๆ ดังนี้

๑. เรื่อง การปฏิบัติกรณีไฟฟ้าดับ
๒. เรื่อง การปฏิบัติกรณีเครื่องคอมพิวเตอร์ลูกข่าย/อุปกรณ์เครือข่ายขัดข้อง
๓. เรื่อง การปฏิบัติกรณีเครื่อง Server /Database มีปัญหา
๔. เรื่อง การปฏิบัติกรณีเกิดอัคคีภัย

แผนทำระบบคอมพิวเตอร์กลับสู่สภาพปกติเดิม

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติ ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูล กลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๒๔ ชั่วโมง
๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
๕. นำ BACKUP / DVD/ HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบผู้ดูแลระบบ ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๒๔ ชั่วโมง
๖. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง