แผนการดูแลบำรุงรักษาระบบงานเทคโนโลยีสารสนเทศ
โรงพยาบาลสมเด็จพระยุพราชฉวาง

---

๑. หลักการและเหตุผล

โรงพยาบาลสมเด็จพระยุพราชฉวาง ได้ใช้เทคโนโลยีสารสนเทศในการดำเนินงาน และการให้บริการผู้ผู้มารับบริการ เพื่อให้ได้รับความสะดวก รวดเร็วขึ้น ระบบเทคโนโลยีสารสนเทศภายในโรงพยาบาลอาจจะได้รับความเสียหายจากปัจจัยทั้งภายในและภายนอกต่าง ๆ เช่น ไวรัสคอมพิวเตอร์ บุคคล ปัญหาไฟฟ้าขัดข้อง อัคคีภัย ซึ่งอาจจะทำให้ระบบเทคโนโลยีสารสนเทศเกิดความเสียหาย ส่งผลกระทบต่อระบบฐานข้อมูล ฮาร์ดแวร์ การปฏิบัติงาน และการให้บริการผู้มารับบริการทางด้านต่างๆของโรงพยาบาลสมเด็จพระยุพราชฉวางได้

เพื่อเป็นการป้องกันและแก้ไขปัญหาดังกล่าว ทางโรงพยาบาลจึงได้จัดทำแผนการดูแลบำรุงรักษาระบบเทคโนโลยีสารสนเทศเพื่อใช้เป็นแนวทางในการปฏิบัติงาน

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบฐานข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์ ระบบอินเทอร์เน็ต และอุปกรณ์ต่อพ่วง ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสี่ยงและความเสียหายที่จะอาจเกิดกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ

๓. เป้าหมาย

เพื่อให้ระบบเทคโนโลยีสารสนเทศ ของโรงพยาบาลสมเด็จพระยุพราชฉวาง ใช้งานอย่างเป็นระบบและมีประสิทธิภาพ และสามารถใช้ได้ในกรณีที่มีภาวะฉุกเฉิน เช่น ไฟดับ อินเตอร์เน็ตขัดข้อง ระบบเครือข่ายใช้งานไม่ได้โดยระบบเทคโนโลยีสารสนเทศ ต้องสามารถกลับมาดำเนินการได้ในระยะเวลา ดังนี้

๓.๑ ระบบสำรองไฟฟ้า สามารถสำรองไฟฟ้า ให้ระบบไม่น้อยกว่า ๑๕ นาที และเครื่อง Server สามารถใช้ไฟสำรองได้ ไม่น้อยกว่า ๔๕ นาที

๓.๒ ระบบ Network (เครือข่าย) เมื่อขัดข้องจะต้องกลับสู่สภาวะปกติภายในระยะเวลา ๒ ชั่วโมง

๓.๓ ระบบ Internet เมื่อขัดข้องจะต้องกลับสู่สภาวะปกติภายในระยะเวลา ๖ ชั่วโมง ทั้งนี้ขึ้นอยู่กับเครือข่ายผู้ให้บริการ ถ้าแก้ไขไม่ได้ในเวลา ต้องใช้ระบบ Internet สำรอง

๔. การประเมินสถานการณ์ความเสี่ยง

การตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศ พบว่าสาเหตุของความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ เกิดขึ้นได้จากปัจจัยเสี่ยง ดังนี้

๔.๑ เจ้าหน้าที่หรือบุคลากร ของหน่วยงาน (Human error) ซึ่งขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ทำให้ระบบเทคโนโลยีสารสนเทศ เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน ส่งผลให้ไม่สามารถ ใช้งานระบบเทคโนโลยี สารสนเทศได้อย่างเต็มประสิทธิภาพ

๔.๒ ภัยไซเบอร์คุกคาม มัลแวร์ ไวรัสคอมพิวเตอร์ (Computer virus) อาจสร้างความเสียหายให้แก่เครื่อง คอมพิวเตอร์หรือ ระบบเครือข่ายคอมพิวเตอร์ถึงขั้นใช้งานไม่ได้

๔.๓ ระบบไฟฟ้าขัดข้อง หรือความเสียหายจากความร้อนหรือเพลิงไหม้

๔.๔ การขโมยอุปกรณ์คอมพิวเตอร์ในห้องคอมพิวเตอร์แม่ข่าย

๔.๕ ปัจจัยภายนอก เช่น ระบบ Internet ไม่สามารถใช้งานได้หรืออาจเกิดจากการบุกรุกโจมตีจากภายนอก

๕. ข้อปฏิบัติในการป้องกัน แก้ไขปัญหาสถานการณ์ความเสี่ยงและภัยพิบัติ

๕.๑ จัดฝึกอบรม สัมมนา หรือแนะนำแนวทางใช้งาน เสริมสร้างความรู้ความเข้าใจการใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งด้าน Hardware และ Software เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุด

๕.๒ การสำรองข้อมูล (Backup) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์หรือมีผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูลให้สามารถนำข้อมูลดังกล่าวกลับมาใช้งานได้โดยมีแนวทางดำเนินการ ดังนี้

๕.๒.๑ การตั้งค่าระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ให้มีการสำรองข้อมูลโดยอัตโนมัติเป็นประจำทุกวัน

๕.๒.๒ การสำรองข้อมูลไว้ใน อุปกรณ์บันทึกหรือคอมพิวเตอร์เครื่องอื่นๆ

๕.๓ การป้องกันมัลแวร์ ไวรัสคอมพิวเตอร์มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยมีวิธีการดังนี้

๕.๓.๑ ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง (Update) ข้อมูลไวรัสอยู่เสมอ

- ติดตั้งโปรแกรมป้องกันไวรัส
- Update ข้อมูลไวรัส
- ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นหรือสื่อบันทึกข้อมูล ต่างๆ

๕.๓.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ เช่น Flash drive/Thumb drive เป็นต้น

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกๆ ที่ไม่รู้จักหรือน่าสงสัย เช่น .pif ,.inf เป็นต้น
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๕.๓.๓ ใช้ความระมัดระวังในการเปิด e-Mail

- อย่าเปิดไฟล์e-Mail ถ้าไม่ทราบแหล่งที่มา
- ลบ e-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๕.๓.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จาก Internet

- ไม่ควรเปิดไฟล์ที่ไม่รู้จักที่แนบมากับโปรแกรมสนทนาต่างๆ เช่น Facebook, Twitter และ Skype เป็นต้น หรือสอบถามคนที่ส่งไฟล์มาให้ก่อนกดรับ

- ไม่ควรเข้าไปเปิด Website ที่แนะนำมาทาง e-Mail ที่ไม่ทราบแหล่งที่มา
- ไม่ดาวน์โหลด ไฟล์จาก Website ที่ไม่น่าเชื่อถือ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๕.๔ เครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครือข่าย Internet ขัดข้อง ดำเนินการดังนี้

๕.๔.๑ ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่าย และเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๕.๔.๒ ตรวจสอบแผนผังเครือข่ายอุปกรณ์เพื่อหาสาเหตุการขัดข้อง และดำเนินการแก้ไข หากเครือข่ายอินเทอร์เน็ต แจ้งผู้ให้บริการ

๕.๔.๓ กรณีไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพ ของ เครื่องสำรองไฟฟ้า

๕.๔.๔ กรณีเกิดเหตุไฟไหม้เครื่องคอมพิวเตอร์และเครือข่าย ให้ตัดระบบ จ่ายไฟและใช้ถังดับเพลิงฉีดควบคุมเพลิงโดยเร็วรีบขนย้ายเครื่องคอมพิวเตอร์และเครือข่ายไปไว้ในที่ปลอดภัย

๕.๔.๕ กรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง และซ่อมให้สามารถใช้งานได้ให้เร็วที่สุดถ้าเกินขีดความสามารถในการ ดูแล ติดต่อร้านซ่อมหรือผู้เชี่ยวชาญมาดูแลให้เป็นปกติ

๕.๕ ซอฟแวร์ หรือโปรแกรม เสียหาย ให้ดำเนินการติดตั้งซอฟแวร์ หรือโปรแกรมใหม่เพื่อกลับมาใช้งานได้ตามปกติภายใน ๑-๒ วัน

๕.๖ กู้ระบบคอมพิวเตอร์กลับสู่สภาพปกติตามเดิม

การกู้ระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณ (System recovery) โดยปกติระบบเครื่องแม่ข่ายคอมพิวเตอร์และอุปกรณ์กระจายสัญญาณจะต้องอยู่ในสภาพพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องดำเนินการกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้โดยแผนการกู้ระบบคอมพิวเตอร์นี้เป็นวิธีการที่จะทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และฐานข้อมูลสารสนเทศ กลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยให้ดำเนินการดังนี้

๕.๖.๑ จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๕.๖.๒ เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๕.๖.๓ กรณีเครื่อง Server เสียหาย ใช้คอมพิวเตอร์เครื่องอื่นทดแทนชั่วคราว

๕.๖.๔ นำ Backup ที่ได้สำรองข้อมูลไว้กลับมา

๕.๖.๕ ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูลสารสนเทศ และความถูกต้อง ของข้อมูล รวมทั้งระบบเครือข่ายคอมพิวเตอร์อื่น ๆ ที่เกี่ยวข้อง

๕.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง ที่ซึ่งอาจสร้าง ความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ

๕.๗.๑ ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับ อุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ทั้งในส่วนของเครื่อง

คอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าได้นาน ประมาณ ๑๕ - ๒๐ นาที

๕.๗.๒ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๕.๗.๓ เมื่อเกิดกระแสไฟฟ้าดับ หากมีเครื่องสำรองไฟฟ้าใช้งานอยู่ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ด้วย

๕.๘ ติดตั้งระบบป้องกันไฟไหม้โดยติดตั้งอุปกรณ์ดับเพลิงทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น

๕.๙ การนำมาตรการความปลอดภัยด้วยรหัสผ่าน เพื่อการเข้าใช้งานเครื่อง Server รหัสผ่านการเข้าโปรแกรม และรหัสผ่านการใช้งานระบบเครือข่ายไร้สาย (Wireless LAN) ภายในบริเวณอาคาร