นโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยในระบบสารสนเทศ

ตามประกาศโรงพยาบาลลานกระบือ เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โรงพยาบาลลานกระบือ กำหนดให้มีการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของโรงพยาบาลลานกระบือ เพื่อให้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลลานกระบือ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และจากการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายต่อโรงพยาบาลลานกระบือ นั้น โรงพยาบาลลานกระบือ จึงกำหนดแนวปฏิบัติในการใช้ระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

หมวดที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

- การควบคุมการเข้าถึงสารสนเทศ
- การบริหารจัดการการเข้าถึงของผู้ใช้
- การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน
- การบริหารจัดการสินทรัพย์
- การควบคุมการเข้าถึงเครือข่าย
- การควบคุมการเข้าถึงระบบปฏิบัติการ
- การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
- การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี
- การปฏิบัติงานจากภายนอกสำนักงาน
- การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
- การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย
- การควบคุมการใช้จดหมายอิเล็กทรอนิกส์
- การควบคุมการใช้อินเตอร์เน็ต
- การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
- การใช้งานเครื่องคอมพิวเตอร์แบบพกพา
- การตรวจจับการบุกรุก
- การติดตั้งและกำหนดค่าของระบบ
- การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

หมวดที่ ๒ การรักษาความปลอดภัยฐานข้อมูลและสำรองข้อมูล

- การรักษาความปลอดภัยฐานข้อมูล
- การสำรองข้อมูล

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

- การตรวจสอบและประเมินความเสี่ยง
- ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพสถานที่และสภาพแวดล้อม

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความปลอดภัยของระบบสารสนเทศ

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

มาตรการบริหารความเสี่ยงของระบบสารสนเทศ
งานศูนย์คอมพิวเตอร์โรงพยาบาลลานกระบือ

ความเสี่ยง (Risk) เป็นสิ่งที่เกิดจากการรวมตัวกันของข้อจำกัด (Constraint) และความไม่แน่นอน (Uncertainly) การบริหารความเสี่ยง (Risk Management) เป็นการปฏิบัติการควบคุมความเสี่ยง ซึ่งจะประกอบด้วยการวางแผนความเสี่ยง การประเมินความเสี่ยงด้านต่าง ๆ การพัฒนาทางเลือกในการบริหารความเสี่ยง การตรวจสอบความเสี่ยงว่าเป็นไปได้มากน้อยเพียงใด งานศูนย์คอมพิวเตอร์ จึงมีมาตรการในการบริหารความเสี่ยง เพื่อลดโอกาสที่จะเกิดความเสี่ยง ดังนี้

๑. การสร้างความปลอดภัยทางกายภาพ เพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้ามาในบริเวณซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์

๑.๑ มาตรการ

๑.๑.๑) ห้ามบุคคลผู้ที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่ายหรือห้องที่มีความสำคัญต่าง ๆหากจำเป็นให้เจ้าหน้าที่ของศูนย์คอมฯ ที่เป็นผู้รับผิดชอบในการนำพาเข้าไป และเฝ้าดูตลอดเวลาที่บุคคลนั้นอยู่ในห้องดังกล่าว และนำกลับออกมาเมื่อเสร็จสิ้นภารกิจ

๑.๑.๒) การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ของเจ้าหน้าที่ฯ จะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือรหัสผ่าน (Password)

๑.๒ การดำเนินการ

มีการควบคุมการเข้าออกห้องห้องคอมพิวเตอร์แม่ข่าย (Server) ห้องที่มีความสำคัญต่าง ๆ รวมทั้งการควบคุมและจำกัดการใช้งานเครื่องคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆให้เป็นไปตามระเบียบของทางราชการฯ

๑.๓ สิ่งที่จะต้องดำเนินการในอนาคต

ปรับปรุงห้องเครื่องคอมพิวเตอร์แม่ข่าย (Server) และห้องที่มีความสำคัญต่าง ๆ ให้มีความมั่นคงมากยิ่งขึ้น

๒. การป้องกันและแก้ไขปัญหากระแสไฟฟ้าขัดข้อง เพื่อป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและระบบคอมพิวเตอร์

๒.๑ มาตรการ

๒.๑.๑) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาที่เปิดใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ส่วนบุคคล

๒.๑.๒) เมื่อเกิดกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูล (Save) คอมพิวเตอร์ที่ยังค้างอยู่และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย (Safety) รวมทั้งการปิดอุปกรณ์เครื่องใช้ไฟฟ้าอื่นภายในศูนย์คอมพิวเตอร์ด้วย

๒.๒ การดำเนินการ

การติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (Uninterruptible Power Supply: UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์ คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐ นาที และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๕-๑๐ นาที

๒.๓ สิ่งที่จะต้องดำเนินการในอนาคต

บำรุงรักษาเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ ให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓. การสร้างความปลอดภัยให้กับระบบปฏิบัติการ เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server) และคอมพิวเตอร์ส่วนบุคคล

๓.๑ มาตรการ

๓.๑.๑) ผู้ใช้งานจะต้องตั้งค่าให้ระบบปฏิบัติการ ทำการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอ (Patch Update)

๓.๑.๒) ผู้ใช้งานจะต้องเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล (Recovery) ของระบบปฏิบัติการตลอดเวลา

๓.๒ การดำเนินการ

มีการควบคุมการติดตั้งระบบปฏิบัติการ และมีการปรับปรุงระบบปฏิบัติการให้ทันสมัยอยู่เสมอและใช้ความสามารถของระบบปฏิบัติการในการสร้างความปลอดภัยให้กับระบบคอมพิวเตอร์ ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟร์วอลล์ (Firewall) การกู้คืนข้อมูล เป็นต้น

๓.๓ สิ่งที่จะต้องดำเนินการในอนาคต

ให้ความรู้และความเข้าใจแก่บุคลากรของสำนักงานฯ ในการใช้งานระบบปฏิบัติการของคอมพิวเตอร์อย่างมีประสิทธิภาพ

๔. การสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อเป็นการสร้างพื้นฐานความปลอดภัยและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์แก่เครื่องคอมพิวเตอร์แม่ข่าย (Server)

๔.๑ มาตรการ

๔.๑.๑) ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่าย จะต้องเฝ้าระวังภัยคุกคามทางคอมพิวเตอร์ที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายอย่างต่อเนื่อง

๔.๑.๒) เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการใส่บัญชีผู้ใช้ (Username) และ/หรือรหัสผ่าน (password) ในการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของศูนย์คอมพิวเตอร์เสมอ

๔.๑.๓) เจ้าหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย จะต้องทำการตั้งค่าและเปิดใช้งานบริการ (Service) ต่าง ๆของระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย ที่เกี่ยวข้องกับการรักษาความปลอดภัยของระบบตลอดเวลา

๔.๒ การดำเนินการ

มีการติดตั้งระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งเป็นระบบปฏิบัติการที่มีความสามารถในการบริหารจัดการความปลอดภัยสูง และใช้ความสามารถของระบบปฏิบัติการ ในการสร้างความปลอดภัยให้กับเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ การควบคุมและจำกัดสิทธิของผู้ใช้ได้ตามอำนาจหน้าที่และความรับผิดชอบ การเปิดใช้งานไฟล์วอลล์ การกู้คืนข้อมูล การสำรองข้อมูลเป็นต้น รวมทั้ง การใช้โปรโตคอล Secure Shell (SSH) ในการติดต่อกับ Server เพื่อเพิ่มความปลอดภัยให้สูงกว่าการ FTP หรือ Telnet

๔.๓ สิ่งที่จะต้องดำเนินการในอนาคต

การดำเนินการตามมาตรการดังกล่าวอย่างต่อเนื่อง

๕. การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕.๑ มาตรการ

๕.๑.๑) เจ้าหน้าที่ผู้รับผิดชอบจะต้องเปิดใช้งานไฟล์วอลล์และระบบป้องกันไวรัสคอมพิวเตอร์ตลอดเวลา

๕.๑.๒) ผู้ดูแลระบบ Gateway Server จะต้องมีการกำหนดค่า (Configuration) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของศูนย์คอมพิวเตอร์

๕.๑.๓) เจ้าหน้าที่ดูแลระบบเครือข่าย จะต้องทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตอย่างสม่ำเสมอ

๕.๑.๔) เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่า (Setup) ให้ซอฟท์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติ หรือการลงซอฟท์แวร์ที่มีเวอร์ชั่นใหม่กว่าตามความเหมาะสม

๕.๑.๕) ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นการแสดงตนก่อนอนุญาตให้เข้าสู่ระบบต่าง ๆ ของศูนย์คอมพิวเตอร์ตามอำนาจหน้าที่และความรับผิดชอบ

๕.๑.๖) ห้ามไม่ให้ผู้ที่มีอำนาจหน้าที่เข้ามาใช้งานซอฟท์แวร์ระบบหรือซอฟท์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟท์แวร์อื่น หรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง

๕.๒ การดำเนินการ

๕.๒.๑) การติดตั้งไฟล์วอลล์ (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และคอมพิวเตอร์ส่วนบุคคล (PC) ได้

๕.๒.๒) การติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายสำหรับโปรแกรมป้องกันไวรัสคอมพิวเตอร์ทั้งศูนย์คอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่าย (PC) และคอมพิวเตอร์ส่วนบุคคล (PC) โดยใช้โปรแกรม Trend Micro Office Scan ซึ่งกำหนดให้มีการ Update โปรแกรมอัตโนมัติและทำการ Scan ไวรัส ทุกวันศุกร์ของสัปดาห์

๕.๒.๓) การติดตั้ง Proxy Sever เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของศูนย์คอมพิวเตอร์ และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศ

๕.๒.๔) มีระบบการตรวจสอบปริมาณข้อมูลการใช้งานเครือข่ายอินเตอร์เน็ตของศูนย์คอมพิวเตอร์ผ่านซอฟท์แวร์ของศูนย์คอมพิวเตอร์

๕.๒.๕) มีการเฝ้าดูการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และใช้ความสามารถของซอฟท์แวร์ในการนำข้อมูลเข้าสู่เครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อบันทึกกิจกรรม วัน เวลาที่มีการนำเข้าข้อมูล หรือ การปรับปรุงแก้ไขข้อมูล

๕.๒.๖) มีการอุดช่องโหว่ของซอฟท์แวร์คอมพิวเตอร์ทั้งซอฟท์แวร์ระบบปฏิบัติการและซอฟท์แวร์ประยุกต์ โดยการตั้งค่า (Setup) ให้ซอฟท์แวร์สามารถ Update โปรแกรมสำหรับการอุดช่องโหว่โดยอัตโนมัติ หรือการลงซอฟท์แวร์ที่มีเวอร์ชั่นใหม่กว่าตามความเหมาะสม

๕.๒.๗) มีระบบสารสนเทศซึ่งบังคับให้ผู้ใช้จะต้องบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อเป็นกากรแสดงตนก่อนอนุญาตให้เข้าสู่ระบบ

๕.๒.๘) มีการควบคุมและป้องกันไม่ให้ผู้ที่ไม่มีอำนาจหน้าที่เข้ามาใช้งานซอฟท์แวร์ระบบหรือซอฟท์แวร์บางประเภทที่มีผลต่อการควบคุมการทำงานของซอฟท์แวร์อื่น หรือเป็นตัวกลางในการแก้ไขเปลี่ยนแปลงข้อมูลโดยตรง

๕.๓ สิ่งที่จะต้องดำเนินการในอนาคต

๕.๓.๑) พัฒนาและปรับปรุงระบบให้มีความพร้อมใช้งานอยู่ตลอดเวลา อย่างต่อเนื่อง

๕.๓.๒) การให้ความรู้อย่างต่อเนื่องแก่บุคลากรในโรงพยาบาล ในการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

๖. การพัฒนานโยบายการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ เพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของงานศูนย์คอมพิวเตอร์โรงพยาบาลลานกระบือเป็นไปอย่างมีประสิทธิภาพและลดความเสี่ยงจากภัยคุกคามทางคอมพิวเตอร์

๖.๑ มาตรการ

๖.๑.๑) มีหลักเกณฑ์หรือแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๖.๑.๒) มีการมอบหมายเจ้าหน้าที่ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๖.๒ การดำเนินการ

๖.๒.๑) ออกระเบียบหรือแนวปฏิบัติในการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๖.๒.๒) ออกบันทึกมอบหมายเจ้าหน้าที่ดูแลระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๖.๓ สิ่งที่จะต้องดำเนินการในอนาคต

กำกับการดำเนินการให้เป็นไปตามระเบียบฯว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ อย่างต่อเนื่อง

๗. การสร้างความตระหนักให้กับผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ เพื่อให้การใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของโรงพยาบาลลานกระบือ เป็นไปอย่างมีประสิทธิภาพและสัมฤทธิผลตามนโยบายการใช้งานดังกล่าว

๗.๑ มาตรการ

ประชาสัมพันธ์ให้บุคลากรโรงพยาบาลลานกระบือ ตระหนักและเห็นความจำเป็นของการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๗.๒ การดำเนินการ

๗.๒.๑) ประชาสัมพันธ์ให้มีการดำเนินการตามระเบียบหรือแนวปฏิบัติว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๗.๒.๒) การประชาสัมพันธ์ให้ผู้ใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ ได้รับทราบและปฏิบัติตามมาตรการบริหารความเสี่ยง

๗.๓.๓) การเผยแพร่ความรู้และคู่มือการใช้ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัยแก่ผู้ใช้งานโดยผ่านทางหนังสือเวียน อินทราเน็ต และเว็บไซต์

๗.๓ สิ่งที่จะต้องดำเนินการในอนาคต

๗.๓.๑) การประชาสัมพันธ์ให้มีการดำเนินการตามระเบียบหรือแนวปฏิบัติว่าด้วยการรักษาความปลอดภัยระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ อย่างต่อเนื่อง

๗.๓.๒) การให้ความรู้แก่บุคลากรโรงพยาบาลลานกระบือ อย่างต่อเนื่องในด้านการใช้งานระบบสารสนเทศและเครือข่ายคอมพิวเตอร์อย่างปลอดภัย

๘. การฟื้นฟูระบบ / ข้อมูลจากความเสียหาย (Recovery) เพื่อให้การฟื้นฟูระบบ/ ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลผลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งอาจส่งผลให้เครื่องคอมพิวเตอร์หรือการประมวลผลของคอมพิวเตอร์หยุด

๘.๑ มาตรการ

๘.๑.๑) ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืนข้อมูล (Recovery) ของระบบ ปฏิบัติการตลอดเวลา

๘.๑.๒) เจ้าหน้าที่ผู้รับผิดชอบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟท์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหายไป

๘.๑.๓) เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

๘.๒ การดำเนินการ

๘.๒.๑) มีการตั้งค่าให้ระบบ ปฏิบัติการของเครื่องคอมพิวเตอร์ทำการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย โดยอัตโนมัติหรือการดำเนินการโดยผู้ใช้งานในการฟื้นฟูระบบ/ข้อมูลจากความเสียหาย

๘.๒.๒) มีการจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์และการติดตั้งซอฟท์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

๘.๒.๓) มีการบำรุงรักษาระบบเครื่องคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

๘.๓ สิ่งที่จะต้องดำเนินการในอนาคต

การดำเนินการตามมาตรการดังกล่าวอย่างต่อเนื่อง

๙.การสำรองข้อมูล (Back up) เพื่อลดความเสี่ยงจากที่อาจเกิดขึ้นกับข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ ในกรณีที่ฮาร์ดิสก์เสียหาย ไวรัสคอมพิวเตอร์ทำลายข้อมูล ผู้บุกรุกทำการลบข้อมูลหรือเปลี่ยนแปลงข้อมูล การเผลอลบข้อมูลหรือเปลี่ยนแปลงข้อมูล โดยผู้ใช้งานเอง

๙.๑ มาตรการ

๙.๑.๑) เจ้าหน้าที่ผู้รับผิดชอบจะต้องตั้งค่าระบบให้มีสำรองข้อมูลโดยอัตโนมัติหรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบ แต่ไม่ต่ำกว่า ๑ ครั้ง / เดือน และมีการสำรอง ข้อมูลกับ G(OOGLE DRIVE

๙.๑.๒) ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไป จะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสม แต่ไม่ต่ำกว่า ๑ ครั้งต่อเดือน

๙.๑.๓) เมื่อทางศูนย์คอมพิวเตอร์ ประกาศให้มีการสำรองข้อมูล เนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าว ภายในระยะเวลาที่กำหนด

๙.๑.๔) หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บไว้ในรูปของเอกสารกระดาษ (Hard Copy)

๙.๑.๖) เจ้าหน้าที่ผู้รับผิดชอบเครื่องคอมพิวเตอร์แม่ข่าย และผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องมีการทดสอบความถูกต้องของข้อมูลสำรอง และการรายงานผลตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูล หรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ

๙.๒ การดำเนินการ

๙.๒.๑) การติดตั้งระบบสำรองข้อมูลสำหรับเครื่องคอมพิวเตอร์แม่ข่าย

๙.๒.๒) การสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์ของผู้ใช้โดยการบันทึกไว้คนละ Drive หรือ Handydrive

๙.๒.๓) การสำรองข้อมูลไว้ใน แผ่น CD

๙.๒.๔) การสำรองข้อมูลโดยการพิมพ์ (Print) ออกมาเก็บไว้ในกระดาษสำหรับข้อมูลที่สำคัญ

๙.๒.๕) มีการทดสอบความถูกต้องของข้อมูลสำรองและการรายงานผลการตรวจสอบเป็นครั้งคราว ทั้งนี้ขึ้นอยู่กับความสำคัญของข้อมูลในแต่ละระบบฐานข้อมูล หรือของผู้ใช้งานเครื่องคอมพิวเตอร์นั้น ๆ

๙.๓ สิ่งที่จะต้องดำเนินการในอนาคต

๙.๓.๑) มีการกำหนดมาตรการและแนวทางในการสำรองข้อมูลที่เป็นระบบมากยิ่งขึ้น

๙.๓.๒) มีการทดสอบและเรียกใช้งานข้อมูล สำรองตามระยะเวลาที่เหมาะสม

๑๐.การป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีเกิดเหตุการณ์ที่ไม่ปลอดภัยหรือภัยพิบัติขึ้น

๑๐.๑ มาตรการ

๑๐.๑.๑) เมื่อเกิดภัยพิบัติ เช่น อัคคีภัย ให้ผู้ใช้งานรีบเก็บแผ่น CD ซึ่งบรรจุข้อมูลสำรองซึ่งมีความสำคัญไปด้วยแล้วดำเนินการตามหลักปฏิบัติ/ขั้นตอนในแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ

๑๐.๑.๒) เมื่อเกิดกรณีการเชื่อมโยงเครือข่ายล้มเหลว เจ้าหน้าที่ผู้รับผิดชอบจะต้องรีบรายงานให้ผู้บังคับบัญชาทราบ และดำเนินการประสานผู้ที่เกี่ยวข้องเพื่อดำเนินการแก้ไขโดยด่วนที่สุด และให้ใช้การเชื่อมโยงเครือข่ายสำรองแทนการเชื่อมโยงหลักในระหว่างที่ดำเนินการแก้ไข ทั้งนี้หากมีเหตุจำเป็นที่ต้องใช้เวลามากกว่า ๑ วัน ในการดำเนินการแก้ไข ให้ออกประกาศแจ้งแก่ผู้ใช้งานทราบ พร้อมกำหนดเวลาที่จะทำการแก้ไขเสร็จสิ้น

๑๐.๑.๓) เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบทำการแก้ไขแล้วเสร็จ

๑๐.๑.๔) เมื่อเกิดกรณีที่อุปกรณ์จัดเก็บข้อมูลเสียหายให้เจ้าหน้าที่ผู้รับผิดชอบ ทำการตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้น พร้อมรายงานให้ผู้บังคับบัญชาทราบ พบว่าหากมีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมา ได้ให้ดำเนินการโดยด่วน ทั้งนี้อาจประสานงานขอความช่วยเหลือจากผู้ที่ชำนาญในเรื่องดังกล่าว เพื่อดำเนินการด้วยก็ได้ หากไม่สามารถกู้คืนข้อมูลกลับมาได้ให้นำข้อมูลที่สำรองไว้มาใช้แทน

กรณีที่เป็นผู้ใช้งานคอมพิวเตอร์ทั่วไป เมื่อเกิดเหตุอุปกรณ์จัดเก็บข้อมูลเสียหาย ให้รายงานผู้บังคับบัญชาของตนทราบ แล้วแจ้งให้กลุ่มงานศูนย์คอมพิวเตอร์ เพื่อตรวจสอบเหตุแห่งความเสียหายนั้นในเบื้องต้น หากพบว่ามีแนวทางที่จะทำการกู้คืนข้อมูลในอุปกรณ์นั้นกลับมาได้ให้ดำเนินการโดยด่วน หากไม่สามารถกู้คืนข้อมูลกลับมาได้ ให้นำข้อมูลที่สำรองไว้มาใช้แทน

จากนั้นให้ทำการส่งซ่อมอุปกรณ์จัดเก็บข้อมูลที่เสียหายดังกล่าวตามระเบียบของทางราชการต่อไป

๑๐.๑.๕) เมื่อมีการระบาดของไวรัสคอมพิวเตอร์ในเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบจะต้องทำการวิเคราะห์ความรุนแรงของไวรัสคอมพิวเตอร์และตัดการเชื่อมต่อของเครือข่ายคอมพิวเตอร์ เพื่อดำเนินการแก้ไขปัญหาโดยรีบด่วนที่สุด พร้อมทั้งรายงานให้ผู้บังคับบัญชาทราบ

๑๐.๒ การดำเนินการ

๑๐.๒.๑) มีการจัดทำแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ

๑๐.๒.๒) มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนดังกล่าว

๑๐.๓ สิ่งที่จะต้องดำเนินการในอนาคต

มีการประชาสัมพันธ์และดำเนินการให้เป็นไปตามแผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan) ของศูนย์คอมพิวเตอร์

๑๑.การป้องกันความผิดพลาดระบบคิว เพื่อให้การบริหารและจัดการกับระบบสารสนเทศและเครือข่ายคอมพิวเตอร์เป็นไปอย่างมีประสิทธิภาพ ในกรณีเกิดเหตุการณ์ที่ระบบขัดข้อง

๑๑.๑ มาตรการ

๑๑.๑.๑) เมื่อเกิดเหตุการณ์ เช่น ระบบคอมพิวเตอร์ขัดข้องให้ผู้ปฏิบัติงาน ทำหน้าที่จัดคิวและเรียกคิวตามลำดับ

๑๑.๒ การดำเนินการ

๑๑.๒.๑) มีการจัดทำแผนการแก้ปัญหาระบบคิว เช่นการอธิบายขั้นตอนการรับบริการ

๑๑.๒.๒) มีการประชาสัมพันธ์และการดำเนินการให้เป็นไปตามแผนดังกล่าว

๑๐.๓ สิ่งที่จะต้องดำเนินการในอนาคต

มีการประชาสัมพันธ์และดำเนินการให้เป็นไปตามแผน และพัฒนาระบบคิวให้สามาร๔มีเสียงเรียกได้