

แผนการจัดการหรือแก้ไขปัญหาจากภัยพิบัติ (Contingency Plan)

กรมส่งเสริมวัฒนธรรม ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อสนับสนุนงานวัฒนธรรม เพื่อเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการประชาชน ซึ่งระบบข้อมูลสารสนเทศ มีความสำคัญต่อการปฏิบัติงาน และการตัดสินใจของผู้บริหาร จึงมีความจำเป็นต้องได้รับการดูแลเพื่อให้เกิดความมั่นคงปลอดภัย ซึ่งอาจมีปัจจัยทั้งภายในและภายนอกมากระทบทำให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ ส่งผลกระทบต่อการดำเนินงานขององค์กร อาทิ ความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ ถูกโจมตีระบบจาก Hacker บุคลากรทั้งจากภายในและภายนอกหน่วยงาน ระบบไฟฟ้า อัคคีภัย ดังนั้น เพื่อป้องกันและแก้ไขปัญหาดังกล่าว กลุ่มเทคโนโลยีสารสนเทศได้เล็งเห็นความจำเป็นที่จะต้องมีการจัดการหรือแก้ไขปัญหาจากภัยพิบัติเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ พร้อมทั้งแก้ไขปัญหาที่อาจส่งผลกระทบต่อระบบข้อมูลสารสนเทศของทั้งองค์กร

การประเมินสถานการณ์ความเสี่ยง

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ในระบบเทคโนโลยีสารสนเทศขององค์กร พบว่า ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ มีดังนี้

๑. เกิดจากบุคลากรของหน่วยงาน (Human error) ขาดความรู้ความเข้าใจในเครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย เกิดการชะงักงัน หรือหยุดการทำงาน ส่งผลให้ไม่สามารถใช้งานระบบได้อย่างเต็มประสิทธิภาพ ดังนั้น เพื่อเป็นการเสริมสร้างความรู้ ความเข้าใจ ในการใช้ระบบเทคโนโลยีสารสนเทศในเบื้องต้น จึงได้จัดทำคู่มือเพื่อเผยแพร่ความรู้ ความเข้าใจในการทำงานทั้งด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้านความผิดพลาดที่เกิดจากบุคลากรให้น้อยที่สุด

๒. เกิดจากการบุกรุก ถูกโจมตีและภัยคุกคามทางคอมพิวเตอร์อื่น ๆ ดังนั้น เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๒.๑) ติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้

๒.๒) มีการบันทึกชื่อผู้ใช้ (user name) และรหัสผ่าน (password) ในการเรียกใช้ระบบสารสนเทศจากหน่วยงานต่างๆ เพื่อตรวจสอบก่อนจะอนุญาตให้ใช้งานได้ตามสิทธิ์และอำนาจหน้าที่ ความรับผิดชอบ

๒.๓) ติดตั้งซอฟต์แวร์ป้องกันไวรัสสำหรับเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย เพื่อปิดกั้นช่องทางมิให้ผู้ประสงค์ร้ายเข้ามาบุกรุก โจรกรรม หรือทำลายระบบได้ โดยมีการอัปเดตข้อมูลไวรัส และตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์

๒.๔) การสำรองข้อมูล (Back up) ไว้ใน Harddisk และ DVD ทุก ๆ ๓ เดือน เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น หรือถูกทำลายจากไวรัสคอมพิวเตอร์ โดยสามารถนำข้อมูลที่สำรองไว้กลับมาใช้งานได้ (Recovery)

๓ ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง



๔. ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ได้แก่

๔.๑) ติดตั้งระบบควบคุม ดักจับควันไฟ เพื่อป้องกันการเกิดความเสียหายจากเพลิงไหม้



๔.๒) เนื่องจากห้อง Server อยู่บนอาคารสูงจึงไม่มีปัญหาเรื่องอุทกภัย แต่เนื่องจากห้อง Server อยู่ติดหลังคา จึงมีความเสี่ยงต่อการที่ฝนตกจะก่อให้เกิดการรั่วซึม ป้องกันโดยตรวจสอบการรั่วซึมของหลังคาเพื่อป้องกันปริมาณน้ำฝนที่ค้างสะสม

๕. ติดตั้งเครื่องอ่านบัตรแถบแม่เหล็กสำหรับประตูเข้าออกห้องคอมพิวเตอร์แม่ข่าย(Server) เพื่อป้องกันไม่ให้นักภายนอกหรือผู้ไม่มีหน้าที่เกี่ยวข้องเข้าไปในบริเวณโดยไม่ได้รับอนุญาต ยกเว้นจะต้องมีเจ้าหน้าที่ของงานเทคโนโลยีสารสนเทศเป็นผู้พาเข้าไป



การกำหนดผู้รับผิดชอบ

๑. ระดับนโยบาย ผู้รับผิดชอบ ได้แก่

๑.๑ รองเลขาธิการฯ ที่ทำหน้าที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ (CIO)

๑.๒ เลขาธิการกรมและผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๒. ระดับปฏิบัติ ประกอบไปด้วย ๒ กลุ่ม ได้แก่

๒.๑ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ มีหน้าที่รับผิดชอบ กำกับดูแล ประสานงาน ให้ความคิดเห็น เสนอแนะวิธีการปฏิบัติงาน ศึกษาทบทวน วางแผน ติดตาม แนวทางการแก้ไขปัญหา การบริหารความเสี่ยง และระบบรักษาความปลอดภัยฐานข้อมูลและเทคโนโลยีสารสนเทศ

๒.๒ กลุ่มเจ้าหน้าที่ปฏิบัติงาน ผู้รับผิดชอบ ได้แก่

๒.๒.๑ นางสาวอิมใจ แก้วชื่นชัย นักวิชาการคอมพิวเตอร์ชำนาญการ

๒.๒.๒ นางสาวผกามาส ปรินัญญาปราชนธ์ นักวิชาการคอมพิวเตอร์ชำนาญการ
มีหน้าที่รับผิดชอบ ดังนี้

๑. ควบคุม ดูแล บำรุงรักษา ระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และระบบความปลอดภัยทั้งหมด

๒. ตรวจสอบ แก้ไขข้อบกพร่องปัญหาและอุปสรรค จากความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์และระบบเครือข่าย

๓. รักษาความปลอดภัยของระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการต่าง ๆ รวมทั้งการทำสำเนาฐานข้อมูล และกู้คืนระบบ

๔. ควบคุมการเข้าออกห้อง Server



ลงชื่อ

ผู้เห็นชอบ

(นางสาวทัศน เทพกำปนาท)

รองอธิบดีกรมส่งเสริมวัฒนธรรม

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)