แผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน
(IT Contingency Plan) ของคณะวิทยาศาสตร์ มหาวิทยาลัยมหิดล
โดยงานสารสนเทศและห้องห้องสมุดสตางค์ มงคลสุข
ปีงบประมาณ พ.ศ.๒๕๕๙-๒๕๖๔

วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของคณะวิทยาศาสตร์
๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศของคณะวิทยาศาสตร์
๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และสามารถตอบสนองสถานการณ์ได้อย่างทันท่วงที

กรอบแนวทางในการจัดทำแผน

การจัดทำแผนรับสถานการณ์ฉุกเฉิน ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) คณะวิทยาศาสตร์มีแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. กำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. มาตรการในการป้องกันและแก้ไขปัญหา
๖. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
๗. การติดตามและรายงานผล

ภัยที่ก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของคณะวิทยาศาสตร์ สามารถจำแนกได้ ดังนี้

๑. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น
๒. การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
๓. ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายของคณะวิทยาศาสตร์
๔. ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ
๕. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
๖. ไวรัสคอมพิวเตอร์
๗. ระบบเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ
๘. ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
๙. เจ้าหน้าที่หรือบุคลากรของหน่วยงาน

แนวทางการป้องกันความเสียหายจากภัยพิบัติ

๑. **ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย** ได้แก่ อัคคีภัย อุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

- ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย
- เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง
- เปิดเครื่องปรับอากาศพร้อมอุปกรณ์ควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

๒. **การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล**

- ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำเข้าไป
- ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๓. **ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายของคณะวิทยาศาสตร์**

- การตรวจสอบระบบเครือข่ายให้สามารถใช้งานได้ตลอดเวลา
- จัดให้มีอุปกรณ์ของระบบเครือข่ายสำรอง สำหรับใช้ในกรณีที่อุปกรณ์หลักไม่สามารถใช้งานได้
- ประสานงานกับหน่วยงานที่เกี่ยวข้องเพื่อแก้ไขปัญหา

๔. **ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ**

- ติดตั้งเครื่องสำรองไฟฟ้า (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที
- เครื่องสำรองไฟฟ้า (UPS) มีระบบตรวจสอบการทำงานผ่านระบบซอฟท์แวร์ และมีการทดสอบเครื่องสำรองไฟฟ้าจากบริษัทผู้เชี่ยวชาญ ในทุก 6 เดือน

๕. **การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล**

- อัพเดท Security patch เพื่อปิดกั้นช่องโหว่และจุดอ่อนของระบบปฏิบัติการ
- เปิดใช้งาน Firewall ของเครื่องแม่ข่ายตลอดเวลา เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่าย
- ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน
- กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้
    - (๑) ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
    - (๒) ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น
    - (๓) จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
    - (๔) เปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

(๕) ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ

(๖) เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๖. ไวรัสคอมพิวเตอร์

- ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอและต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง
- ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(๑) สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง

(๒) ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย

(๓) ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๗. ระบบเสียหายจากภัยสงคราม/เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

- การสำรองข้อมูล มีการแบ่งระยะเวลาในการจัดเก็บเป็น 2 ระดับ
  - สำคัญ มีการจัดเก็บไม่น้อยกว่า 120 วัน
  - เฝ้าระวัง มีการจัดเก็บไม่น้อยกว่า 30 วัน
- คัดลอกข้อมูลที่เป็นปัจจุบันผ่านระบบเครือข่าย โดยจัดเก็บข้อมูลที่ DR-site สำหรับกรณีฉุกเฉิน Siteสำรองสามารถดำเนินงานได้ตามมาตรฐานของ Cold Site

๘. ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

- การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน
- ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

๙. เจ้าหน้าที่หรือบุคลากรของหน่วยงาน

- ให้ความรู้แก่เจ้าหน้าที่หรือบุคลากรของหน่วยงานผ่านช่องทางต่างๆ เช่น website, โปสเตอร์, แผ่นพับ, หนังสือเวียน เป็นต้น
- ดำเนินการตามแผนฝึกอบรมบุคลากรที่ได้รับมอบหมายให้มีความรู้เท่าทันกับเทคโนโลยี
- จัดกิจกรรมอบรม เสวนาทางวิชาการเพื่อให้ความรู้ ความเข้าใจแก่เจ้าหน้าที่ บุคลากรให้ตระหนักรู้ภัยที่เกิดจากเทคโนโลยีในปัจจุบัน

ขั้นตอนปฏิบัติ

กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๑. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ

๒. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓. ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

๕. ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลระบบ Server และระบบเครือข่ายโดยเร็วที่สุด

๖. ในกรณีอุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๗. ผู้ดูแลระบบ ต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว

แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การคืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

๑. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน

๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว

๕. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง

๖. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

๑. ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของหน่วย (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๒. ระดับปฏิบัติ

เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกไตรมาส และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้