แผนรองรับภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศ
คณะเวชศาสตร์เขตร้อน มหาวิทยาลัยมหิดล

แผนรองรับภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศ จัดทำขึ้นเพื่อให้สอดคล้องกับนโยบายความปลอดภัยสารสนเทศของมหาวิทยาลัยมหิดล และเพิ่มประสิทธิภาพในการดำเนินงาน และให้บริการของหน่วยงาน แนวปฏิบัตินี้ครอบคลุมถึงระบบเทคโนโลยีสารสนเทศที่อยู่ภายใต้การดูแลของงานเทคโนโลยีสารสนเทศ ได้แก่ระบบต่างๆ ดังต่อไปนี้

1) ระบบเครือข่ายสื่อสารคอมพิวเตอร์ของมหาวิทยาลัย ส่วนที่ติดตั้งภายในคณะเวชศาสตร์เขตร้อน
2) ระบบเครือข่ายสื่อสารคอมพิวเตอร์ภายในคณะเวชศาสตร์เขตร้อน
3) ห้องควบคุมระบบเครือข่ายที่อยู่ภายใต้การดูแลของงานเทคโนโลยีสารสนเทศ
4) ระบบสารสนเทศต่างๆ ที่อยู่ภายใต้การดูแลของกองเทคโนโลยีสารสนเทศ ได้แก่
    1. Internet website
    2. Intranet website
    3. ระบบ Tropmed e-service
    4. ระบบ Backup
    5. ระบบอื่นๆ ที่พัฒนาหรือจัดหามาโดยงานทคโนโลยีสารสนเทศ

แผนรองรับภัยพิบัติด้านระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

- แผนรองรับสถานการณ์ กรณีกระแสไฟฟ้าขัดข้อง
- แผนรองรับสถานการณ์ กรณีที่เกิดเหตุขัดข้องกับอุปกรณ์เครือข่าย
- แผนรองรับสถานการณ์ กรณีที่เกิดเหตุขัดข้องกับเครื่อง Server
- แผนรองรับสถานการณ์ กรณีการป้องกันไวรัส

แผนรองรับสถานการณ์ กรณีกระแสไฟฟ้าขัดข้อง มีแนวปฏิบัติดังนี้

ก่อนเกิดเหตุ

- สร้างความรู้ ความเข้าใจเกี่ยวกับจุดจ่ายกระแสไฟฟ้ากับอุปกรณ์
- ติดตั้งระบบสำรองไฟฟ้า สำหรับเครื่องคอมพิวเตอร์ตามความจำเป็นและความพร้อมด้านงบประมาณ
- สำรองข้อมูลสำคัญลงบนสื่อจัดเก็บที่มีความเหมาะสม
- จัดหาอุปกรณ์ดับเพลิงที่จำเป็น

ขณะเกิดเหตุ

- ผู้พบเหตุตรวจสอบ หากสามารถแก้ไขปัญหาเบื้องต้นให้ดำเนินการก่อน
- ผู้พบเหตุแจ้งหน่วยซ่อมบำรุง งานกายภาพและสิ่งแวดล้อมเพื่อส่งเจ้าหน้าที่ตรวจสอบ
- รายงานเหตุการณ์ให้ผู้บังคับบัญชาทราบและประเมินสถานการณ์ร่วมกับงานกายภาพและสิ่งแวดล้อม
- สื่อสารข้อมูลระหว่างผู้ปฏิบัติงาน ผู้บริหารและหน่วยงาน ผ่านช่องทางที่รวดเร็ว มีประสิทธิภาพ เช่น โทรศัพท์ หรือ line เป็นต้น
- ภายในห้องควบคุมระบบเครือข่ายติดตั้ง UPS ของ server แต่ละ Rack ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ 15 นาที
- หากกระแสไฟฟ้าสำรองไม่ทำงาน ดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้นหรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

หลังเกิดเหตุ

- ตรวจสอบสภาพและความเสียหายของระบบอุปกรณ์
- ซ่อมบำรุงระบบและอุปกรณ์ให้พร้อมใช้งาน
- กู้คืนระบบ เพื่อให้สามารถใช้งานได้
- ประเมินความเสียหายของระบบและอุปกรณ์ เพื่อรายงานต่อผู้บังคับบัญชา
- จัดทำแผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ

แผนรองรับสถานการณ์ กรณีที่เกิดเหตุขัดข้องกับอุปกรณ์เครือข่าย มีแนวปฏิบัติดังนี้

ก่อนเกิดเหตุ

- สร้างความรู้ ความเข้าใจเกี่ยวกับจุดติดตั้งอุปกรณ์เครือข่าย
- ติดตั้งระบบสำรองไฟฟ้า สำหรับอุปกรณ์เครือข่ายตามความจำเป็น

ขณะเกิดเหตุ

- ผู้พบเหตุตรวจสอบ รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา หากสามารถแก้ไขปัญหาเบื้องต้นให้ดำเนินการก่อน
- รายงานเหตุการณ์ให้ผู้บังคับบัญชาทราบและประเมินสถานการณ์เบื้องต้น
- กรณี ที่เป็นการขัดข้องที่เกี่ยวข้องกับระบบเครือข่ายสื่อสารคอมพิวเตอร์ของมหาวิทยาลัย ประสานงานกับผู้รับผิดชอบของกองเทคโนโลยีสารสนเทศ มหาวิทยาลัย
- กรณี ที่เป็นการขัดข้องที่เกี่ยวข้องกับระบบเครือข่ายสื่อสารคอมพิวเตอร์ภายในคณะฯ และมีสัญญาบำรุงรักษากับบริษัทภายนอก ดำเนินการประสานงานกับผู้เชี่ยวชาญของบริษัท
- ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดอุปกรณ์เครือข่ายก่อน และประสานงานกับหน่วยซ่อมบำรุงงานกายภาพและสิ่งแวดล้อม หากเป็นอุปกรณ์เครือข่ายหลักของอาคาร พิจารณาลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
- ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ

หลังเกิดเหตุ

- ตรวจสอบสภาพและความเสียหายของระบบอุปกรณ์
- ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
- ประเมินความเสียหายของระบบและอุปกรณ์ เพื่อรายงานต่อผู้บังคับบัญชา
- จัดทำแผนฟื้นฟูระบบเทคโนโลยีสารสนเทศ

แผนรองรับสถานการณ์ กรณีที่เกิดเหตุขัดข้องกับเครื่อง Server มีแนวปฏิบัติดังนี้

ก่อนเกิดเหตุ

- สร้างความรู้ ความเข้าใจเกี่ยวกับจุดจ่ายกระแสไฟฟ้ากับเครื่องแม่ข่าย
- ติดตั้งเครื่องสำรองไฟฟ้า สำหรับเครื่องแม่ข่ายตามความจำเป็นและความพร้อมด้านงบประมาณ
- ติดตั้งระบบไฟฟ้าสำรอง โดยการดูแลของหน่วยซ่อมบำรุง งานกายภาพและสิ่งแวดล้อม
- สำรองข้อมูลสำคัญลงบนสื่อจัดเก็บที่มีความเหมาะสม
- จัดหาอุปกรณ์ดับเพลิงที่จำเป็น

ขณะเกิดเหตุ

- ผู้ใช้บริการ หรือผู้พบเหตุ แจ้งเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ
- เจ้าหน้าที่งานเทคโนโลยีสารสนเทศตรวจสอบ หากสามารถแก้ไขปัญหาเบื้องต้นให้ดำเนินการก่อน
- รายงานเหตุการณ์ให้ผู้บังคับบัญชาทราบและประเมินสถานการณ์เบื้องต้น
- ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดระบบก่อน เพื่อป้องกันความเสียหาย
- ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้ น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

หลังเกิดเหตุ

- ผู้ดูแล server นั้นๆ ตรวจสอบสภาพและความเสียหายของระบบ
- ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
- ประเมินความเสียหายของระบบ เพื่อรายงานต่อผู้บังคับบัญชา

แผนรองรับสถานการณ์ กรณีการป้องกันไวรัส มีแนวปฏิบัติดังนี้

ก่อนเกิดเหตุ

- งานเทคโนโลยีสารสนเทศ ดำเนินกิจกรรม IT onsite service ให้แก่ภาควิชาหน่วยงาน/ ทุกปี เพื่อ update โปรแกรม antivirus และ OS
- งานเทคโนโลยีสารสนเทศให้คำแนะนำ แก่บุคลากรในการเปิด e-mail การ share file การสำรองข้อมูล
- ตรวจเช็คข้อมูลและการ update จาก ThaiCERT และเจ้าของผลิตภัณฑ์
- ประสานงานกองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล
- Download patch และวิธีการทำ

ขณะเกิดเหตุ

- ผู้ใช้บริการ หรือผู้พบเหตุ แจ้งเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ
- กรณีที่ไวรัสหรือมัลแวร์แพร่ทาง LAN นั้น หากเครื่องติดไวรัสหรือมัลแวร์ให้ถอดสาย LAN
- รายงานเหตุการณ์ให้ผู้บังคับบัญชาทราบและประเมินสถานการณ์เบื้องต้น
- งานเทคโนโลยีสารสนเทศ ประสานงาน/แจ้งเตือนเจ้าหน้าที่คอมพิวเตอร์สำหรับภาควิชา/ หน่วยงานที่มีเจ้าหน้าที่ เพื่อ update ระบบปฏิบัติการ และ update โปรแกรม antivirus ภายในภาควิชาหน่วยงาน/
- ทีมไอทีคณะฯ onsite service ดำเนินการตรวจเช็คและ update เครื่องคอมพิวเตอร์และให้คำแนะนำกับผู้ใช้งาน ให้แก่ภาควิชาหน่วยงานที่ไม่มีเจ้าหน้าที่คอมพิวเตอร์โดยเฉพาะ/
- กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล ออกประกาศเวียนบุคลากรทุกคน

หลังเกิดเหตุ

- เจ้าหน้าที่ฝ่ายบริการ ตรวจสอบและแก้ไขให้กับผู้ใช้บริการ
- ประเมินความเสียหายของระบบ เพื่อรายงานต่อผู้บังคับบัญชา