แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ
คณะเวชศาสตร์เขตร้อน มหาวิทยาลัยมหิดล

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ คณะเวชศาสตร์เขตร้อนจัดทำขึ้น เพื่อให้สอดคล้องกับนโยบายความปลอดภัยสารสนเทศของคณะฯ และมหาวิทยาลัย โดยประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ

1. วัตถุประสงค์

1. เพื่อใช้เป็นแนวทางการปฏิบัติงานอย่างต่อเนื่อง
2. เพื่อเตรียมความพร้อมล่วงหน้าในการรับมือกับเหตุการณ์ฉุกเฉินต่างๆ ที่อาจเกิดขึ้น
3. เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานต่างๆ ของคณะฯ

2. ขอบเขต

ใช้รับรองกรณีเกิดสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินที่เกิดขึ้น ทำให้ไม่สามารถใช้ระบบคอมพิวเตอร์ที่สำคัญภายในของหน่วยงานได้ตามปกติ ประกอบด้วยเหตุการณ์ต่อไปนี้

1. อัคคีภัย
2. อุทกภัย
3. ชุมนุมประท้วง/จลาจล
4. ไฟฟ้าดับ
5. Cyber Attack
6. ระบบเครือข่ายคอมพิวเตอร์ล่ม

ฯลฯ

3. ขอบเขต

1. ด้านกายภาพและสิ่งแวดล้อม
2. ด้านอุปกรณ์เทคโนโลยีสารสนเทศ
3. ด้านโปรแกรมระบบสารสนเทศและข้อมูล
4. ด้านบุคลากร

ด้านกายภาพและสิ่งแวดล้อม

ความเสี่ยงที่เกิดจากภัยคุกคามทั้งภัยจากธรรมชาติ และภัยที่มนุษย์ทำขึ้น เช่น อุทกภัย วาตภัย ฟ้าผ่า กระแสไฟฟ้าขัดข้อง การก่อการร้าย เป็นต้น มีแนวทาง ดังนี้

1. การติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย และ Core switch มีความปลอดภัยโดยติดตั้งในตู้ Rack
2. การควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่าย เป็นพื้นที่เขตหวงห้ามเฉพาะ
3. การป้องกันความเสียหาย และบรรเทาภัยพิบัติเบื้องต้น มีอุปกรณ์ถังดับเพลิงด้วยสารเคมี
4. การป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้องสำหรับเครื่องคอมพิวเตอร์แม่ข่าย (Server) และ Core switch โดยติดตั้งเครื่องสำรองไฟ (UPS)
5. การป้องกันความเสี่ยงจากระบบไฟฟ้าขัดข้องสำหรับระบบต่างๆ ภายในห้องควบคุมระบบเครือข่าย โดยการติดตั้งระบบไฟสำรองสำหรับห้องควบคุมระบบเครือข่าย

ด้านอุปกรณ์เทคโนโลยีสารสนเทศ

ความเสี่ยงที่เกิดจากความผิดพลาดของอุปกรณ์ ระบบเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง เช่น การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากไวรัสคอมพิวเตอร์ เป็นต้น มีแนวทาง ดังนี้

1. การจัดหาอุปกรณ์เทคโนโลยีสารสนเทศที่เหมาะสมกับลักษณะของงานและขององค์กร มีการจัดหาเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ให้ได้ตามมาตรฐานของอุปกรณ์คอมพิวเตอร์ จัดหาและติดตั้งอุปกรณ์เทคโนโลยีสารสนเทศให้เหมาะสมตามลักษณะงานและงบประมาณที่ได้รับการจัดสรร
2. การบำรุงรักษาอุปกรณ์เทคโนโลยีสารสนเทศ (IT Support)
   - สามารถแก้ไขปัญหาเบื้องต้นของเครื่องคอมพิวเตอร์ได้ อย่างถูกต้องและต่อเนื่อง
   - ควรปิดเครื่องคอมพิวเตอร์ทุกครั้งเมื่อใช้งานเสร็จเรียบร้อยแล้ว
   - มีการ Update Antivirus อย่างสม่ำเสมอ
   - การรักษาความปลอดภัยในการใช้ระบบสารสนเทศ โดยกำหนดรหัสผู้ใช้และรหัสผ่าน
3. จัดหาระบบสำรองข้อมูลในระบบสารสนเทศ (Backup System) ไปยังมหาวิทยาลัย

ด้านโปรแกรมระบบสารสนเทศและข้อมูล

ความเสี่ยงที่เกิดจากระบบการทำงานของโปรแกรมต่างๆ เช่น Hacker การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ โปรแกรมคอมพิวเตอร์ที่พัฒนาทำงานไม่ตรงตามที่กำหนด ข้อมูลถูกทำลาย ความเสี่ยงจากผู้บุกรุกข้อมูล การโจรกรรมข้อมูลที่สำคัญ การลักลอบเข้ามาแก้ไขเปลี่ยนแปลงข้อมูล เป็นต้น มีแนวทาง ดังนี้

1. พัฒนาโปรแกรมให้สามารถบริหารจัดการฐานข้อมูลให้มีมาตรฐาน และแบ่งสรรการใช้ทรัพยากรฐานข้อมูลจากโปรแกรมร่วมกันได้
2. พัฒนาโปรแกรมให้สามารถจัดเก็บ รวบรวม ประมวลผลข้อมูล ศึกษา วิเคราะห์ เพื่อการนำเสนอและสนับสนุนการบริหาร และพัฒนา ส่งเสริม บำรุงรักษาระบบ และการเผยแพร่ข้อมูลข่าวสารได้ในลักษณะของ Web Application เพื่อความสะดวกในการใช้งานและแสดงผล

3. การรักษาความปลอดภัยของข้อมูลในระบบคอมพิวเตอร์และระบบเครือข่าย
4. การจัดการสำรองข้อมูล และระบบงานคอมพิวเตอร์ (Backup) ของหน่วยงานภายในคณะฯ และการเตรียมพร้อมสำหรับสภาวะฉุกเฉิน
    - กำหนดสถานที่ในการเก็บรักษาข้อมูลสำรองโดยเฉพาะ
    - การสำรองข้อมูลภายในระบบสารสนเทศต่างๆ ของคณะฯ มีระบบ Backup System ไปยัง Backup site อย่างต่อเนื่องทุกวันตามตารางที่กำหนด
    - ภาควิชา กำหนดหน้าที่ให้เลขานุการของทุกภาควิชา ทำการสำรองข้อมูลของภาควิชาเก็บไว้ใน External Hard Disk แล้วเก็บรักษาในที่ปลอดภัย และ/หรือเก็บไว้ที่ Google drive
    - สำนักงานทั้ง 5 สำนักงาน ได้แก่ สำนักงานบริหารการศึกษา สำนักงานบริการการวิจัย สำนักงานนโยบายและยุทธศาสตร์ สำนักงานความร่วมมือระหว่างประเทศ และสำนักงานคณบดี ทำการสำรองข้อมูลของสำนักเก็บไว้ใน External Hard Disk แล้วเก็บรักษาในที่ปลอดภัย และ/หรือเก็บไว้ที่ Google drive รวมทั้ง TM-HERA
    - โรงพยาบาลเวชศาสตร์เขตร้อน มีแผนบริหารความพร้อมต่อสภาวะการณ์วิกฤตด้านเทคโนโลยีสารสนเทศ ภายใต้การควบคุมและดูแลของผู้อำนวยการโรงพยาบาลฯ และคณะกรรมการการจัดการสารสนเทศ เทคโนโลยีสารสนเทศและการจัดการความรู้ (ISMS)
    - ข้อมูลของแต่ละบุคคล งานเทคโนโลยีสารสนเทศทำหน้าที่ให้คำแนะนำปรึกษา การสำรองข้อมูล
5. การบำรุงรักษาอุปกรณ์เครือข่ายและระบบคอมพิวเตอร์

ด้านบุคลากร

ความเสี่ยงที่เกิดจากบุคลากรที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ การตรวจสอบการทำงาน การมอบหมายหน้าที่และสิทธิของบุคลากรที่เกี่ยวข้อง การดูแลรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ รวมทั้งบุคลากรภายนอกที่เกี่ยวข้องทั้งทางตรงและทางอ้อม มีแนวทาง ดังนี้

1. การมอบหมายบุคลากรที่เกี่ยวข้องและมีความเหมาะสม ในการเข้าถึงระบบสารสนเทศต่างๆ
2. การบริหารจัดการสิทธิในการเข้าถึงและการควบคุมการใช้งานสารสนเทศ
3. การรักษาความปลอดภัยข้อมุลระบบคอมพิวเตอร์และระบบเครือข่าย โดยกำหนดรหัสผ่านของแต่ละบุคคล และการยืนยันหรือพิสูจน์ตัวตน การจำกัดสิทธิการเข้าใช้งานสารสนเทศ
4. การว่าจ้างบุคคลภายนอก (Outsourcing) เพื่อการพัฒนาระบบข้อมูลสารสนเทศ ที่ต้องการผู้มีความชำนาญเป็นพิเศษ มีการกำกับดูแลอย่างต่อเนื่อง
5. การพัฒนาบุคลากรโดยการส่งบุคลากรไปอบรมด้านที่เกี่ยวข้อง

การสำรองข้อมูลภายในระบบสารสนเทศ

ระบบสารสนเทศ	Owner	ผู้ใช้	ผู้รับผิดชอบ	Site
ระบบ MU-ERP ทำงานแบบ Remote Site ได้	มหาวิทยาลัยมหิดล	งานคลัง งานพัสดุ งานทรัพยากรบุคคล สำนักยุทธฯ รองคลังฯ	กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล	ศาลายา
ระบบ MU-SIS ทำงานแบบ Remote Site ได้	มหาวิทยาลัยมหิดล	งานบริหารฯ	กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล	ศาลายา
ระบบ MU-Webmail	มหาวิทยาลัยมหิดล	บุคลากร	กองเทคโนโลยีสารสนเทศ มหาวิทยาลัยมหิดล	ศาลายา
ระบบ HIS	คณะ	โรงพยาบาล ภาควิชาพยาธิวิทยา งานคลัง รองคลังฯ	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบ LIS	คณะ	โรงพยาบาล	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบ PACs	คณะ	โรงพยาบาล	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบ e-Services	คณะ	บุคลากร	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบ e-Billing	คณะ	งานคลัง	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบพิพิธภัณฑ์หอย	ภาควิชาเวชศาสตร์สังคมฯ	ภาควิชาเวชศาสตร์สังคมฯ	งานเทคโนโลยีสารสนเทศ	คณะฯ ศาลายา
ระบบ TM-HERA	คณะ	สำนักยุทธศาสตร์	สำนักยุทธศาสตร์	สำนักยุทธศาสตร์