แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
มหาวิทยาลัยสงขลานครินทร์

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศซึ่งจัดเก็บไว้ที่ห้องศูนย์กลางข้อมูล (Data Center) ถือเป็นทรัพย์สินทางการบริหารสำคัญของมหาวิทยาลัยสงขลานครินทร์ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนด้านบริหาร การจัดการเรียนการสอน การวิจัย และการให้บริการวิชาการ ดังนั้น เพื่อป้องกันปัจจัยจากภายนอกและปัจจัยภายในมากระทบ และทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งอุปกรณ์ต่าง ๆ เกิดความเสียหายได้ มหาวิทยาลัยสงขลานครินทร์จึงได้จัดทำแผนป้องกันปัญหาระบบเทคโนโลยีสารสนเทศจากเหตุการณ์ฉุกเฉิน (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบป้องกันและแก้ไขปัญหาที่อาจกระทบต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยสงขลานครินทร์

๒. วัตถุประสงค์

๒.๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

๒.๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยสงขลานครินทร์ ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยสงขลานครินทร์

๓. เหตุภัยพิบัติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยสงขลานครินทร์ ซึ่งสามารถจำแนกประเภทของภัยได้ดังนี้

๓.๑. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องศูนย์กลางข้อมูล (Data Center) ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๓.๒. การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓.๓. ระบบสื่อสารของห้องศูนย์กลางข้อมูลที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๓.๔. กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๓.๕. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

๓.๖. ไวรัสคอมพิวเตอร์

๓.๗. ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๓.๘. ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

๔. แนวทางการป้องกันและแก้ไขความเสียหายจากภัยพิบัติ

๔.๑. ภัยธรรมชาติ

ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องศูนย์กลางข้อมูล ได้แก่ อัคคีภัย อุทกภัย และการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๔.๑.๑. การป้องกันอัคคีภัย

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน

(๒) จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากรทุกคนอย่างน้อยปีละ 1 ครั้ง

(๓) จัดทำระบบดับเพลิงอัตโนมัติสำหรับห้องศูนย์กลางข้อมูล

๔.๑.๒. การป้องกันอุทกภัย ความชื้น และอุณหภูมิที่ไม่เหมาะสม

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น และติดตั้งระบบอัตโนมัติตรวจสอบการทำงานตลอด ๒๔ ชั่วโมง

(๒) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๔.๒. การโจรกรรมอุปกรณ์ส่วนของการจัดเก็บและให้บริการข้อมูล

๔.๒.๑. ควบคุมการเข้าออกห้องศูนย์กลางข้อมูล โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป

๔.๒.๒. จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan)

๔.๒.๓. มีเวรเฝ้าระวังและตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๔.๒.๔. ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๓. ระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๔.๓.๑. ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา

๔.๓.๒. ต้องจัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้ในกรณีที่ระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

๔.๔. กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๔.๔.๑. มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๒๐ นาที

๔.๔.๒. เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาให้บริการ ตรวจสอบการทำงานของระบบทุกวัน และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอย่างน้อยเดือนละ ๑ ครั้ง

๔.๕. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๔.๕.๑. ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบตลอดเวลา

๔.๕.๒. จัดเวรเฝ้าระวังระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือมีความถี่ในการเรียกใช้งานผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกัน

๔.๕.๓. ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และปรับปรุงอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่ใช้งาน

๔.๕.๔. กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๔.๕.๕. ป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรส (IP address) โดยการกรองแพ็คเกทที่มาจากภายนอก

๔.๖. ไวรัสคอมพิวเตอร์

๔.๖.๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๔.๖.๒. ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

๔.๖.๓. ใช้ความระมัดระวังในการเปิดอีเมล เช่น ไม่เปิดอีเมลที่ไม่ทราบแหล่งที่มา หรือลบอีเมลทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔.๖.๔. ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

๔.๗. ระบบเสียหายจากภัยสงครามหรือเหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากภัยดังกล่าวเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ สามารถป้องกันได้โดยการจัดทำศูนย์กลางข้อมูลสำรองนอกอาคารศูนย์คอมพิวเตอร์ และมีระบบสำรองข้อมูลโดยแยกสถานที่จัดเก็บมากกว่า ๑ ที่ หากความเสียหายกับข้อมูลก็จะสามารถนำข้อมูลที่มีในศูนย์กลางข้อมูลสำรองหรือข้อมูลในระบบสำรองที่จัดเก็บไว้มาใช้แทนได้ทันที

๔.๘. ระบบบริการหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๔.๘.๑. สำรองข้อมูลอัตโนมัติโดยเครื่องคอมพิวเตอร์แม่ข่ายจะสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน โดยเครื่องจะบันทึกประวัติการทำงานไว้ทุกวัน และเครื่องดังกล่าวจะกระจายข้อมูลที่สำรองไว้ไปยังฮาร์ดดิสก์ภายนอก (External Harddisk) และเครื่องคอมพิวเตอร์แม่ข่ายที่ไซต์สำรองที่คณะทันตแพทยศาสตร์และวิทยาเขตตรัง

๔.๘.๒. ทดสอบกู้คืนข้อมูลและฐานข้อมูล ที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๑ ครั้ง

๔.๘.๓. บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสียหายของข้อมูล

๔.๙. การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๔.๙.๑. มีระบบยืนยันตัวตน เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๔.๙.๒. กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๔.๙.๓. หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องศูนย์กลางข้อมูล จะต้องให้เจ้าหน้าที่ผู้ดูแลศูนย์กลางข้อมูลเป็นผู้รับผิดชอบนำเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกต้องติดตั้งระบบสแกนลายนิ้วมือ และติดตั้งกล้องวงจรปิดเพื่อป้องกันการโจรกรรม

๔.๙.๔. ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งานตลอดเวลา

๔.๙.๕. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕. การกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ต้องอยู่ในสภาพพร้อมให้บริการได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเกิดความเสียหายหรือหยุดทำงาน ต้องดำเนินการ ดังนี้

๕.๑. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

๕.๒. จัดหาอุปกรณ์หรือชิ้นส่วน เพื่อทดแทน

๕.๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๕.๔. นำข้อมูลจากสื่อบันทึกข้อมูลสำรองหรือจากระบบสำรองข้อมูลกลับมาใช้งานโดยเร็วภายใน ๔๘ ชั่วโมง

๖. ผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน่วยงานต้องจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๖.๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๖.๑.๑. ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)

๖.๑.๒. ผู้อำนวยการศูนย์คอมพิวเตอร์

๖.๒. ระดับปฏิบัติ

๖.๒.๑. ทีมบริการเครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่

(๑) บริหารจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายให้อยู่ในสภาพพร้อมใช้งานและกู้คืนเมื่อเครื่องไม่ทำงาน

(๒) เฝ้าระวังการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

(๓) ดูแลการสำรองและกู้คืนข้อมูลและฐานข้อมูลจากความเสียหายให้กลับมาใช้งานตามปกติ

(๔) ทดสอบการกู้คืนข้อมูลในระบบสำรองข้อมูล เพื่อทดสอบว่าข้อมูลที่สำรองไว้สามารถนำกลับมาใช้งานได้เมื่อจำเป็น

(๕) บำรุงรักษาและทดสอบการกู้คืนระบบสำรองข้อมูล เพื่อให้ระบบมีความพร้อมใช้อยู่เสมอ

๖.๒.๒. ทีมบริการระบบเครือข่ายและสื่อสาร

(๑) อยู่เวรเฝ้าระวังการทำงานของระบบเครือข่ายและสื่อสารให้ทำงานได้ตลอดเวลาที่เปิดบริการ

(๒) บำรุงรักษาและกู้คืนระบบเครือข่ายและสื่อสารให้ทำงานได้ปกติ

(๓) ค้นหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์

(๔) จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบสื่อสาร ระบบปรับอากาศให้พร้อมใช้งาน

(๕) บำรุงรักษาศูนย์กลางข้อมูลเป็นประจำทุกเดือน เพื่อให้ศูนย์กลางข้อมูลอยู่ในสภาพพร้อมใช้อยู่เสมอ

๖.๒.๓. ทีมไฟฟ้า

(๑) ติดตั้งระบบดับเพลิงอัตโนมัติในห้องศูนย์กลางข้อมูล

(๒) ดูแลและบำรุงรักษาอุปกรณ์ในห้องศูนย์กลางข้อมูลแห่งที่สองที่อาคารศูนย์ทรัพยากรการเรียนรู้

(๓) ดูแลและบำรุงรักษาระบบไฟฟ้า ระบบปรับอากาศ การควบคุมความชื้นห้องศูนย์กลางข้อมูลที่อาคารศูนย์คอมพิวเตอร์และห้องศูนย์กลางข้อมูลที่อาคารศูนย์ทรัพยากรการเรียนรู้

(๔) ดูแลระบบแจ้งเตือนระบบไฟฟ้าขัดข้องนอกเวลาราชการ เพื่อให้เจ้าหน้าที่ผู้รับผิดชอบสามารถเข้าไปแก้ไขปัญหาได้อย่างรวดเร็ว

(๕) ตรวจสอบและเตรียมน้ำมันสำรองสำหรับเครื่องกำเนิดไฟฟ้า เพื่อให้เครื่องพร้อมใช้งานเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๖) รับผิดชอบการเปิดเครื่องกำเนิดไฟฟ้าเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๗) จัดเวรเฝ้าระวังระบบไฟฟ้า

๗. การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามที่ระบุอย่างน้อยปีละ ๑ ครั้ง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการศูนย์คอมพิวเตอร์ทราบเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) ทราบ และหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที