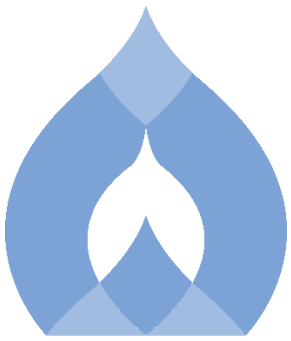

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

มหาวิทยาลัยกาฬสินธุ์

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ มหาวิทยาลัยได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบสารสนเทศรวมทั้งอุปกรณ์เสียหายได้

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ
๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ฯ
๗. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
๘. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
๙. การติดตามและรายงานผล

โดยอธิบายรายละเอียดดังต่อไปนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑. วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

๔) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

๕) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล ๑

๖) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

๑) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน

๑.๒. การประเมินสถานการณ์ และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้วจะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติเพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ (Security Log Management System) โดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เพื่อนำมาสรุปเป็นข้อมูลต่อไป

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน ๕ คะแนน)		คะแนนรวม	จัดเรียงลำดับ
	ต่อระบบงาน	ต่อพันธ์กิจตามกฎหมาย		
ไฟไหม้	๕	๕	๑๐	๑
โดนเจาะระบบ	๕	๕	๑๐	๑
ไฟฟ้าดับ	๕	๒	๗	๒
น้ำท่วม / น้ำรั่ว	๔	๒	๖	๓
แผนดินไหว	๔	๒	๖	๓
จลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	๒	๓	๕	๔
สถานการณ์ทางการเมือง	๒	๒	๔	๕

๒. แนวทางการป้องกันและเตรียมการเบื้องต้น

๒.๑. การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ~~ผู้อำนวยการ~~ ฝ่ายเทคโนโลยีสารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ของมหาวิทยาลัยทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

๒.๒. กระบวนการดำเนินงาน (Procedure)

มหาวิทยาลัยจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้นทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๒.๓. การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า, สถานีดับเพลิง, สถานีตำรวจ เป็นต้นมีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

๒.๔. การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

๑) แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
๒) เทปสำรองข้อมูลและระบบงานที่สำคัญ
๓) โปรแกรม antivirus/spyware
๔) แผ่น driver อุปกรณ์ต่างๆ
๕) ระบบสำรองไฟฉุกเฉิน
๖) อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๕. การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูลโดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๒.๖. การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยมหาวิทยาลัยมีนโยบายจัดหาซอฟต์แวร์ป้องกันไวรัสมาใช้ในองค์

๒.๗. การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณไม่น้อยกว่า ๓๐-๖๐ นาที
๒) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๒.๘. การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) หรือบันทึกลายนิ้วมือเพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้ บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของมหาวิทยาลัย เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๒.๙. การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็นกรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณี เกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

๑) เตรียมไฟฉายอุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

๓) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๔) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๕) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจนและเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๓. การเตรียมความพร้อม

๓.๑. การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์ และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณไม่น้อยกว่า ๓๐-๖๐ นาที

๓) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔) เมื่อเกิดกระแสไฟฟ้าดับให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๕) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๓.๒. การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณฉุกเฉินอันเกิดจากไฟไหม้

๒) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องตน

๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้ง เป็นอย่างน้อย

๓.๓. การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม /น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องตนเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณฉุกเฉินอันเกิดจากน้ำท่วม /น้ำรั่ว

๒) มีการตรวจสอบระบบท่อน้ำเครื่องปรับอากาศ ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้ง เป็นอย่างน้อย

๓.๔. การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัสคอมพิวเตอร์

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ขาย และป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวรป้องกันไวรัสที่เครื่องแม่ขาย (Server) และเครื่องลูกขาย (Client)

๓) อัพเดตโปรแกรมกำจัดไวรัสทุก ๑ เดือน เป็นอย่างน้อย (Update Patch)

๔) ให้เจ้าหน้าที่ศูนย์สารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่องสม่ำเสมอรวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๓.๕. การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) กำหนดมาตรการควบคุมการเขาออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๒) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวของ จำเป็นต้องเขาไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของศูนย์สารสนเทศผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออกและคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเขาออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มีเจ้าหน้าที่ดูแลระบบเครือข่ายตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของมหาวิทยาลัย เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๖) มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๓.๖. การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบเจ้าหน้าที่แผนกต่างๆ

ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัยเพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กรเพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติเพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศเป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๓.๗. การเตรียมความพร้อมรับสถานการณภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูลประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้นเตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๑) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

- กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)
- ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (www.ndwc.thaigov.go.th)
- กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม / แผ่นดินไหว (www.dmr.go.th)
- หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)
- กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการ และแนวทางปฏิบัติ (www.disaster.go.th)

๒. การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมง หรือเป็นวันก็ได้ เช่น

- สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู
- แมลงสาบจำนวนมากวิ่งเพ่นพ่าน
- หนู งู วิ่งออกมาจากที่อาศัยถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน
- ปลากระโดดขึ้นมาจากผิวน้ำ

การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

- ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
- ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่างๆ ตามความจำเป็นและเหมาะสม
- สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร
- สำรวจ จัดทำบัญชียานพาหนะ และเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิ ภาพเมื่อเกิดภัย
- จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

- สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม
- เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

การปฏิบัติขั้นเตรียมการ

- การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
- การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญและกำหนดมาตรการในการเผชิญภัย
- อบรม ให้ความรู้ การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่มแก่เจ้าหน้าที่ บุคลากรในองค์กร

- รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๘. การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจลเตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๑) ดำเนินการหาข่าวจากแหล่งต่างๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง
๒) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม
๓) ตรวจสอบระบบไฟฟ้าให้อยู่ในสภาพที่พร้อมใช้งาน
๔) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมทีมงานและมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบายให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแลควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ผู้บริหารระดับสูง (อธิการบดี,รองอธิการบดี)
ผู้บริหารระดับกลาง (คณบดี,ผู้อำนวยการ,รองผู้อำนวยการ,ผู้ช่วยอธิการบดี)
ผู้บริหารระดับต้น (รองคณบดี,รองผู้อำนวยการสำนัก/สภาบัน,ผู้อำนวยการกอง)

๔.๒. ระดับปฏิบัติ

ระดับปฏิบัติการ (หัวหน้าฝ่ายเทคโนโลยีสารสนเทศ,เจ้าหน้าที่) โดยมีหน้าที่ปฏิบัติงานดังนี้

๑) บริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ
๒) กู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ
๓) กู้คืนแอพพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน
๔) ประเมินความเสียหาย ตรวจสอบข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มา
๕) แก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่มหาวิทยาลัยได้จัดหาไว้

๖) แก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิดทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่

๗) แก้ไขปัญหาเนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

๘) สำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ ได้ทันทีและครบถ้วนสมบูรณ์

๙) แก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชาเพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลงให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศหรือผู้บริหารระดับสูงเพื่อทราบและสั่งการต่อไป

๑๐) แก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม

๑๑) แก้ไขปัญหา เนื่องจากแผ่นดินไหว ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ ควบคุมและผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ หรือผู้บริหารระดับสูงเพื่อทราบและสั่งการต่อไป

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

๕.๑. กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ ระบบสารสนเทศได้ ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณีเกิดจากฝ่ายเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ฝ่ายเทคโนโลยีสารสนเทศต้องประกาศให้ ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้นถ้าหากไม่สามารถแก้ไขปัญหาได้ แจ้งเหตุขัดข้องให้ ฝ่ายเทคโนโลยีสารสนเทศเพื่อแก้ไขปัญหาต่อไป

๕.๒. กรณีเครื่องแม่ข่ายบริการ (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็วแล้วปิดอุปกรณ์ เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) กรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๖) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

๗) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๘) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์ มาเปลี่ยนโดยเร็วที่สุด

๙) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศทราบโดยเร็ว

๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

กรณีจากไฟไหม้ห้องควบคุมระบบ

๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

๒) แจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานเพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓) เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่มหาวิทยาลัยได้จัดหาไว้ดำเนินการดับเพลิง และจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัย แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องดำเนินการในข้อ ๔ ต่อไป

๔) แจ้งสถานีดับเพลิงที่ใกล้ที่สุด

๕) ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

กรณีไฟดับ / หม้อไฟระเบิด

๑) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

๒) แจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานเพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓) ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

กรณีน้ำท่วมหรือน้ำรั่วซึมห้องควบคุมระบบ

๑) ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์สารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมหรือน้ำรั่วซึมลงทุกระบบ จากนั้นทำระบายน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำพร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ

๒) แจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานเพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓) ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

๑. ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์

๒. แจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้าควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

๑) ควบคุมสถานการณ์

ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๒) วิเคราะห์การถูกโจมตี

ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่นๆ

ข) วิเคราะห์ล็อกไฟล์ (Log file) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้

ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๓) กู้คืนระบบคอมพิวเตอร์

ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหายหรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

ข) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

๓. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่ายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

กรณีแผ่นดินไหว

๑. ผู้ที่อยู่เวรรักษาการณ์ เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้น

๒. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือนเจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย

๓. เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้

๔. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณี ดังนี้

ขั้นตอนการปฏิบัติ กรณี เกิดแผ่นดินไหว

๑) การปฏิบัติ ขณะเกิดแผ่นดินไหว

- ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน
- ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู /กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

- อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร
- ห้ามใช้เทียนไข ไม้ ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้
- อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น
- ห้ามใช้ลิฟต์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น
- ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า /สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด
- ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้ /อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า
- ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด
- หลังจากการสั่นสะเทือนสิ้นสุด ให้รีบออกจากอาคาร
- ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้อง โดยยึดหลัก “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ
- ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่
- ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

๒) เมื่อแผ่นดินไหวสงบลง

- ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนำส่งโรงพยาบาล
- รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ
- ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบการทำงานทั้งหมดทันที
- หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

๓) ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

- อยู่กับที่ป้องกันศีรษะและหน้าจากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่มหนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ
- พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัสดุหล่นใส่
- หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย
- ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น
- ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย

๔) การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

- ระงับสติอารมณ์ ปฏิบัติตามแผนอพยพ
- เชื่อฟังคำแนะนำของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.
- เก็บทรัพย์สิน/เอกสารสำคัญ ไว้ในลิ้นชักโต๊ะและล็อคกุญแจ
- เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด
- ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ
- ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า
- ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ ๒ คน
- ห้ามพูดคุย สายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง
- ห้ามใช้ลิฟต์ โดยเด็ดขาด
- เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที
- ไปรวมพล ณ จุดนัดพบที่กำหนดไว้
- ตรวจสอบจำนวนผู้อพยพ
- เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป
- ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

๑) ผู้ที่อยู่เวรรักษาการณ์ เมื่อได้รับสิ่งแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้น

๒) เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย

๓) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณี ดังนี้

ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจลาจล

- แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของผู้ปฏิบัติงานและของมหาวิทยาลัย
- เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า
- ปิดประตูทั้ง ๒ ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาใน กรมประมง

- กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของมหาวิทยาลัยให้แจ้งไปยังสถานีตำรวจนครบาล หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่างๆ และรายงานให้ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเพื่อทราบ

ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

- เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที
- รปภ. หรือเจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศ พร้อมทั้งติดต่อเจ้าหน้าที่ตำรวจในพื้นที่มาตรวจสอบวัตถุต้องสงสัย
- ในกรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกั้นพื้นที่อันตรายที่พบวัตถุระเบิดกันบุคคลที่ไม่เกี่ยวข้องออกจากบริเวณที่พบวัตถุระเบิด และแจ้งอพยพผู้ปฏิบัติงานออกจากบริเวณหรือรัศมีของวัตถุระเบิด
- เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป
- ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ

๗. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้ เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
๓) ซ่อมบำรุงวัสดุอุปกรณ์ ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง
๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
๕) นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน ๔๘ ชั่วโมง
๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้องจากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ

หน่วยงานจึงมีแผนจัดทำการสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศ ให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งไซต์ได้ ๓ ไซต์ คือ

๗) Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลัก มีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำสูง

๘) Warm Site เป็นไซต์ที่คล้ายกับ Hot site แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่างกว่า Hot site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า Hot site

๙) Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง Hardware และ Software ในการกู้คืน มีต้นทุนการจัดทำต่ำ แต่ระยะเวลาในการกู้คืนนาน

แผนการดำเนินการ

๑. สำรวจความต้องการของระบบสำรอง
๒. สำรวจไซต์สำรองที่เหมาะสม
๓. การประเมินความเสี่ยงจากสิ่งต่างๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง
๔. การจัดลำดับผลกระทบขององค์กร
๕. การจัดทำแผนกู้คืน
๖. การวางแผน การแต่งตั้งทีมงานลำดับการทำงานหลังระบบได้รับความเสียหาย
๗. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่รวมถึงการฝึกอบรมทางด้านเทคนิค
๘. การทดสอบแผน อาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง
๙. การปรับปรุงแผนการกู้คืน

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ ผู้อำนวยการฝ่ายเทคโนโลยีสารสนเทศทราบ เพื่อนำเสนอรายงานสรุปให้ CEO หรือ CIO เป็นประจำทุกเดือน และให้ รายงานการเกิดปัญหาและผลการแก้ไขให้ ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงที ในกรณีที่เกิดภัยพิบัติต่อไป