แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) มหาวิทยาลัยแม่โจ้ ปีงบประมาณ พ.ศ.๒๕๗๐-๒๕๗๔

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานตามภารกิจของมหาวิทยาลัยแม่โจ้ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ กองเทคโนโลยีดิจิทัลได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้ ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ ดังนี้

วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้
๒. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้
๓. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่กองเทคโนโลยีดิจิทัล มหาวิทยาลัยแม่โจ้ จัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ ประกอบด้วย

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ (Business Impact Analysis (BIA))
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. ผังงานกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
๖. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
๗. การติดตามและรายงานผล

โดยอธิบายรายละเอียดดังต่อไปนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ (Business Impact Analysis (BIA))

๑.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่าย ได้แก่ อัคคีภัย อุทกภัยการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม แมลงสัตว์กัดแทะ เป็นต้น

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อกับระบบเครือข่ายภายนอกองค์กรเกิดความขัดข้อง

๔) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

๕) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๖) ไวรัสคอมพิวเตอร์

๗) ระบบเสียหายจากภัยสงครามเหตุจลาจลและการเกิดสถานการณ์ความไม่สงบ

๘) การโจมตีด้วยโปรแกรมเรียกค่าไถ่ (Ransomware)

๙) การโจมตีแบบปฏิเสธการให้บริการ (Distributed Denial of Service : DDoS)

๑๐)การรั่วไหลของข้อมูลสารสนเทศหรือข้อมูลส่วนบุคคลจากการโจมตีทางไซเบอร์

ภัยพิบัติจากภายใน

๑) ระบบเครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๔) ความผิดพลาดจากการปฏิบัติงานของผู้ดูแลระบบ (Human Error)

๕) การลบหรือแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๖) การใช้งานรหัสผ่านที่ไม่ปลอดภัยหรือการเปิดเผยข้อมูลบัญชีผู้ใช้งาน

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ(Security Log Management System) โดยเจ้าหน้าที่งานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ กองเทคโนโลยีดิจิทัล เพื่อนำมาจัดทำกระบวนการและผังงานการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ รวมทั้งแผนกู้คืนระบบกลับสู่สภาพเดิมต่อไป

๑.๒.๑ หลักเกณฑ์การกำหนดระดับความรุนแรงของเหตุการณ์

มหาวิทยาลัยแม่โจกำหนดระดับความรุนแรงของเหตุการณ์ด้านเทคโนโลยีสารสนเทศ เพื่อใช้เป็นแนวทางในการตอบสนองและบริหารจัดการเหตุการณ์ ดังนี้

ระดับ	รายละเอียด
ระดับ ๑ (ต่ำ)	ผู้ใช้งานบางส่วนได้รับผลกระทบ แต่ยังสามารถปฏิบัติงานได้
ระดับ ๒ (ปานกลาง)	ระบบหรือบริการบางส่วนหยุดให้บริการ ส่งผลกระทบต่อหน่วยงานหนึ่งหรือหลายหน่วยงาน
ระดับ ๓ (สูง)	ระบบสารสนเทศสำคัญหยุดให้บริการ ส่งผลกระทบต่อภารกิจหลักของมหาวิทยาลัย
ระดับ ๔ (วิกฤต)	ศูนย์ข้อมูล ระบบเครือข่ายหลัก หรือข้อมูลสำคัญเสียหาย ไม่สามารถให้บริการได้ในวงกว้าง

ตัวอย่างการจัดระดับเหตุการณ์

เหตุการณ์	ระดับ
เครื่องคอมพิวเตอร์ผู้ใช้เสีย	ระดับ ๑
Switch อาคารขัดข้อง	ระดับ ๒
ระบบสารสนเทศหรือระบบการเรียนการสอนหยุดให้บริการ	ระดับ ๓
ระบบ Data Center ล่ม หรือถูก Ransomware	ระดับ ๔

๑.๒.๒ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

การวิเคราะห์ผลกระทบทางธุรกิจเป็นกระบวนการประเมินผลกระทบที่อาจเกิดขึ้นหากระบบเทคโนโลยีสารสนเทศไม่สามารถให้บริการได้ตามปกติ เพื่อจัดลำดับความสำคัญของระบบและกำหนดแนวทางการกู้คืนระบบเมื่อเกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติ

ระบบสารสนเทศ	ผลกระทบเมื่อหยุดให้บริการ	ความสำคัญ
ระบบเครือข่ายอินเทอร์เน็ต	ไม่สามารถใช้งานระบบสารสนเทศได้	สูงมาก
ระบบทะเบียนนักศึกษา	ไม่สามารถลงทะเบียนเรียนและตรวจสอบผลการเรียน	สูงมาก
ระบบการเงินและบัญชี	การเบิกจ่ายและการดำเนินงานด้านการเงินหยุดชะงัก	สูงมาก
ระบบ ERP , LMS	ส่งผลกระทบต่อการเรียนการสอนและการทำงาน	สูง
ระบบอีเมลมหาวิทยาลัย	การสื่อสารภายในองค์กรล่าช้า	สูง
เว็บไซต์มหาวิทยาลัย	ไม่สามารถเผยแพร่ข้อมูลและประชาสัมพันธ์ได้	ปานกลาง

การจัดลำดับความสำคัญในการกู้คืนระบบ

๑) ระบบไฟฟ้า ระบบปรับอากาศ และระบบเครือข่ายหลัก
๒) ระบบอินเทอร์เน็ตและ Firewall
๓) ระบบ DNS และระบบยืนยันตัวตน
๔) ระบบฐานข้อมูลกลาง
๕) ระบบทะเบียนนักศึกษาและระบบการเงิน
๖) ระบบสนับสนุนการเรียนการสอน
๗) เว็บไซต์และบริการอื่น ๆ

ผลกระทบที่อาจเกิดขึ้นต่อมหาวิทยาลัย

๑) การหยุดชะงักของการจัดการเรียนการสอน
๒) การไม่สามารถให้บริการแก่นักศึกษา บุคลากร และหน่วยงานภายนอก
๓) ความเสียหายต่อข้อมูลสารสนเทศที่สำคัญ
๔) ความเสียหายต่อชื่อเสียงและภาพลักษณ์ของมหาวิทยาลัย
๕) ความเสียหายด้านงบประมาณและค่าใช้จ่ายในการฟื้นฟูระบบ

๖) ความเสี่ยงด้านการปฏิบัติตามกฎหมายและข้อกำหนดที่เกี่ยวข้อง

ตารางประเมินความรุนแรงของเหตุการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

ลำดับ	สถานการณ์หรือภาวะฉุกเฉิน	ต่อระบบงาน (ผลกระทบต่อการให้บริการระบบสารสนเทศ)	ต่อพันธกิจ/กฎหมาย (ผลกระทบต่อภารกิจหลักและการปฏิบัติตามกฎหมาย)	ต่อผู้รับบริการ (ผลกระทบต่อผู้ใช้บริการและผู้มีส่วนได้ส่วนเสีย)	คะแนนรวม (เต็ม 15 คะแนน)	ระดับความรุนแรง	จัดลำดับความสำคัญ
		คะแนน (1-5)	คะแนน (1-5)	คะแนน (1-5)			
1	ไฟไหม้ห้องศูนย์ข้อมูล (Data Center)	5	5	5	15	วิกฤต (Critical)	1
2	การโจมตีด้วย Ransomware	5	5	5	15	วิกฤต (Critical)	1
3	ข้อมูลส่วนบุคคลรั่วไหล (Data Breach)	4	5	5	14	วิกฤต (Critical)	2
4	การบุกรุกหรือเจาะระบบสารสนเทศ	5	4	5	14	วิกฤต (Critical)	2
5	ระบบเครือข่ายหลัก / Internet Gateway ขัดข้อง	5	2	5	12	สูง (High)	3
6	ไฟฟ้าดับ / หม้อแปลงไฟฟ้าขัดข้อง	5	2	5	12	สูง (High)	3
7	น้ำท่วม / น้ำรั่วซึมห้องควบคุมระบบเครือข่าย	4	3	4	11	สูง (High)	4
8	แผ่นดินไหว	4	2	5	11	สูง (High)	4
9	ระบบฐานข้อมูลหลักเสียหาย	4	4	3	11	สูง (High)	4
10	การชุมนุมประท้วง / เหตุการณ์ความไม่สงบ	2	3	4	9	ปานกลาง (Medium)	5
11	โรคระบาดที่ส่งผลต่อการปฏิบัติงาน	3	2	4	9	ปานกลาง (Medium)	5
12	พายุรุนแรง	2	1	4	7	ปานกลาง-ต่ำ (Medium-Low)	6

เกณฑ์การให้คะแนน (1-5 คะแนน)

ต่อระบบงาน (ผลกระทบต่อการให้บริการ)
1 = กระทบเล็กน้อยมาก
2 = กระทบเล็กน้อย
3 = กระทบปานกลาง (บางส่วนหยุดให้บริการ)
4 = กระทบสูง (ระบบสำคัญหยุดให้บริการ)
5 = กระทบสูงมาก (ระบบหลักไม่สามารถให้บริการได้)

ต่อพันธกิจ/กฎหมาย (ผลกระทบต่อภารกิจหลักและกฎหมาย)
1 = ไม่กระทบต่อภารกิจหลัก
2 = กระทบภารกิจรองเล็กน้อย
3 = กระทบการดำเนินงานของหน่วยงาน
4 = กระทบภารกิจหลักบางส่วน
5 = กระทบภารกิจหลักอย่างรุนแรง หรือมีความเสี่ยงต่อการไม่ปฏิบัติตามกฎหมาย/ข้อกำหนด

ต่อผู้รับบริการ (ผลกระทบต่อผู้ใช้บริการ/ผู้มีส่วนได้ส่วนเสีย)
1 = กระทบผู้ใช้บริการจำนวนน้อยมาก
2 = กระทบผู้ใช้บริการบางกลุ่ม
3 = กระทบหลายกลุ่ม/หลายหน่วยงาน
4 = กระทบในวงกว้าง
5 = กระทบผู้ใช้บริการจำนวนมากในระดับมหาวิทยาลัย

การแปลผลคะแนนรวม

13 - 15 คะแนน = ระดับวิกฤต (Critical)
10 - 12 คะแนน = ระดับสูง (High)
7 - 9 คะแนน = ระดับปานกลาง (Medium)
1 - 6 คะแนน = ระดับต่ำ (Low)

หมายเหตุ : ต้องกำหนดมาตรการตอบสนองและแผนกู้คืนระบบตามระดับความรุนแรงและลำดับความสำคัญที่กำหนด

๑.๓ การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA)

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis : BIA) เป็นกระบวนการวิเคราะห์และประเมินผลกระทบที่อาจเกิดขึ้นต่อการดำเนินงานของมหาวิทยาลัยแม่โจ้ กรณีระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์หยุดให้บริการ ไม่สามารถใช้งานได้ หรือได้รับความเสียหายจากเหตุการณ์ฉุกเฉินและภัยพิบัติต่าง ๆ เพื่อกำหนดลำดับความสำคัญของระบบสารสนเทศ กำหนดแนวทางการกู้คืนระบบและสนับสนุนการจัดทำแผนบริหารความต่อเนื่องและแผนกู้คืนระบบสารสนเทศให้สามารถกลับมาให้บริการได้อย่างมีประสิทธิภาพ

๑.๓.๑ การวิเคราะห์ระบบสารสนเทศที่สำคัญของมหาวิทยาลัย

มหาวิทยาลัยแม่โจ้ได้วิเคราะห์และจัดลำดับความสำคัญของระบบสารสนเทศที่มีผลกระทบต่อการดำเนินงาน ดังนี้

ระบบสารสนเทศ	หน่วยงานรับผิดชอบ	ผลกระทบเมื่อหยุดให้บริการ	ระดับความสำคัญ
ระบบเครือข่ายคอมพิวเตอร์และ Internet Gateway	กองเทคโนโลยีดิจิทัล	ไม่สามารถใช้งานระบบสารสนเทศและบริการออนไลน์ของมหาวิทยาลัยได้	สูงมาก
ระบบ DNS และระบบยืนยันตัวตนผู้ใช้งาน	กองเทคโนโลยีดิจิทัล	ผู้ใช้งานไม่สามารถเข้าสู่ระบบหรือใช้งานบริการเครือข่ายได้	สูงมาก
ระบบฐานข้อมูลกลางของมหาวิทยาลัย	กองเทคโนโลยีดิจิทัล	ข้อมูลสำคัญไม่สามารถเข้าถึงได้ กระทบต่อทุกระบบงาน	สูงมาก

ระบบสารสนเทศ	หน่วยงานรับผิดชอบ	ผลกระทบเมื่อหยุดให้บริการ	ระดับความสำคัญ
ระบบ ERP (การเงิน บัญชี พัสดุ ทรัพยากรบุคคล และระบบสารสนเทศเพื่อการบริหารจัดการ)	กองคลัง / กองบริหารทรัพยากรบุคคล / กองเทคโนโลยีดิจิทัล	ไม่สามารถดำเนินงานด้านการเงิน งบประมาณ พัสดุ บุคลากรและการใช้งานระบบสารสนเทศภายในได้	สูงมาก
ระบบทะเบียนและประมวลผลการศึกษา	สำนักบริหารและพัฒนาวิชาการ	ไม่สามารถให้บริการด้านการลงทะเบียนและผลการศึกษา	สูงมาก
ระบบสารสนเทศเพื่อการเรียนการสอน (LMS)	กองเทคโนโลยีดิจิทัล	กระทบต่อการเรียนการสอนออนไลน์	สูง
ระบบอีเมลมหาวิทยาลัย	กองเทคโนโลยีดิจิทัล	การติดต่อสื่อสารภายในและภายนอกองค์กรหยุดชะงัก	สูง
ระบบเว็บไซต์มหาวิทยาลัย	กองเทคโนโลยีดิจิทัล	ไม่สามารถเผยแพร่ข่าวสารและประชาสัมพันธ์ข้อมูลได้	ปานกลาง

๑.๓.๒ การวิเคราะห์ผลกระทบต่อภารกิจของมหาวิทยาลัย

กรณีระบบเทคโนโลยีสารสนเทศไม่สามารถให้บริการได้ อาจส่งผลกระทบต่อภารกิจของมหาวิทยาลัยในด้านต่าง ๆ ดังนี้

๑) ด้านการเรียนการสอน ไม่สามารถให้บริการระบบทะเบียนนักศึกษา ระบบสนับสนุนการเรียนการสอน และระบบการเรียนการสอนออนไลน์ได้

๒) ด้านการบริหารจัดการองค์กร การรับส่งข้อมูลข่าวสาร การปฏิบัติงาน และการตัดสินใจของผู้บริหารอาจเกิดความล่าช้า

๓) ด้านการเงินและพัสดุ ไม่สามารถดำเนินการด้านงบประมาณ การเบิกจ่าย การจัดซื้อจัดจ้าง และการบริหารพัสดุได้ตามปกติ

๔) ด้านการบริหารทรัพยากรบุคคล การบริหารข้อมูลบุคลากร การประมวลผลเงินเดือน และการให้บริการด้านทรัพยากรบุคคลอาจหยุดชะงัก

๕) ด้านการวิจัยและบริการวิชาการ ไม่สามารถเข้าถึงข้อมูล งานวิจัย หรือระบบสนับสนุนการดำเนินงานที่เกี่ยวข้องได้

๖) ด้านภาพลักษณ์และชื่อเสียงของมหาวิทยาลัย ผู้รับบริการอาจขาดความเชื่อมั่นในการให้บริการของมหาวิทยาลัย

๗) ด้านกฎหมายและข้อกำหนดที่เกี่ยวข้อง อาจส่งผลกระทบต่อการปฏิบัติตามกฎหมาย ระเบียบ และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA)

๑.๓.๓ ลำดับความสำคัญในการกู้คืนระบบ

เพื่อให้การดำเนินงานของมหาวิทยาลัยสามารถกลับสู่ภาวะปกติได้โดยเร็ว มหาวิทยาลัยกำหนดลำดับความสำคัญในการกู้คืนระบบ ดังนี้

ลำดับ	ระบบที่ต้องกู้คืน
๑	ระบบไฟฟ้า ระบบปรับอากาศ และระบบโครงสร้างพื้นฐานของศูนย์ข้อมูล
๒	ระบบเครือข่ายคอมพิวเตอร์ และ Internet Gateway
๓	ระบบ Firewall ระบบรักษาความมั่นคงปลอดภัย และระบบยืนยันตัวตน
๔	ระบบ DNS และระบบฐานข้อมูลกลาง
๕	ระบบ ERP
๖	ระบบทะเบียนและประมวลผลการศึกษา
๗	ระบบสารสนเทศเพื่อการเรียนการสอน (LMS)
๘	ระบบอีเมลมหาวิทยาลัย
๙	ระบบเว็บไซต์และระบบบริการสนับสนุนอื่น ๆ

๑.๓.๔ สรุปผลการวิเคราะห์

ผลการวิเคราะห์พบว่าระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูลกลาง ระบบ ERP และระบบทะเบียนนักศึกษา เป็นระบบสารสนเทศที่มีความสำคัญสูงต่อพันธกิจหลักของมหาวิทยาลัย จึงจำเป็นต้องได้รับการป้องกัน ดูแลรักษา และกำหนดมาตรการกู้คืนระบบเป็นลำดับแรกเมื่อเกิดสถานการณ์ฉุกเฉินหรือภัยพิบัติ เพื่อให้มหาวิทยาลัยสามารถดำเนินภารกิจด้านการศึกษา การวิจัย การบริการวิชาการ และการบริหารจัดการได้อย่างต่อเนื่อง

๒. แนวทางการป้องกันและเตรียมการเบื้องต้น

๒.๑ การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการกองเทคโนโลยีดิจิทัลจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

๒.๒ กระบวนการดำเนินงาน (Procedure)

กองเทคโนโลยีดิจิทัลจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๒.๓ การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

๒.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกองเทคโนโลยีดิจิทัล ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

๑) แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
๒) อุปกรณ์สำรองข้อมูลของระบบงานที่สำคัญ เช่น External Hard disk / SAN Storage / Cloud
๓) แผ่นโปรแกรม Antivirus / Spyware
๔) แผ่น Driver อุปกรณ์ต่างๆ
๕) ระบบสำรองไฟฉุกเฉิน

๒.๕ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๒.๖ การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยองค์กรมีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

๒.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย(Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๙๐-๑๒๐ นาที
๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ
๔) ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ปริมาณน้ำมันแบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติ ๒ สัปดาห์ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้ อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

๒.๘ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้มีเจ้าหน้าที่ของงานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ กองเทคโนโลยีดิจิทัล เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) หรือการแสกนนิ้วเข้าห้องควบคุมระบบเครือข่าย เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Endpoint Security เพื่อเพิ่มประสิทธิภาพของเครื่องแม่ข่ายคอมพิวเตอร์และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ของงานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ และ พ.ร.บ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๒.๙ การบริหารจัดการสิทธิ์การเข้าถึงระบบ (Access Control)

เพื่อป้องกันการเข้าถึงระบบสารสนเทศและข้อมูลสำคัญโดยไม่ได้รับอนุญาต มหาวิทยาลัยกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

๑) กำหนดสิทธิ์การใช้งานตามหน้าที่และความรับผิดชอบ (Role-Based Access Control)

๒) ผู้ใช้งานต้องมีชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เป็นของตนเอง

๓) กำหนดให้มีการเปลี่ยนรหัสผ่านตามระยะเวลาที่เหมาะสม

๔) ยกเลิกสิทธิ์การใช้งานทันทีเมื่อบุคลากรพ้นสภาพหรือมีการเปลี่ยนหน้าที่

๕) ทบทวนสิทธิ์การเข้าถึงระบบอย่างน้อยปีละ ๑ ครั้ง

๖) สำหรับระบบที่มีข้อมูลสำคัญหรือข้อมูลส่วนบุคคล ควรพิจารณาใช้งานการยืนยันตัวตนแบบหลายปัจจัย (Multi-Factor Authentication : MFA)

๒.๑๐ การบริหารจัดการช่องโหว่และการปรับปรุงระบบ (Vulnerability and Patch Management)

เพื่อป้องกันความเสี่ยงจากช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศ และลดโอกาสการถูกโจมตีทางไซเบอร์ มหาวิทยาลัยกำหนดแนวทางการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ดังนี้

๑) ตรวจสอบช่องโหว่ของระบบปฏิบัติการ ระบบฐานข้อมูล และระบบสารสนเทศอย่างสม่ำเสมอ

๒) ติดตั้ง Security Patch และ Firmware ของอุปกรณ์เครือข่ายให้เป็นปัจจุบัน

๓) ทดสอบการปรับปรุงระบบก่อนนำไปใช้งานจริงสำหรับระบบสำคัญ

๔) บันทึกและจัดเก็บข้อมูลการปรับปรุงระบบทุกครั้ง

๕) ตรวจสอบและประเมินช่องโหว่ด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๖) กรณีพบช่องโหว่ระดับรุนแรง ให้ดำเนินการแก้ไขโดยเร่งด่วน

๒.๑๑ การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

๑) เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

๓) ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า

๔) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๕) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๖) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๓. การเตรียมความพร้อม

๓.๑การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

๒) ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ปริมาณน้ำมันแบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

๓) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๒ ชั่วโมง

๔) ตรวจสอบระบบไฟฟ้าและอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ

๕) จัดทำ Checklist ระยะเวลาในการปิด / เปิด ระบบสารสนเทศมหาวิทยาลัยแม่โจ้ ที่มีเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย กรณีที่ระบบไฟฟ้าดับหรือถูกตัด

๖) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และ บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๗) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๘) ให้มีการสำรองข้อมูลตามนโยบายการสำรองข้อมูลของมหาวิทยาลัย และดำเนินการตรวจสอบความสามารถในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้
๒) ติดตั้งระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ในห้องควบคุมระบบเครือข่าย
๓) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น สำหรับห้องปฏิบัติงานคอมพิวเตอร์ควรติดตั้งถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ได้เป็นอย่างน้อย (อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์)
๔) ให้มีการสำรองข้อมูลตามนโยบายการสำรองข้อมูลของมหาวิทยาลัย และดำเนินการตรวจสอบความสามารถในการกู้คืนข้อมูลอย่างสม่ำเสมอ
๕) มีการทดสอบระบบดับเพลิงอัตโนมัติและอุปกรณ์แจ้งเหตุเพลิงไหม้อย่างน้อยปีละ ๑ ครั้ง

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุน้ำท่วม /น้ำรั่วซึม

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม /น้ำรั่ว
๒) ติดตั้งระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detection System) ในห้องควบคุมระบบเครือข่าย
๓) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ
๔) ให้มีการสำรองข้อมูลตามนโยบายการสำรองข้อมูลของมหาวิทยาลัย และดำเนินการตรวจสอบความสามารถในการกู้คืนข้อมูลอย่างสม่ำเสมอ
๕) มีการตรวจสอบและทดสอบระบบตรวจจับน้ำรั่ว (Water Leak Detection System) อย่างน้อยปีละ ๑ ครั้ง

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากมัลแวร์และโปรแกรมเรียกค่าไถ่ (Malware and Ransomware)

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก
๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)
๓) ติดตั้งและปรับปรุงโปรแกรมป้องกันมัลแวร์และโปรแกรมเรียกค่าไถ่ให้เป็นปัจจุบันอยู่เสมอ
๔) ตรวจสอบและติดตั้ง Security Patch ของระบบปฏิบัติการและระบบสารสนเทศอย่างสม่ำเสมอ
๕) ทดสอบการกู้คืนข้อมูลจากระบบสำรองอย่างน้อยปีละ ๑ ครั้ง

๓.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๒) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของงานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ กองเทคโนโลยีดิจิทัล เป็นรับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card หรือการแสกนนิ้วเข้าห้องควบคุมระบบเครือข่าย และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Endpoint Security เพื่อเพิ่มประสิทธิภาพในการให้บริการเครื่องแม่ข่ายและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มีเจ้าหน้าที่ของงานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ กองเทคโนโลยีดิจิทัล ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๖) มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๗) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log Files) และตรวจสอบเหตุการณ์ผิดปกติอย่างสม่ำเสมอ

๘) เมื่อพบเหตุการณ์ความผิดปกติให้ดำเนินการแยกระบบที่ได้รับผลกระทบออกจากเครือข่ายโดยเร็ว เพื่อลดผลกระทบต่อระบบสารสนเทศส่วนอื่น

๓.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่แผนกต่างๆภายในองค์กร ขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๓) จัดอบรมด้านความมั่นคงปลอดภัยไซเบอร์และการป้องกันภัยคุกคามทางไซเบอร์ให้แก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง

๓.๗ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ 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 มาตรการและแนวทางปฏิบัติ (www.disaster.go.th)

๒) การสังเกตพฤติกรรมของสัตว์

- สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น
- สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู
- แมลงสาบจำนวนมากวิ่งเพ่นพ่าน
- หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน
- ปลากระโดดขึ้นมาจากผิวน้ำ

๓) การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

- ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
- ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุอุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
- สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร
- สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย
- จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๔) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

- สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้

ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

- เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคาร ดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๕) การปฏิบัติขั้นเตรียมการ

- การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
- การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย
- อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่ บุคลากรในองค์กร
- รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๘ การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

๑) จัดทำแผนเตรียมความพร้อมรับสถานการณ์การชุมนุมทางการเมืองด้านเทคโนโลยีสารสนเทศของกองเทคโนโลยีดิจิทัล มหาวิทยาลัยแม่โจ้

๒) จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ (Business Continuity Planning) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่มหาวิทยาลัยแม่โจ้ได้

๓) ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๔) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้นและมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๕) ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมระบบเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน

๖) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๗) สำรองข้อมูล

๘) จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงานที่มหาวิทยาลัยแม่โจ้

๙) จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมคณะทำงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑ โครงสร้างการสั่งการ (Incident Command Structure)

เมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้บัญชาการเหตุการณ์ (Incident Commander) มีอำนาจในการสั่งการ ประสานงาน และติดตามการดำเนินงานของคณะทำงานทุกชุด จนกว่าสถานการณ์จะกลับสู่ภาวะปกติ

หน้าที่	ผู้รับผิดชอบ
ผู้อนุมัติประกาศใช้แผน	CIO / รองอธิการบดี
ผู้บัญชาการเหตุการณ์ (Incident Commander)	ผู้อำนวยการกองเทคโนโลยีดิจิทัล
ผู้ประสานงานการกู้คืนระบบ	หัวหน้างานโครงสร้างพื้นฐานเทคโนโลยีสารสนเทศ
ผู้ประเมินความเสียหาย	คณะประเมินความเสียหาย
ผู้รายงานสถานการณ์ต่อผู้บริหาร	คณะบริหารจัดการการกู้คืนระบบ

รองอธิการบดี (Chief Executive Officer : CEO) และ (Chief Information Officer : CIO)

ผู้อำนวยการกองเทคโนโลยีดิจิทัล (Director of Digital Technology Division)

ผู้อำนวยการกองกายภาพและสิ่งแวดล้อม (Director of Division of Physical Systems and Environment)

๔.๒ การปฏิบัติหน้าที่

กรณีผู้รับผิดชอบหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้ผู้รับผิดชอบในลำดับถัดไปหรือผู้ที่ได้รับมอบหมายทำหน้าที่แทน และมีอำนาจตัดสินใจในขอบเขตเดียวกันจนกว่าสถานการณ์จะคลี่คลาย

๑) คณะบริหารจัดการการกู้คืนระบบ

มีหน้าที่หลักในการจัดการและประสานงานการกู้คืนระบบต่างๆ ผู้รับผิดชอบได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐

นายอาทิตย์ แก้วถาวร เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๘๕๖๑

นายประวิทย์ วิมานทอง เบอร์โทรศัพท์ติดต่อ ๐๙๕-๗๒๗-๔๓๔๔

นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗

นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙

นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๒) คณะกู้คืนเครือข่ายอินเทอร์เน็ต

มีหน้าที่ดูแลกู้คืนให้เครือข่ายอินเทอร์เน็ตกลับมาใช้งานได้ปกติ ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐

นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗

นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙

นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๓) คณะกู้คืนระบบสารสนเทศ

มีหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายอาทิตย์ แก้วถาวร เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๘๕๖๑

๑) กองเทคโนโลยีดิจิทัล

นายสมชาย อารยพิทยา เบอร์โทรศัพท์ติดต่อ ๐๘๑-๙๕๒-๑๗๘๕

นายวสุ ไชยศรีหา เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๓๙-๔๑๓๒

นายสุรเดช ไชยมงคล เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๙๕-๑๑๕๔

นางนพมาศ ริยะนา เบอร์โทรศัพท์ติดต่อ ๐๘๓-๕๖๔-๕๐๔๘

นางสาวณัฐกฤตา โกมลนาค เบอร์โทรศัพท์ติดต่อ ๐๙๗-๙๒๑-๖๒๐๙

นายคล๊อก ประถมทรัพย์ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๐๔๓-๑๗๖๙

นางสาวอทิตยา คำภิระ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๘๘๔-๘๙๑๖

๒) สำนักบริหารและพัฒนาวิชาการ

นายเดชา ผิวผ่อง เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๔๕๗

นายพงษ์ศักดิ์ มังมติ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๔๕๕

นายณัฐพล อาจิน เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๔๗๐

๓) สำนักวิจัยและส่งเสริมวิชาการการเกษตร

นายภาณุลักษณ์ ศรีรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๔๒๓

นายปริญญา เพียรอุตส่าห์ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๔๐๐

๔) สำนักหอสมุด

นายณัฐชาพงษ์ รักสกุลกานต์ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๕๐๖

๕) กองการเจ้าหน้าที่

นางสาวละออศิริ พรหมศร เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๑๓๓

๖) กองคลัง

นางสาวสุพรรณิการ์ สิทธิสังข์ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๒๘๑

นางสาวดุษฎี ดวงบาล เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๒๘๑

๔) คณะกู้คืนระบบสารสนเทศเพื่อการเรียนการสอน

มีหน้าที่ติดตั้ง กู้คืนระบบการเรียนการสอนให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายประวิทย์ วิมานทอง เบอร์โทรศัพท์ติดต่อ ๐๙๕-๗๒๗-๔๓๔๔

นางสาวสุมาลี สุพรรณนอก เบอร์โทรศัพท์ติดต่อ ๐๘๙-๔๓๕-๓๐๔๔

นางอภิญญา โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๗๓๒-๔๒๑๗

นางสาวศุภวรรณ สัจจากุล เบอร์โทรศัพท์ติดต่อ ๐๙๐-๓๑๘-๑๘๕๖

นางสาวมนสิชา มีแสงแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๙-๙๙๒-๑๗๓๖

นางสาวกรกช เจริญทรัพย์ เบอร์โทรศัพท์ติดต่อ ๐๘๙-๗๕๗-๓๗๗๗

๕) คณะประเมินความเสียหาย

มีหน้าที่ตรวจสอบและประเมินความความเสียหายทั้งด้าน Hardware และ Softwareพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐

นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗

นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙

นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๖) คณะอาคารสถานที่

มีหน้าที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร แอร์ให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นางเนตรนภา ธะนันต์ เบอร์โทรศัพท์ติดต่อ ๐๘๓-๖๕๘-๙๙๒๒
นางพรสวรรค์ นักดนตรี เบอร์โทรศัพท์ติดต่อ ๐๘๗-๑๘๕-๙๙๙๘
นางจุรีรัตน์ สุยะเขต เบอร์โทรศัพท์ติดต่อ ๐๙๔-๖๒๓-๗๑๙๓
นางอาจารียา ปิยะจันทร์ เบอร์โทรศัพท์ติดต่อ ๐๙๔-๗๔๖-๕๑๕๕

๗) คณะการจัดการทั่วไป

มีหน้าที่ประสานงานช่วยเหลือคณะอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงานผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นางเนตรนภา ธะนันต์ เบอร์โทรศัพท์ติดต่อ ๐๘๓-๖๕๘-๙๙๒๒
นางพรสวรรค์ นักดนตรี เบอร์โทรศัพท์ติดต่อ ๐๘๗-๑๘๕-๙๙๙๘
นางจุรีรัตน์ สุยะเขต เบอร์โทรศัพท์ติดต่อ ๐๙๔-๖๒๓-๗๑๙๓
นางอาจารียา ปิยะจันทร์ เบอร์โทรศัพท์ติดต่อ ๐๙๔-๗๔๖-๕๑๕๕

๘) คณะแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบเครือข่าย และห้องปฏิบัติงานคอมพิวเตอร์

มีหน้าที่แก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่กองเทคโนโลยีดิจิทัลและการสื่อสารได้จัดหาไว้ ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐
นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗
นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙
นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๙) คณะแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิด

มีหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐
นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗
นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙
นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๑๐) คณะแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วม/น้ำรั่วซึม ห้องควบคุมระบบเครือข่าย

มีหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบฯ และตรวจสอบการรั่วซึม ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐
นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗
นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙
นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๑๑) คณะแก้ไขปัญหาเนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์

มีหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐
นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗
นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙
นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๑๒) คณะสำรองและกู้คืนข้อมูล (Backup & Recovery)

มีหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์ ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายบรรพต โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๗๘๙๐
นายอาทิตย์ แก้วถาวร เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๗๑-๘๕๖๑
นายประวิทย์ วิมานทอง เบอร์โทรศัพท์ติดต่อ ๐๙๕-๗๒๗-๔๓๔๔
นายปานศักดิ์ ชัยภักดี เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๖-๙๖๗๗
นายพันธมิตร ใจรินทร์ เบอร์โทรศัพท์ติดต่อ ๐๘๑-๕๓๑-๙๓๘๙
นายเสกสรรค์ สอนยศ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๕๑๕-๔๕๔๙

๑๓) คณะแก้ไขปัญหาเนื่องจากแผ่นดินไหว

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากแผ่นดินไหว แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกัน เหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการกองเทคโนโลยีดิจิทัลเพื่อทราบและสั่งการต่อไปผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นางเนตรนภา ธะนันต์ เบอร์โทรศัพท์ติดต่อ ๐๘๓-๖๕๘-๙๙๒๒
นางพรสวรรค์ นักดนตรี เบอร์โทรศัพท์ติดต่อ ๐๘๗-๑๘๕-๙๙๙๘
นางจุรีรัตน์ สุยะเขต เบอร์โทรศัพท์ติดต่อ ๐๙๔-๖๒๓-๗๑๙๓
นางอาจารียา ปิยะจันทร์ เบอร์โทรศัพท์ติดต่อ ๐๙๔-๗๔๖-๕๑๕๕

๑๔) คณะแก้ไขปัญหาเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการกองเทคโนโลยีดิจิทัล เพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นางเนตรนภา ธะนันต์ เบอร์โทรศัพท์ติดต่อ ๐๘๓-๖๕๘-๙๙๒๒
นางพรสวรรค์ นักดนตรี เบอร์โทรศัพท์ติดต่อ ๐๘๗-๑๘๕-๙๙๙๘
นางจุรีรัตน์ สุยะเขต เบอร์โทรศัพท์ติดต่อ ๐๙๔-๖๒๓-๗๑๙๓
นางอาจารียา ปิยะจันทร์ เบอร์โทรศัพท์ติดต่อ ๐๙๔-๗๔๖-๕๑๕๕

๔.๓ ช่องทางการสื่อสารในภาวะฉุกเฉิน

ช่องทาง	วัตถุประสงค์
โทรศัพท์มือถือ	แจ้งเหตุเร่งด่วน
E-mail มหาวิทยาลัย	สื่อสารรายละเอียด
Microsoft Teams	ประชุมและประสานงาน
Line Group IT Emergency	แจ้งเตือนและติดตามสถานการณ์
เว็บไซต์มหาวิทยาลัย	ประกาศสถานการณ์

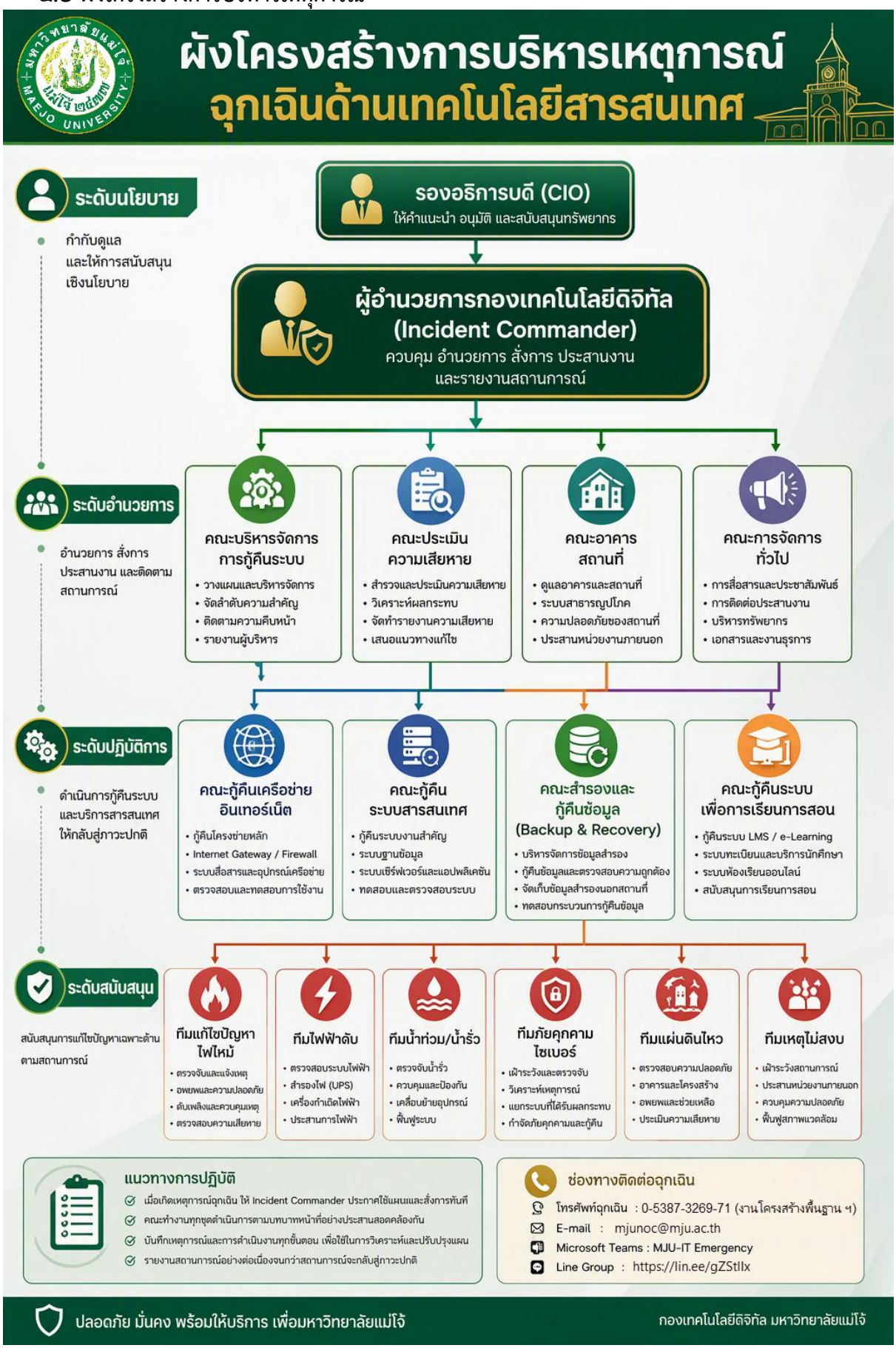
๔.๔ หน่วยงานสนับสนุนภายนอก

หน่วยงาน	หน้าที่
การไฟฟ้าส่วนภูมิภาค	สนับสนุนระบบไฟฟ้า
สถานีดับเพลิง	เหตุเพลิงไหม้
สถานีตำรวจ	เหตุโจรกรรมและอาชญากรรม
ผู้ให้บริการอินเทอร์เน็ต	กู้คืนวงจรสื่อสาร
ผู้จำหน่าย Firewall	สนับสนุนอุปกรณ์ความปลอดภัย
ผู้พัฒนาระบบ ERP	กู้คืนระบบงาน
Microsoft / Cloud Provider	Cloud Service Recovery

๔.๕ การรายงานสถานการณ์

เมื่อเกิดเหตุการณ์ฉุกเฉิน ให้คณะทำงานจัดทำรายงานสถานการณ์เบื้องต้นภายใน ๒๔ ชั่วโมง และจัดทำรายงานสรุปผลการดำเนินงาน ภายใน ๗ วันหลังจากสถานการณ์กลับสู่ภาวะปกติ เพื่อนำมาวิเคราะห์และปรับปรุงแผนในอนาคต

๔.๖ ผังโครงสร้างการบริหารเหตุการณ์



๕. ผังงานกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

๕.๑ สถานการณ์ฉุกเฉิน กรณีมัลแวร์และโปรแกรมเรียกค่าไถ่ (Malware / Ransomware)

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีมัลแวร์และโปรแกรมเรียกค่าไถ่ (Malware / Ransomware)

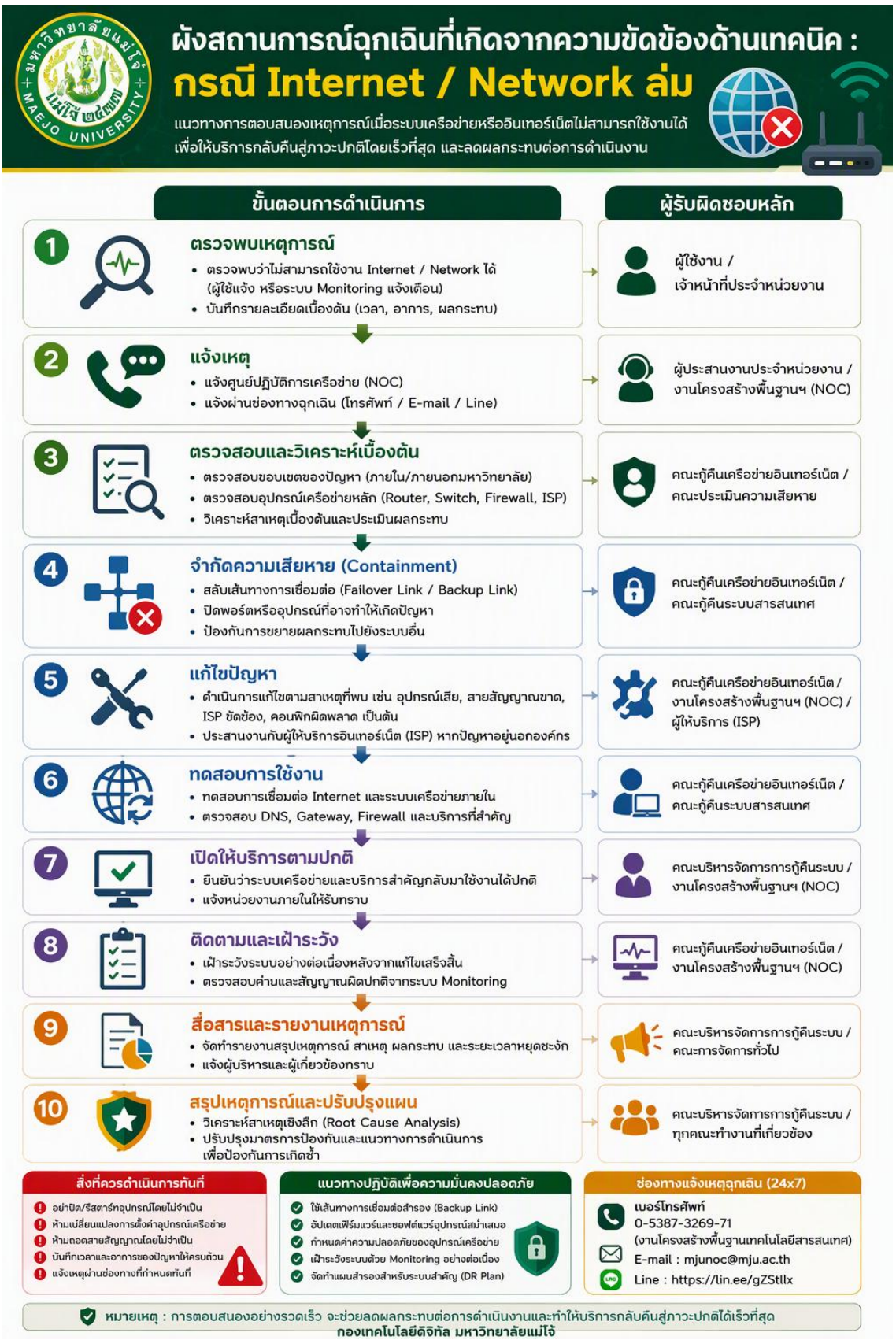
๕.๒ สถานการณ์ฉุกเฉิน กรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีข้อมูลส่วนบุคคลรั่วไหล (Data Breach)

๕.๓ สถานการณ์ฉุกเฉิน กรณีถูกเจาะระบบ (Cyber Attack)

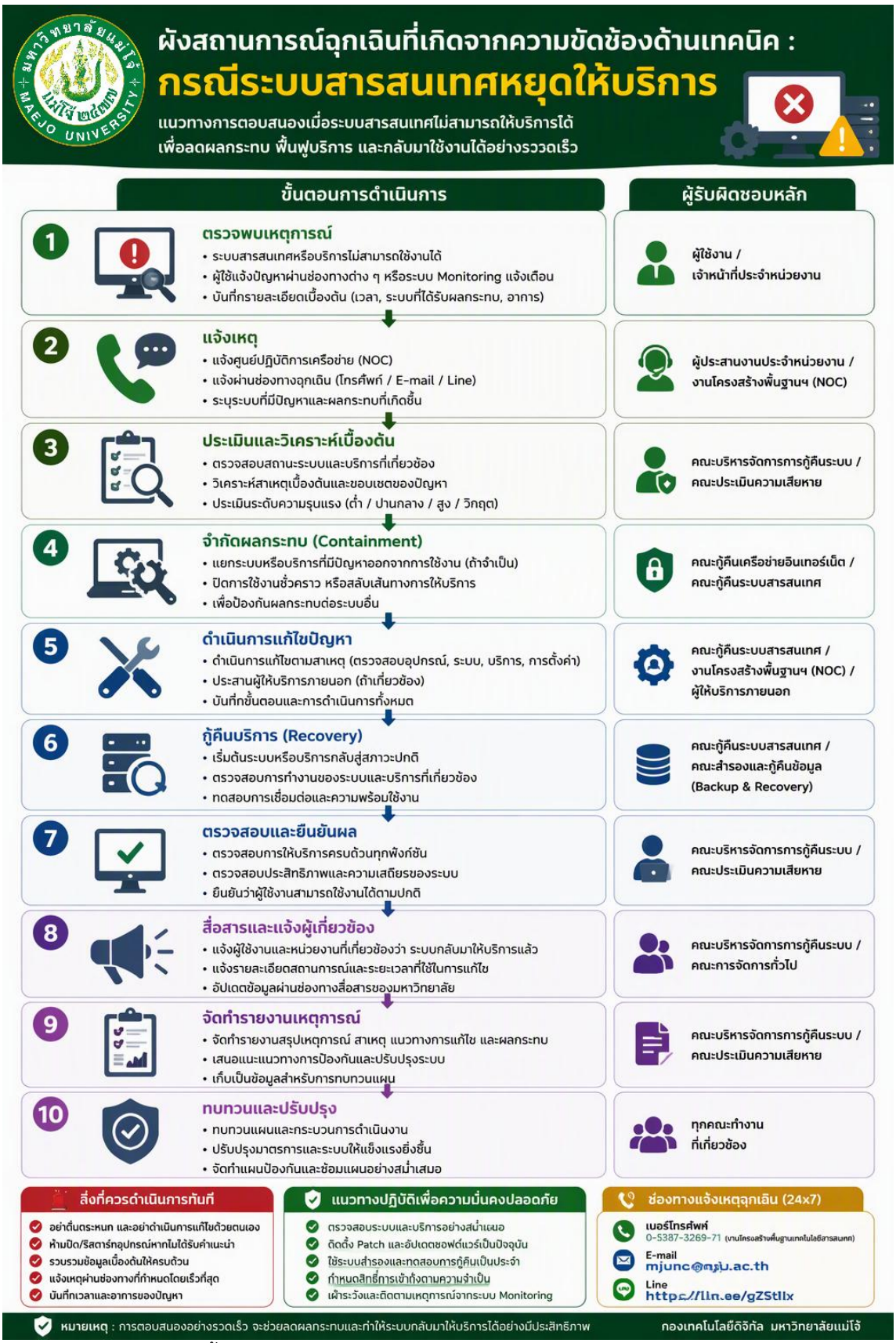
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีถูกเจาะระบบ (Cyber Attack)

๕.๔ สถานการณ์ฉุกเฉิน กรณี Internet / Network ล่ม



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณี Internet / Network ล่ม

๕.๕ สถานการณ์ฉุกเฉิน กรณีระบบสารสนเทศหยุดให้บริการ



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีระบบสารสนเทศหยุดให้บริการ

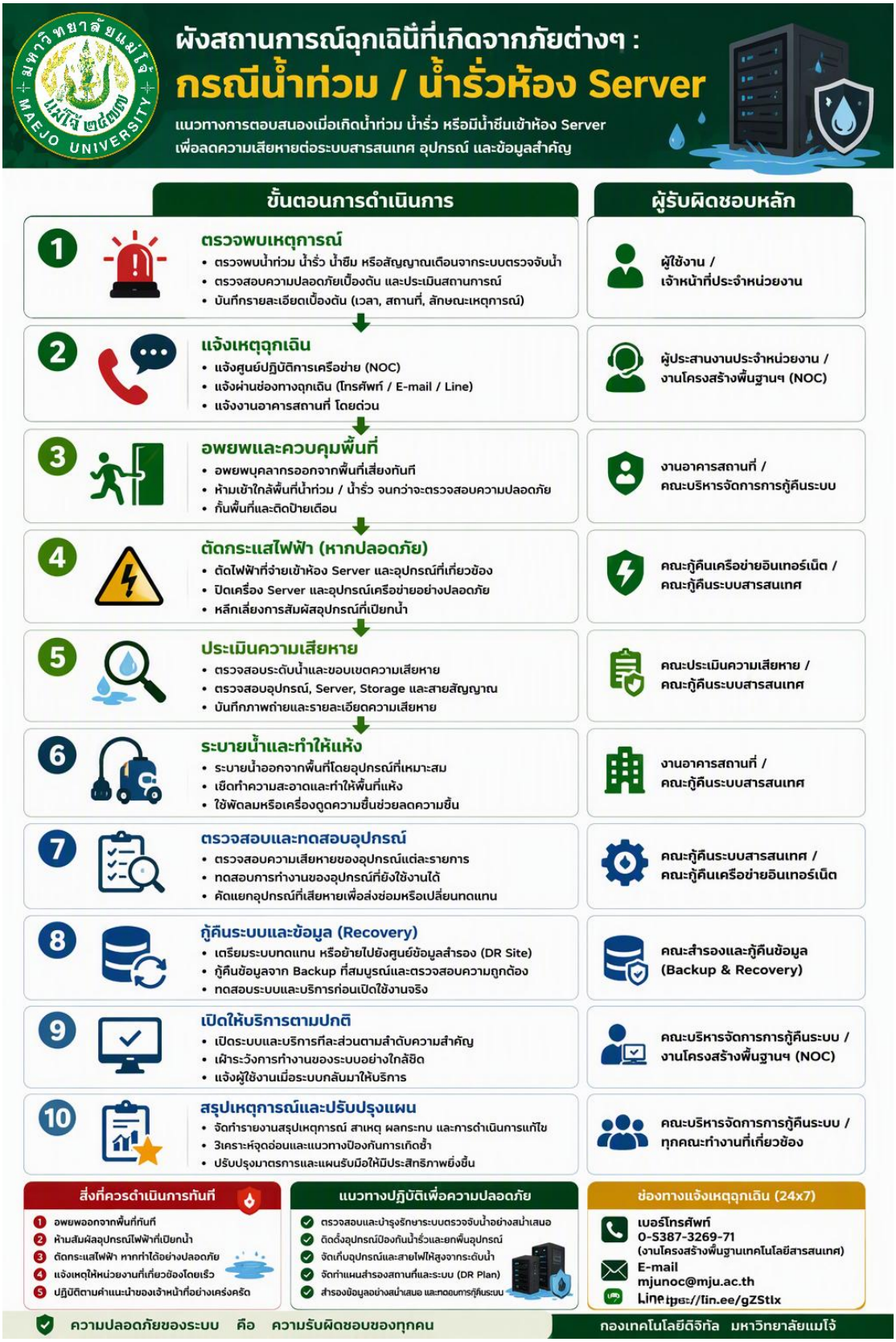
๕.๖ สถานการณ์ฉุกเฉิน กรณีไฟไหม้ Data Center

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ Data Center

๕.๗ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ กรณีไฟฟ้าดับ / UPS ขัดข้อง

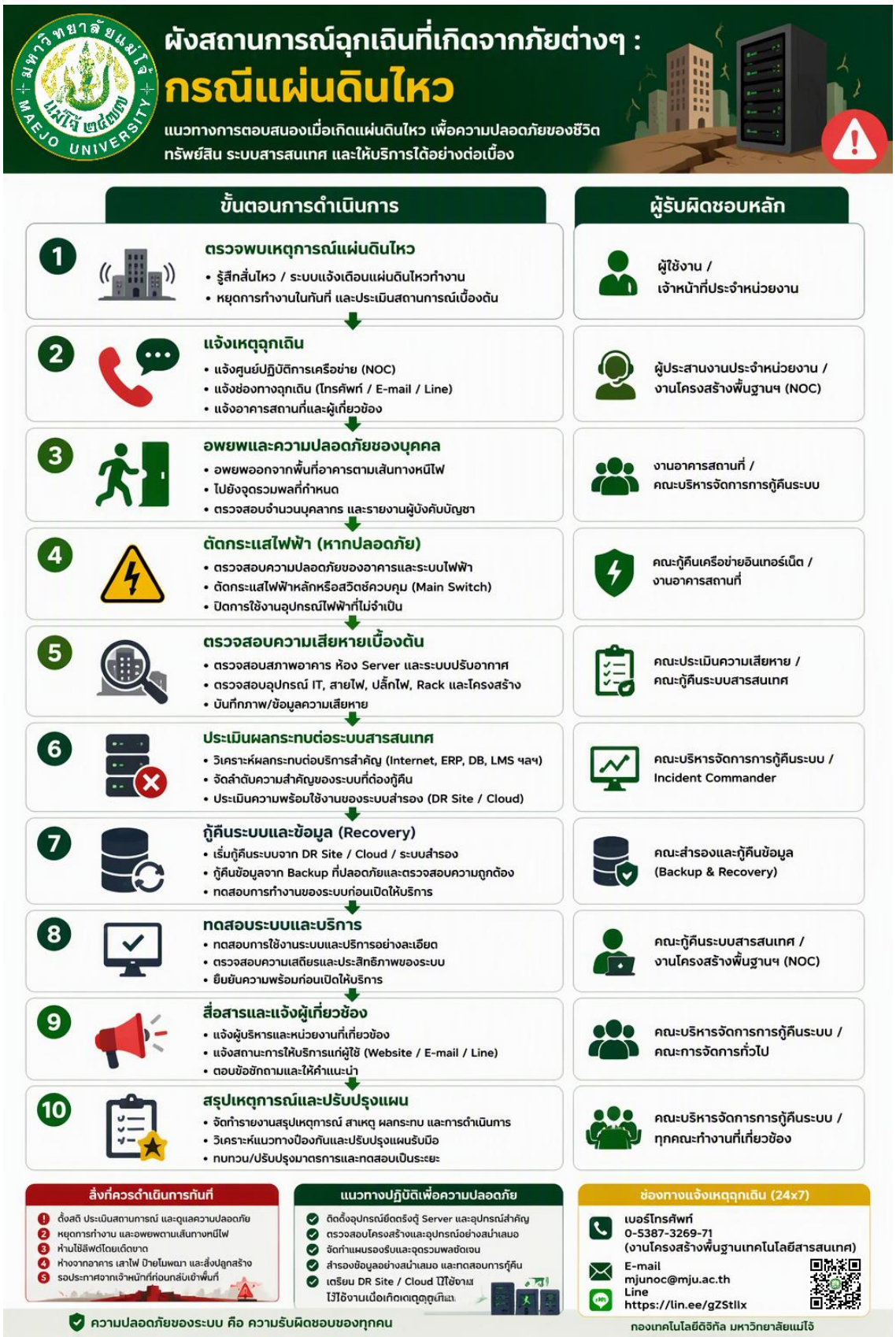
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ กรณีไฟฟ้าดับ / UPS ขัดข้อง

๕.๘ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ กรณีน้ำท่วม / น้ำรั่วห้อง Server



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม / น้ำรั่วห้อง Server

๕.๙ สถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

๕.๑๐ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๕.๑๑ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคลกรณีโจรกรรม

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากการบุคคลกรณีโจรกรรม

๖. การกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

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

๖.๑ หลักการกู้คืนระบบ

เมื่อเกิดเหตุการณ์ฉุกเฉินหรือภัยพิบัติที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้จะดำเนินการกู้คืนระบบและข้อมูลตามลำดับความสำคัญของบริการ เพื่อให้สามารถกลับมาให้บริการได้อย่างต่อเนื่อง และลดผลกระทบต่อภารกิจหลักของมหาวิทยาลัยให้เหลือน้อยที่สุด

๖.๒ ลำดับความสำคัญในการกู้คืนระบบ

ลำดับ	ระบบ
๑	ระบบไฟฟ้าและระบบปรับอากาศ
๒	ระบบเครือข่ายหลักและ Internet Gateway
๓	Firewall และระบบรักษาความมั่นคงปลอดภัย
๔	ระบบ DNS และ Authentication
๕	ระบบฐานข้อมูลกลาง
๖	ระบบ ERP (การเงิน บัญชี พัสดุ ทรัพยากรบุคคล และระบบสารสนเทศเพื่อการบริหารจัดการ)
๗	ระบบทะเบียนนักศึกษา
๘	ระบบ LMS
๙	ระบบ E-mail
๑๐	ระบบ Website

๖.๓ Recovery Time Objective (RTO)

Recovery Time Objective (RTO) หมายถึง ระยะเวลาสูงสุดที่มหาวิทยาลัยสามารถยอมรับให้ระบบหยุดให้บริการได้

ระบบสารสนเทศ	RTO
ระบบเครือข่ายหลัก	๔ ชั่วโมง
ระบบ ERP (การเงิน บัญชี พัสดุ ทรัพยากรบุคคล และระบบสารสนเทศเพื่อการบริหารจัดการ)	๘ ชั่วโมง
ระบบทะเบียนนักศึกษา	๘ ชั่วโมง
LMS	๒๔ ชั่วโมง
Website	๔๘ ชั่วโมง

๖.๔Recovery Point Objective (RPO)

Recovery Point Objective (RPO) หมายถึง ระยะเวลาข้อมูลสูญหายย้อนหลังที่สามารถยอมรับได้

ระบบสารสนเทศ	RPO
ERP	๑ ชั่วโมง
ระบบทะเบียนนักศึกษา	๑ ชั่วโมง
E-Mail	๔ ชั่วโมง
LMS	๒๔ ชั่วโมง
Website	๒๔ ชั่วโมง

๖.๕ ขั้นตอนการกู้คืนระบบ

ปัจจุบันมหาวิทยาลัยแม่โจ้ดำเนินการสำรองข้อมูลและกู้คืนระบบโดยใช้อุปกรณ์สำรอง ทรัพยากรด้านเทคโนโลยีสารสนเทศ และระบบจัดเก็บข้อมูลสำรองที่มีอยู่ภายในมหาวิทยาลัย รวมถึงบริการ Cloud ตามความเหมาะสม โดยมหาวิทยาลัยมีแผนศึกษาความเป็นไปได้ในการจัดตั้งศูนย์ข้อมูลสำรอง (Disaster Recovery Site : DR Site) เพื่อเพิ่มความพร้อมในการรองรับสถานการณ์ฉุกเฉินในอนาคต

ขั้นตอนการกู้คืนระบบสารสนเทศ

๑) ตรวจสอบและประเมินความเสียหาย
๒) กำหนดขอบเขตการกู้คืนระบบ
๓) จัดเตรียมสถานที่และอุปกรณ์สำรอง
๔) กู้คืนระบบเครือข่ายและระบบพื้นฐาน
๕) กู้คืนฐานข้อมูลจาก Backup
๖) กู้คืนระบบสารสนเทศตามลำดับความสำคัญ
๗) ทดสอบการใช้งาน
๘) เปิดให้บริการ
๙) ติดตามผลและเฝ้าระวัง
๑๐)จัดทำรายงานสรุป

๖.๖ การทดสอบแผนกู้คืนระบบ

มหาวิทยาลัยกำหนดให้มีการทดสอบการกู้คืนระบบสารสนเทศและข้อมูลจากระบบสำรองอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าสามารถกู้คืนระบบได้ภายในระยะเวลาที่กำหนด

กิจกรรม	ความถี่
Restore Backup Test	ปีละ ๑ ครั้ง
Disaster Recovery Drill	ปีละ ๑ ครั้ง
Failover Test	ปีละ ๑ ครั้ง

๗. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้ผู้อำนวยการกองเทคโนโลยีดิจิทัลทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยี

สารสนเทศระดับสูง เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

๗.๑ การรายงานเหตุการณ์

เมื่อเกิดสถานการณ์ฉุกเฉินหรือภัยพิบัติที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ให้คณะทำงานที่เกี่ยวข้องดำเนินการรายงานเหตุการณ์ต่อผู้อำนวยการกองเทคโนโลยีดิจิทัลและผู้บริหารเทคโนโลยีสารสนเทศ (CIO) โดยเร็วที่สุด เพื่อใช้ในการติดตามสถานการณ์ ตัดสินใจ และสั่งการตามความเหมาะสม

รายงานเหตุการณ์ควรประกอบด้วย

๑) วัน เวลา และสถานที่เกิดเหตุ
๒) ลักษณะของเหตุการณ์
๓) ระบบที่ได้รับผลกระทบ
๔) ระดับความรุนแรงของเหตุการณ์
๕) แนวทางการแก้ไขปัญหาเบื้องต้น
๖) ผลกระทบที่เกิดขึ้น
๗) สถานะการกู้คืนระบบ

๗.๒ การจัดทำรายงานสรุปเหตุการณ์

ภายหลังจากสถานการณ์กลับเข้าสู่ภาวะปกติ ให้คณะทำงานจัดทำรายงานสรุปผลการดำเนินงานเสนอผู้บริหาร โดยอย่างน้อยต้องประกอบด้วย

๑) สาเหตุของเหตุการณ์
๒) ผลกระทบที่เกิดขึ้น
๓) ระยะเวลาที่ระบบหยุดให้บริการ
๔) แนวทางการแก้ไขและกู้คืนระบบ
๕) ปัญหาและอุปสรรคที่พบ
๖) ข้อเสนอแนะเพื่อป้องกันการเกิดเหตุซ้ำ

๗.๓ การทบทวนและปรับปรุงแผน

กองเทคโนโลยีดิจิทัลจะดำเนินการทบทวนแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดเหตุการณ์สำคัญที่ส่งผลกระทบต่อระบบสารสนเทศ เพื่อให้แผนมีความเหมาะสม ทันสมัย และสอดคล้องกับเทคโนโลยีที่เปลี่ยนแปลงไป

กรณีมีการเปลี่ยนแปลงในด้านต่อไปนี้ ให้ดำเนินการทบทวนแผนเพิ่มเติม

๑) โครงสร้างองค์กร
๒) รายชื่อผู้รับผิดชอบ
๓) ระบบสารสนเทศที่สำคัญ
๔) โครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ
๕) ความเสี่ยงและภัยคุกคามรูปแบบใหม่
๖) กฎหมายหรือข้อกำหนดที่เกี่ยวข้อง

๗.๔ การทดสอบและประเมินประสิทธิภาพแผน

มหาวิทยาลัยกำหนดให้มีการทดสอบแผนรับสถานการณ์ฉุกเฉินและแผนกู้คืนระบบสารสนเทศอย่างสม่ำเสมอ เพื่อประเมินความพร้อมของบุคลากร อุปกรณ์ และกระบวนการปฏิบัติงาน

กิจกรรม	ความถี่
ทดสอบการกู้คืนข้อมูล (Restore Test)	อย่างน้อยปีละ ๑ ครั้ง
ซักซ้อมแผนรับสถานการณ์ฉุกเฉิน	อย่างน้อยปีละ ๑ ครั้ง
ทดสอบการกู้คืนระบบ (DR Drill)	อย่างน้อยปีละ ๑ ครั้ง
ทบทวนบัญชีผู้ติดต่อฉุกเฉิน	อย่างน้อยปีละ ๑ ครั้ง

๗.๕ การบริหารจัดการองค์ความรู้และบทเรียนที่ได้รับ

ภายหลังการเกิดเหตุการณ์หรือการทดสอบแผน ให้มีการรวบรวมบทเรียนที่ได้รับ (Lessons Learned) เพื่อใช้ในการปรับปรุงกระบวนการปฏิบัติงาน แผนรับสถานการณ์ฉุกเฉิน และแผนกู้คืนระบบสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น

โดยให้มีการจัดเก็บข้อมูลดังนี้

๑) แนวทางการแก้ไขที่ประสบผลสำเร็จ
๒) ปัญหาและอุปสรรคที่พบ
๓) ข้อเสนอแนะจากคณะทำงาน
๔) แนวทางป้องกันเหตุการณ์ซ้ำ
๕) มาตรการปรับปรุงในอนาคต