แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) มหาวิทยาลัยแม่โจ้ ปีงบประมาณ พ.ศ.๒๕๖๘-๒๕๗๒

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
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
๕. ผังงานกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
๖. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
๗. การติดตามและรายงานผล

โดยอธิบายรายละเอียดดังต่อไปนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

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

ภัยพิบัติจากภายใน

๑. ระบบเครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒. ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓. เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมือ อุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟท์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ หรือหยุดการทำงาน

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

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

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (1 รุนแรงต่ำสุด, 5 รุนแรงสูงสุด)			คะแนนรวม	จัดลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อประชาชน		
ไฟไหม้	5	5	5	15	1
โดนเจาะระบบ	5	3	5	13	2
ไฟฟ้าดับ	5	1	5	11	3
น้ำท่วม / น้ำรั่วซึม	4	2	4	10	4
แผ่นดินไหว	4	1	5	10	4
จลาจล การชุมนุม / เหตุการณ์ความไม่สงบ / สถานการณ์ทางการเมือง	2	3	4	9	5
ภัยแล้ง / คลื่นความร้อน	2	1	5	8	6
พายุ	1	1	5	7	7
โรคระบาด	1	1	4	6	8

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

- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลของระบบงานที่สำคัญ เช่น External Hard disk / SAN Storage / Cloud
- แผ่นโปรแกรม Antivirus / Spyware
- แผ่น Driver อุปกรณ์ต่างๆ
- 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 ให้มีเจ้าหน้าที่ของงานระบบเครือข่ายและบริการอินเทอร์เน็ต กองเทคโนโลยีดิจิทัล เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) หรือการแสกนนิ้วเข้าห้องควบคุมระบบเครือข่าย เพื่อใช้ในการเข้าออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Endpoint Security เพื่อเพิ่มประสิทธิภาพของเครื่องแม่ข่ายคอมพิวเตอร์และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ของงานระบบเครือข่ายและบริการอินเทอร์เน็ต ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

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

๒.๙ 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 พร้อมกำหนดจุดรวมพลที่ชัดเจนและเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๓. การเตรียมความพร้อม

๓.๑ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๓.๑.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

๓.๑.๒ ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ปริมาณน้ำมันแบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ ๑ ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้า

เข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลาประมาณ ๘ ชั่วโมง

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

๓.๑.๔ ตรวจสอบระบบไฟฟ้าและอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ

๓.๑.๕ จัดทำ Checklist ระยะเวลาในการปิด / เปิด ระบบสารสนเทศกรมประมงที่มีเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย กรณีที่ระบบไฟฟ้าดับหรือถูกตัด

๓.๑.๖ เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓.๑.๗ เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๓.๑.๘ ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๓.๒.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

๓.๒.๒ ติดตั้งระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ในห้องควบคุมระบบเครือข่าย

๓.๒.๓ ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น สำหรับห้องปฏิบัติงานคอมพิวเตอร์ควรติดตั้งถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ได้เป็นอย่างน้อย (อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์)

๓.๒.๔ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุน้ำท่วม /น้ำรั่วซึม

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๓.๓.๑ จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม /น้ำรั่ว

๓.๓.๒ ติดตั้งระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detection System) ในห้องควบคุมระบบเครือข่าย

๓.๓.๓ มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

๓.๓.๔ ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัสคอมพิวเตอร์

๓.๔.๑ ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และป้องกันการบุกรุกจากบุคคลภายนอก

๓.๔.๒ มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๓.๔.๓ อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย (Update Patch)

๓.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๓.๕.๑ กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๓.๕.๒ หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของงานระบบเครือข่ายและบริการอินเทอร์เน็ต กองเทคโนโลยีดิจิทัล เป็นรับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card หรือการแสกนนิ้วเข้าห้องควบคุมระบบเครือข่าย และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓.๕.๓ มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๓.๕.๔ มีการติดตั้ง Endpoint Security เพื่อเพิ่มประสิทธิภาพในการให้บริการเครื่องแม่ข่าย และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๓.๕.๕ มีเจ้าหน้าที่ของงานระบบเครือข่ายและบริการอินเทอร์เน็ต กองเทคโนโลยีดิจิทัล ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๓.๕.๖ มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๓.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ เจ้าหน้าที่แผนกต่างๆภายในองค์กร ขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์(Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๓.๖.๑ สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๓.๖.๒ วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๓.๗ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูลประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

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

๑) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)

๒) ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (www.ndwc.thaigov.go.th)

๓) กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม / แผ่นดินไหว (www.dmr.go.th)

๔) หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)

๕) กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการและแนวทางปฏิบัติ (www.disaster.go.th)

๓.๗.๒ การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

๑) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

๒) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน

๓) หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

๔) ปลากระโดดขึ้นมาจากผิวน้ำ

๓.๗.๓ การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

๑) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

๒) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุอุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

๓) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่มสำหรับบุคลากรขององค์กร

๔) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

๕) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๓.๗.๔ การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๑) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

๒) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคาร ดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๓.๗.๕ การปฏิบัติขั้นเตรียมการ

๑) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

๒) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย

๓) อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่บุคลากรในองค์กร

๔) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๘ การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

๓.๘.๑ จัดทำแผนเตรียมความพร้อมรับสถานการณ์การชุมนุมทางการเมืองด้านเทคโนโลยีสารสนเทศของกองเทคโนโลยีดิจิทัล มหาวิทยาลัยแม่โจ้

๓.๘.๒ จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ (Business Continuity Planning) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่มหาวิทยาลัยแม่โจ้ได้

๓.๘.๓ ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๓.๘.๔ จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้นและมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓.๘.๕ ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมระบบเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน

๓.๘.๖ ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๓.๘.๗ สำรองข้อมูล

๓.๘.๘ จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงานที่มหาวิทยาลัยแม่โจ้

๓.๘.๙ จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมคณะทำงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

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 ระดับปฏิบัติ

๔.๒.๑ **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

๔.๒.๒ **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

๔.๒.๓ **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

นายธีรวัฒน์ สุนทรีศิลปกรณ์ เบอร์โทรศัพท์ติดต่อ ๐๕๓-๘๗๓-๒๘๖

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

๔.๒.๔ **คณะกู้คืนระบบสารสนเทศเพื่อการเรียนการสอน**

มีหน้าที่ติดตั้ง กู้คืนระบบการเรียนการสอนให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

หัวหน้าควบคุม นายประวิทย์ วิมานทอง เบอร์โทรศัพท์ติดต่อ ๐๙๕-๗๒๗-๔๓๔๔
นางสาวสุมาลี สุพรรณนอก เบอร์โทรศัพท์ติดต่อ ๐๘๙-๔๓๕-๓๐๔๔
นางสาวศุภวรรณ สัจจากุล เบอร์โทรศัพท์ติดต่อ ๐๙๐-๓๑๘-๑๘๕๖
นางสาวมนสิชา มีแสงแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๙-๙๙๒-๑๗๓๖
นางอภิญญา โตสิตารัตน์ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๗๓๒-๔๒๑๗
นางสาวกรกช เจริญทรัพย์ เบอร์โทรศัพท์ติดต่อ ๐๘๙-๗๕๗-๓๗๗๗

๔.๒.๕ **คณะประเมินความเสียหาย**

มีหน้าที่ตรวจสอบและประเมินความความเสียหายทั้งด้าน Hardware และ Software พร้อมทั้งจัดทำรายงานความเสียหาย 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

๔.๒.๖ **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

๔.๒.๗ **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

๔.๒.๘ **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

๔.๒.๙ **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

๔.๒.๑๐ **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

๔.๒.๑๑ **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

๔.๒.๑๒ **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

๔.๒.๑๓ **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

๔.๒.๑๔ **คณะแก้ไขปัญหาเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล**

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการกองเทคโนโลยีดิจิทัลเพื่อทราบและสั่งการต่อไป 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

๕. ผังงานกระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

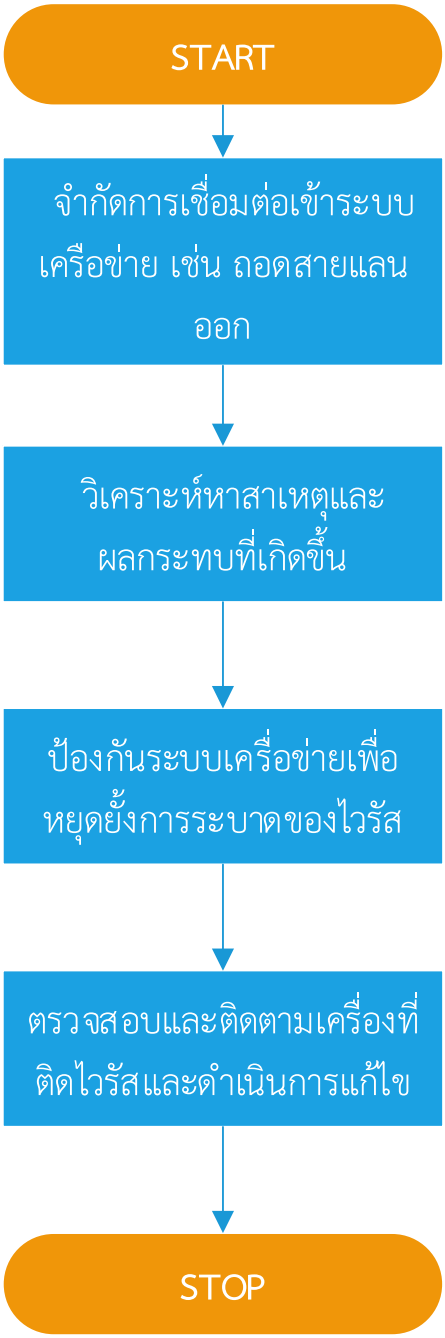
๕.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๕.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุให้เจ้าหน้าที่กองเทคโนโลยีดิจิทัล ทราบ หรือกรณีมีเหตุอันทำให้ระบบเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายอินเทอร์เน็ตได้ กองเทคโนโลยีดิจิทัลจะต้องประกาศให้ทุกคณะฯ/สำนักฯ / หน่วยงาน ทราบ

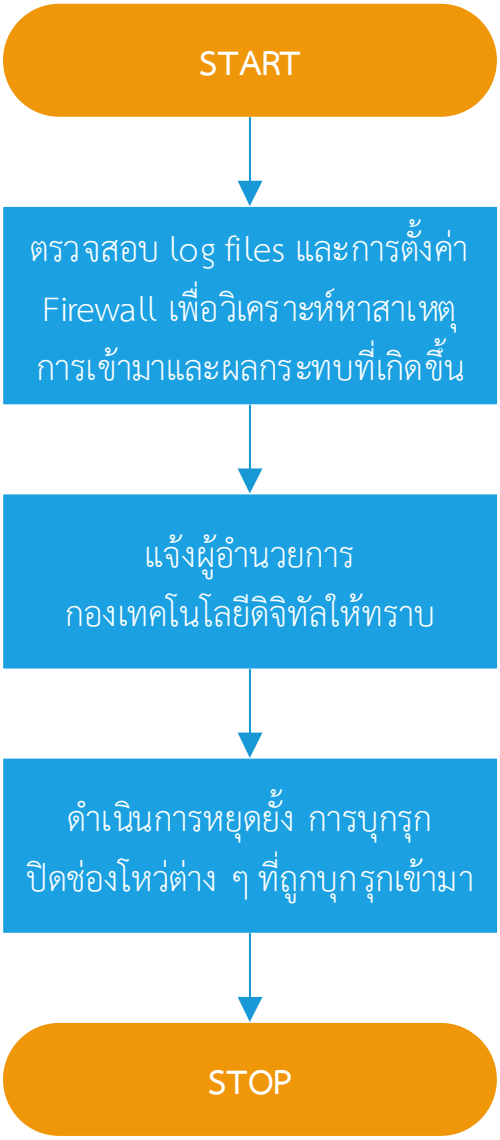
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



๕.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log files และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว

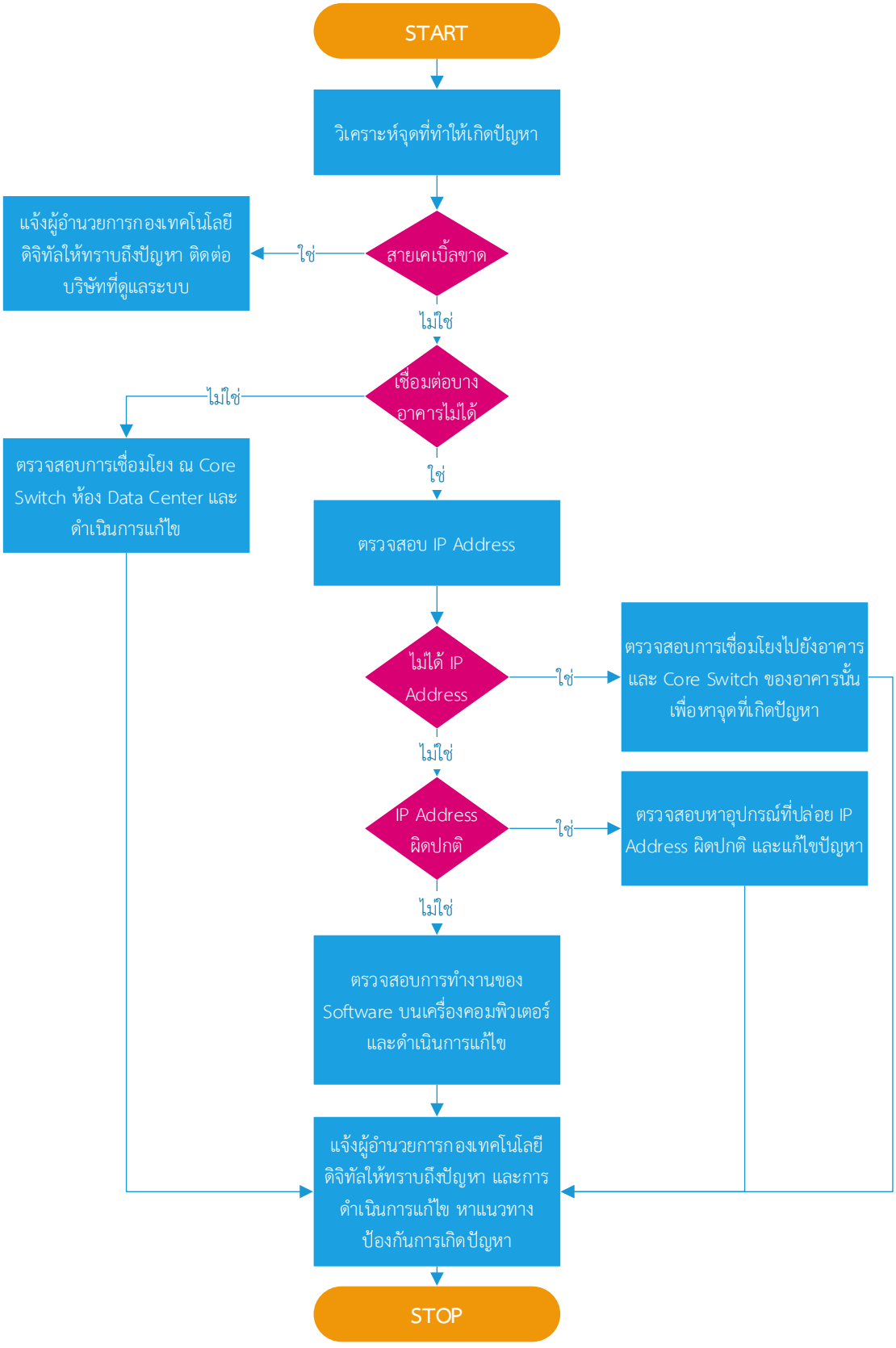


๕.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบแจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลพร้อมติดต่อบริษัทฯ ภายนอกเพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

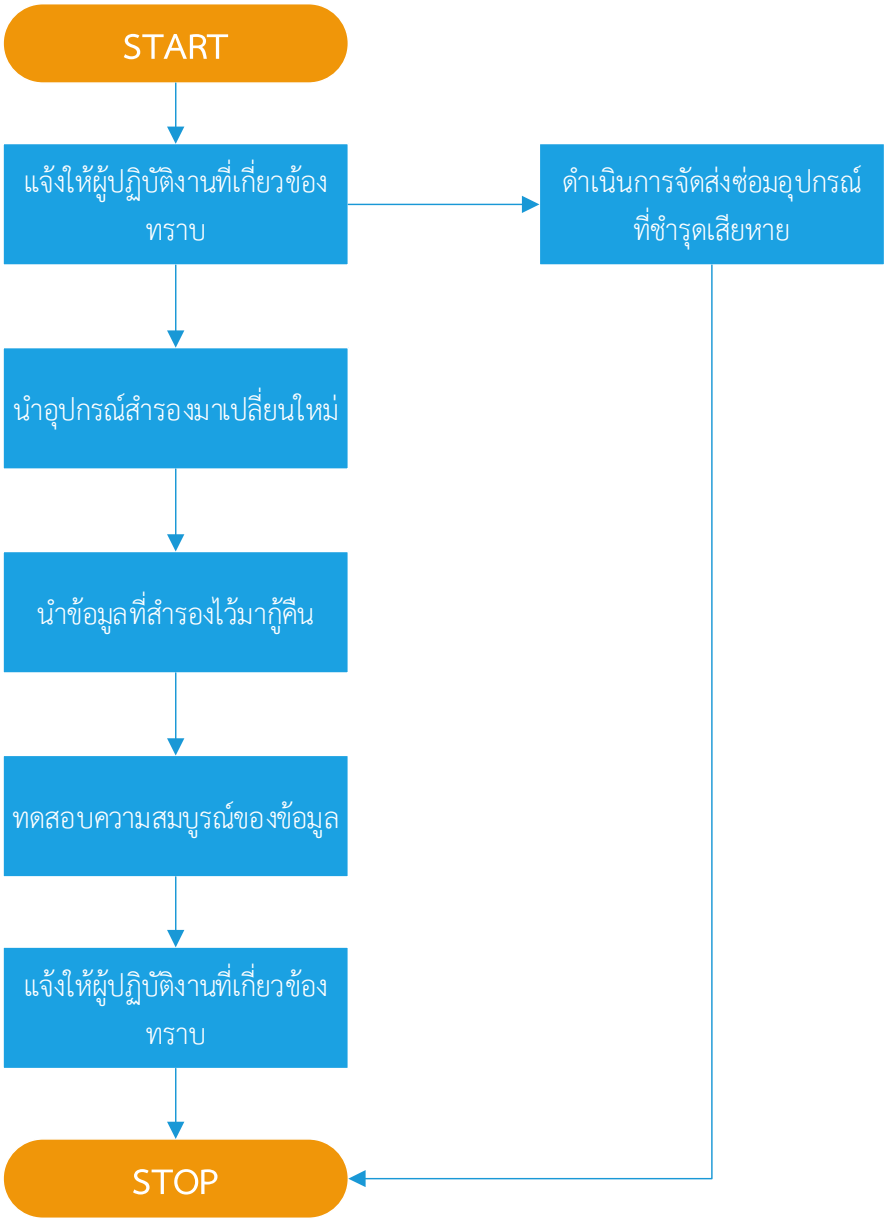
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



๕.๑.๔ กรณีอุปกรณ์หรือคอมพิวเตอร์ขัดข้อง

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์มาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

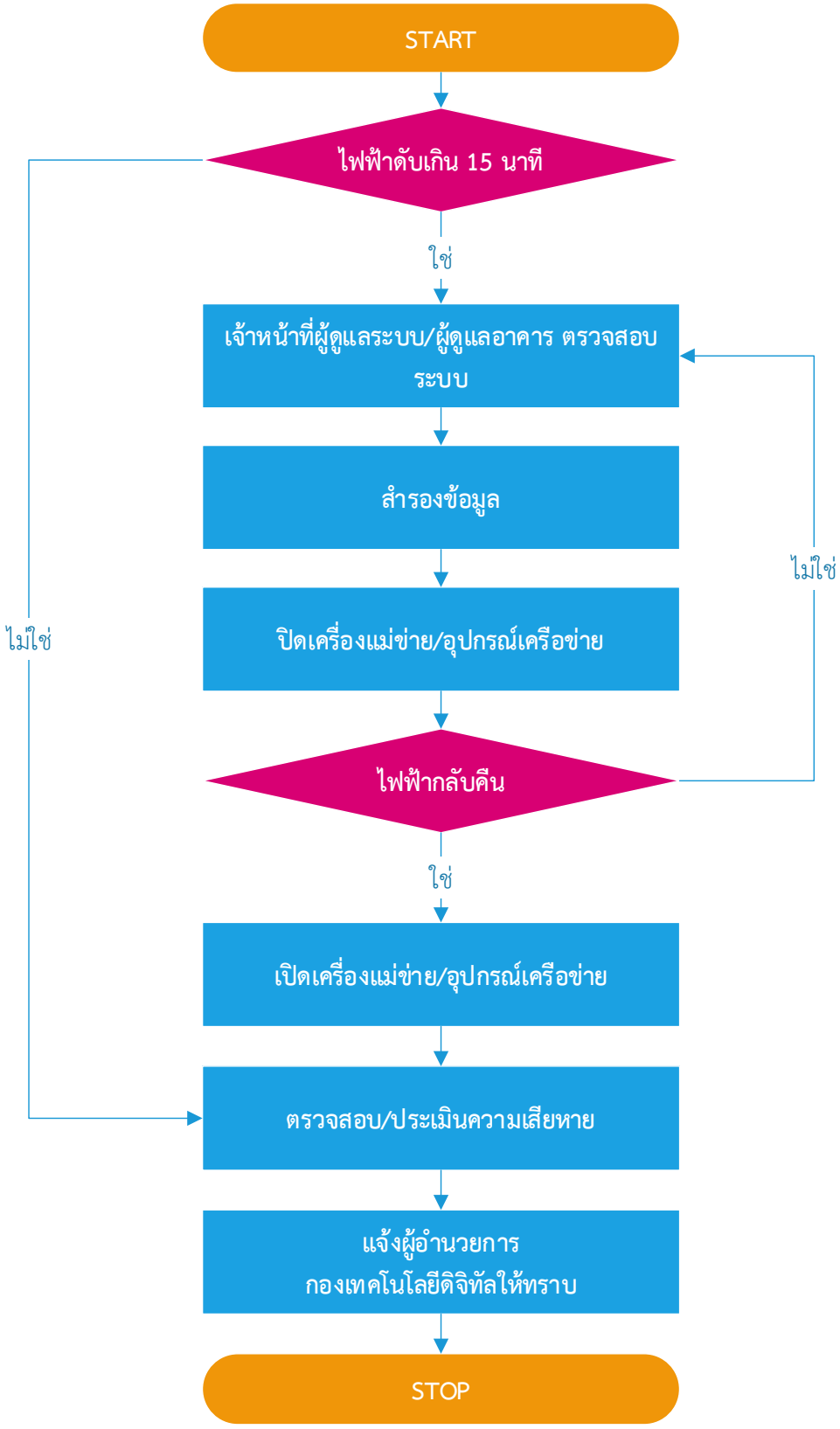
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



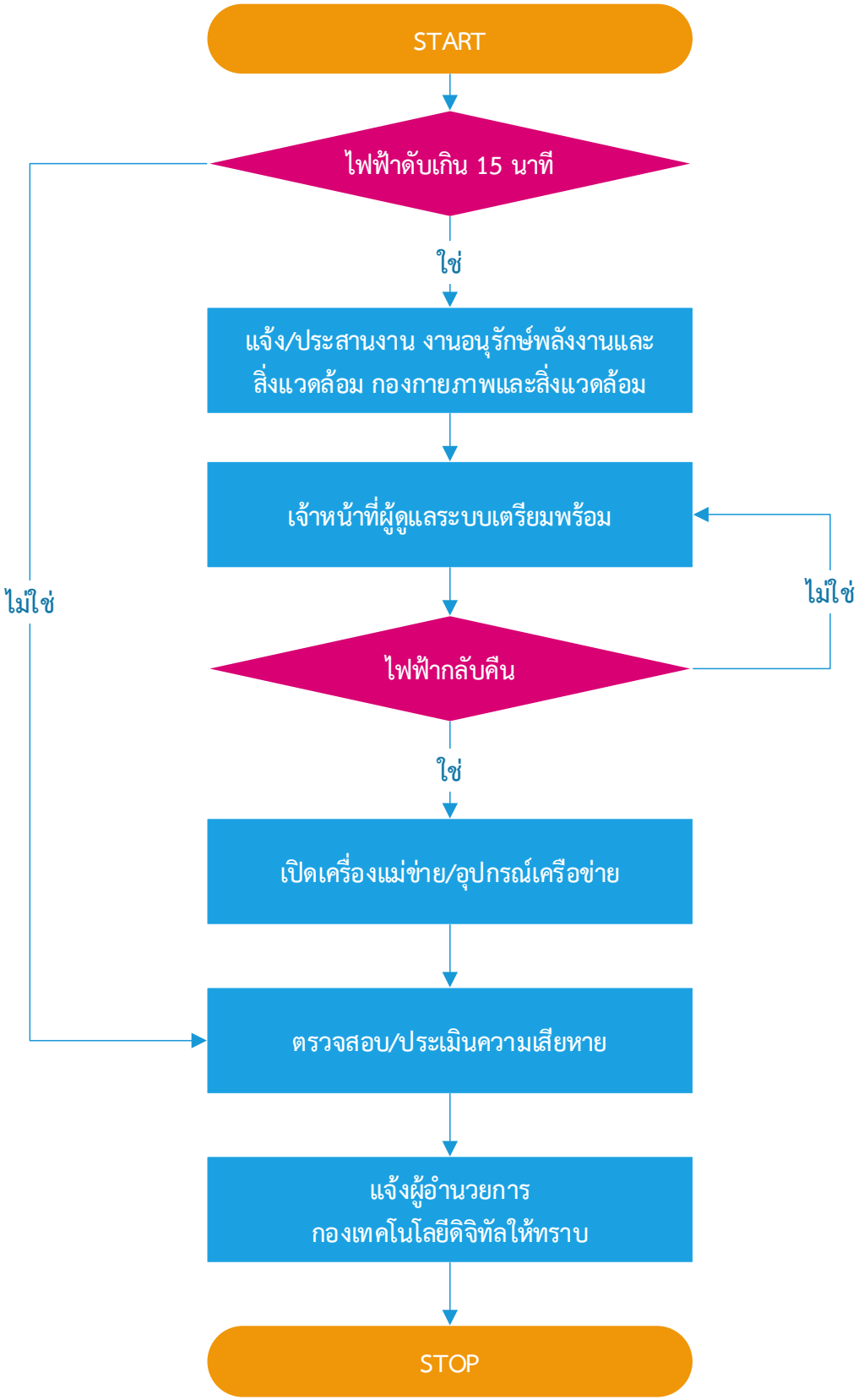
๕.๑.๕ กรณีไฟฟ้าขัดข้อง

- กองเทคโนโลยีดิจิทัลมีเครื่อง UPS สามารถสำรองกระแสไฟฟ้าได้ ๙๐-๑๒๐ นาที
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัล เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน
- ระบบสำรองไฟฟ้ามีการทดสอบการใช้งานของระบบทุก ๆ วันจันทร์ เวลา ๘.๓๐ น.
- ระบบสำรองไฟฟ้ามีการบำรุงรักษาและตรวจเช็คความพร้อมของอุปกรณ์ ทุก ๆ ๓ เดือน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าดับตามแผนตัดกระแสไฟฟ้ามหาวิทยาลัยแม่โจ้



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง/หม้อแปลงระเบิด

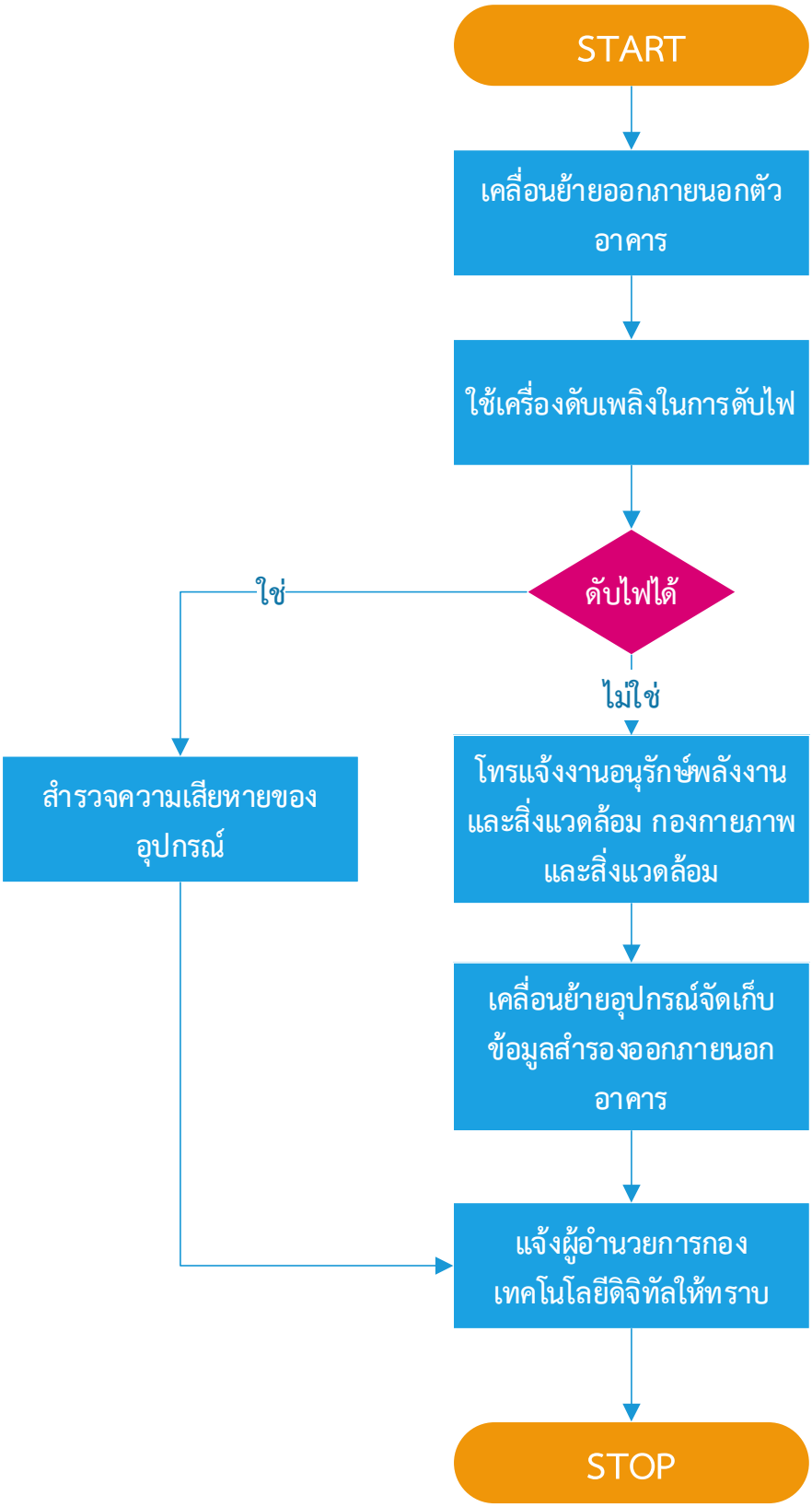


๕.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

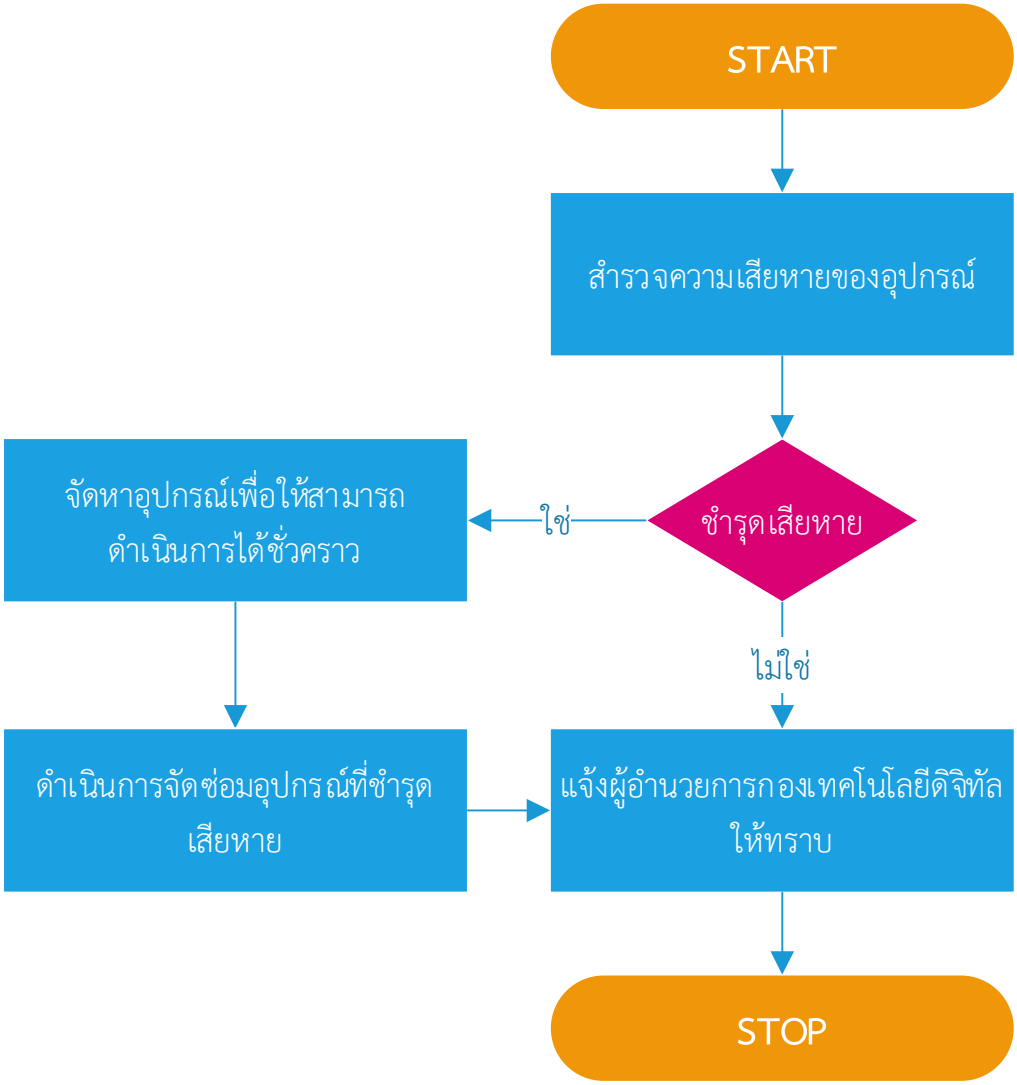
๕.๒.๑ กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้งงานระบบสาธารณูปโภค กองกายภาพและสิ่งแวดล้อม เบอร์ ๓๒๓๐ ทันที หรือผู้อำนวยการกองกายภาพและสิ่งแวดล้อม เบอร์ ๓๒๔๐
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การ
- ปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และ/หรือ ระบบดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑-๒ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



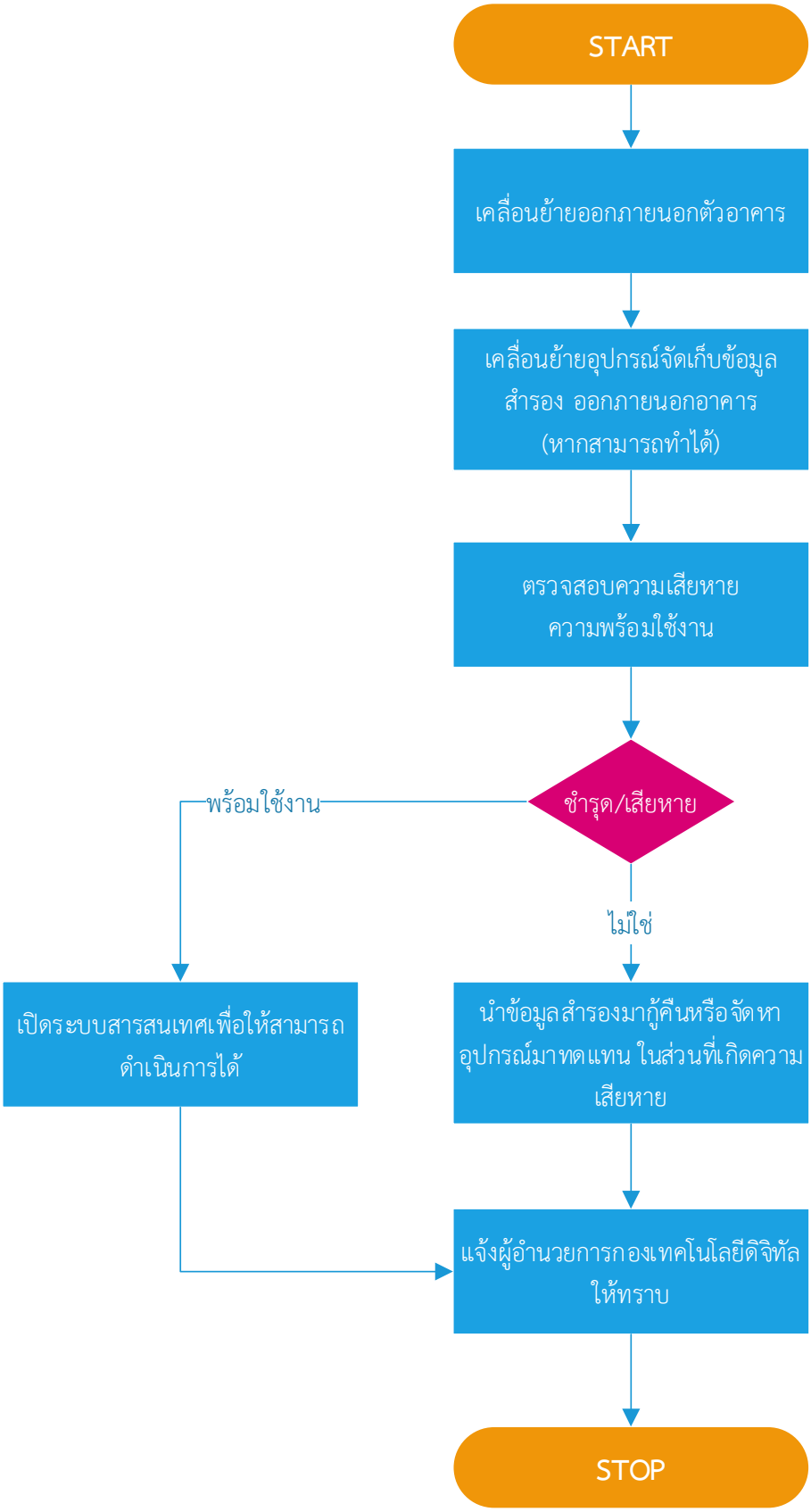
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้(ขณะไม่มีผู้ปฏิบัติงานอยู่)



๕.๒.๒ กรณีแผ่นดินไหว/อาคารถล่ม

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

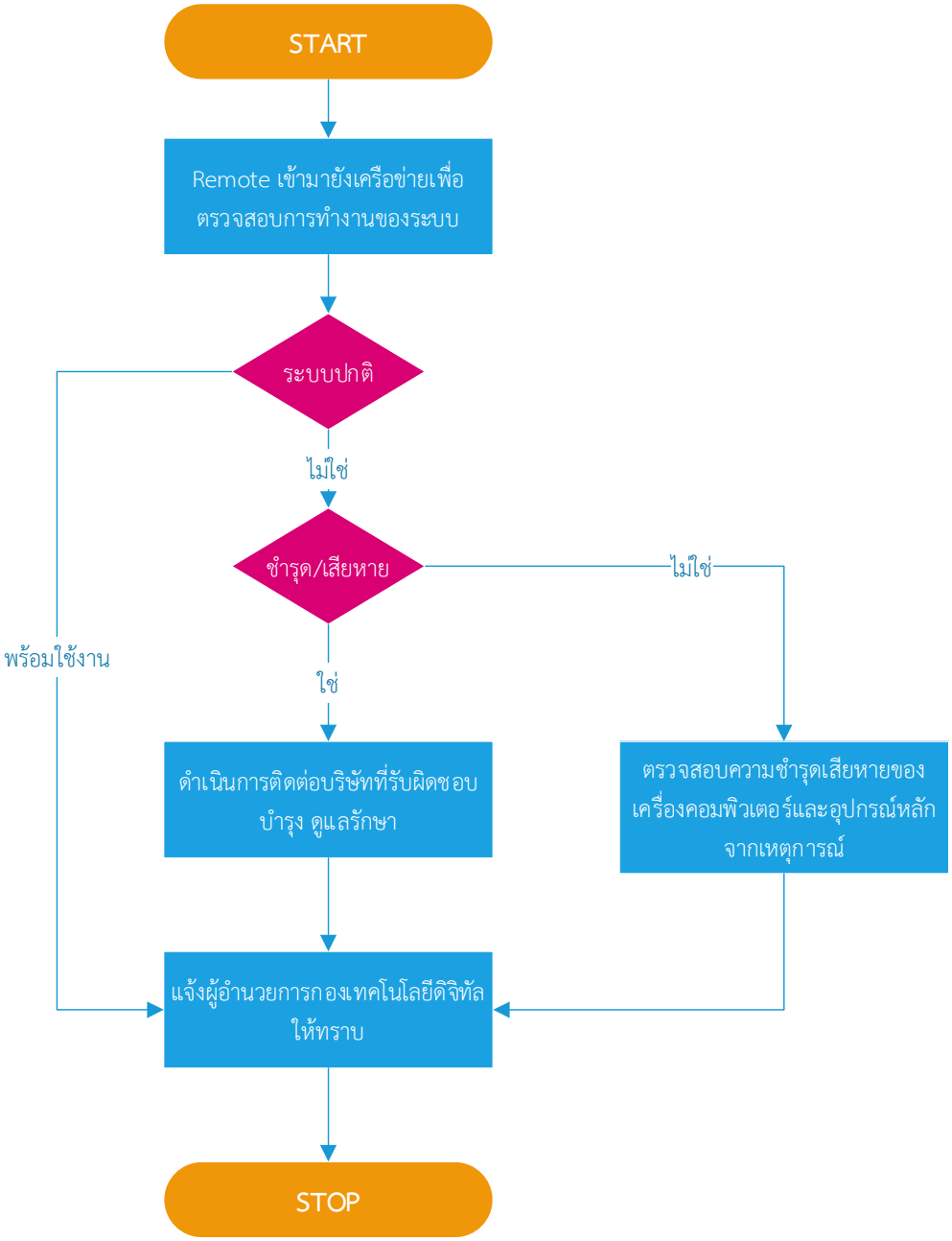


๕.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๕.๓.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดาเนินการได้ตามปกติ แจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลทราบ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สิน ตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้แจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลทราบพร้อมดำเนินการติดต่อบริษัทภายนอกดำเนินการซ่อมแซมแก้ไขหากจำเป็น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

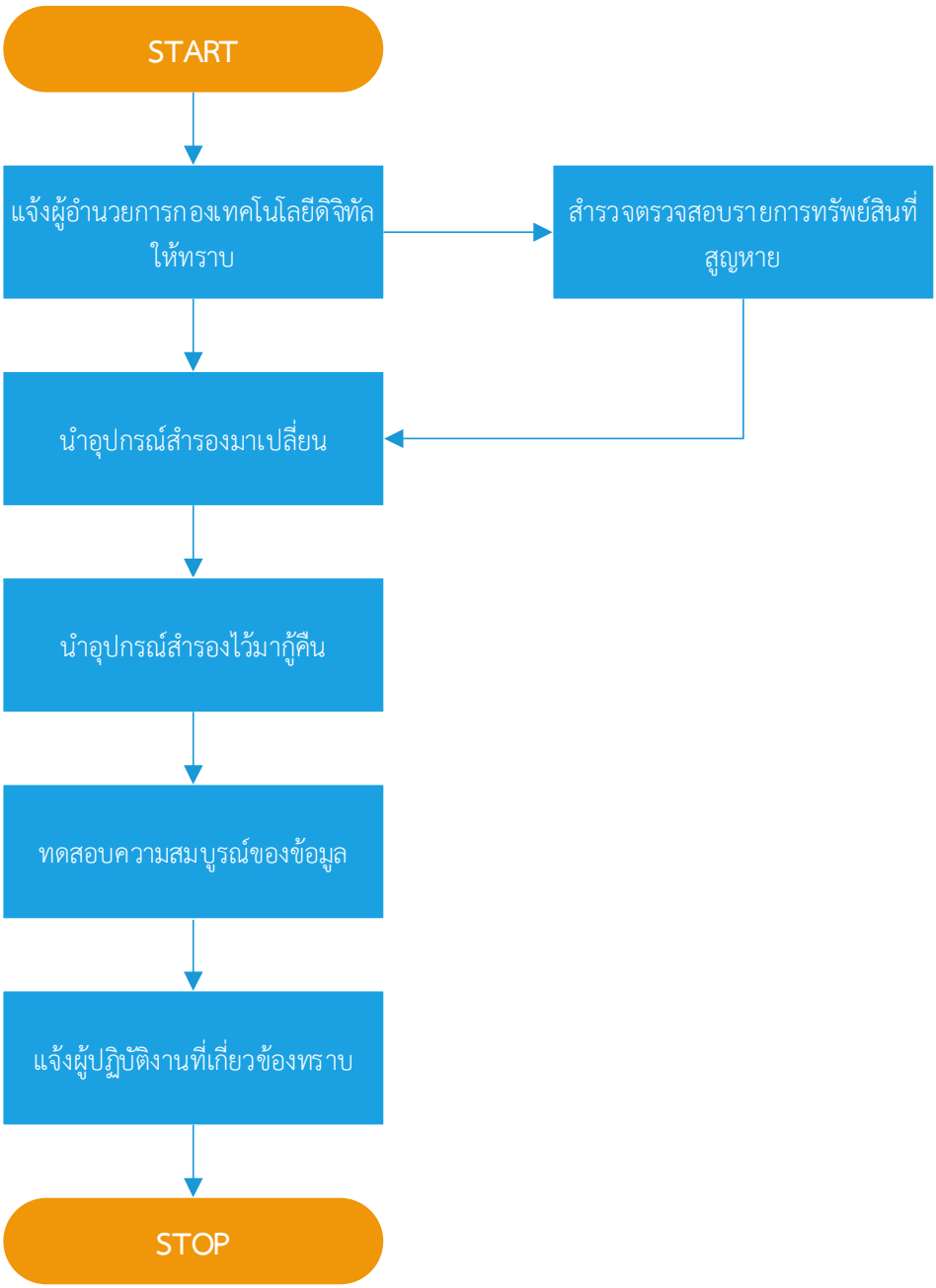


๕.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

๕.๔.๑ กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

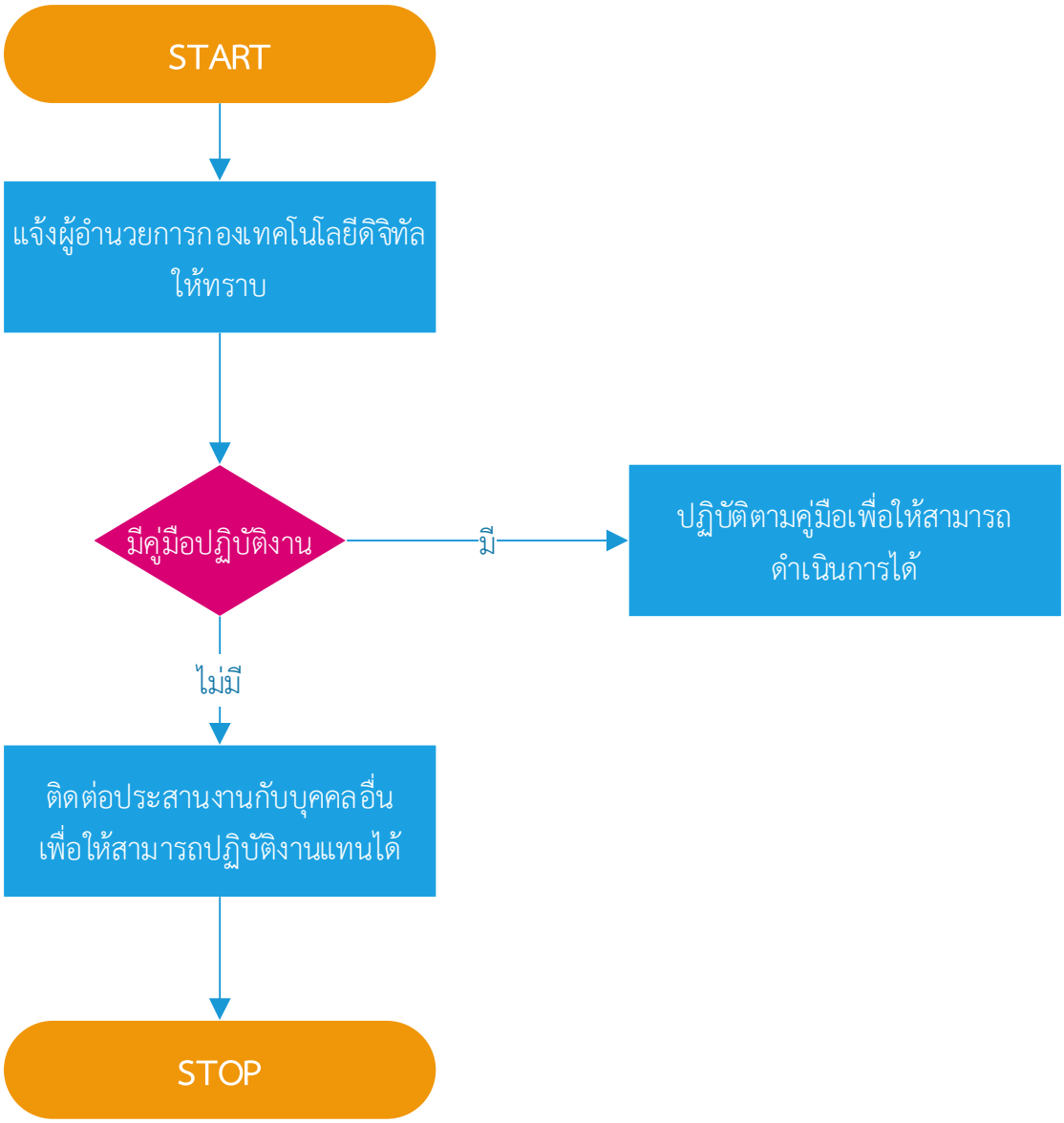
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



๕.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้อำนวยการกองเทคโนโลยีดิจิทัลทราบ
- ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



๖. การกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

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

๑. จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน
๒. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
๓. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง
๔. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้เป็นการชั่วคราว
๕. นำสื่อที่ได้สำรองข้อมูลไว้กลับมา Restore โดยเร็วภายใน ๔๘ ชั่วโมง
๖. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและ ระบบอื่นๆ ที่เกี่ยวข้อง

ผู้รับผิดชอบ

๑. ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของหน่วย (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๒. ระดับปฏิบัติ

เจ้าหน้าที่ผู้ดูแลระบบของหน่วย รับผิดชอบ กำกับ ดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้

๒.๑. ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ
๒.๒. ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ
๒.๓. ทีมกู้คืนแอพพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน
๒.๔. ทีมประเมินความเสียหาย เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน
๒.๕. ทีมอาคารสถานที่ เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร เครื่องปรับอากาศให้พร้อมใช้งาน
๒.๖. ทีมจัดการทั่วไป เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทำงาน
๒.๗. ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง
๒.๘. ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรอง ข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่
๒.๙. ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม
๒.๑๐. ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย

๒.๑๑. ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์

๒.๑๒. ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชา ดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการกองเทคโนโลยีดิจิทัลเพื่อทราบและสั่งการต่อไป

๒.๑๓. ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชา ดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลงให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการกองเทคโนโลยีดิจิทัล เพื่อทราบและสั่งการต่อไป

๗. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้ผู้อำนวยการกองเทคโนโลยีดิจิทัลทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป