แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (BUSINESS CONTINUITY PLAN :BCP) และ แผนกู้คืนระบบสารสนเทศ (DISASTER RECOVERY PLAN : DRP)

ศูนย์เทคโนโลยีสารสนเทศ
กลุ่มงานดิจิทัลการแพทย์
โรงพยาบาลธัญญารักษ์ขอนแก่น

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan :BCP) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP)

ศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานดิจิทัลการแพทย์
โรงพยาบาลธัญญารักษ์ขอนแก่น

คำนำ

ระบบเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศถือเป็นองค์ประกอบสำคัญในการดำเนินงานตามภารกิจของโรงพยาบาลธัญญารักษ์ขอนแก่น ซึ่งจำเป็นต้องได้รับการดูแลและป้องกันเพื่อให้เกิดความมั่นคงปลอดภัย และสามารถใช้งานได้อย่างมีประสิทธิภาพ

ศูนย์เทคโนโลยีสารสนเทศ กลุ่มงานดิจิทัลการแพทย์ โรงพยาบาลธัญญารักษ์ขอนแก่น ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศที่อาจได้รับผลกระทบจากปัจจัยภายนอกและภายใน ซึ่งอาจส่งผลให้ระบบเครือข่ายและอุปกรณ์เทคโนโลยีสารสนเทศได้รับความเสียหายและเกิดการหยุดชะงักในการให้บริการ จึงได้จัดทำแผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan :BCP) ขึ้นเพื่อเป็นแนวทางในการเตรียมความพร้อมและจัดการกับสถานการณ์ฉุกเฉินอย่างมีประสิทธิภาพ

แผนดังกล่าวมีวัตถุประสงค์เพื่อกำหนดแนวทางในการป้องกัน บรรเทาผลกระทบ และฟื้นฟูระบบเทคโนโลยีสารสนเทศให้สามารถกลับมาใช้งานได้โดยเร็ว ลดความเสี่ยงที่อาจเกิดขึ้น และรับประกันว่าการให้บริการของโรงพยาบาลสามารถดำเนินการได้อย่างต่อเนื่อง ทั้งนี้เพื่อสนับสนุนการให้บริการทางการแพทย์ที่มีคุณภาพและมีประสิทธิภาพต่อไป

สารบัญ

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan : BCP) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้น จึงได้จัดทำแผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan :BCP) และแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP) เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. แนวทางการป้องกันและเตรียมการเบื้องต้น
3. การเตรียมความพร้อม
4. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
5. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ
6. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
7. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
8. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
9. การติดตามและรายงานผล

โดยอธิบายรายละเอียดดังต่อไปนี้

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1. วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ ฯลฯ

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศ เสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

1.2. การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์ เหตุการณ์ต่างๆ (Security Log Management System) โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อนำมาสรุปเป็นข้อมูลต่อไป

สถานการณ์ หรือภาวะ ฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)			คะแนนรวม	จัดเรียงลาดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อประชาชน		
ไฟไหม้	5	5	5	15	1
โดนเจาะระบบ	5	5	5	15	2
ไฟฟ้าดับ	5	1	5	11	3
น้ำท่วม / น้ำรั่ว	4	2	4	10	4
จลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	2	3	4	9	5
สถานการณ์ทางการเมือง	2	2	4	8	6
พายุ	2	1	5	8	6
โรคระบาด	1	1	5	7	7
ภัยแล้ง	1	1	4	6	8

2. แนวทางการป้องกันและเตรียมการเบื้องต้น

2.1. การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติ ตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์ เทคโนโลยีสารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

2.2. กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุ ที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญ ต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

2.3. การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอกเพื่อใช้สำหรับการติดต่อ ทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

2.4. การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์ เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม antivirus/spyware
- แผ่น driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2.5. การสำรองข้อมูล (Backup)

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

2.6. การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบ คอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยองค์กรมีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy

2.7. การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

2.7.1. ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 30-60 นาที

2.7.2. เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

2.7.3. เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

2.8. การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

2.8.1 มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่ายหากจำเป็น ให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไปห้องควบคุมระบบเครือข่าย และมีการติดตั้ง กล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

2.8.2 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

2.8.3 มีเจ้าหน้าที่ดูแลระบบเครือข่ายทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

2.8.4 การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

3. การเตรียมความพร้อม

3.1. การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสียงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.1.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

3.1.2 ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้า และป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ 30 - 60 นาที

3.1.3 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และเครื่องสำรองไฟให้พร้อมพร้อมใช้อยู่เสมอ

3.1.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่อง คอมพิวเตอร์และอุปกรณ์ต่างๆ

3.1.5 ให้มีการสำรองฐานข้อมูลทุกวัน

3.2. การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆกำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.2.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

3.2.2 ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องต้น

3.2.3 ให้มีการสำรองฐานข้อมูลทุกวัน

3.3. การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม / น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.3.1. จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิด/น้ำรั่ว

3.3.2. มีการตรวจสอบระบบท่อนาประปา ฝ้าเพดานห้องควบคุมระบบเครือข่ายเพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

3.3.3. ให้มีการสำรองฐานข้อมูลทุกวัน

3.4. การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

3.4.1 ทำการติดตั้ง Firewall ซึ่งหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ขาย และป้องกันการบุกรุกจากบุคคลภายนอก

3.4.2 มีการติดตั้ง ซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client) อัพเดตโปรแกรมกำจัดไวรัส ทุก 1 เดือน เป็นอย่างน้อย (Update Patch)

3.4.3 ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนาวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

3.5 การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุกและภัยคุกคามทางคอมพิวเตอร์โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

3.5.1 กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

3.5.2 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

3.5.3 เจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

3.5.4 มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

3.6 การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบเจ้าหน้าที่แผนกต่าง ๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Sofware) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

3.6.1 สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

3.6.2 วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่าย คอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

3.7 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารขอมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อ จลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

3.7.1 ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

3.7.2 จัดเตรียมกาลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

3.7.3 ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

3.7.4 ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

4. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมทีมงาน และมอบหมายหนาที่ความรับผิดชอบอย่างชดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

4.1 ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการโรงพยาบาลธัญญารักษ์ขอนแก่น (CEO)
รองผู้อำนวยการด้านการแพทย์ โรงพยาบาลธัญญารักษ์ขอนแก่น
รองผู้อำนวยการด้านอำนวยการ โรงพยาบาลธัญญารักษ์ขอนแก่น
รองผู้อำนวยการด้านการพยาบาล โรงพยาบาลธัญญารักษ์ขอนแก่น
รองผู้อำนวยการด้านการพัฒนาระบบและสุขภาพ (CIO)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (Information Security Manager)

4.2. ระดับปฏิบัติ

ก) ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

นายนัฐพล ประชุมแสน เบอร์โทรศัพท์ติดต่อ 086-859-8742
ส.อ.นาวิน ศรีสอน เบอร์โทรศัพท์ติดต่อ 086-326-8627

ข) ทีมกู้คืนเครือข่าย

ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติผู้รับผิดชอบ ได้แก่

นายนัฐพล ประชุมแสน เบอร์โทรศัพท์ติดต่อ 086-859-8742
ส.อ.นาวิน ศรีสอน เบอร์โทรศัพท์ติดต่อ 086-326-8627

5. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศกำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

5.1 กรณีเครือลูกข่าย

5.1.1 ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณี เกิดจากศูนย์เทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศ ต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

5.1.2 กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น แก้ไขปัญหาได้ แจ้งเหตุขัดข้องให้ศูนย์สารเทศเพื่อแก้ไขปัญหาต่อไป

5.1.3 ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น แก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์สารเทศเพื่อแก้ไขปัญหาต่อไป

5.2 กรณีเครื่องแม่ข่ายบริการ (Server)

5.2.1 ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

5.2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ขายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

5.2.3 ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

5.2.4 ตรวจสอบปัญหาที่เกิดขึ้น ในกรณที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

5.2.5 กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

5.2.6 รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

5.2.7 ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

5.2.8 ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนาอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

5.2.9 ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยเร็วผู้ดูแลระบบ

6 กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

6.1 กรณีจากไฟไหม้ห้องควบคุมระบบ

6.1.1 ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

6.1.2 แจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์ ทางโทรศัพท์ 086-859-8742 และผู้มีหน้าที่รับผิดชอบทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เขาปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

6.1.3 เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศได้จัดหาไว้ดำาเนินการดับเพลิงและจัดการขนย้ายอุปกรณ์ ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัยได้แก่ หรือจุดร่วมพล

6.1.4 แจ้งสถานีดับเพลิงที่ใกล้ที่สุด ซึ่งในเขตคืองานป้องกันและบรรเทาสาธารณภัย เทศบาลเมืองศิลา 0 4323 5179 เพื่อดำเนินการต่อไป หรือ เบอร์โทรศัพท์ 199

6.1.5 ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ แก่ผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศ เพื่อทราบและสั่งการต่อไป

6.1.6 ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเขาตรวจสอบระบบและอุปกรณ์ ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์ และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

6.2 กรณีไฟดับ / หม้อไฟระเบิด

6.2.1 ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์ จะต้องแก้ไขระบบไฟฟ้าในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ

6.2.2 แจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์ ทางโทรศัพท์ 086-859-8742 และผู้มีหน้าที่รับผิดชอบทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

6.2.3 ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 080-263-4333 แก่ผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศ เพื่อทราบและสั่งการต่อไป

6.2.4 ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

6.3 กรณีน้ำท่วมห้องควบคุมระบบ

6.3.1 ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศจัดหาไว้ มาดำเนินการป้องกันมิให้เกิดความเสียหายใน เบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังอาคารผู้ป่วยนอก ชั้น 2, พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ

6.3.2 แจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์ ทางโทรศัพท์ 086-859-8742 และผู้มีหน้าที่รับผิดชอบทราบและดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานเพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

6.3.3 ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 080-263-4333 แก่ผู้อำนวยการศูนย์เทคโนโลยี สารสนเทศ เพื่อทราบและสั่งการต่อไป

6.3.4 ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำ รายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

6.4 กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

6.4.1 ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบประกอบด้วย

นายนัฐพล ประชุมแสน	เบอร์โทรศัพท์ติดต่อ	086-859-8742
ส.อ.นาวิน ศรีสอน	เบอร์โทรศัพท์ติดต่อ	086-326-8627

6.4.2 แจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์ ทางโทรศัพท์ 086-859-8742 เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้า ควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

6.4.3 ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 080-263-4333 แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป

6.4.4 ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำ รายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานดิจิทัลการแพทย์และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

1) ควบคุมสถานการณ์

ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

2) วิเคราะห์การถูกโจมตี

ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่นๆ

ข) วิเคราะห์ล็อคไฟล์ (Log file) ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้

ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

3) กู้คืนระบบคอมพิวเตอร์

ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดให้

ข) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ด หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

6.5 กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

6.5.1 ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ

6.5.2 เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บงคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชาทราบ

6.5.3 หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควร แก่กรณีดังนี้

ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจราจล

6.5.3.1 แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของผู้ปฏิบัติงานและของโรงพยาบาล

6.5.3.2 เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า

6.5.3.3 ปิดประตูทั้ง 2 ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาใน โรงพยาบาลธัญญารักษ์ขอนแก่น

6.5.3.4 กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของ โรงพยาบาลธัญญารักษ์ขอนแก่น ให้แจ้งไปยังสถานีตำรวจนครบาล หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้อำนวยการ สำนักอำนวยการเพื่อทราบ

ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

6.5.3.5 เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที

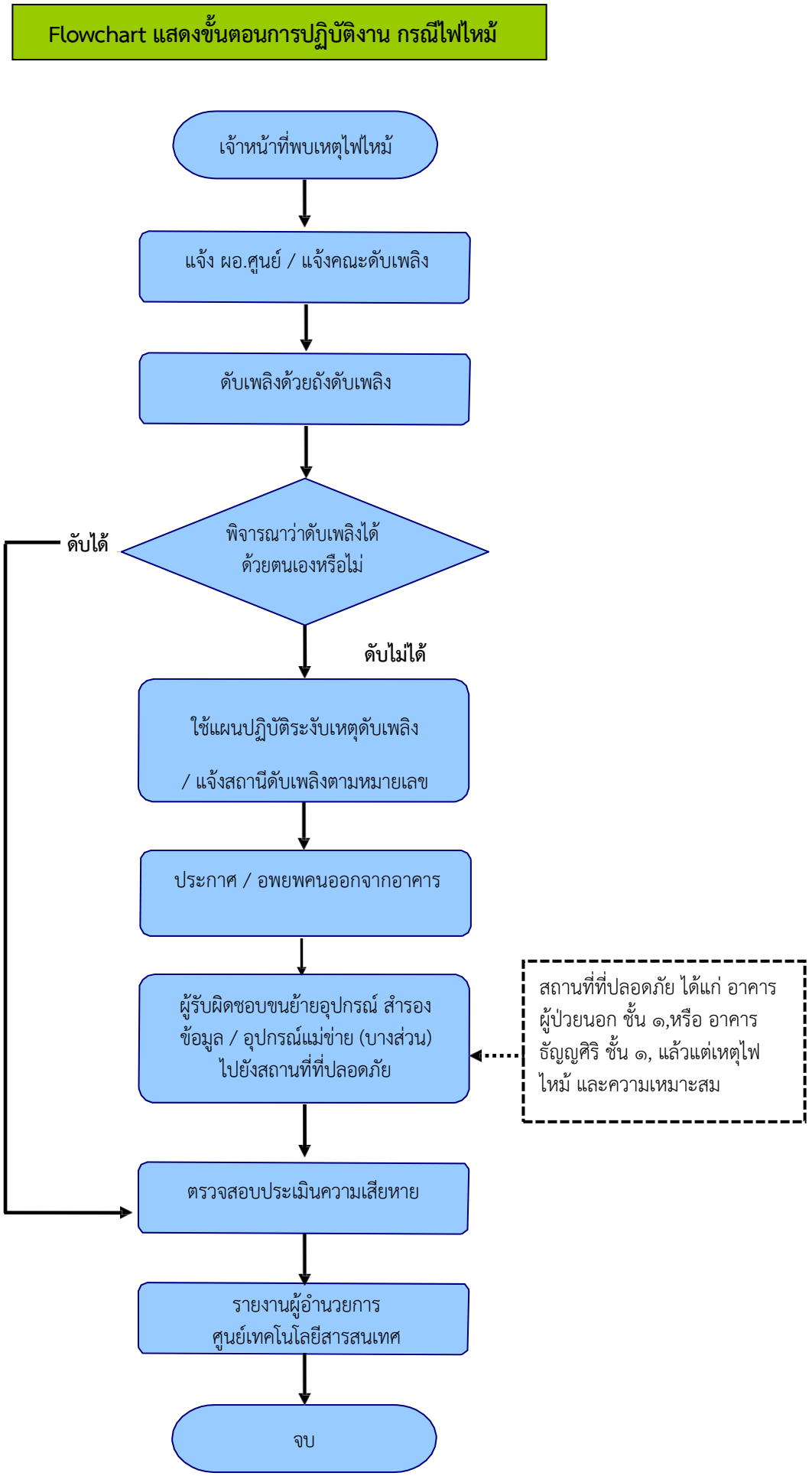
6.5.3.6 รปภ. หรือเจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ พร้อมทั้งติดต่อเจ้าหน้าที่ ตำรวจในพื้นที่มาตรวจสอบวัตถุต้องสงสัย

6.5.3.7 ในกรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกันพื้นที่อันตรายที่พบวัตถระเบิดกันบุคคลที่ไม่เกี่ยวข้อง ออกจากบริเวณที่พบวัตถุระเบิด และแจ้งอพยพผู้ปฏิบัติงานออกจากบริเวณหรือรัศมีของวัตถุระเบิด

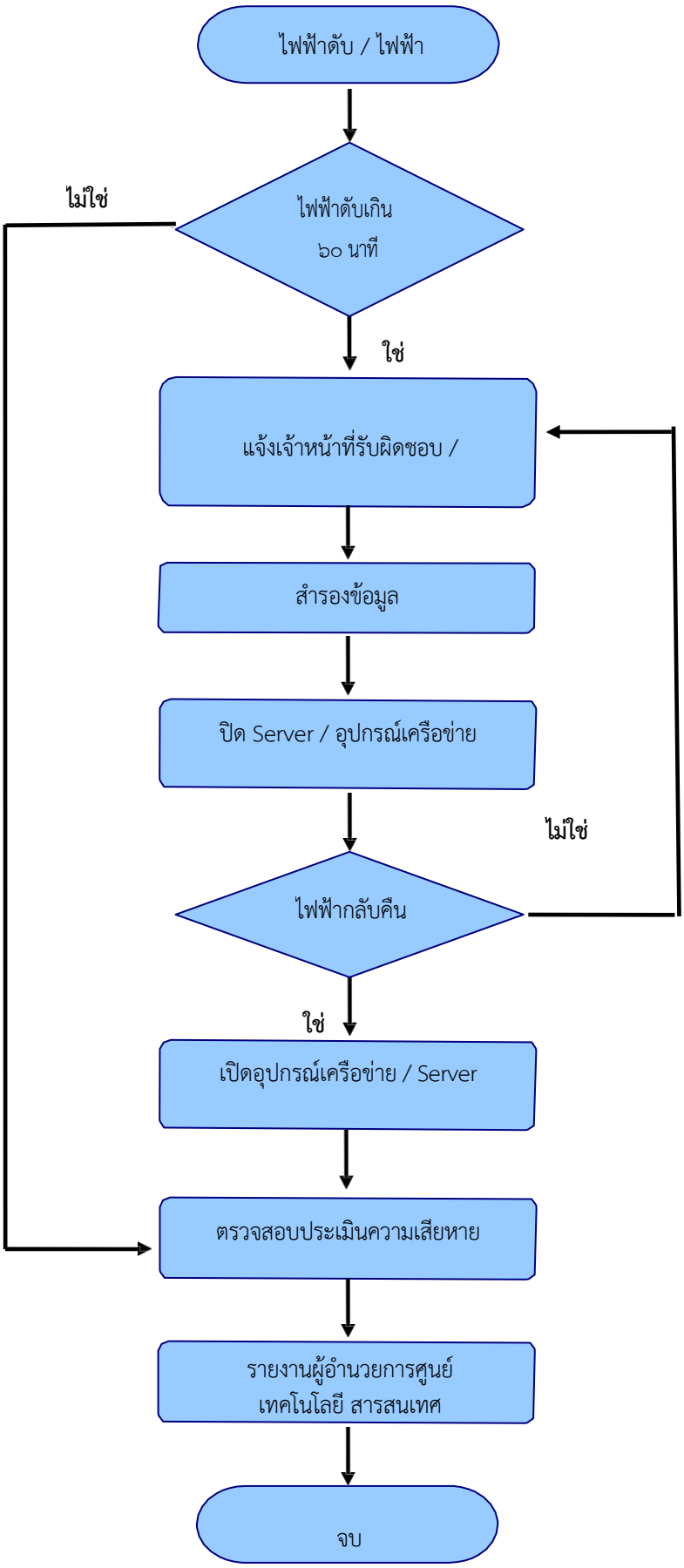
6.5.3.8 เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้าน อย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศผ่านทางโทรศัพท์ 080-263-4333 เพื่อทราบและสั่งการต่อไป

6.5.3.9 ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหายเพื่อแจ้งผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศทราบ

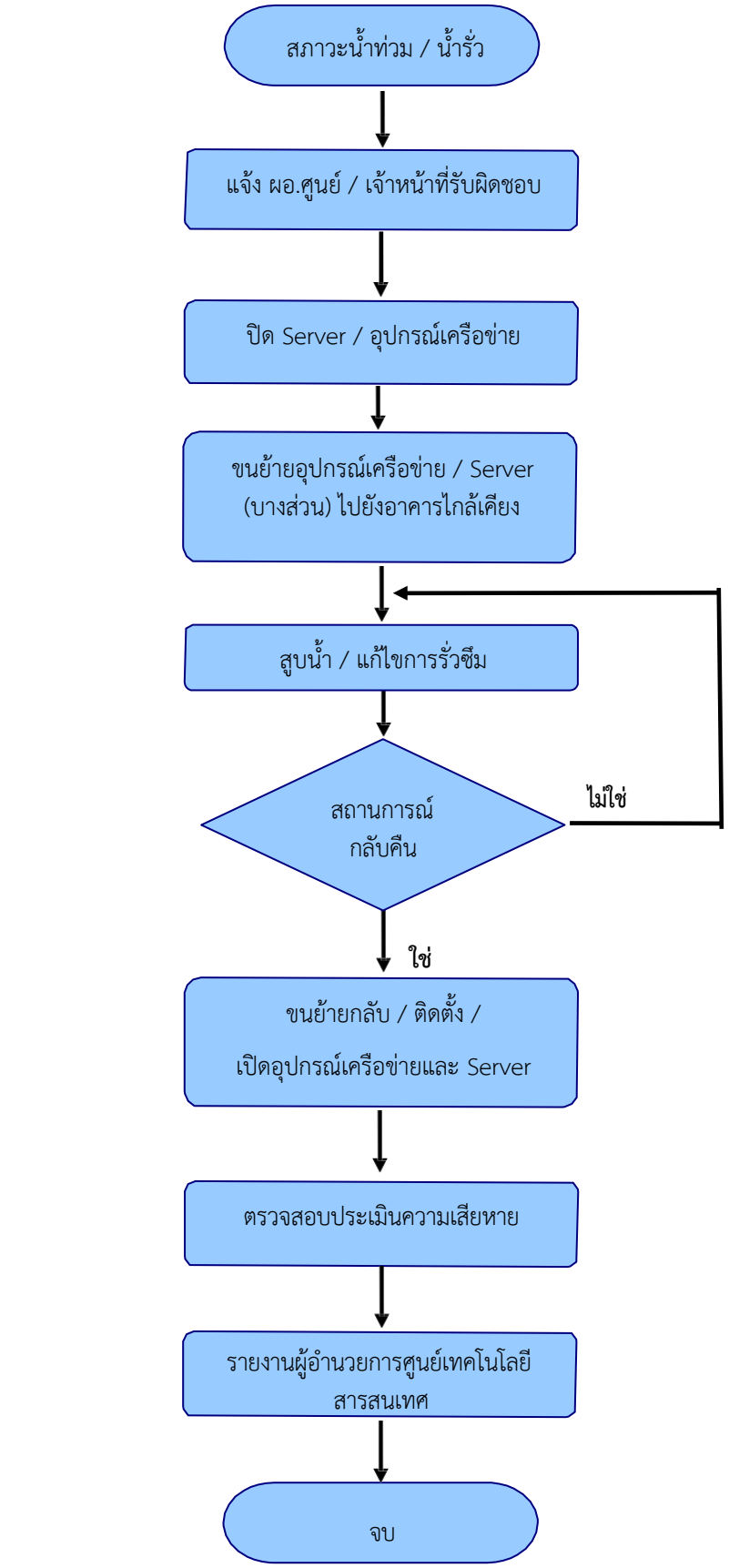
4) ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ



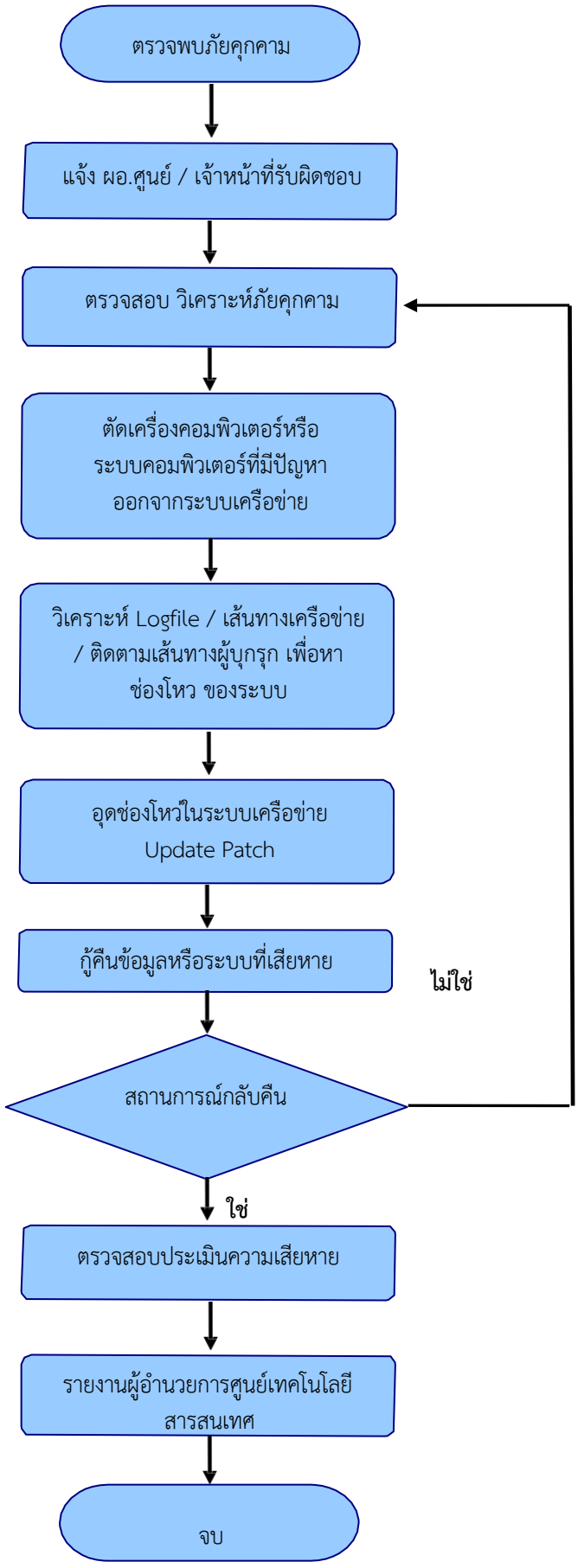
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีไฟฟ้าดับ / ไฟฟ้ากระชาก / หม้อไฟระเบิด



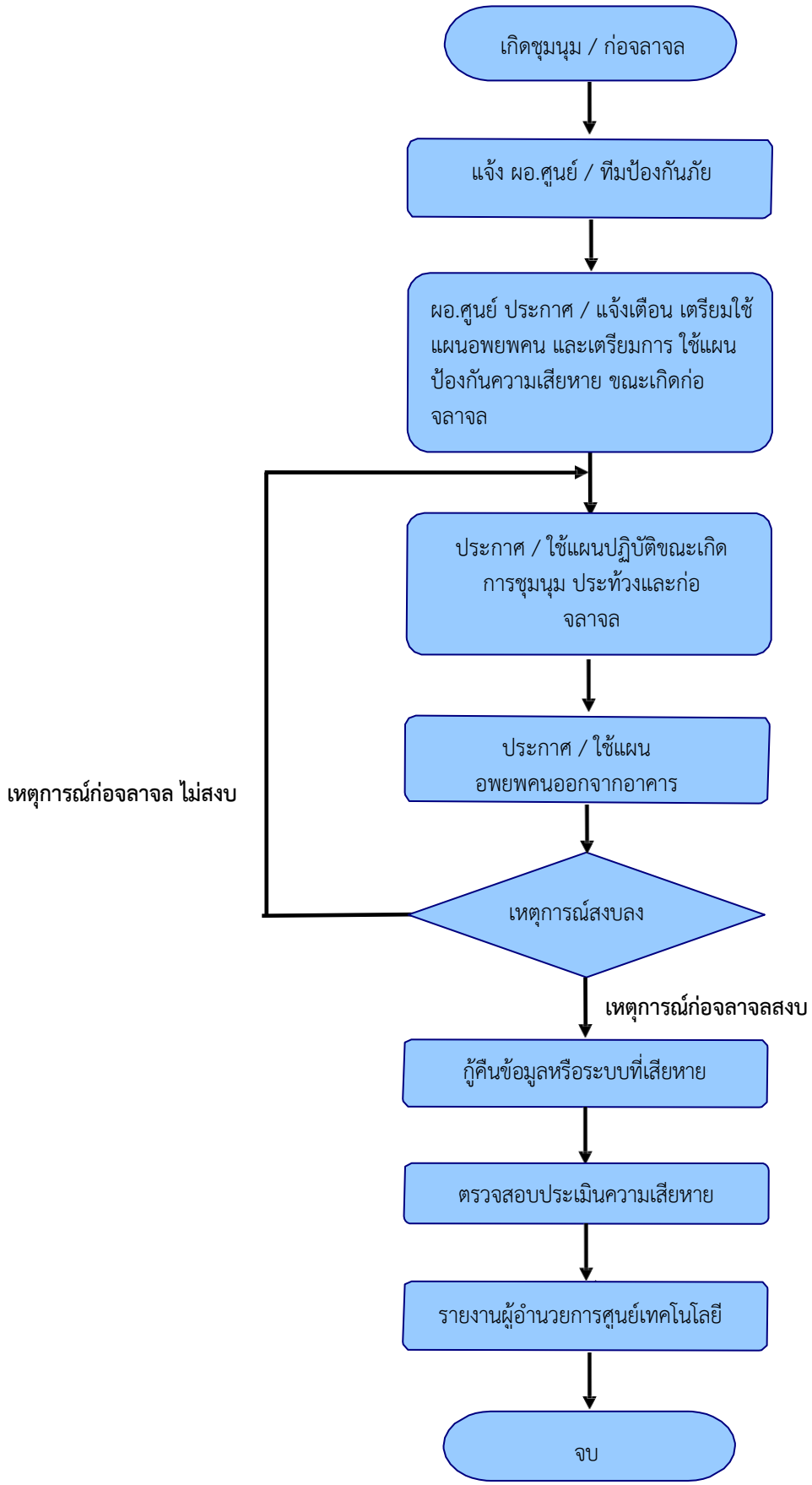
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีน้ำท่วม



Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม



Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



7 แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (**System Recovery)** โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบ เสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

7.1 จัดหาอุปกรณ์ชิ้นส่วนให้เพื่อทดแทน

7.2 เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

7.3 ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

7.4 ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

7.5 นำ **BACKUP TAPE / CD-ROM / HARDDISK** ที่ได้สำรองข้อมูลไว้นำกลับมา **Restore** โดยใช้ทีมกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน **48** ชั่วโมง

7.6 ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่ เกี่ยวข้อง จากภัยพิบัติดังกล่าวไม่เฉพาะทาง **Hardware** เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ หน่วยงานจึงมีแผนจัดทำการสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มี ความต่อเนื่องอยู่เสมอ โดยแบ่งไซต์ ได้ **3** ไซต์ คือ

7.6.1 **Hot Site** เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลัก มีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำที่สูง

7.6.2 **Warm Site** เป็นไซต์ที่คล้ายกับ **Hot site** แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่ำกว่า **Hot site** ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า **Hot site**

7.6.3 **Cold Site** เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง **Hardware** และ **Software** ในการกู้คืนมีต้นทุนการจัดทำต่ำ แต่ระยะเวลาในการกู้คืนนาน

แผนการดำเนินการ

1. สำรวจความต้องการของระบบสำรอง

2. สำรวจไซต์สำรองที่เหมาะสม

3. การประเมินความเสี่ยงจากสิ่งต่างๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง

4. การจัดลำดับผลกระทบขององค์กร

5. การจัดทำแผนกู้คืน

6. การวางแผน การแต่งตั้งทีมงาน ลำดับการทำงานหลังระบบได้รับความเสียหาย

7. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่ รวมถึงการฝึกอบรมทางด้านเทคนิค

8. การทดสอบแผน อาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง

9. การปรับปรุงแผนการกู้คืน

8 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (**Information Security Manager)** ทราบ เพื่อนำเสนอรายงานสรุปให้ **CEO** หรือ **CIO** เป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณี ตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัย