



แผนรับสถานการณ์ฉุกเฉิน จากภัยพิบัติระดับเทคโนโลยีสารสนเทศ



โรงพยาบาลพนมเปญ

สารบัญ

บทที่	หน้า
1. คำนิยาม	1
2. วัตถุประสงค์.....	2
3. ผู้รับผิดชอบ.....	2
4. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ	2
5. แนวทางการป้องกันและเตรียมการเบื้องต้น	3
6. การเตรียมความพร้อม	6
7. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน.....	9
8. มาตรการในการป้องกันและแก้ไขปัญหากลภัยพิบัติ	12
9. กระบวนการแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูล และ สารสนเทศ	13
10. ผัง Flowchart กระบวนการแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ.....	20
11. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)	26
12.การติดตามและรายงานผล	27

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมี ปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์ เสียหายได้

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหา ที่อาจส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

1. คำนินยาม
2. วัตถุประสงค์
3. ผู้รับผิดชอบ
4. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
5. แนวทางการป้องกันและเตรียมการเบื้องต้น
6. การเตรียมความพร้อม
7. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
8. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ
9. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
10. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ
11. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม
12. การติดตามและรายงานผล

โดยอธิบายรายละเอียดดังต่อไปนี้

1. คำนินยาม

“สำนักงานฯ” หมายความว่า ห้องงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

“ภัยพิบัติ” หมายความว่า ภัยที่ก่อให้เกิดความเสียหายต่อชีวิต และทรัพย์สิน โดยส่งผลกระทบต่อภาวะเศรษฐกิจ และวิถีชีวิตของผู้นคนในสังคมทั้งในระยะสั้น และระยะยาว ภัยพิบัติแบ่งเป็น 2 ประเภท คือ ภัยพิบัติทางธรรมชาติ และภัยพิบัติที่มนุษย์สร้างขึ้น

“ภัยพิบัติทางธรรมชาติ” หมายความว่า ภัยที่มีสาเหตุมาจากธรรมชาติ อาทิ แผ่นดินไหว อุทกภัย อัคคีภัย พายุ การระเบิด โดยการระเบิดที่กล่าวถึงนี้คือการระเบิดของแก๊สที่มีความไวไฟสูงที่ธรรมชาติปล่อยออกมาสู่ภายนอก นอกจากนี้ภัยพิบัติทางธรรมชาติยังรวมถึงภัยจากนอกโลกด้วย เช่น อุกกาบาต

“ภัยพิบัติที่มนุษย์สร้างขึ้น” หมายความว่า ภัยพิบัติที่มีสาเหตุจากมนุษย์ เช่น การปล่อยก๊าซเรือนกระจก ปริมาณมากจากโรงงานอุตสาหกรรมจนส่งผลให้ระดับน้ำทะเลเพิ่มสูงขึ้นและท่วมพื้นที่ในระดับต่ำ การเปลี่ยนทาง

น้ำจนทำให้เกิดภัยแล้งในบางพื้นที่ เป็นต้น รวมถึงการจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ และการเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ที่มนุษย์เป็นผู้กระทำ

“เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์” หมายความว่า ผู้ใช้งานประจำเครื่อง นั้นๆ

2. วัตถุประสงค์

- 2.1 เพื่อใช้เป็นแนวทางการรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของโรงพยาบาลเมืองจันทร์
- 2.2 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติ ในการดูแลรักษาความปลอดภัยของ ฐานข้อมูล และสารสนเทศของโรงพยาบาลเมืองจันทร์
- 2.3 เพื่อเป็นแนวทางในการรักษาความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและ มีความพร้อมสำหรับการใช้งาน
- 2.4 เพื่อให้การปฏิบัติเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทัน่วงทีกรณีเกิดเหตุการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อสารสนเทศ
- 2.5 เพื่อให้สอดคล้องตามนโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โรงพยาบาล โพนทราย

3. ผู้รับผิดชอบ

- 3.1 ผู้บังคับบัญชา
- 3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย
- 3.3 ผู้ใช้งาน

4. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

4.1 วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้ เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

- ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของ เครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ
- ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อบริเวณอินเทอร์เน็ตเกิดความขัดข้อง
- ง) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ
- จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
- ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

- ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- ข) ไวรัสมัลแวร์คอมพิวเตอร์จากผู้ใช้งานภายในองค์กร
- ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

4.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและ

วิเคราะห์เหตุการณ์ต่างๆ (Security Log Management System) โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อนำมา สรุปเป็นข้อมูลต่อไป

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)			คะแนนรวม	จัดเรียงลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อประชาชน		
ไฟไหม้	5	5	5	15	1
โดนเจาะระบบ	5	3	5	13	2
ไฟฟ้าดับ	5	1	5	11	3
น้ำท่วม / น้ำรั่ว	4	2	4	10	4
แผ่นดินไหว	4	1	5	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

5. แนวทางการป้องกันและเตรียมการเบื้องต้น

5.1 การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้ เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคน รับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการ

ศูนย์ เทคโนโลยีสารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณา และประกาศใช้แผนต่อไป

5.2 กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

5.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับ หน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อ ทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่ อาคารและเส้นทางเดินทาง

5.4 การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่ จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้โดยเตรียมอุปกรณ์ดังนี้

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

5.5 การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูลโดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยองค์กรมี นโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

5.6 การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่อง คอมพิวเตอร์ลูกข่าย ที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นต้องระมัดระวังในการใช้งานระบบ คอมพิวเตอร์ โดยเฉพาะในการเชื่อมต่อกับอินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือ ทำลายระบบได้ โดยองค์กรมีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

5.7 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

- 1) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิด ขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนเครื่อง คอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 30 - 60 นาที
- 2) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
- 3) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

5.8 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

- 1) มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบพาเข้าไป เจ้าหน้าที่ทุกคนต้องสแกนลายนิ้วมือ เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิด เพื่อป้องกันการโจรกรรม
- 2) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา
- 3) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กรและกั้นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัย ต่อระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์
- 4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต ขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบ สารสนเทศมีความถี่ใน การเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป
- 5) การดำเนินการตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

5.9 การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นดินไหว โดยเตรียมอุปกรณ์ดังนี้

- 1) เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ
- 2) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- 3) ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า
- 4) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง
- 5) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง
- 6) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วน ของแต่ละชั้นหรือหน่วยงาน

6. การเตรียมความพร้อม

6.1 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหามาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

6.1.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไพระเปิด

6.1.2 ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 30 - 60 นาที

6.1.3 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

6.1.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

6.1.5 ให้มีการสำรองฐานข้อมูลทุก 1 เดือนเป็นอย่างน้อย

6.2 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหามาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

6.2.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

6.2.2 ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่าย เพื่อการควบคุมเพลิงในเบื้องต้น

6.2.3 ให้มีการสำรองฐานข้อมูลเดือนละ 1 ครั้งเป็นอย่างน้อย

6.3 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม / น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหามาจากสถานการณ์น้ำท่วม / น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

6.3.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม / น้ำรั่ว

6.3.2 มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

6.3.3 ให้มีการสำรองฐานข้อมูลเดือนละ 1 ครั้งเป็นอย่างน้อย

6.4 การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

6.4.1 ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

6.4.2 มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

6.4.3 อัปเดตโปรแกรมกำจัดไวรัส ทุก 1 เดือน เป็นอย่างน้อย (Update Patch)

6.4.4 ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

6.5 การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์โจมตี ระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

6.5.1 กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

6.5.2 หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่ายจะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบพาเข้าไปที่ ประตูเข้า-ออก และคอยกำกับดูแลตลอดการปฏิบัติงานสำหรับประตูเข้า-ออก มีการติดตั้ง ระบบ Access Control โดยการใช้การสแกนลายนิ้วมือ และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อ ป้องกันการโจรกรรม

6.5.3 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

6.5.4 มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

6.5.5 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ ผิดปกติ เพื่อจะได้สืบหาสาเหตุและป้องกันต่อไป

6.5.6 มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

6.6 การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบเจ้าหน้าที่แผนกต่างๆ ภายใน องค์กร ขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

6.6.1 สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

6.6.2 วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

6.7 การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

6.7.1 ติดตามข้อมูลข่าวสารเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมาย ที่เกี่ยวข้องเชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

- 1) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ, ข้อมูลอุณหภูมิจากเตือนภัย (www.tmd.go.th)
- 2) ศูนย์เตือนภัยพิบัติแห่งชาติ: การแจ้งเตือนล่วงหน้า
- 3) กรมทรัพยากรธรณี: ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม / แผ่นดินไหว (http://www.dmr.go.th/index_.php)
- 4) กรมป้องกันและบรรเทาสาธารณภัย: การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการ และแนวทางปฏิบัติ (<https://www.disaster.go.th/th/home/>)

6.7.2 การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้า เป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

- 1) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู
- 2) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน
- 3) หนู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน
- 4) ปลากระโดดขึ้นมาจากผิวน้ำ

6.7.3 การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

- 1) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
- 2) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ ต่างๆ ตามความจำเป็นและเหมาะสม
- 3) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่มสำหรับบุคลากรขององค์กร
- 4) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ ประโยชน์อย่างมีประสิทธิภาพเมื่อเกิดภัย
- 5) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

6.7.4 การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

- 1) สํารวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม
- 2) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สิน ของประชาชน

6.7.5 การปฏิบัติขั้นเตรียมการ

- 1) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
- 2) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย
- 3) อบรมให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่บุคลากรในองค์กร
- 4) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

6.8 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและ ก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

- 1) ดำเนินการหาข่าวจากแหล่งต่างๆ เช่น ตำรวจ นักข่าว โทรทัศน์วิทยุ และหน่วยงานที่เกี่ยวข้อง
- 2) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม
- 3) ตรวจสอบระบบไฟฟ้า ระบบปั้มน้ำให้อยู่ในสภาพที่พร้อมใช้งาน
- 4) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

7. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อบรรเทาภัยฉุกเฉินที่ อาจจะเกิดขึ้น ดังนี้

7.1 ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบายให้ข้อเสนอแนะ ปรีกษา ตลอดจนติดตาม กากับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการโรงพยาบาลโพธาราย (CEO)

รองผู้อำนวยการฝ่ายการแพทย์ โรงพยาบาลโพธาราย (CIO)

รองผู้อำนวยการฝ่ายบริหาร โรงพยาบาลโพธาราย

รองผู้อำนวยการฝ่ายการพยาบาล โรงพยาบาลโพธาราย

หัวหน้าศูนย์เทคโนโลยีสารสนเทศ (Information Security Manager)

7.2 ระดับปฏิบัติ

- ก) ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- ข) ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- ค) ทีมกู้คืนแอปพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งานผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- ง) ทีมประเมินความเสียหาย เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software , Network เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- จ) ทีมอาคารสถานที่ / ความปลอดภัย / ไฟฟ้า / ประปา เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร เครื่องปรับอากาศให้พร้อมใช้งาน ผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- ฉ) ทีมการจัดการทั่วไป/ ประสานงานองค์กรภายนอก/สุศึกษาประชาสัมพันธ์ / วิทยุชุมชน เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุล่วงวัตถุประสงค์ในการทำงาน ผู้รับผิดชอบได้แก่

นายสิทธิกร อุดะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศได้จัดหาไว้ ผู้รับผิดชอบได้แก่

- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- ข) ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไพระเปิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหาย กับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่
- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- ฅ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบสูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม ผู้รับผิดชอบได้แก่
- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบได้แก่
- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- ฎ) ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานให้ได้ทันที และครบถ้วนสมบูรณ์ผู้รับผิดชอบ ได้แก่
- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- ฏ) ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหวทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลง ให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่
- | | | |
|-----------------------------|----------------|--------------|
| นายสิทธิกร อุดะโชติ | เบอร์โทรติดต่อ | 094-049-0302 |
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรันธนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |

ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อกวนจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อกวนจลาจล สิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหาย ทุกด้านอย่างละเอียด แล้วรายงานแก่ ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นายสิทธิกร อุตะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

8. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

8.1 กรณีเครื่องลูกข่าย

- 1) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบหรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่าย ได้ ศูนย์เทคโนโลยีสารสนเทศต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ
- 2) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดขึ้นจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด
- 3) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์เทคโนโลยีสารสนเทศเพื่อแก้ไขปัญหาต่อไป

8.2 กรณีเครื่องแม่ข่ายบริการ (Server)

- 1) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ
- 2) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรอง ไฟฟ้า
- 3) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
- 4) ตรวจสอบปัญหาที่เกิดขึ้นในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปที่ปลอดภัย
- 5) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว
- 6) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

- 7) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือ ผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด
- 8) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
- 9) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการ หรือศูนย์เทคโนโลยีสารสนเทศทราบโดยเร็ว

9. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบฐานข้อมูล และสารสนเทศ

9.1 ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

- 1) ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายสิทธิกร อุตะโชติ	เบอร์โทรศัพท์	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรศัพท์	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรศัพท์	087-854-8687
- 2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 094-049-0302 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
- 3) ใช้อุปกรณ์ที่น้ำยาดับเพลิง ฉีดควบคุมเพลิงดับและจัดการขนย้ายอุปกรณ์ที่สามารถ ขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัย ได้แก่ นอกตึกอาคารสำนักงาน จุฬารวมพล หรือแล้วแต่เหตุไฟไหม้และความเหมาะสม แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้อง ดำเนินการในข้อต่อไป
- 4) แจ้งหน่วยงานที่มีระดับเพลิงที่ใกล้ที่สุด คือเทศบาลตำบลหนองใหญ่ ตั้งอยู่ที่หมู่ที่ 10 ตำบลหนองใหญ่ อำเภอโพธาราย จังหวัดศรีสะเกษ และเทศบาลตำบลโพธาราย ตั้งอยู่ เลขที่ 70 หมู่ 6 ตำบลโพธาราย อำเภอโพธาราย จังหวัดศรีสะเกษ เพื่อดำเนินการต่อไป
- 5) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
- 6) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการทราบ

9.2 กรณีไฟดับ / หม้อไพ้ระเบิด

- 1) ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายสิทธิกร อุตะโชติ	เบอร์โทรศัพท์	094-049-0302
---------------------	---------------	--------------

- | | | |
|---------------------------|----------------|--------------|
| นายอภิชาติ คำภีระ | เบอร์โทรติดต่อ | 088-375-9210 |
| นายจิรณนิน ประสารกุลนันท์ | เบอร์โทรติดต่อ | 087-854-8687 |
- 2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 082-362-9362 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
 - 3) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
 - 4) แจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการโดย การไฟฟ้าส่วนภูมิภาคสาขาอำเภออุทุมพรพิสัย ตั้งอยู่ที่ 677 หมู่ที่ 7 ถนนศรีบุญลือ ตำบลกำแพง เบอร์โทรศัพท์ 045-638295 เพื่อดำเนินการต่อไป
 - 5) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการ ทราบ

9.3 กรณีน้ำท่วมห้องควบคุมระบบ

- 1) ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการ เกิดน้ำท่วมลงทุกระบบ จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไป ยังชั้น 2 , 3 พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายสิทธิกร อุตะโชติ	เบอร์โทรติดต่อ	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687
- 2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 082-362-9362 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่ เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
- 3) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
- 4) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการ ทราบ

9.4 กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

- 1) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบประกอบด้วย

นายสิทธิกร อุตะโชติ	เบอร์โทรติดต่อ	094-049-0302
---------------------	----------------	--------------

นายอภิชาติ คำภีระ	เบอร์โทรติดต่อ	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรติดต่อ	087-854-8687

- 2) แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้า ควบคุมสถานการณ์ เพื่อระบบงาน และเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

- 3) ให้ผู้รับผิดชอบสารสนเทศของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ ศูนย์สนับสนุนบริการสุขภาพที่ 10 เพื่อแก้ไขปัญหาต่อไป

9.4.1 ขั้นตอนในการกู้คืนระบบความปลอดภัยกรณีโดนเจาะระบบและภัยคุกคามทาง คอมพิวเตอร์ มีดังนี้

- 1) ควบคุมสถานการณ์
 - ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา
 - ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย
 - ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก
- 2) วิเคราะห์การถูกโจมตี
 - ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่น ๆ
 - ข) วิเคราะห์ล็อกไฟล์ (Log file) ตรวจสอบโปรแกรมหรือข้อมูลที่ผู้บุกรุกทิ้งไว้
 - ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System
 - ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ
- 3) กู้คืนระบบคอมพิวเตอร์
 - ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดให้
 - ข) งดใช้เซิร์ฟเวอร์ที่ไม่จำเป็น
 - ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)
 - ง) อุดช่องโหว่ในระบบเครือข่าย
 - จ) เปลี่ยนแปลงพาสเวิร์ดให้ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว
- 4) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานการถูกโจมตีผ่านทางโทรศัพท์ 092-561-8295 แก่ ผู้อำนวยการ เพื่อทราบและสั่งการต่อไป
- 5) ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่าย พร้อมทั้งจัดทำ รายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการ แพทย์และผู้อำนวยการ ทราบ

9.5 กรณีแผ่นดินไหว

- 1) ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้นที่อาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นายสิทธิกร อุตะโชติ	เบอร์โทรศัพท์	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรศัพท์	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรศัพท์	087-854-8687
- 2) เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้ง เตือนเจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและ ความเสียหาย ผู้บังคับบัญชาได้แก่

นายสิทธิกร อุตะโชติ	เบอร์โทรศัพท์	094-049-0302
นายอภิชาติ คำภีระ	เบอร์โทรศัพท์	088-375-9210
นายจิรณนิน ประสารกุลนันท์	เบอร์โทรศัพท์	087-854-8687
- 3) เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้
- 4) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ ล่วงหน้าตามควรแก่กรณีดังนี้

9.5.1 ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

- 1) การปฏิบัติขณะเกิดแผ่นดินไหว
 - ก) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน
 - ข) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กำแพงด้านนอก/ ชั้นวางของ/สิ่งนี้อาจล้มหรือหล่นได้
 - ค) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร
 - ง) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้
 - จ) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น
 - ฉ) ห้ามใช้ลิฟต์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น
 - ช) ถ้าอยู่นอกอาคารให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด
 - ซ) ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า
 - ณ) ถ้าอาคารเก่าหรือไม่นั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด
 - ญ) หลังจากการสั่นสะเทือนสิ้นสุดให้รีบออกจากอาคาร
 - ฎ) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุดห้อยโดยยึดหลัก “หมอบ” “ป้อง” “เกาะ” จนกว่าจะมีผู้เข้าไปช่วยเหลือ

ฎ) ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมี วัสดุ หล่นใส่

ฐ) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

ฑ) ห้ามใช้ลิฟต์โดยเด็ดขาด

ฒ) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

- 1) ถ้าอาคารมั่นคงแข็งแรงให้หลบอยู่ในอาคารนั้น
- 2) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น
- 3) หลังการสั่นสะเทือนสิ้นสุดลงให้หาทางออกจากอาคารนั้น
- 4) ถ้าไม่อยู่ใกล้ทางออกให้ “หมอบ” “ป้อง” “เกาะ” จนกว่าจะมีผู้เข้าไปช่วยเหลือ
- 5) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดอุบัติเหตุ
- 6) ห้ามใช้ลิฟต์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

- 1) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่า การ สั่นไหวจะหยุด
- 2) หลีกเลียงสิ่งของที่อาจโค่นล้มลงมาทำอันตราย เช่น ตู้ เสาไฟฟ้า ป้ายโฆษณา ต้นไม้ใหญ่
- 3) หลีกเลียงอาคารสูง กำแพง รั้ว ระเบียง กระจก ขึ้นส่วนของอาคารที่อาจหล่นลงมา
- 4) วิ่งไปสู่ที่โล่ง
- 5) รีบออกจากอาคารที่ชำรุดเสียหายโดยเร็วที่สุด

กรณีอยู่ใกล้ชายฝั่ง

หากได้รับการแจ้งเตือนหรือรู้สึกได้ถึงแรงสั่นสะเทือนให้รีบอพยพจากบริเวณชายฝั่ง และ ริมแม่น้ำลำคลองที่เชื่อมต่อกับทะเลโดยด่วน เพราะอาจเกิดคลื่นสึนามิได้

- 2) เมื่อแผ่นดินไหวสงบลง
 - 1) ตรวจสอบอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนำส่งโรงพยาบาล
 - 2) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ
 - 3) ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ ปิด ระบบ การทำงานทั้งหมดทันที
 - 4) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้ง เจ้าหน้าที่ทันที
- 3) ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง
 - 1) อยู่กับที่ ป้องกันศีรษะและหน้าจากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ

- 2) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัตถุหล่นใส่ แตกหักพังทลาย
- 3) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจาก สิ่งของ
- 4) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น
- 5) ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย
- 4) การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว
 - 1) ระวังสติอารมณ์ ปฏิบัติตามแผนอพยพ
 - 2) เชื่อฟังคำแนะนำของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.
 - 3) เก็บทรัพย์สิน/เอกสารสำคัญไว้ในลิ้นชักโต๊ะและล็อกกุญแจ
 - 4) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด
 - 5) ห้ามชนสัมภาระใดๆ ติดตัวขณะอพยพ
 - 6) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า
 - 7) ใช้ช่องทางหนีไฟ เรียงแถว ขึ้นบันไดละ 2 คน
 - 8) ห้ามพูดคุย สายตามองขึ้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง
 - 9) ห้ามใช้ลิฟต์ โดยเด็ดขาด
 - 10) เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที
 - 11) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้
 - 12) ตรวจสอบจำนวนผู้อพยพ
- 5) เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการ ผ่านทางโทรศัพท์ 092-561-8295 เพื่อทราบและสั่งการต่อไป
- 6) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการ และหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ทราบ

9.6 กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

- 1) ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้น ทีมอาคารสถานที่ผู้รับผิดชอบ ได้แก่
5555
- 2) เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย ผู้บังคับบัญชาได้แก่
555
- 3) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ ล่วงหน้าตามควรได้แก่ กรณีดังนี้

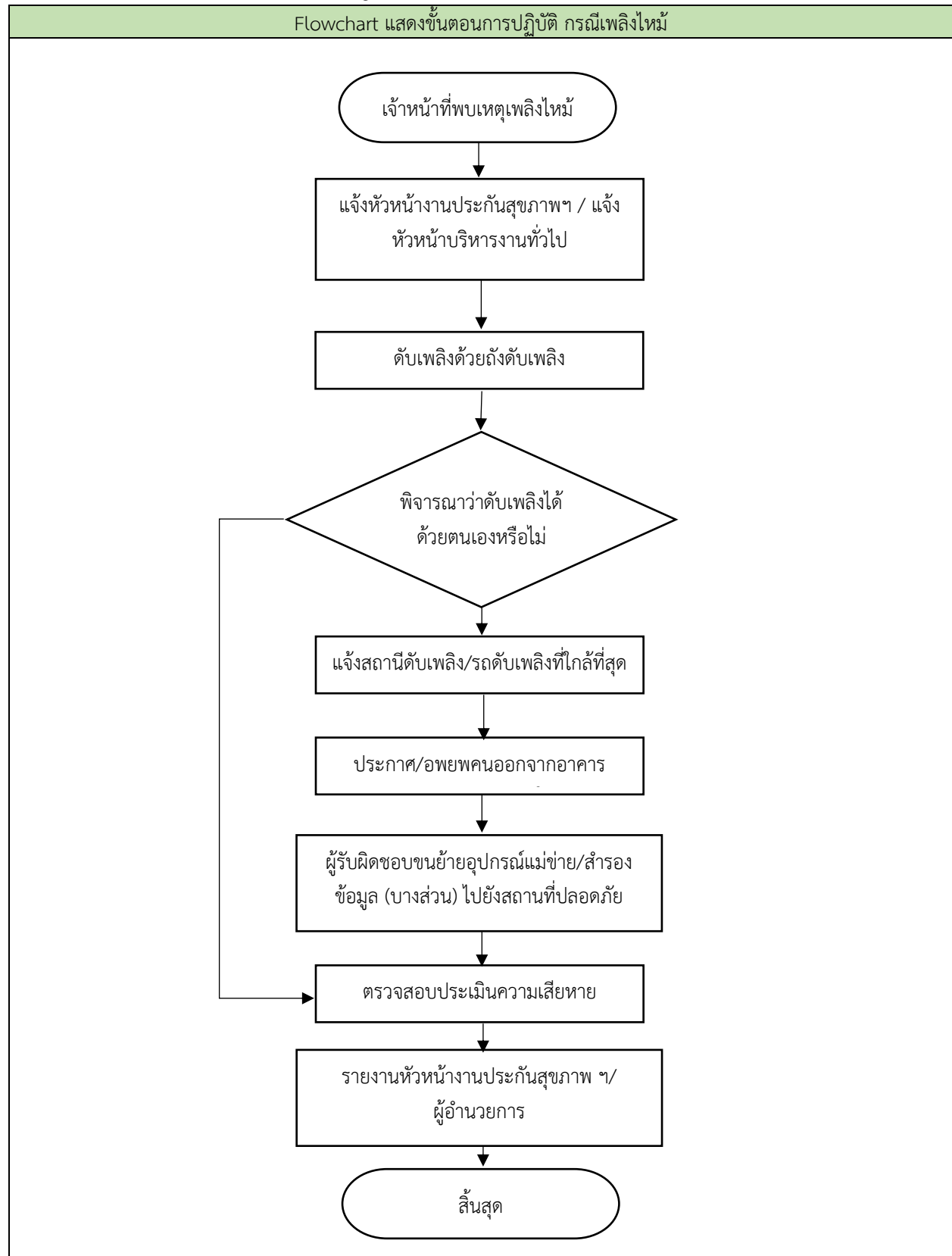
9.6.1 ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อกวน

- ก) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของ ผู้ปฏิบัติงานและของโรงพยาบาล
- ข) เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า
- ค) ปิดประตูทั้ง 2 ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาในโรงพยาบาลโพนทราย
- ง) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของโรงพยาบาลโพนทราย ให้แจ้งไปยังสถานีตำรวจภูธร อำเภอโพนทราย หรือหน่วยงาน รับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้รองผู้อำนวยการกลุ่มบริหารงานทั่วไปเพื่อทราบ

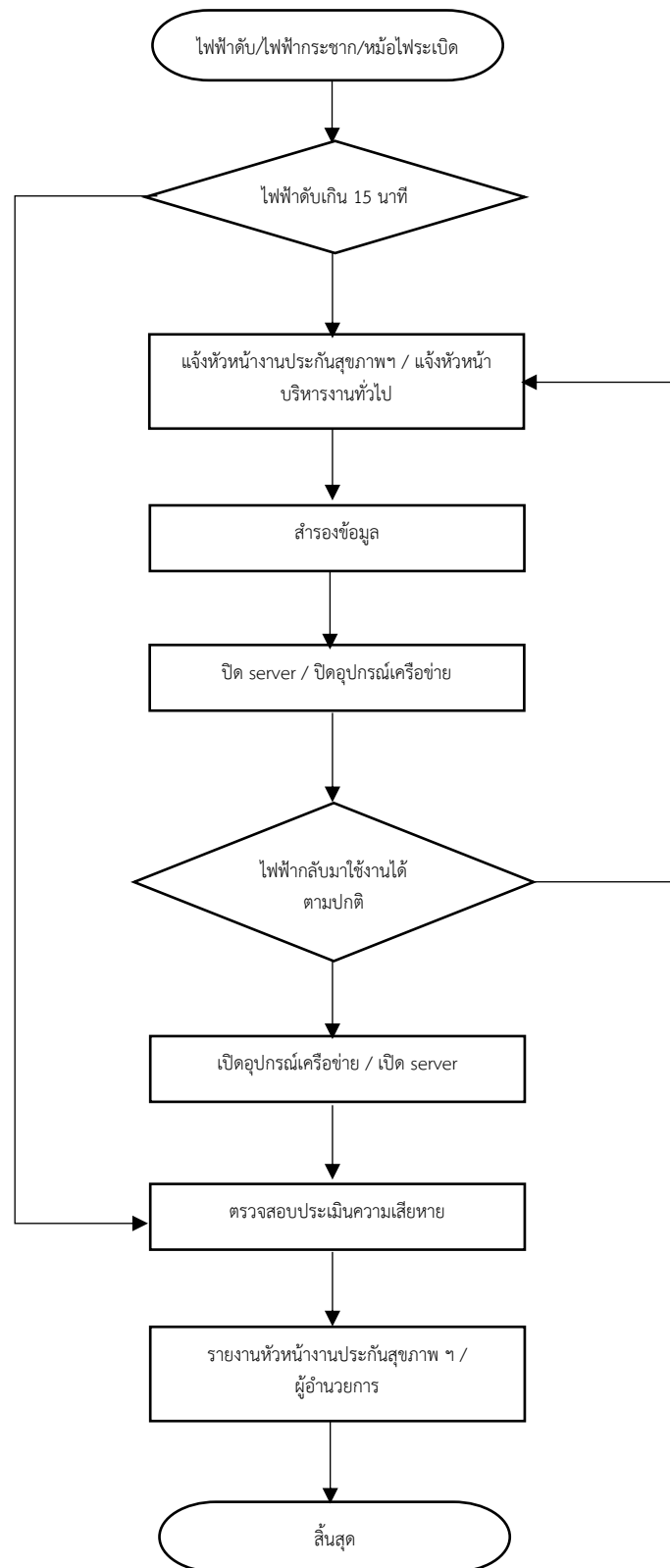
9.6.2 ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

- ก) เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที
- ข) เจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการและหัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์ พร้อมทั้งติดต่อเจ้าหน้าที่ตำรวจมาตรวจสอบวัตถุต้องสงสัย
- ค) กรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกั้นพื้นที่อันตรายที่พบวัตถุระเบิด กั้นบุคคล ที่ไม่เกี่ยวข้องออกจากบริเวณ และแจ้งอพยพผู้ออกจากบริเวณหรือรัศมีของวัตถุระเบิด
- ง) เมื่อการชุมนุมประท้วงและก่อกวนสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ ผู้อำนวยการ และหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ เพื่อทราบและสั่งการต่อไป
- จ) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหายเพื่อแจ้งผู้อำนวยการ และหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทราบ

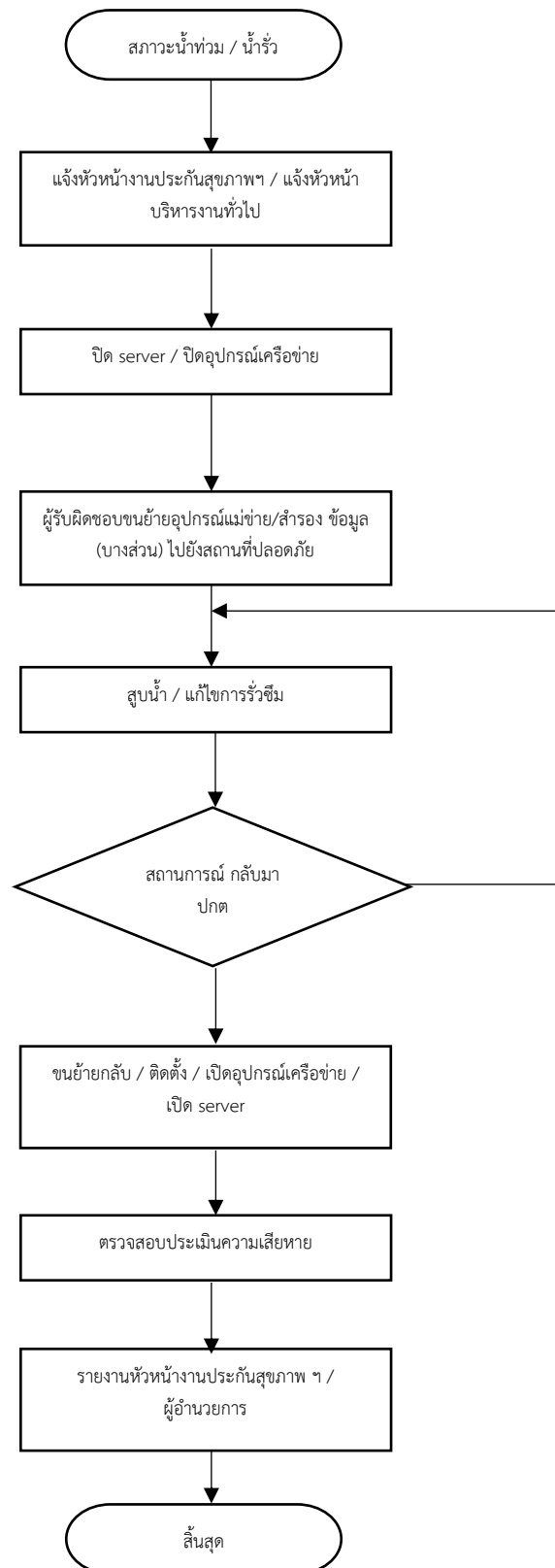
10. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ



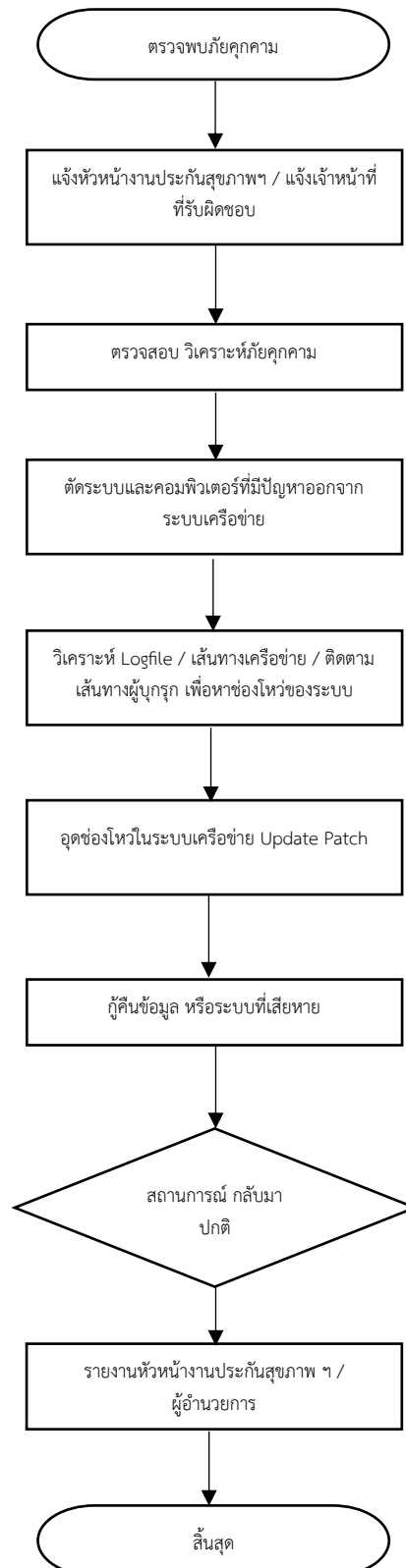
Flowchart แสดงขั้นตอนการปฏิบัติ กรณีไฟฟ้าดับ/ไฟฟ้ากระชาก/หม้อไพระเบิด

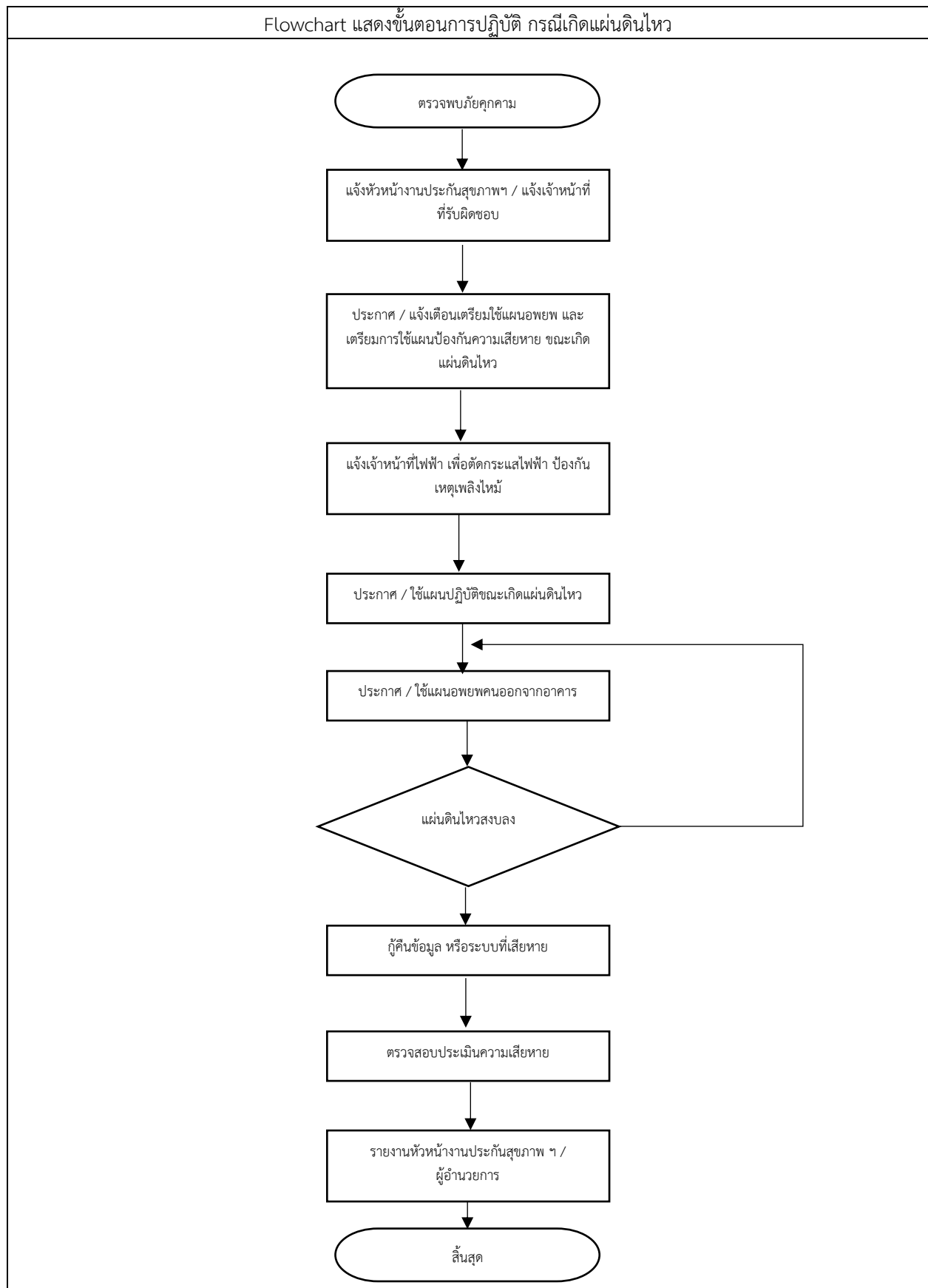


Flowchart แสดงขั้นตอนการปฏิบัติ กรณีน้ำท่วม

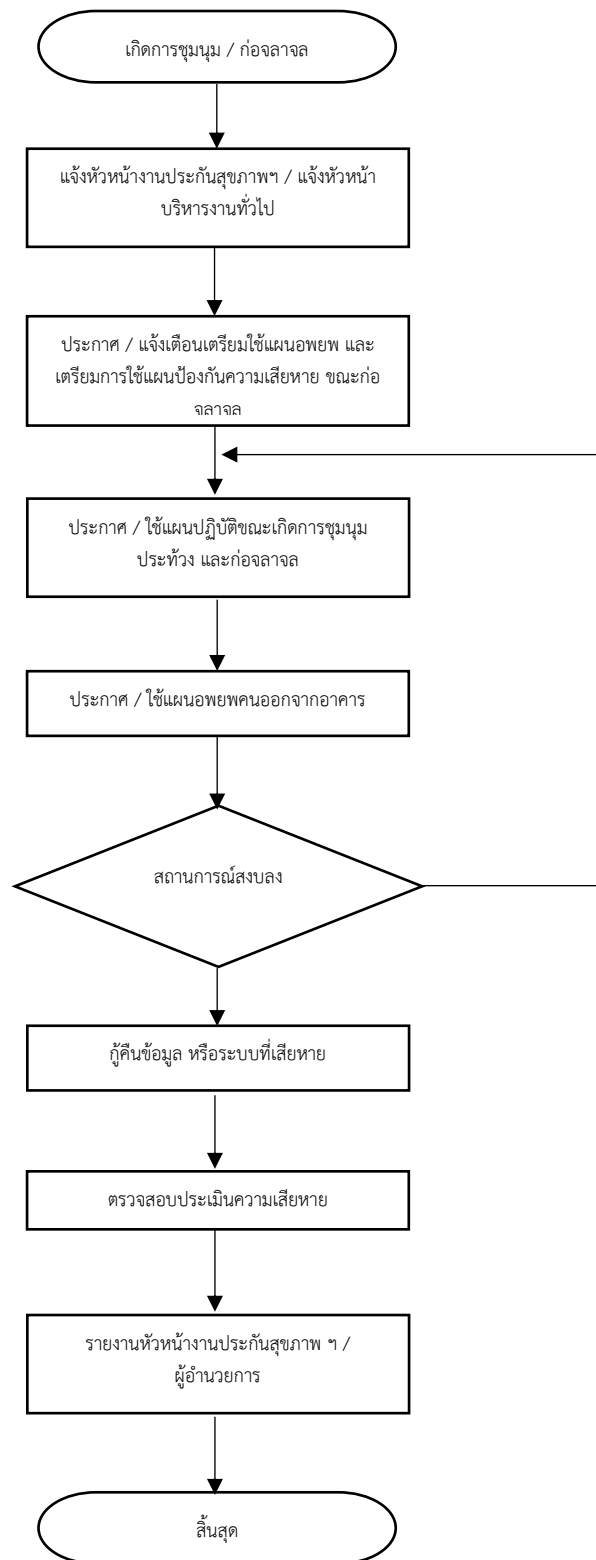


Flowchart แสดงขั้นตอนการปฏิบัติ กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม





Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



11. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุด หรือเท่าที่จะดำเนิน การได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

- 1) จัดหาอุปกรณ์ชิ้นส่วนให้เพื่อทดแทน
- 2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
- 3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
- 4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
- 5) นำ BACKUP TAPE / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบกู้ระบบ กลับมาโดยเร็วภายใน 48 ชั่วโมง
- 6) ตรวจสอบระบบปฏิบัติการฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้อง จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยัง รวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ หน่วยงานจึงมีแผนสำรองแหล่งข้อมูล เพื่อให้มีความต่อเนื่องอยู่เสมอ คือ
 - 1) การสำรองข้อมูล จะมีเครื่อง Server 2 เครื่อง ติดตั้งระบบปฏิบัติการ Ubuntu 12.04 LTS โดยเครื่องที่ 1 จะเป็น Server1 หลัก และ Server2 จะเป็นตัวสำรองข้อมูล โดยการทำ Replication อัตโนมัติ ด้วยคำสั่ง โดย Server ทั้งสองตัวจะทำงานเหมือนกันทุกประการ ถ้าเกิดเครื่อง Server1 เกิดความเสียหายก็จะสามารถนำ Server2 ใช้งานแทน เครื่อง server1 ได้ทันที
 - 2) สำรองข้อมูล ทั้งหมดเก็บไว้ใน External Harddisk หรือฮาร์ดดิสพกพา เพื่อป้องกันกรณีข้อมูลใน ข้อที่ 1) หายทั้งหมด ไม่สามารถนำมาใช้งานได้

แผนการดำเนินการ

1. สำรวจความต้องการของระบบสำรอง
2. สำรวจการสำรองที่เหมาะสม
3. การประเมินความเสี่ยงจากสิ่งต่างๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง
4. การจัดลำดับผลกระทบขององค์กร
5. การจัดทำแผนกู้คืน
6. การวางแผน การแต่งตั้งทีมงาน ลำดับการทำงานหลังระบบได้รับความเสียหาย
7. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่ รวมถึงการฝึกอบรมทางด้านเทคนิค
8. การทดสอบแผน อาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง

9. การปรับปรุงแผนการกู้คืน

12. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้หัวหน้ากลุ่มงานประกันสุขภาพยุทธศาสตร์และสารสนเทศทางการแพทย์ทราบ เพื่อนำเสนอรายงานสรุปให้ผู้อำนวยการทราบ เป็นประจำ และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันที ที่สามารถดำเนินการได้ในทุกกรณี ตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มี ประสิทธิภาพ สามารถนำมาใช้งานได้ทันเวลาที่ในกรณีที่เกิดภัยพิบัติต่อไป



(นายแพทย์ธนพล วิมลวรรณ)

ผู้อำนวยการโรงพยาบาลโพนทราย

