แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ของศูนย์เทคโนโลยีสารสนเทศ โรงพยาบาลน่าน

พ.ศ. 2561

สารบัญ

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ 1
2. แนวทางการป้องกันและเตรียมการเบื้องต้น 3
3. การเตรียมความพร้อม 5
4. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน 9
5. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ 12
6. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ 13
    - กรณีไฟดับ / หม้อไฟระเบิด 14
    - กรณีน้ำท่วมห้องควบคุมระบบ 15
    - กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ 16
    - กรณีแผ่นดินไหว 17
    - กรณีเกิดการชุมนุมประท้วงและก่อจลาจล 20
7. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนฯ 21
    - กรณีจากไฟไหม้ห้องควบคุมระบบ 21
    - กรณีไฟดับ / หม้อไฟระเบิด 23
    - กรณีน้ำท่วมห้องควบคุมระบบ 24
    - กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ 25
    - กรณีแผ่นดินไหว 26
    - กรณีเกิดการชุมนุมประท้วงและก่อจลาจล 27
8. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม 28
9. การติดตามและรายงานผล 29

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนาไปใช้ประโยชน์ต่อการทางานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจาก ภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) 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

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

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

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทางาน

1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ (Security Log Management System) โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศ เพื่อนำมาสรุปเป็น ข้อมูลต่อไป

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)			คะแนนรวม	จัดเรียงลาดับ
	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

2. แนวทางการป้องกันและเตรียมการเบื้องต้น

2.1 การประกาศแผน (Activation)

องค์กรมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

2.2 กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุ ที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการ เตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

2.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

2.4 การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็น หน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณี คอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

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

2.5 การสำรองข้อมูล (Backup)

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

2.6 การป้องกันไวรัสคอมพิวเตอร์

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

2.7 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

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

2) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

3) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

2.8 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

1) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องทำบัตรผ่าน (Key Card) เพื่อใช้ในการเข้าออกห้องควบคุม ระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

2) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

3) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

5) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

2.9 การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว 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 และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

3. การเตรียมความพร้อม

3.1 การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสียงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.1.1 จัดทำแผนรองรับสถานการณ์ ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด

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

3.1.3 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และ บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพรอมใช้งานอยู่เสมอ

3.1.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ตางๆ

3.1.5 ให้มีการสำรองฐานข้อมูลทุก 1 เดือนเป็นอย่างน้อย

3.2 การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม ซึงอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.2.1 จัดทำแผนรองรับสถานการณ์ ฉุกเฉินอันเกิดจากไฟไหม้

3.2.2 ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่ายเพื่อการควบคุมเพลิงในเบื้องต้น

3.2.3 ให้มีการสำรองฐานขอมูลเดือนละ 1 ครั้งเป็นอย่างน้อย

3.3 การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม /น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

3.3.1 จัดทำแผนรองรับสถานการณ์ ฉุกเฉินอันเกิดจากน้ำท่วม /น้ำรั่ว

3.3.2 มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

3.3.3 ให้มีการสำรองฐานข้อมูล เดือนละ 1 ครั้งเป็นอย่างน้อย

3.4 การเตรียมความพรอมรับสถานการณ์ภัยจากไวรัส

3.4.1 ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเขาใช้งานเครื่องคอมพิวเตอร์แมขาย และป้องกันการบุกรุกจากบุคคลภายนอก

3.4.2 มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกขาย (Client)

3.4.3 อัพเดตโปรแกรมกาจัดไวรัส ทุก 1 เดือน เป็นอย่างน้อย (Update Patch)

3.4.4 ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศแจงข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนาวิธีการป้องกันและการกาจัดไวรัสในเบื้องต้น

3.5 การเตรียมความพรอมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือขาย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

3.5.1 กำหนดมาตรการควบคุมการเขาออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

3.5.2 หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศผู้ดูแลระบบเครือข่าย เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออกและคอย กำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเขาออกมีการติดตั้งระบบ Access Control โดยใช้ Key Card และ ติดตั้งกลองโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

3.5.3 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ไดรับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

3.5.4 มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยตอระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

3.5.5 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

3.5.6 มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

3.6 การเตรียมความพรอมรับสถานการณ์จากเจาหนาที่ผูรับผิดชอบ เจ้าหน้าที่แผนกต่างๆ ภายในองค์กร ขาดทักษะความรูความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสียงให้เกิดขึ้นน้อยที่สุด

3.6.1 สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

3.6.2 วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

3.7 การเตรียมความพรอมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

3.7.1 ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัย จากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

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

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

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

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

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

3.7.2 การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

1) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

2) แมลงสาบจานวนมากวิ่งเพ่นพ่าน

3) หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศิลของพวกมัน

4) ปลากระโดดขึ้นมาจากผิวน้ำ

3.7.3 การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

1) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

2) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกาลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

3) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร

4) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

5) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

3.7.4 การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

1) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

2) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

3.7.5 การปฏิบัติขั้นเตรียมการ

1) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

2) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย

3) อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่ บุคลากรในองค์กร

4) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

3.8 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

1) ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

2) จัดเตรียมกาลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

3) ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

4) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

4. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

4.1 ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คาปรึกษา ตลอดจนติดตาม กากับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการโรงพยาบาลน่าน (CEO)

รองผู้อำนวยการฝ่ายการแพทย์ โรงพยาบาลน่าน (CIO)

รองผู้อำนวยการฝ่ายบริหาร โรงพยาบาลน่าน

รองผู้อำนวยการฝ่ายการพยาบาล โรงพยาบาลน่าน

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (Information Security Manager)

4.2 ระดับปฏิบัติ

ก) ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศ ัพท์ติดต่อ 086-116-2239
น.ส.คีรีมาศ มีสุข เบอร์โทรศัพท์ติดต่อ 090-316-6483
นายสมบัติ แก้วจันทร์ฉาย เบอร์โทรศ ัพท์ติดต่อ 081-347-1533
นายสิทธิโชค สุภา เบอร์โทรศัพท์ติดต่อ 089-636-1221
นายอานัน ไชยช่อฟ้า เบอร์โทรศัพท์ติดต่อ 085-034-4939

ข) ทีมกู้คืนเครือข่าย
ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ ผู้รับผิดชอบ ได้แก่

นายสมบัติ แก้วจันทร์ฉาย เบอร์โทรศ ัพท์ติดต่อ 081-347-1533
นายสิทธิโชค สุภา เบอร์โทรศัพท์ติดต่อ 089-636-1221

ค) ทีมกู้คืนแอพพลิเคชัน
ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

นายกิติพงษ์ อะทะจา เบอร์โทรศ ัพท์ติดต่อ 090-054-2484
นายมารุต มหายศ เบอร์โทรศัพท์ติดต่อ 087-788-8150
สมบัติ แก้วจันทร์ฉาย เบอร์โทรศ ัพท์ติดต่อ 081-347-1533
นายสิทธิโชค สุภา เบอร์โทรศัพท์ติดต่อ 089-636-1221

ง) ทีมประเมินความเสียหาย
เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software , Network เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบ ได้แก่

นพ.กนก พิพัฒน์เวช เบอร์โทรศ ัพท์ติดต่อ 081-887-9664
นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศ ัพท์ติดต่อ 086-116-2239
นายกิติพงษ์ อะทะจา เบอร์โทรศ ัพท์ติดต่อ 090-054-2484
นายมารุต มหายศ เบอร์โทรศัพท์ติดต่อ 087-788-8150
สมบัติ แก้วจันทร์ฉาย เบอร์โทรศ ัพท์ติดต่อ 081-347-1533
นายสิทธิโชค สุภา เบอร์โทรศัพท์ติดต่อ 089-636-1221
นายอานัน ไชยช่อฟ้า เบอร์โทรศัพท์ติดต่อ 085-034-4939

จ) ทีมอาคารสถานที่ / ความปลอดภัย / ไฟฟ้า / ประปา
เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร แอร์ ให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

นายเดชพิภัทร์ อมรทิพย์วงศ์	เบอร์โทรศัพท์ติดต่อ	089-631-5814
นางจุรีย์ กุศล	เบอร์โทรศัพท์ติดต่อ	081-287-5567
นางบุรินทร์ ปิติรัตน์	เบอร์โทรศัพท์ติดต่อ	081-746-6525
นายยงยุทธ วุฒิการณ์	เบอร์โทรศัพท์ติดต่อ	081-951-9744
น.ส.คีรีมาศ มีสุข	เบอร์โทรศัพท์ติดต่อ	090-316-6483
นายวิเชษฐ์ ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	089-636-5278

ฉ) ทีมการจัดการทั่วไป/ ประสานงานองค์กรภายนอก/สุขศึกษาประชาสัมพันธ์ / วิทยุชุมชน
เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทางาน ผู้รับผิดชอบ ได้แก่

นางสุปราณี ยะวิญชาญ	เบอร์โทรศัพท์ติดต่อ	084-615-0522
นายสุภาพ สิริบรรสพ	เบอร์โทรศัพท์ติดต่อ	081-531-2219
นางรุ่งทิพย์ กาละดี	เบอร์โทรศัพท์ติดต่อ	089-811-8177
นางอุลี ศักดิ์สุวรรณ	เบอร์โทรศัพท์ติดต่อ	085-039-9083
นายกิติศักดิ์ แก้วนิ่ม	เบอร์โทรศัพท์ติดต่อ	092-103-1192
นายอรรถพล คุณสิทธิ์	เบอร์โทรศัพท์ติดต่อ	085-331-9777
นายสุรชัย คำอ้าย	เบอร์โทรศัพท์ติดต่อ	087-660-7399

ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้ อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศได้จัดหาไว้ ผู้รับผิดชอบ ได้แก่

นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศ	ัพท์ติดต่อ	086-116-2239
นายกิติพงษ์ อะทะจา เบอร์โทรศ	ัพท์ติดต่อ	090-054-2484
นายมารุต มหายศ	เบอร์โทรศัพท์ติดต่อ	087-788-8150
นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายวิเชษฐ์ ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	089-636-5278

ซ) ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรอง ข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่

นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายสุรชัย สุเทปิน	เบอร์โทรศัพท์ติดต่อ	088-409-4484
สมบัติ แก้วจันทร์ฉาย เบอร์โทรศ	ัพท์ติดต่อ	081-347-1533

ฌ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะ เกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและ ตรวจสอบการรั่วซึม
ผู้รับผิดชอบ ได้แก่

นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายสุรชัย คำอ้าย	เบอร์โทรศัพท์ติดต่อ	089-631-5892
นายกิติพงษ์ อะทะจา	เบอร์โทรศัพท์ติดต่อ	090-054-2484

ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทางานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย
ผู้รับผิดชอบ ได้แก่

นายมารุต มหายศ	เบอร์โทรศัพท์ติดต่อ	087-788-8150
นายสิทธิโชค สุภา	เบอร์โทรศัพท์ติดต่อ	089-636-1221

ฎ) ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery)
ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานให้ได้ทันทีและครบถ้วนสมบูรณ์
ผู้รับผิดชอบ ได้แก่

สมบัติ แก้วจันทร์ฉาย	เบอร์โทรศัพท์ติดต่อ	081-347-1533
นายสิทธิโชค สุภา	เบอร์โทรศัพท์ติดต่อ	089-636-1221
นายกิติพงษ์ อะทะจา	เบอร์โทรศัพท์ติดต่อ	090-054-2484
นายมารุต มหายศ	เบอร์โทรศัพท์ติดต่อ	087-788-8150

ฏ) ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว
ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผน ที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและ สั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นพ.กนก พิพัฒน์เวช เบอร์โทรศัพท์ติดต่อ		081-887-9664
นายเดชพิภัทร์ อมรทิพย์วงศ์ เบอร์โทรศัพท์ติดต่อ		089-631-5814
นางนพพร ธนามี เบอร์โทรศัพท์ติดต่อ		091-012-4800
นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศัพท์ติดต่อ		086-116-2239

ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหาย ทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นพ.กนก พิพัฒน์เวช เบอร์โทรศัพท์ติดต่อ		081-887-9664
นายเดชพิภัทร์ อมรทิพย์วงศ์ เบอร์โทรศัพท์ติดต่อ		089-631-5814
นางนพพร ธนามี เบอร์โทรศัพท์ติดต่อ		091-012-4800
นางสุปราณี ยะวิญชาญ	เบอร์โทรศัพท์ติดต่อ	084-615-0522
นางอุลี ศักดิ์สุวรรณ	เบอร์โทรศัพท์ติดต่อ	085-039-9083
นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศัพท์ติดต่อ		086-116-2239
น.ส.คีรีมาศ มีสุข	เบอร์โทรศัพท์ติดต่อ	090-316-6483
นายอรรถพล คุณสิทธิ์ เบอร์โทรศัพท์ติดต่อ		085-331-9777

5. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

5.1 กรณีเครื่องลูกข่าย

1) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศต้องประกาศให้ทุก หน่วยงานในองค์กรทราบ

2) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

3) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์สารเทศเพื่อแก้ไขปัญหาต่อไป

5.2 กรณีเครื่องแม่ข่ายบริการ (Server)

1) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

3) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

4) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

5) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

6) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

7) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

8) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนาอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

9) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบโดยเร็ว

6. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

กรณีจากไฟไหม้ห้องควบคุมระบบ

ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นางโสภา อิสระณรงค์พันธ์ เบอร์โทรศ	ัพท์ติดต่อ	086-116-2239
นายกิติพงษ์ อะทะจา เบอร์โทรศ	ัพท์ติดต่อ	090-054-2484
นายมารุต มหายศ	เบอร์โทรศัพท์ติดต่อ	087-788-8150
นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายวิเชษฐ์ ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	089-636-5278

2. แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

3. เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศได้จัดหาไว้ดำเนินการดับเพลิง และจัดการขนย้ายอุปกรณ์ ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัยได้แก่ อาคารสิริเวชรักษ์หรือจุดร่วมพล

4. แจ้งสถานีดับเพลิงที่ใกล้ที่สุด ซึ่งในเขตที่ตั้งนี้คือสถานีดับเพลิงเทศบาลเมืองน่าน เบอร์โทรศัพท์ 191 หรือ 054-710261 เพื่อดำเนินการต่อไป

5. ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 081-387-9447 แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป

6. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทราบ

กรณีไฟดับ / หม้อไฟระเบิด

1. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายสุรชัย สุเทปิน	เบอร์โทรศัพท์ติดต่อ	088-409-4484
สมบัติ แก้วจันทร์ฉาย	เบอร์โทรศัพท์ติดต่อ	081-347-1533

2. แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

3. ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 081-387-9447 แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป

4. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทราบ

กรณีน้ำท่วมห้องควบคุมระบบ

1. ผู้ที่อยู่เวรรักษาการณ์ต้องนาอุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายใน เบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้น ติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังอาคารสิริเวชรักษ์ ชั้น 2 ,3 พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายอานัน ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	085-034-4939
นายสุรชัย คำอ้าย	เบอร์โทรศัพท์ติดต่อ	089-631-5892
นายกิติพงษ์ อะทะจา	เบอร์โทรศัพท์ติดต่อ	090-054-2484

2. แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 และผู้มีหน้าที่ รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

3. ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 081-387-9447 แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป

4. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทราบ

กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

1. ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบประกอบด้วย

นายมารุต มหายศ	เบอร์โทรศัพท์ติดต่อ	087-788-8150
นายสิทธิโชค สุภา	เบอร์โทรศัพท์ติดต่อ	089-636-1221

2. แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้า ควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความ ปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

1) ควบคุมสถานการณ์

ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

2) วิเคราะห์การถูกโจมตี

ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่นๆ

ข) วิเคราะห์ล็อกไฟล์ (Log file) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้

ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

3) กู้คืนระบบคอมพิวเตอร์

ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดให้

ข) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ดให้ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

3. ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานการถูกโจมตีผ่านทางโทรศัพท์ 081-387-9447 แก่ผู้อำนวยการ ศูนย์เทคโนโลยีสารสนเทศ เพื่อทราบและสั่งการต่อไป

4. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

กรณีแผ่นดินไหว

1. ผู้ที่อยู่เวรรักษาการณ์เมือได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางจุรีย์ กุศล	เบอร์โทรศัพท์ติดต่อ	081-287-5567
นายเจษฎา ใบเจริญ	เบอร์โทรศัพท์ติดต่อ	081-409-3707
นางบุรินทร์ ปิติรัตน์	เบอร์โทรศัพท์ติดต่อ	081-746-6525
นายยงยุทธ วุฒิการณ์	เบอร์โทรศัพท์ติดต่อ	081-951-9744
นางสุปราณี ยะวิญชาญ	เบอร์โทรศัพท์ติดต่อ	084-615-0522
นางอุลี ศักดิ์สุวรรณ	เบอร์โทรศัพท์ติดต่อ	085-039-9083

2. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือนเจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย ผู้บังคับบัญชาได้แก่

ผู้อำนวยการศูนย์เทคโนโลยี	เบอร์โทรศัพท์ติดต่อ	081-387-9447
หัวหน้ากลุ่มเทคโนโลยีเครือข่าย	เบอร์โทรศัพท์ติดต่อ	086-116-2239
น.ส.คีรีมาศ มีสุข	เบอร์โทรศัพท์ติดต่อ	090-316-6483
นายวิเชษฐ์ ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	089-636-5278
นายอรรถพล คุณสิทธิ์	เบอร์โทรศัพท์ติดต่อ	085-331-9777
นายสุรชัย คำอ้าย	เบอร์โทรศัพท์ติดต่อ	087-660-7399

3. เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้

4. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

1. การปฏิบัติขณะเกิดแผ่นดินไหว

1) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน

2) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กาแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

3) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร

4) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้

5) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น

6) ห้ามใช้ลิฟท์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น

7) ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า /สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

8) ถ้ากาลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า

9) ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด

10) หลังจากการสั่นสะเทือนสิ้นสุด ให้รีบออกจากอาคาร

11) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้อง โดยยึดหลัก “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

12) ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่

13) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

14) ห้ามใช้ลิฟต์โดยเด็ดขาด

15) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

1) ถ้าอาคารมั่นคงแข็งแรง ให้หลบอยู่ในอาคารนั้น

2) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น

3) หลังการสั่นสะเทือนสิ้นสุดลง ให้หาทางออกจากอาคารนั้น

4) ถ้าไม่อยู่ใกล้ทางออก ให้ “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

5) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดชุลมุน

6) ห้ามใช้ลิฟท์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

1) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

2) หลีกเลี่ยงสิ่งของที่อาจโค่นล้มลงมาทำอันตราย เช่น ตู้ เสาไฟฟ้า ป้ายโฆษณา ต้นไม้ใหญ่

3) หลีกเลี่ยงอาคารสูง กาแพง ระวังเศษอิฐ กระจก ชิ้นส่วนของอาคารที่อาจหล่นลงมา

4) วิ่งไปสู่ที่โล่ง

5) รีบออกจากอาคารที่ชารุดเสียหายโดยเร็วที่สุด

กรณีอยู่ใกล้ชายฝั่ง

หากได้รับการแจ้งเตือน หรือรู้สึกได้ถึงแรงสั่นสะเทือน ให้รีบอพยพจากบริเวณชายฝั่งและริมแม่น้ำลาคลองที่เชื่อมต่อกับทะเลโดยด่วน เพราะอาจเกิดคลื่นสึนามิได้

2. เมื่อแผ่นดินไหวสงบลง

1) ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนาส่งโรงพยาบาล

2) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ

3) ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบการทางานทั้งหมดทันที

4) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

3. ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

1) อยู่กับที่ ป้องกันศีรษะและหน้า จากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ

2) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัสดุหล่นใส่

3) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลือนย้ายเพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย

4) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น

5) ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย

4. การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

1) ระงับสติอารมณ์ ปฏิบัติตามแผนอพยพ

2) เชื่อฟังคาแนะนาของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.

3) เก็บทรัพย์สิน/เอกสารสำคัญ ไว้ในลิ้นชักโต๊ะและล็อคกุญแจ

4) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด

5) ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ

6) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า

7) ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ 2 คน

8) ห้ามพูดคุย สายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง

9) ห้ามใช้ลิฟต์ โดยเด็ดขาด

10) เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที

11) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้

12) ตรวจสอบจานวนผู้อพยพ

5. เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศผ่านทางโทรศัพท์ 081-387-9447 เพื่อทราบและสั่งการต่อไป

6. ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

1. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีม อาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นพ.กนก พิพัฒน์เวช	เบอร์โทรศัพท์ติดต่อ	081-887-9664
นายเดชพิภัทร์ อมรทิพย์วงศ์	เบอร์โทรศัพท์ติดต่อ	089-631-5814
นางนพพร ธนามี	เบอร์โทรศัพท์ติดต่อ	091-012-4800
นางสุปราณี ยะวิญชาญ	เบอร์โทรศัพท์ติดต่อ	084-615-0522

2. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนา แจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย
ผู้บังคับบัญชาได้แก่

ผู้อำนวยการศูนย์เทคโนโลยี	เบอร์โทรศัพท์ติดต่อ	081-387-9447
หัวหน้ากลุ่มเทคโนโลยีเครือข่าย	เบอร์โทรศัพท์ติดต่อ	086-116-2239
น.ส.คีรีมาศ มีสุข	เบอร์โทรศัพท์ติดต่อ	090-316-6483
นายวิเชษฐ์ ไชยช่อฟ้า	เบอร์โทรศัพท์ติดต่อ	089-636-5278
นายอรรถพล คุณสิทธิ์	เบอร์โทรศัพท์ติดต่อ	085-331-9777
นายสุรชัย คำอ้าย	เบอร์โทรศัพท์ติดต่อ	087-660-7399

3. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควร แก่กรณีดังนี้

ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจราจล

1) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของผู้ปฏิบัติงานและของโรงพยาบาล

2) เพิ่มจานวนยามรักษาความปลอดภัยเป็นสองเท่า

3) ปิดประตูทั้ง 2 ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาใน โรงพยาบาลน่าน

4) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของโรงพยาบาลน่าน ให้แจ้งไปยังสถานีตำรวจนครบาล หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้อำนวยการ สานักอำนวยการเพื่อทราบ

ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

1) เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที

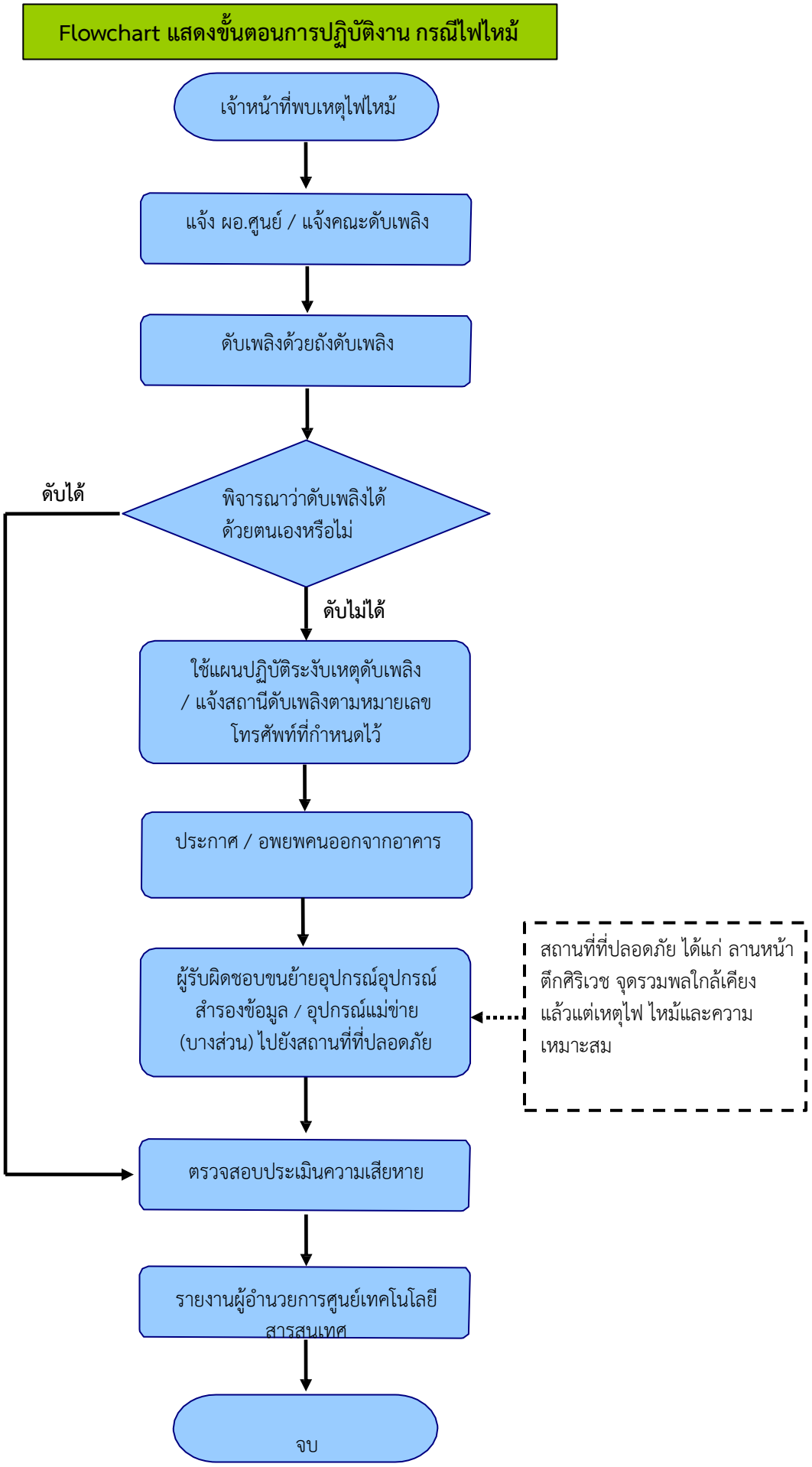
2) รปภ. หรือเจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ พร้อมทั้งติดต่อเจ้าหน้าที่ตำรวจ
ในพื้นที่มาตรวจสอบวัตถุต้องสงสัย

3) ในกรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกั้นพื้นที่อันตรายที่พบวัตถุระเบิด กันบุคคลที่ไม่เกี่ยวข้องออกจากบริเวณที่พบวัตถุระเบิด และแจ้งอพยพผู้ปฏิบัติงานออกจากบริเวณหรือรัศมีของวัตถุระเบิด

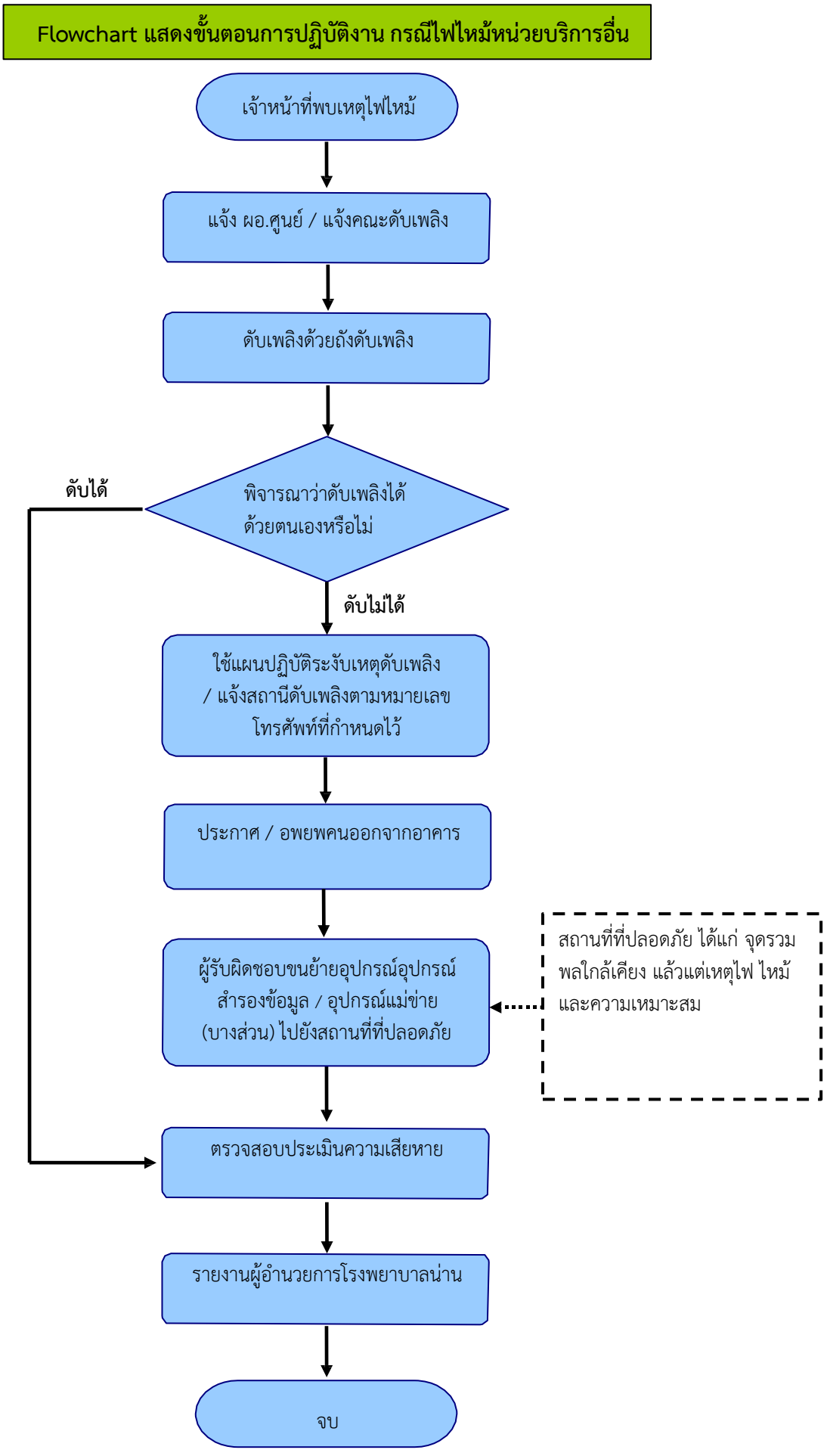
4. เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศผ่านทางโทรศัพท์ 081-387-9447 เพื่อทราบและสั่งการต่อไป

5. ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

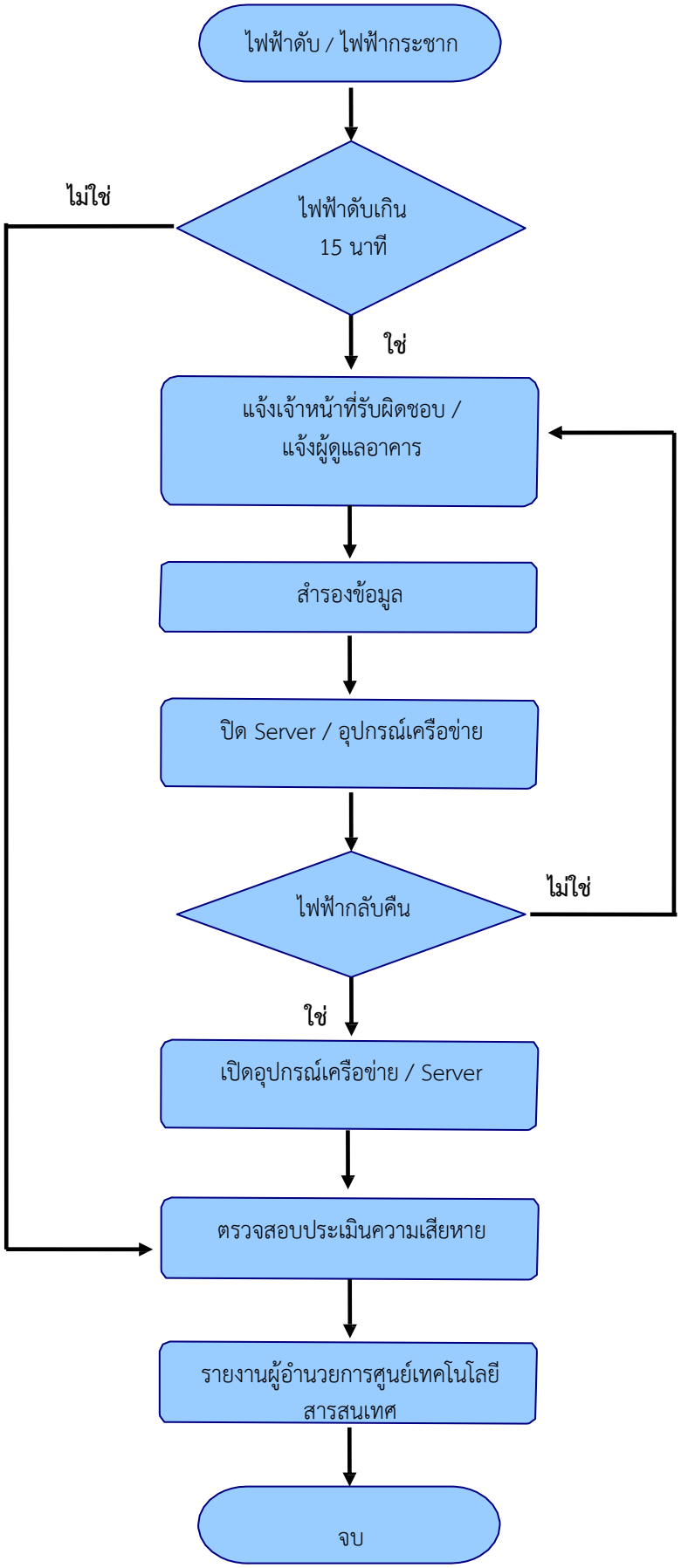
7. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ



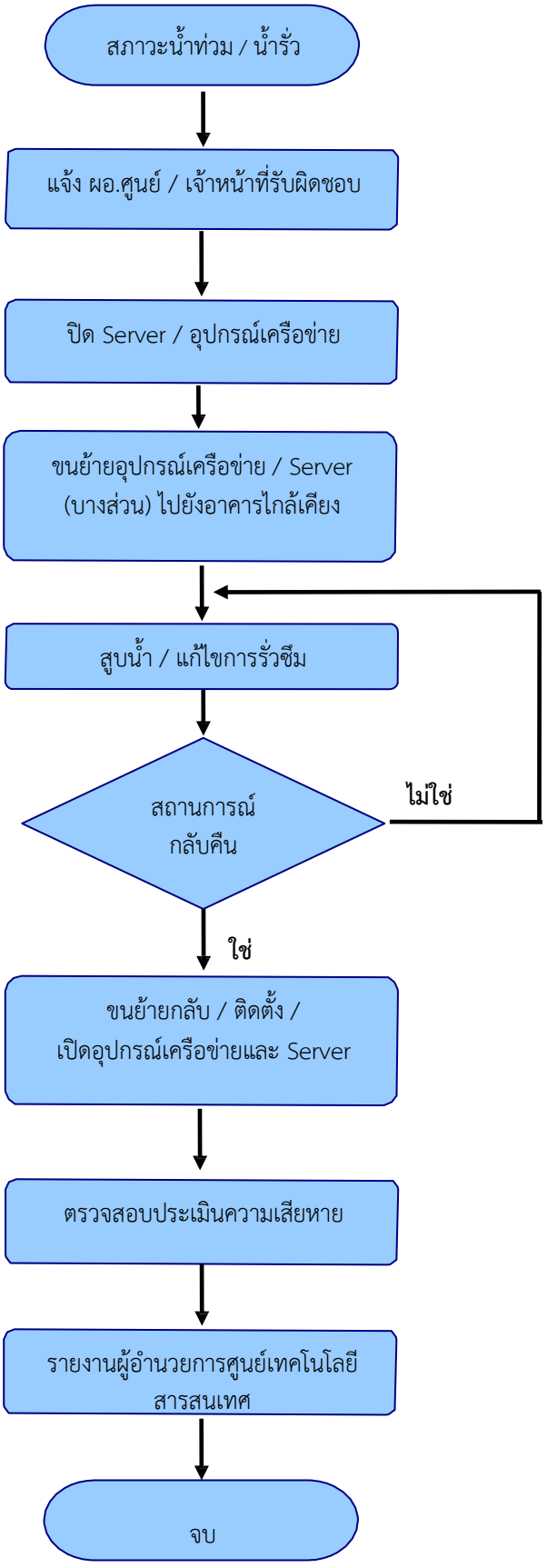
ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ



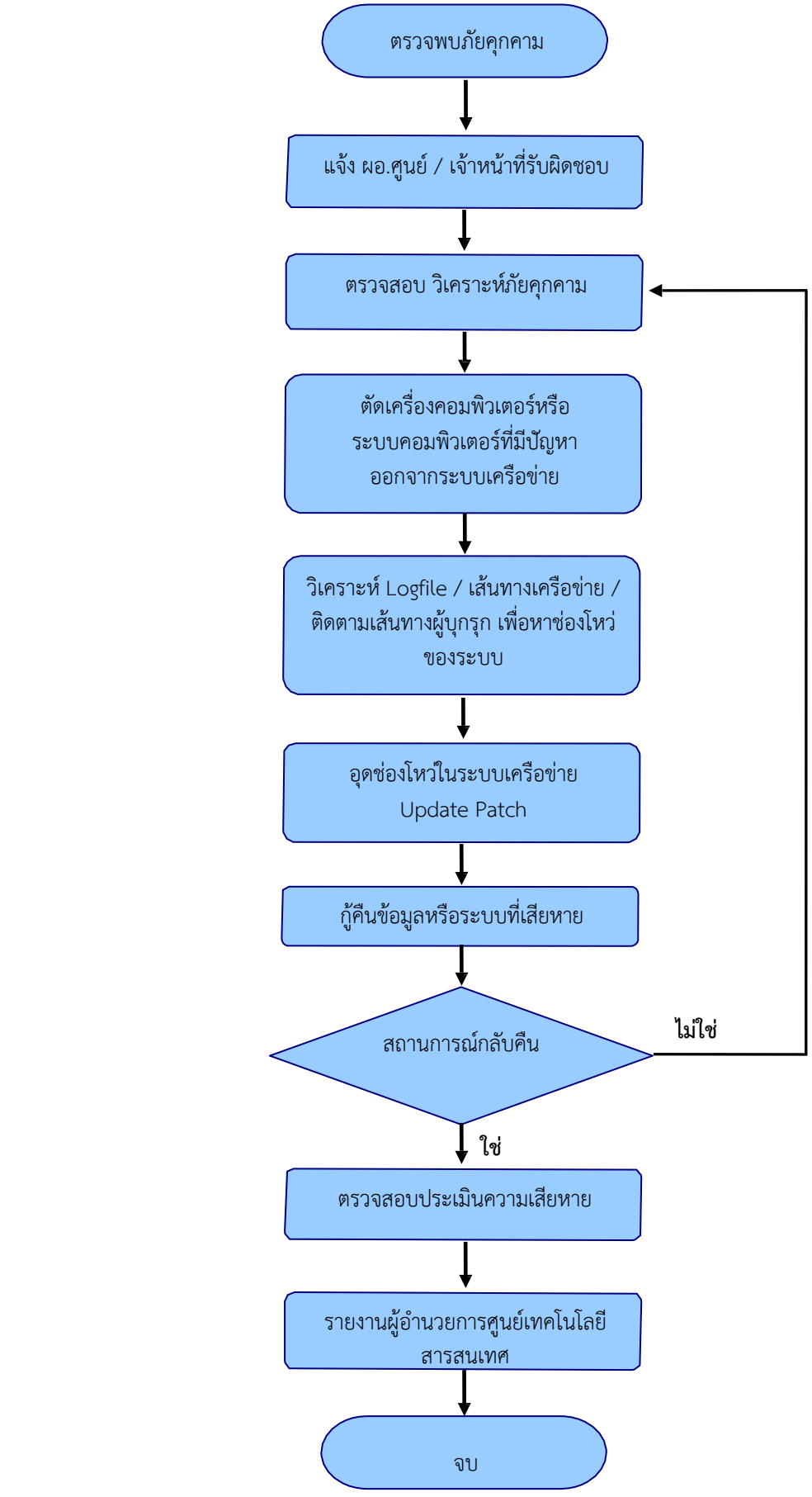
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีไฟฟ้าดับ/ ไฟฟ้ากระชาก / หม้อไฟระเบิด



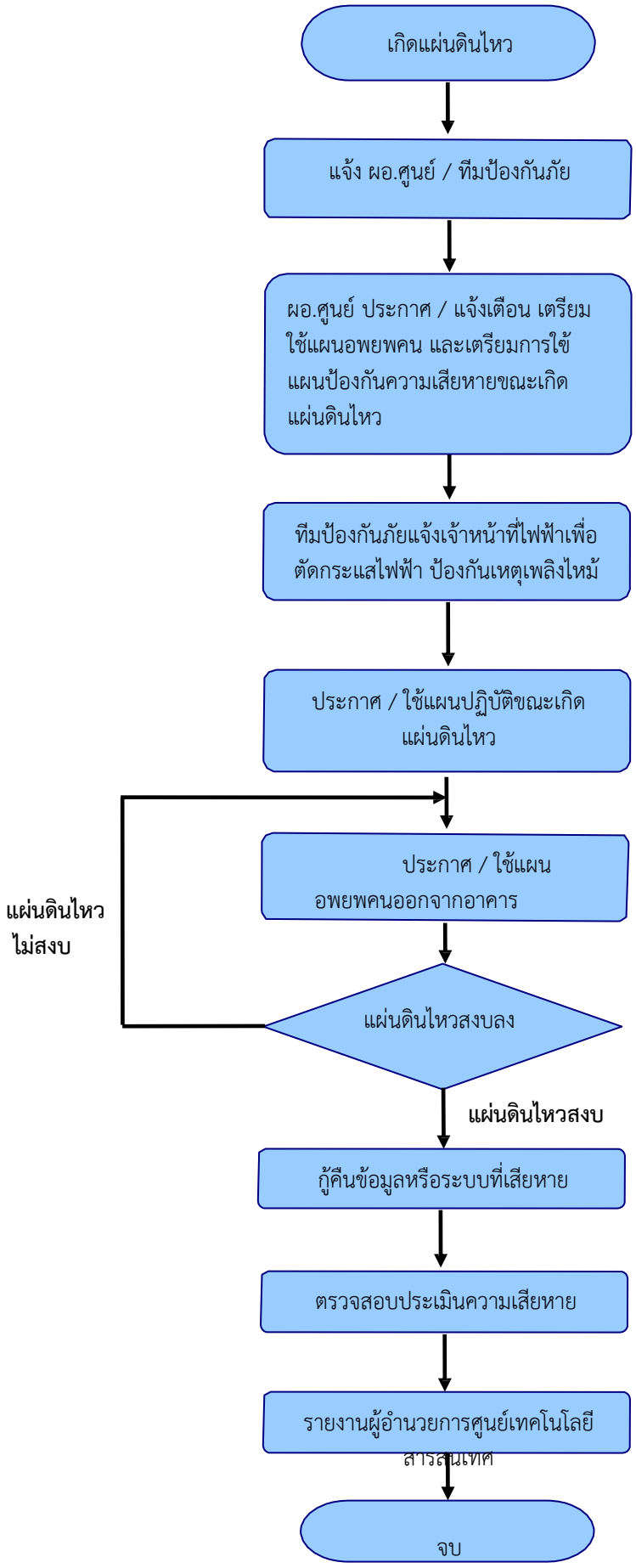
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีน้ำท่วม



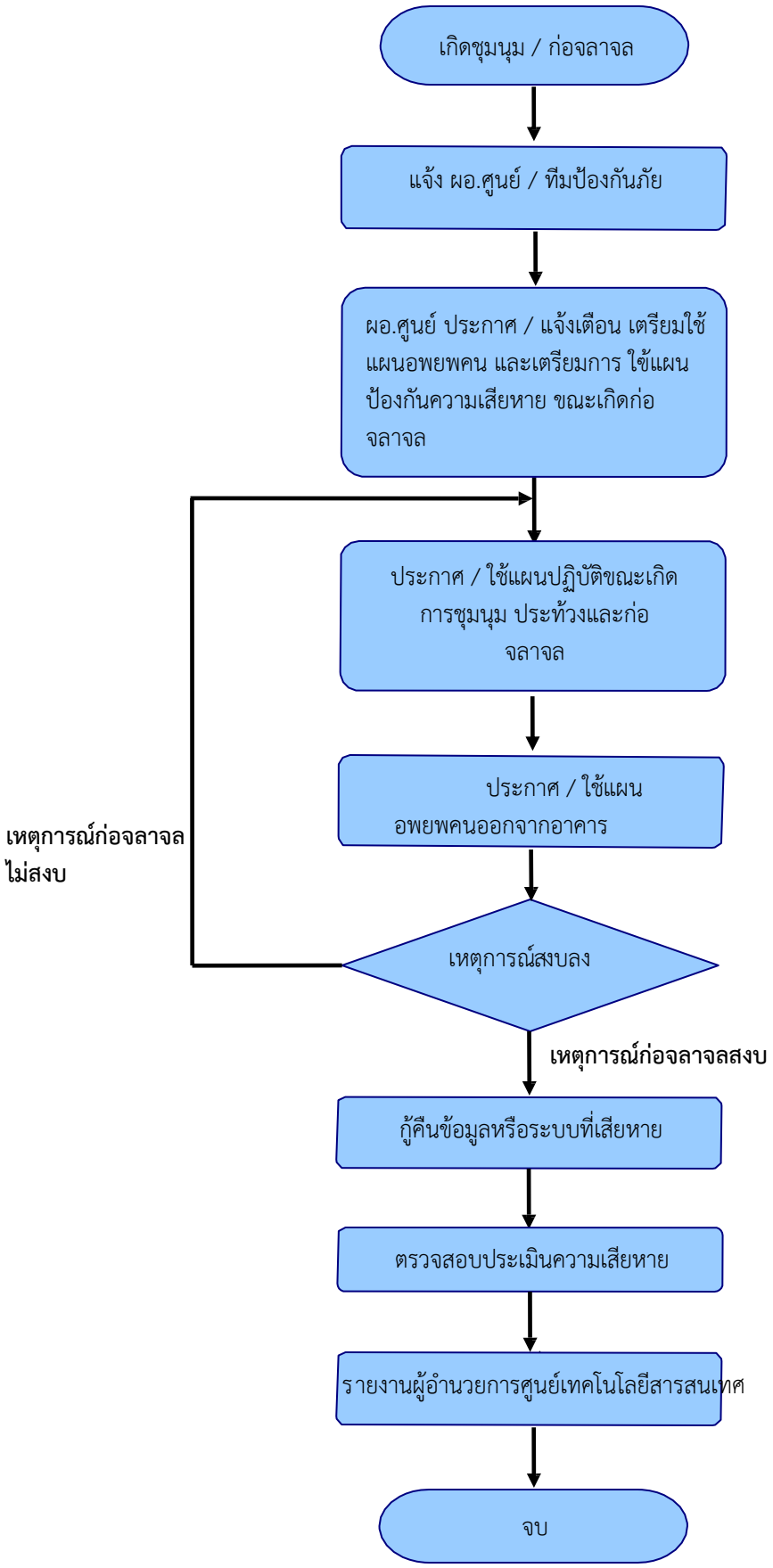
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม



Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดแผ่นดินไหว



Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



8. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทางานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทางานโดยดำเนินการดังนี้

1) จัดหาอุปกรณ์ชิ้นส่วนให้เพื่อทดแทน
2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5) นา BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นากลับมา Restore โดยใช้ทีมกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง
6) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ หน่วยงานจึงมีแผนจัดทำการสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งไซต์ ได้ 3 ไซต์ คือ

1. Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลัก มีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำที่สูง

2. Warm Site เป็นไซต์ที่คล้ายกับ Hot site แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่ำกว่า Hot site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า Hot site

3. Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง Hardware และ Software ในการกู้คืน มีต้นทุนการจัดทำต่า แต่ระยะเวลาในการกู้คืนนาน

แผนการดำเนินการ

1. สำรวจความต้องการของระบบสำรอง
2. สำรวจไซต์สำรองที่เหมาะสม
3. การประเมินความเสี่ยงจากสิ่งต่างๆ รวมถึงการจัดหามาตรการในการลดความเสียง
4. การจัดลำดับผลกระทบขององค์กร
5. การจัดทำแผนกู้คืน
6. การวางแผน การแต่งตั้งทีมงาน ลำดับการทางานหลังระบบได้รับความเสียหาย
7. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่ รวมถึงการฝึกอบรมทางด้านเทคนิค
8. การทดสอบแผน อาจทดสอบกับระบบจาลองก่อนการทดสอบกับระบบจริง
9. การปรับปรุงแผนการกู้คืน

9. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ (Information Security Manager) ทราบ เพื่อนาเสนอรายงานสรุปให้ CEO หรือ CIO เป็นประจาทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนามาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพสามารถ นามาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติต่อไป