แผนรับสถานการณ์ฉุกเฉิน จากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

โรงพยาบาลเมืองจันทร์

งานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

สารบัญ

หน้า

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศ ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์กร ดังนี้

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

โดยอธิบายรายละเอียดดังต่อไปนี้

1. คำนิยาม

“สำนักงานฯ” หมายความว่า ห้องงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์

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

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

“ภัยพิบัติที่มนุษย์สร้างขึ้น” หมายความว่า ภัยพิบัติที่มีสาเหตุมาจากมนุษย์ เช่น การปล่อยก๊าซเรือนกระจกปริมาณมากจากโรงงานอุตสาหกรรมจนส่งผลให้ระดับน้ำทะเลเพิ่มสูงขึ้นและท่วมพื้นที่ในระดับต่ำ การเปลี่ยนทางน้ำจนทำให้เกิดภัยแล้งในบางพื้นที่ เป็นต้น รวมถึงการจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ และการเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ที่มนุษย์เป็นผู้กระทำ

“เจ้าหน้าที่ผู้รับผิดชอบอุปกรณ์” หมายความว่า ผู้ใช้งานประจำเครื่อง นั้นๆ

2. วัตถุประสงค์

2.1 เพื่อใช้เป็นแนวทางการรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศของโรงพยาบาลเมืองจันทร์

2.2 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาลเมืองจันทร์

2.3 เพื่อเป็นแนวทางในการดูรักษาความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.4 เพื่อให้การปฏิบัติเป็นไปอย่างมีระบบและต่อเนื่องและสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดเหตุการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อสารสนเทศ

2.5 เพื่อให้สอดคล้องตามโยบายการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โรงพยาบาลเมืองจันทร์

3. ผู้รับผิดชอบ

3.1 ผู้บังคับบัญชา

3.2 ผู้ดูแลระบบที่ได้รับมอบหมาย

3.3 ผู้ใช้งาน

4. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

4.1 วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กร สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

4.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ 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
น้ำ'ท่วม / 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 เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์ เทคโนโลยีสารสนเทศจะทำการแจ้งให้ CEO หรือ CIO ขององค์กรทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

5.2 กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในองค์กร โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

5.3 การติดต่อสื่อสาร (Communication) มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อ ทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

5.4 การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้โดยเตรียมอุปกรณ์ดังนี้

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

5.5 การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุก ทำลายหรือเปลี่ยนแปลงข้อมูลโดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยองค์กรมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

5.6 การป้องกันไวรัสคอมพิวเตอร์

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

5.7 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

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

5.8 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทางดังนี้

1) มาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบพาเข้าไป เจ้าหน้าที่ทุกคนต้องสแกนลายนิ้วมือเพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่าย และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

2) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา
3) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์
4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ใน การเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป
5) การดำเนินการตาม พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

5.9 การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

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

6. การเตรียมความพร้อม

6.1 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสียงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

6.1.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อไฟระเบิด
6.1.2 ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ 30 - 60 นาที
6.1.3 เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
6.1.4 เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ
6.1.5 ให้มีการสำรองฐานข้อมูลทุก 1 เดือนเป็นอย่างน้อย

6.2 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

6.2.1 จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้

6.2.2 ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบเครือข่าย เพื่อการควบคุมเพลิงในเบื้องต้น

6.2.3 ให้มีการสำรองฐานข้อมูลเดือนละ 1 ครั้งเป็นอย่างน้อย

6.3 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม / น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม /น้ำรั่ว ซึ่งอาจสร้างความเสียหายแกระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ 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 ซึ่งทำหน้าที่กำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

6.4.2 มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

6.4.3 อัพเดตโปรแกรมกำจัดไวรัส ทุก 1 เดือน เป็นอย่างน้อย (Update Patch)

6.4.4 ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

6.5 การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุก และภัยคุกคามทางคอมพิวเตอร์โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

6.5.1 กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

6.5.2 หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องควบคุมระบบเครือข่ายจะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศผู้ดูแลระบบเครือข่ายเป็นผู้รับผิดชอบพาเข้าไปที่ประตูเข้า-ออก และคอยกำกับดูแลตลอดการปฏิบัติงานสำหรับประตูเข้า-ออก มีการติดตั้งระบบ Access Control โดยใช้การสแกนลายนิ้วมือ และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

6.5.3 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

6.5.4 มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

6.5.5 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

6.5.6 มีการป้อนชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

6.6 การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบเจ้าหน้าที่แผนกต่างๆ ภายในองค์กร ขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์

ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสียงให้เกิดขึ้นน้อยที่สุด

6.6.1 สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ขององค์กร เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

6.6.2 วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์ จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

6.7 การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูลประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

6.7.1 ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้องเชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

1) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ,ข้อมูลอุณหภูมิ,ข่าวเตือนภัย (www.tmd.go.th)
2) ศูนย์เตือนภัยพิบัติแห่งชาติ: การแจ้งเตือนล่วงหน้า (www.http://ndwc.disaster.go.th/in.ndwc-9.283/)
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 อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

1) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู
2) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน
3) หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

4) ปลากระโดดขึ้นมาจากผิวน้ำ

6.7.3 การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

1) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
2) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
3) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่มสำหรับบุคลากรขององค์กร
4) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์อย่างมีประสิทธิภาพเมื่อเกิดภัย
5) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่างๆ

6.7.4 การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

1) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม
2) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

6.7.5 การปฏิบัติขั้นเตรียมการ

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

6.8 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

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

7. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

7.1 ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบายให้ข้อเสนอแนะ ปรึกษา ตลอดจนติดตาม กากับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

ผู้อำนวยการโรงพยาบาลเมืองจันทร์ (CEO)

รองผู้อำนวยการฝ่ายการแพทย์ โรงพยาบาลเมืองจันทร์ (CIO)

รองผู้อำนวยการฝ่ายบริหาร โรงพยาบาลเมืองจันทร์

รองผู้อำนวยการฝ่ายการพยาบาล โรงพยาบาลเมืองจันทร์

หัวหน้าศูนย์เทคโนโลยีสารสนเทศ (Information Security Manager)

7.2 ระดับปฏิบัติ

ก) ทีมบริหารจัดการการกู้คืนระบบ ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ข) ทีมกู้คืนเครือข่าย ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติผู้รับผิดชอบ ได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ค) ทีมกู้คืนแอปพลิเคชัน ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

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

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

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

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

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

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศได้จัดหาไว้ ผู้รับผิดชอบ ได้แก่

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ซ) ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อไฟระเบิด ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ฌ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม ผู้รับผิดชอบได้แก่

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์ ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ฎ) ทีมสำรองและกู้คืนข้อมลู (Backup & Recovery) ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมลู และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานให้ได้ทันทีและครบถ้วนสมบูรณ์ผู้รับผิดชอบ ได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ฏ) ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหวทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผนที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลง ให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและกอจลาจล ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชาเพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนมุประทวงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหาย ทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

นางสาวรธิดา มูลลา	เบอร์โทรศัพท์ติดต่อ	093-348-8488
นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

8. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

8.1 กรณีเครื่องลูกข่าย

1) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบหรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ
2) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย(สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงานภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด
3) ให้เจ้าหน้าที่ด้าน IT ของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ศูนย์เทคโนโลยีสารสนเทศเพื่อแก้ไขปัญหาต่อไป

8.2 กรณีเครื่องแม่ข่ายบริการ (Server)

1) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ
2) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

3) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
4) ตรวจสอบปัญหาที่เกิดขึ้นในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย
5) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว
6) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย
7) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด
8) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
9) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการ หรือศูนย์เทคโนโลยีสารสนเทศทราบโดยเร็ว

9. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

9.1 กรณีจากไฟไหม้ห้องควบคุมระบบ

1) ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 082-362-9362 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงานเพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
3) ใช้อุปกรณ์ที่น้ำยาดับเพลิง ฉีดควบคุมเพลิงดับและจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัย ได้แก่ นอกตึกอาคารสำนักงาน จุดรวมพล หรือแล้วแต่เหตุไฟไหม้และความเหมาะสม แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องดำเนินการในข้อต่อไป
4) แจ้งหน่วยงานที่มีรถดับเพลิงที่ใกล้ที่สุด คือเทศบาลตำบลหนองใหญ่ ตั้งอยู่ที่หมู่ที่ 10 ตำบลหนองใหญ่ อำเภอเมืองจันทร์ จังหวัดศรีสะเกษ และเทศบาลตำบลเมืองจันทร์ ตั้งอยู่ เลขที่ 70 หมู่ 6 ตำบลเมืองจันทร์ อำเภอเมืองจันทร์ จังหวัดศรีสะเกษ เพื่อดำเนินการต่อไป
5) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
6) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการทราบ

9.2 กรณีไฟดับ / หม้อไฟระเบิด

1) ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362

นางสาวจุฑารัตน์ โอวาท เบอร์โทรศัพท์ติดต่อ 080-464-6290
นายทวีรัชต์ งาหอม เบอร์โทรศัพท์ติดต่อ 098-983-6165

2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 082-362-9362 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
3) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
4) แจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการโดย การไฟฟ้าส่วนภูมิภาคสาขาอำเภออุทุมพรพิสัย ตั้งอยู่ที่ 677 หมูที่ 7 ถนนศรีบุญลือ ตำบลกำแพง เบอร์โทรศัพท์ 045-638295 เพื่อดำเนินการต่อไป
5) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการ ทราบ

9.3 กรณีน้ำท่วมห้องควบคุมระบบ

1) ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังชั้น 2 , 3 พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์ เบอร์โทรศัพท์ติดต่อ 082-362-9362
นางสาวจุฑารัตน์ โอวาท เบอร์โทรศัพท์ติดต่อ 080-464-6290
นายทวีรัชต์ งาหอม เบอร์โทรศัพท์ติดต่อ 098-983-6165

2) แจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทางโทรศัพท์ 082-362-9362 และผู้มีหน้าที่รับผิดชอบทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด
3) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการเพื่อทราบและสั่งการต่อไป
4) ผู้ควบคุมในกรณีนี้จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการ ทราบ

9.4 กรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์

1) ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบประกอบด้วย

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์ เบอร์โทรศัพท์ติดต่อ 082-362-9362
นางสาวจุฑารัตน์ โอวาท เบอร์โทรศัพท์ติดต่อ 080-464-6290
นายทวีรัชต์ งาหอม เบอร์โทรศัพท์ติดต่อ 098-983-6165

2) แจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่าย ทางโทรศัพท์ 086-116-2239 เพื่อทราบและดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้า ควบคุมสถานการณ์ เพื่อระบบงาน

และเครือข่ายได้รับความเสียหายน้อยที่สุด พร้อมทั้งทำให้ระบบรักษาความ ปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

3) ให้ผู้รับผิดชอบสนเทศของหน่วยงานตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้แจ้งเหตุขัดข้องให้ ศูนย์สนับสนุนบริการสุขภาพที่ 10 เพื่อแก้ไขปัญหาต่อไป

9.4.1 ขั้นตอนในการกู้คืนระบบความปลอดภัยกรณีโดนเจาะระบบและภัยคุกคามทางคอมพิวเตอร์ 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) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ดให้ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

3) ผู้รับผิดชอบในข้อ 2 ดำเนินการรายงานการถูกโจมตีผ่านทางโทรศัพท์ 092-561-8295 แก่ผู้อำนวยการ เพื่อทราบและสั่งการต่อไป

4) ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่ายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์และผู้อำนวยการ ทราบ

9.5 กรณีแผ่นดินไหว

1) ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

2) เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือนเจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย ผู้บังคับบัญชาได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

3) เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้
4) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

9.5.1 ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

1) การปฏิบัติขณะเกิดแผ่นดินไหว

ก) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน
ข) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้
ค) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร
ง) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้
จ) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น
ฉ) ห้ามใช้ลิฟต์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น
ช) ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด
ซ) ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า
ฌ) ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด
ญ) หลังจากการสั่นสะเทือนสิ้นสุดให้รีบออกจากอาคาร
ฎ) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้องโดยยึดหลัก “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ
ฏ) ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่
ฐ) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน
ฑ) ห้ามใช้ลิฟต์โดยเด็ดขาด
ฒ) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

1) ถ้าอาคารมั่นคงแข็งแรงให้หลบอยู่ในอาคารนั้น
2) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น
3) หลังการสั่นสะเทือนสิ้นสุดลงให้หาทางออกจากอาคารนั้น
4) ถ้าไม่อยู่ใกล้ทางออกให้ “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ
5) ล้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดชุลมุน
6) ห้ามใช้ลิฟต์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

1) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด
2) หลีกเลี่ยงสิ่งของที่อาจโค่นล้มลงมาทำอันตราย เช่น ตู้ เสาไฟฟ้า ป้ายโฆษณา ต้นไม้ใหญ่

3) หลีกเลี่ยงอาคารสูง กำแพง ระวังเศษอิฐ กระจก ชิ้นส่วนของอาคารที่อาจหล่นลงมา
4) วิ่งไปสู่ที่โล่ง
5) รีบออกจากอาคารที่ชำรุดเสียหายโดยเร็วที่สุด

กรณีอยู่ใกล้ชายฝั่ง

หากได้รับการแจ้งเตือนหรือรู้สึกได้ถึงแรงสั่นสะเทือนให้รีบอพยพจากบริเวณชายฝั่งและริมแม่น้ำลำคลองที่เชื่อมต่อกับทะเลโดยด่วน เพราะอาจเกิดคลื่นสึนามิได้

2) เมื่อแผ่นดินไหวสงบลง

1) ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทำการปฐมพยาบาลเบื้องต้นและนำส่งโรงพยาบาล
2) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ
3) ตรวจสอบโครงสร้างอาคาร ท่อน้ำ ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบ การทำงานทั้งหมดทันที
4) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

3) ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

1) อยู่กับที่ ป้องกันศีรษะและหน้าจากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อผ้าห่มหนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ
2) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ขั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัสดุหล่นใส่ แตกหักพังทลาย
3) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจากสิ่งของ
4) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น
5) ส่งสัญญาณขอความช่วยเหลือ และรอการช่วยเหลือจากหน่วยกู้ภัย

4) การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

1) ระงับสติอารมณ์ ปฏิบัติตามแผนอพยพ
2) เชื่อฟังคำแนะนำของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.
3) เก็บทรัพย์สิน/เอกสารสำคัญไว้ในลิ้นชักโต๊ะและล็อคกุญแจ
4) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด
5) ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ
6) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินข้า
7) ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ 2 คน
8) ห้ามพูดคุย สายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง
9) ห้ามใช้ลิฟต์ โดยเด็ดขาด
10) เมื่ออพยพถึงขั้นล่างสุดให้ออกจากอาคารทันที
11) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้
12) ตรวจสอบจำนวนผู้อพยพ

5) เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการ ผ่านทางโทรศัพท์ 092-561-8295 เพื่อทราบและสั่งการต่อไป
6) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการ และหัวหน้ากลุ่มงานประกันสุขภาพ ยุทธศาสตร์และสารสนเทศทางการแพทย์ ทราบ

9.6 กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

1) ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้น ทีมอาคารสถานที่ผู้รับผิดชอบ ได้แก่

นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

2) เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือนเจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหาย ผู้บังคับบัญชาได้แก่

นางสาวธัณย์จิรา ปัญโญพิพัฒณ์	เบอร์โทรศัพท์ติดต่อ	082-362-9362
นางสาวจุฑารัตน์ โอวาท	เบอร์โทรศัพท์ติดต่อ	080-464-6290
นายทวีรัชต์ งาหอม	เบอร์โทรศัพท์ติดต่อ	098-983-6165

3) หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรได้แก่ กรณีดังนี้

9.6.1 ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจลาจล

ก) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของ ผู้ปฏิบัติงานและของโรงพยาบาล
ข) เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า
ค) ปิดประตูทั้ง 2 ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาในโรงพยาบาลเมืองจันทร์
ง) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของโรงพยาบาลเมืองจันทร์ ให้แจ้งไปยังสถานีตำรวจภูธร อำเภอเมืองจันทร์ หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้รองผู้อำนวยการกลุ่มบริหารงานทั่วไปเพื่อทราบ

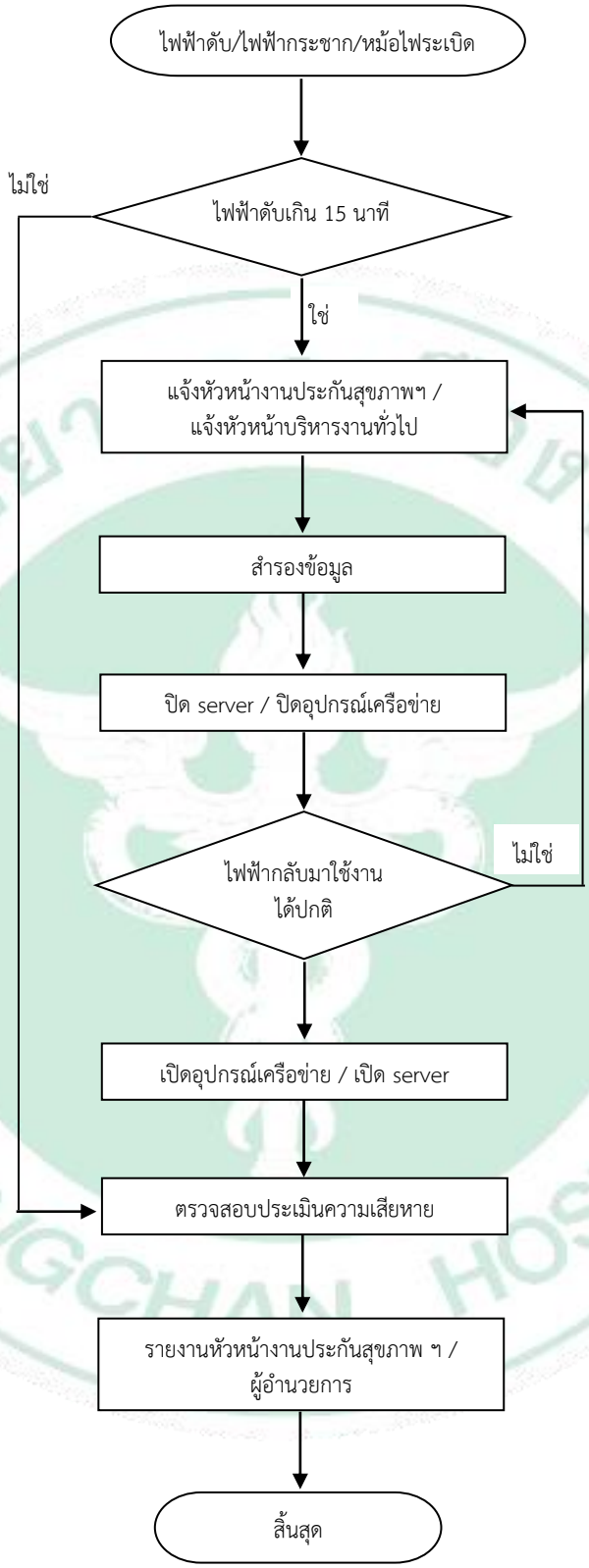
9.6.2 ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

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

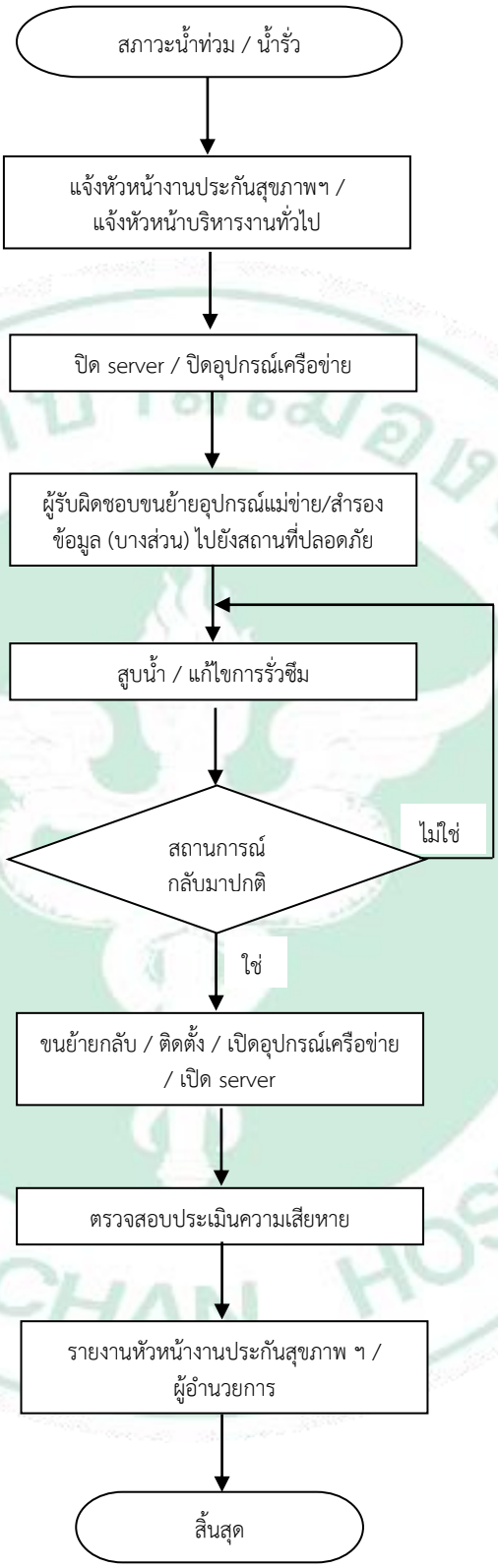
10. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเพลิงไหม้

Flowchart แสดงขั้นตอนการปฏิบัติ กรณีไฟฟ้าดับ/ไฟฟ้ากระชาก/หม้อไฟระเบิด

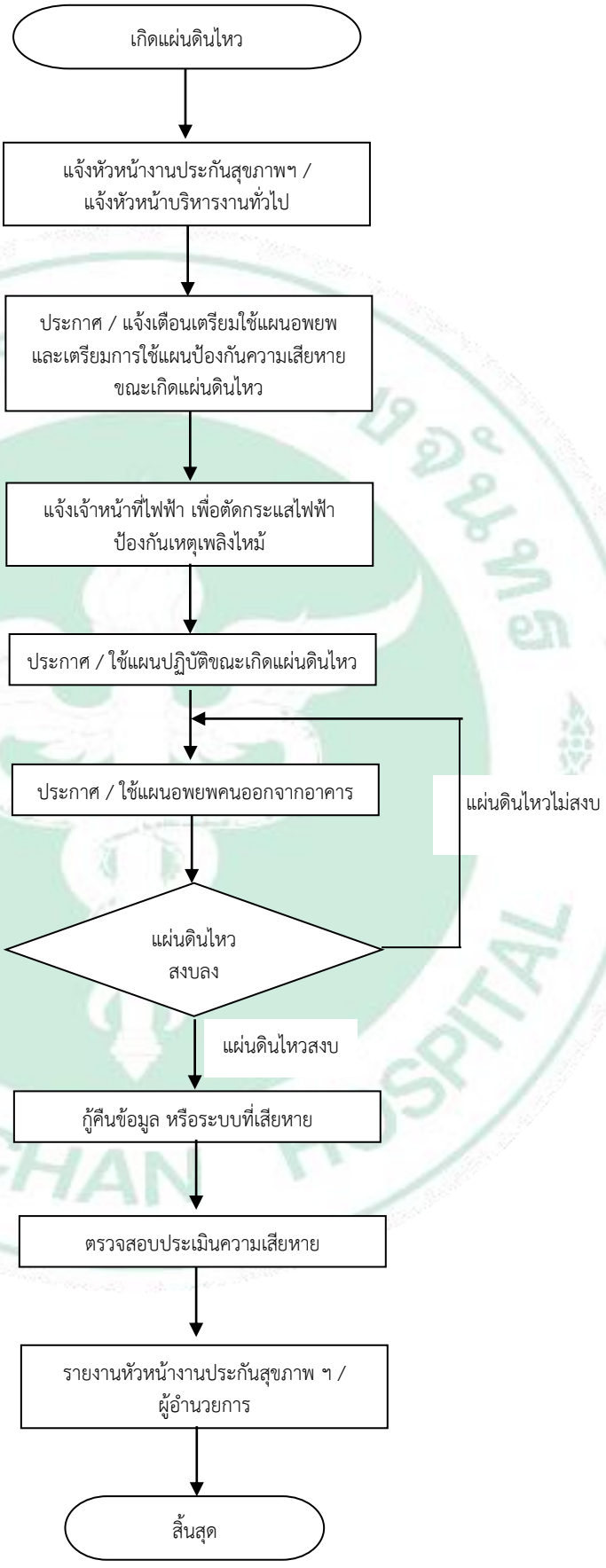


Flowchart แสดงขั้นตอนการปฏิบัติ กรณีน้ำท่วม

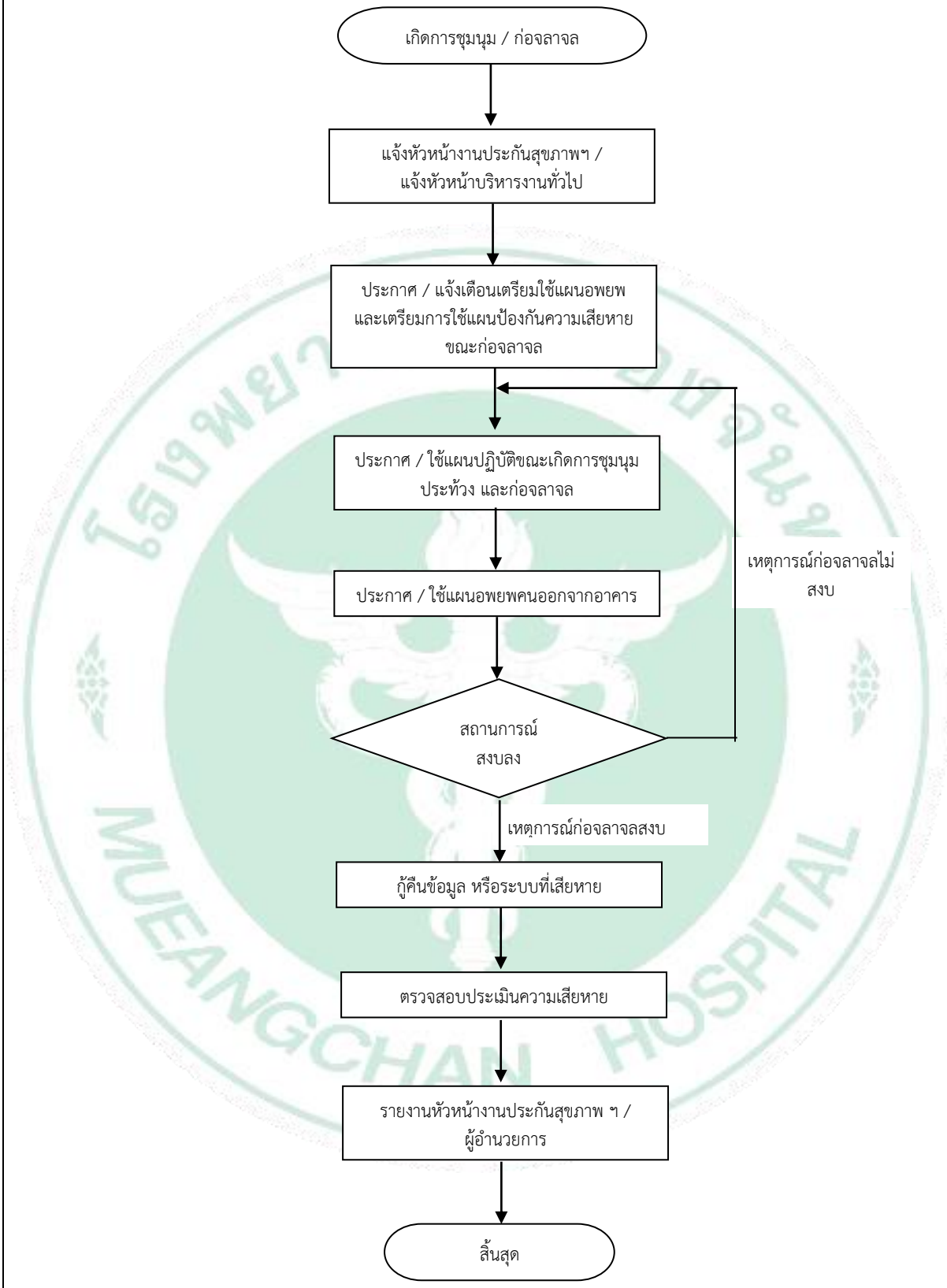


Flowchart แสดงขั้นตอนการปฏิบัติ กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม

Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดแผ่นดินไหว



Flowchart แสดงขั้นตอนการปฏิบัติ กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



11. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม (Disaster Recovery Plan)

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

1) จัดหาอุปกรณ์ชิ้นส่วนให้เพื่อทดแทน
2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5) นำ BACKUP TAPE / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบ กู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง
6) ตรวจสอบระบบปฏิบัติการฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ 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 เพื่อป้องกันกรณีที่ข้อมูลในข้อที่ 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 เพื่อนำเสนอรายงานสรุปให้ผู้อำนวยการทราบเป็นประจำ และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันที ที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติต่อไป


VIRUS