



แผนรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)
โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 19

สารบัญ

	หน้า
บทนำ	1
วัตถุประสงค์	1
การวิเคราะห์ความเสี่ยง	1
แผนรองรับสถานการณ์ฉุกเฉิน	3
สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค	
กรณีการป้องกันไวรัสล้มเหลว	4
กรณีการป้องกันผู้บุกรุกล้มเหลว	4
กรณีการเชื่อมโยงเครือข่ายล้มเหลว	4
กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย	6
กรณีไฟฟ้าขัดข้อง	7
สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ	
กรณีไฟไหม้	8
กรณีน้ำท่วม	9
กรณีแผ่นดินไหว	10
สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง	
กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง	11
สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล	
กรณีโจรกรรม	12
การกำหนดผู้รับผิดชอบ	14

แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency plan)

1. บทนำ

ปัจจุบัน กระทรวงสาธารณสุขมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น โรงพยาบาลจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

โรงพยาบาลสมเด็จพระสังฆราชองค์ที่ 19 ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการทำงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมียุทธศาสตร์รองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันที่
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19

3. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ โรงพยาบาลสมเด็จพระสังฆราชองค์ที่19เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19 พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกรวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น
2. ความเสี่ยงด้านบุคคล เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19 เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศเช่น ไฟฟ้าขัดข้อง น้ำท่วม อัคคีภัย การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19 ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19

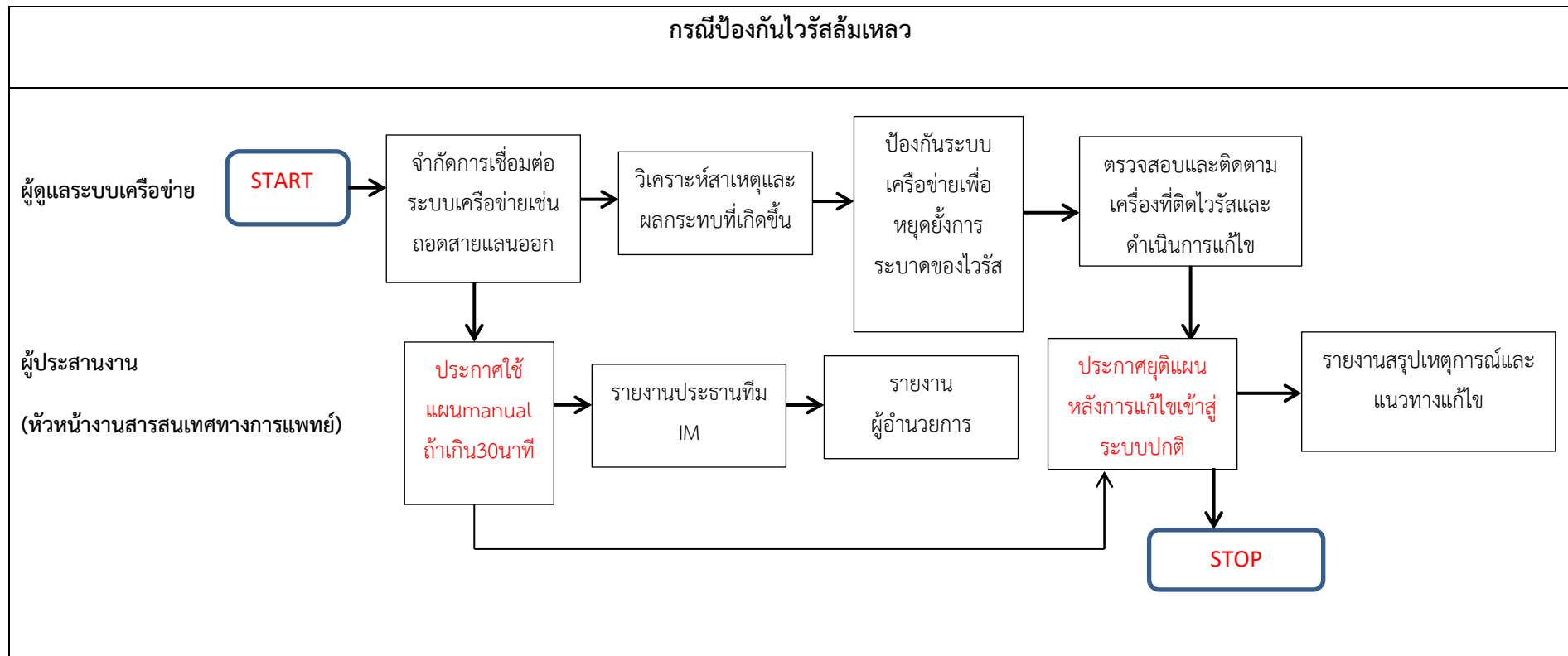
4. แผนรองรับสถานการณ์ฉุกเฉิน

4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

4.1.1 กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าสู่ระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่งานสารสนเทศทางการแพทย์ทราบ หรือกรณีมีเหตุอันทำให้งานสารสนเทศทางการแพทย์ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ งานสารสนเทศทางการแพทย์จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

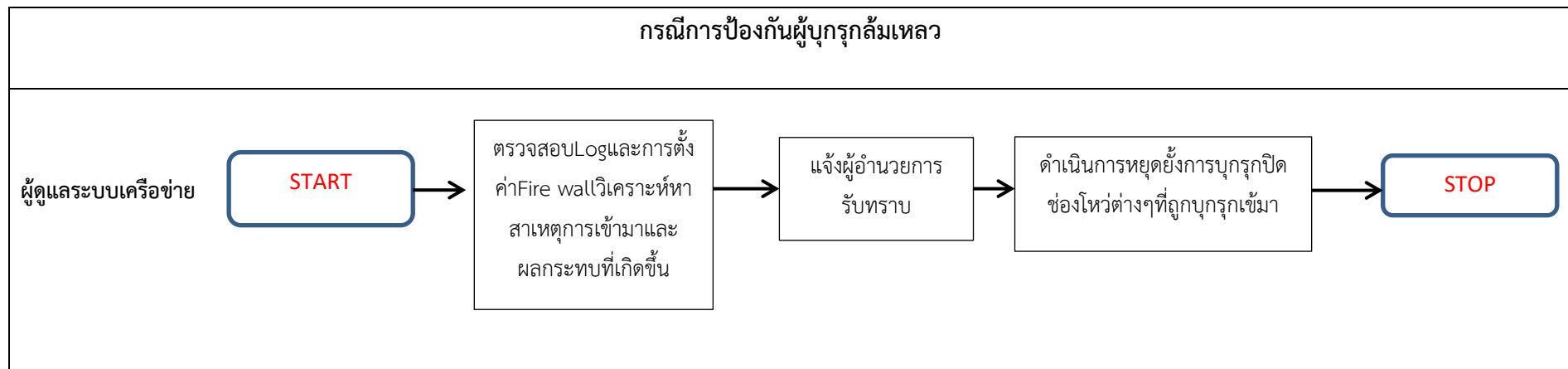
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



4.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งผู้หัวหน้างานสารสนเทศทางการแพทย์ให้ทราบโดยด่วนเพื่อแจ้งผู้อำนวยการโรงพยาบาลในทันที
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

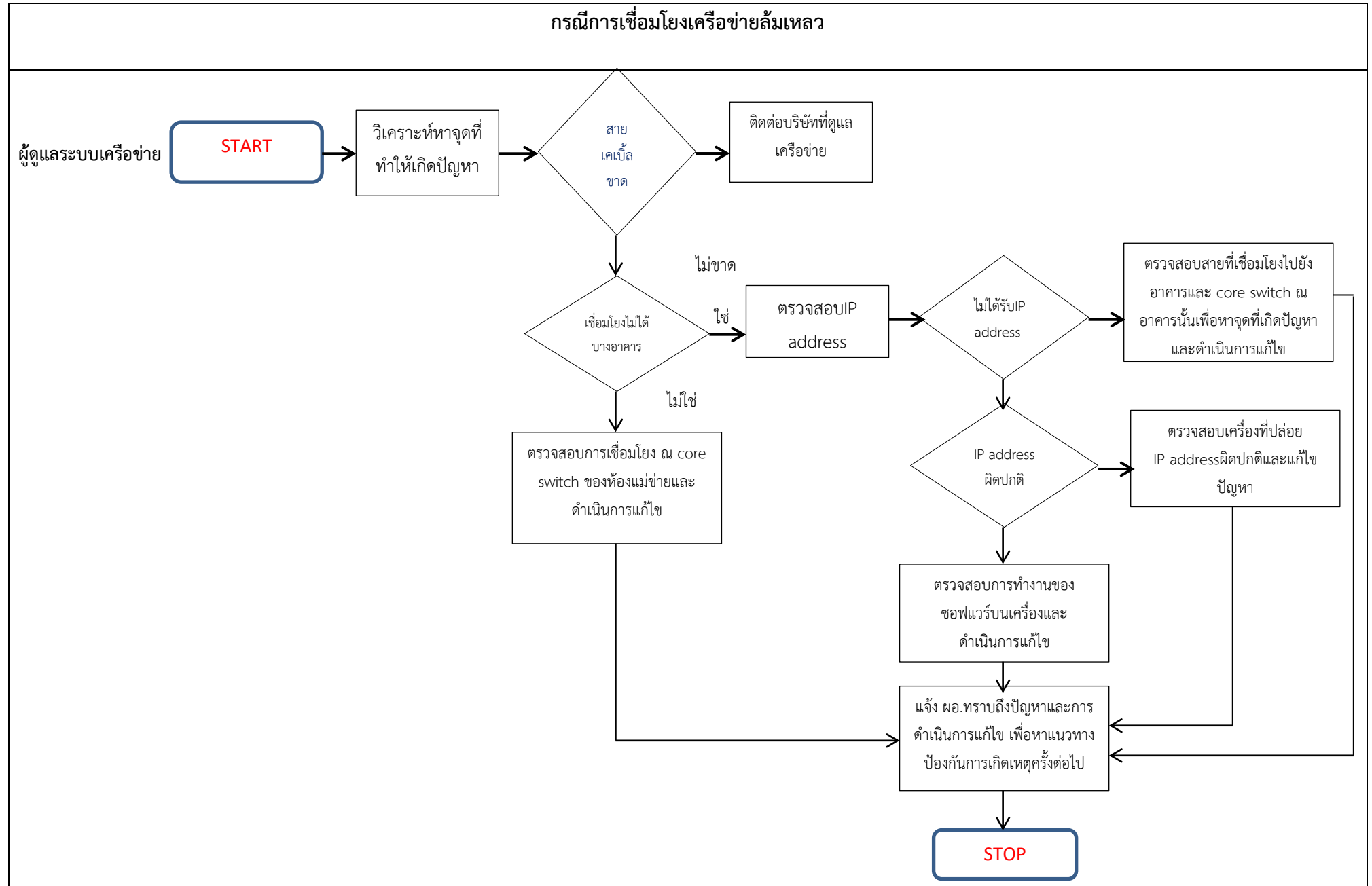
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



4.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รับผิดชอบการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

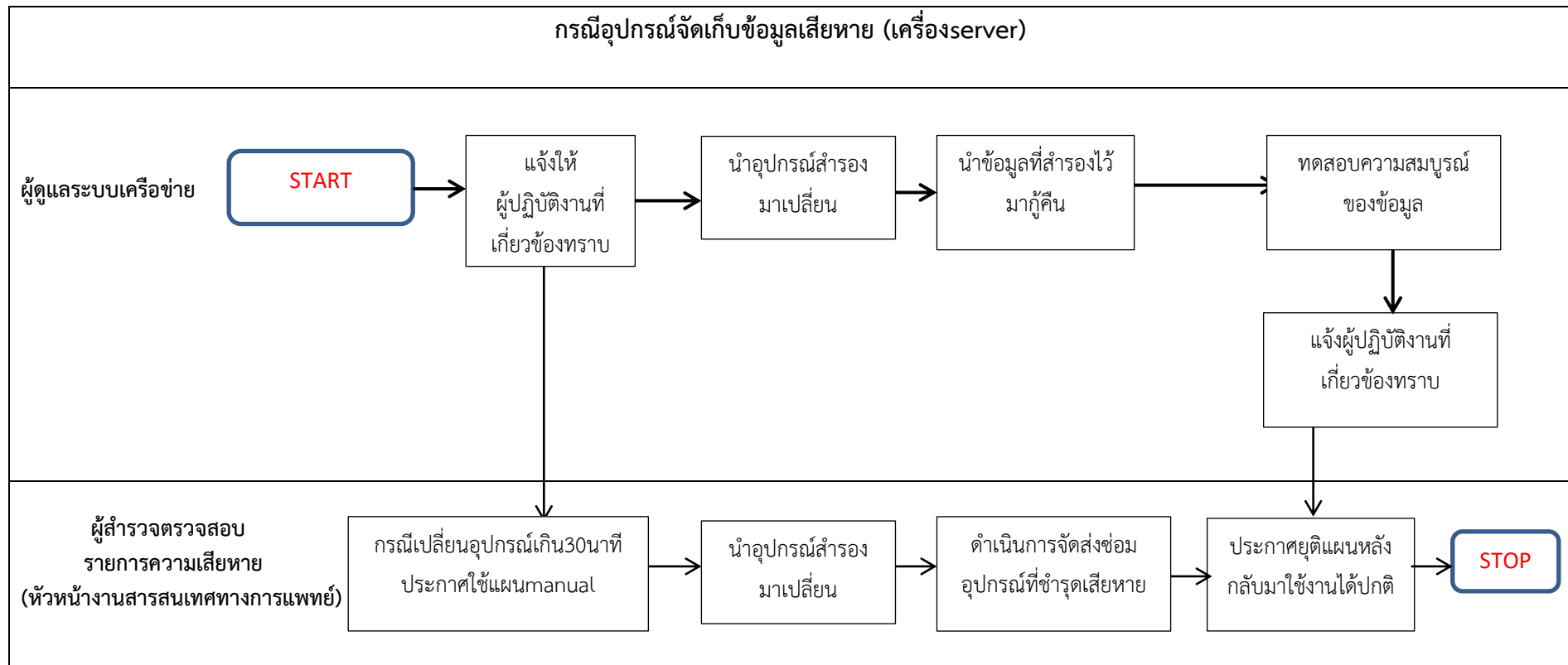
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



4.1.4 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

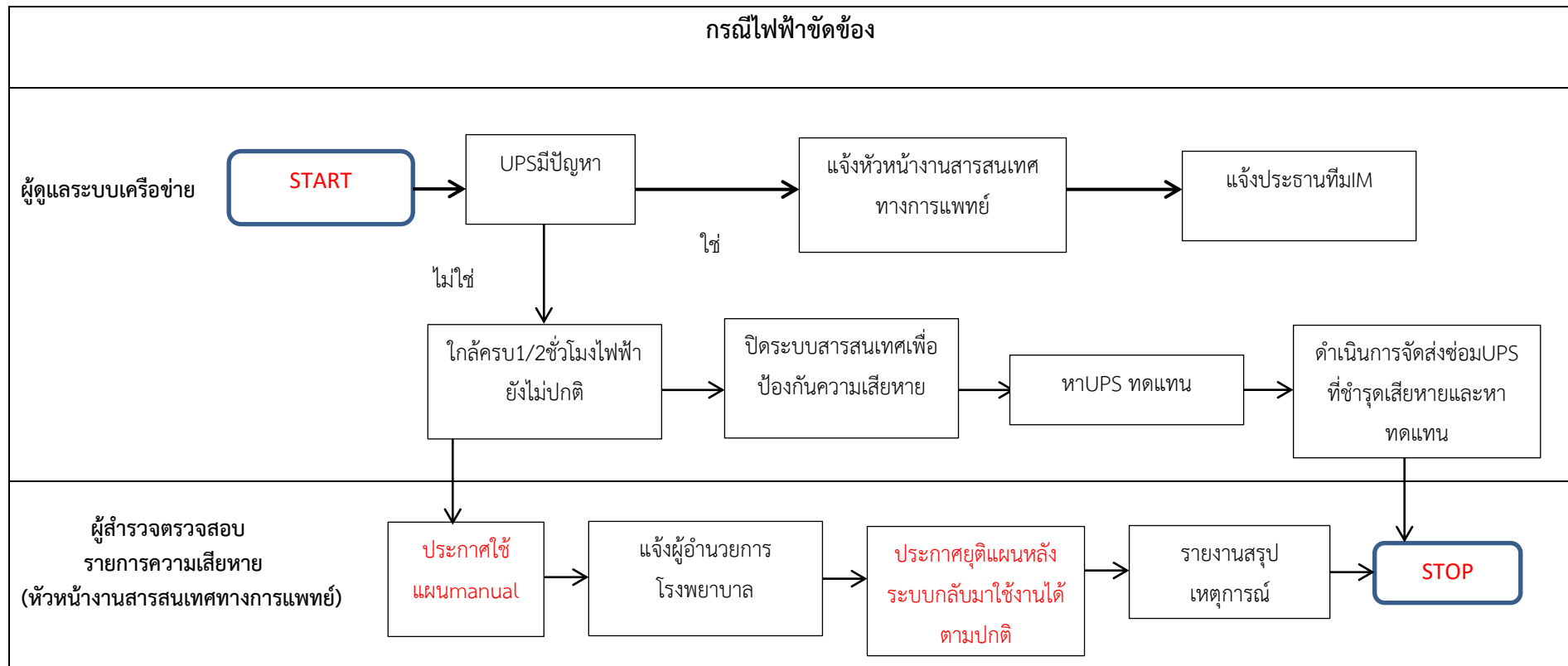
- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รับผิดชอบการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



4.1.5 กรณีไฟฟ้าขัดข้อง

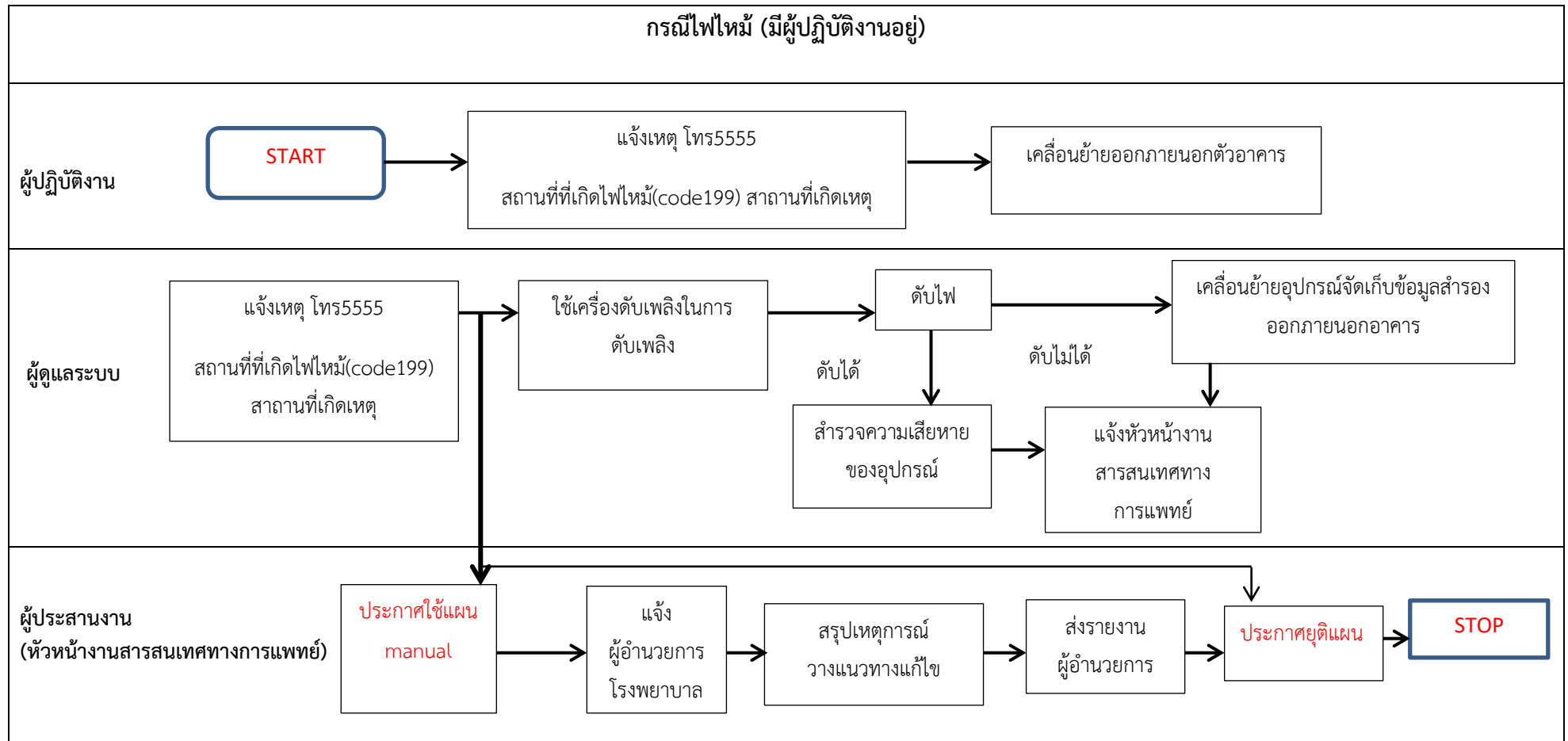
- ระบบฐานข้อมูลสารสนเทศ(เครื่องserver) มี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 1/2 ชั่วโมง
 - หากใกล้ครบ 1/2 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้างานสารสนเทศทางการแพทย์
 - ผู้ดูแลระบบดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
 - หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้อำนวยการโรงพยาบาล เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน
- แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง



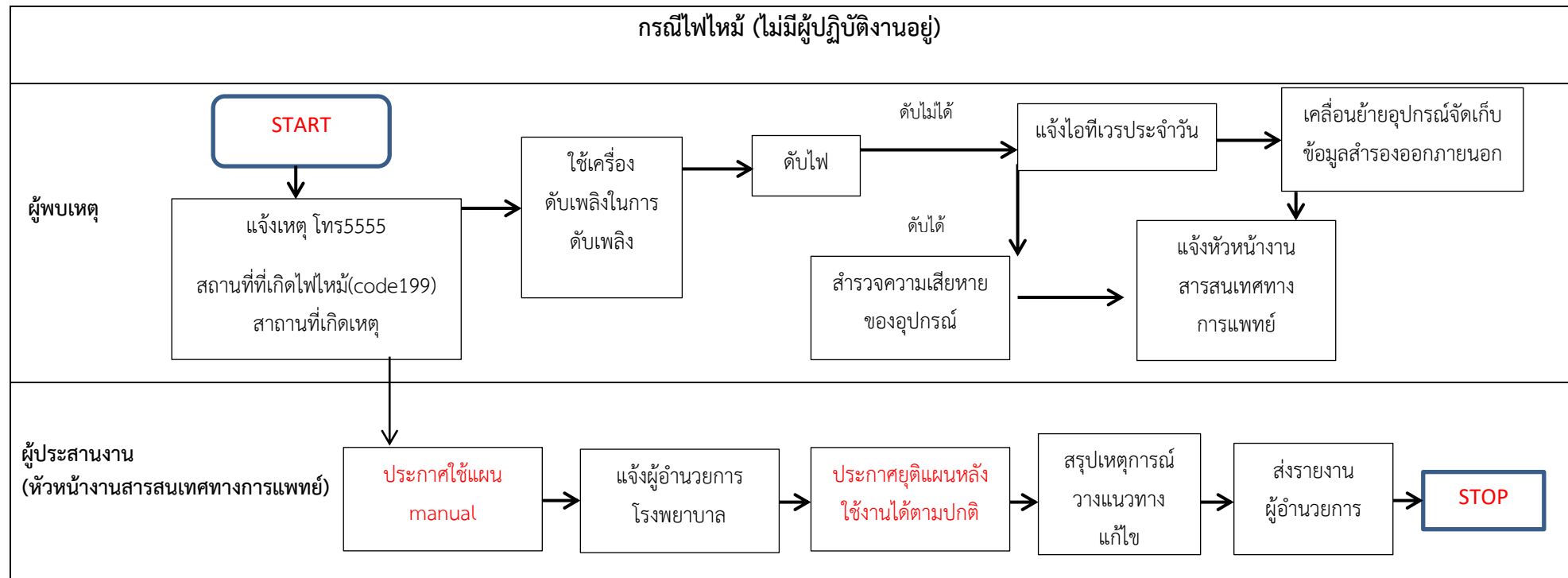
4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

4.2.1 กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
 - หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานห้องเวชระเบียน ที่เบอร์ 5555 CODE แจ้งเหตุ 199 สถานที่เกิดเหตุคือห้องserver ชั้น4ตึกบริหาร/ชั้น3อาคารผู้ป่วยใน6ชั้น
 - หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
 - อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ1ครั้ง
- แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



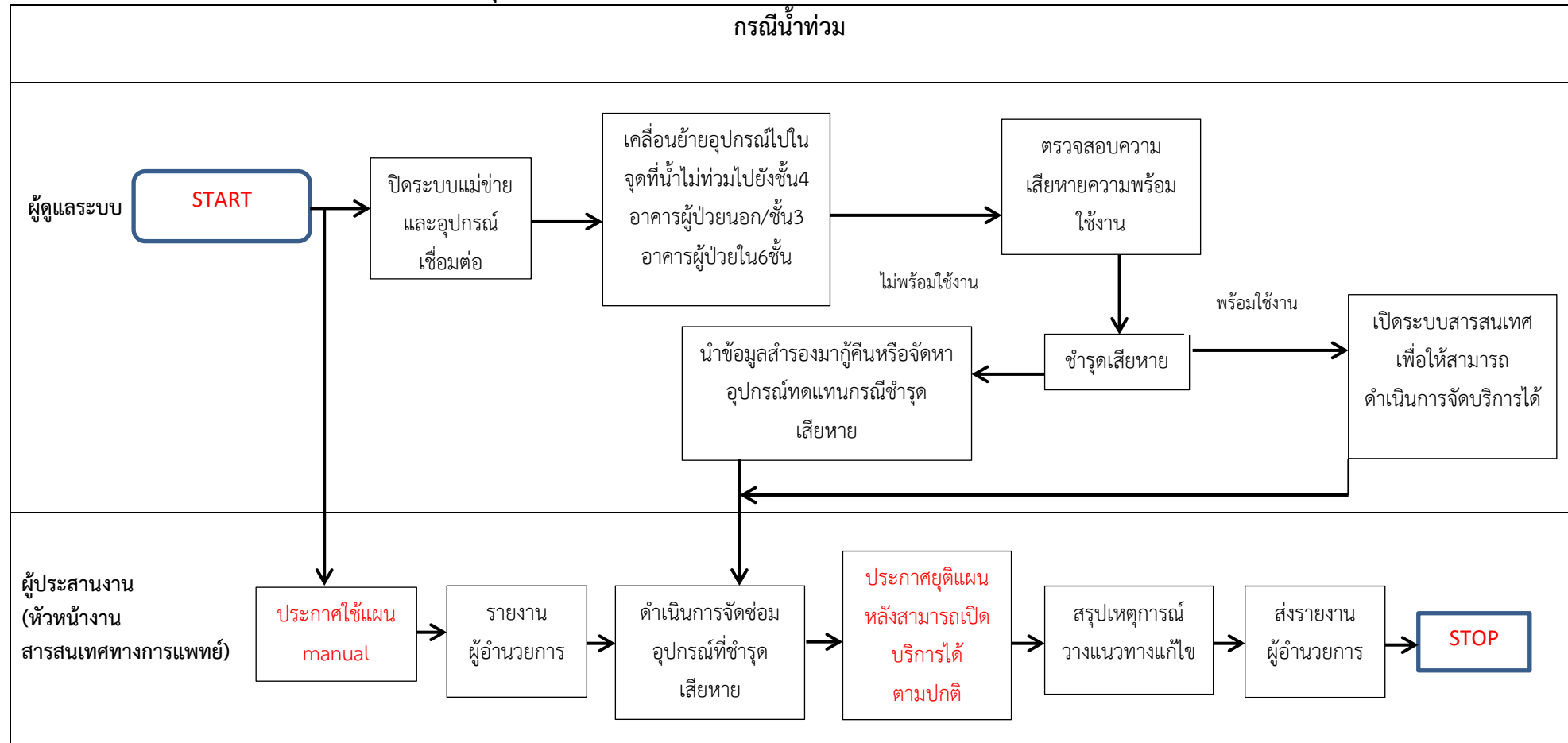
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่ ณ ห้อง server)



4.2.2 กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ห้องแม่ข่ายคอมพิวเตอร์ ชั้น 4 อาคารผู้ป่วยนอกหรือชั้น3อาคารผู้ป่วยใน6ชั้น
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- เจ้าหน้าที่เครื่องคอมพิวเตอร์ ตรวจสอบความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

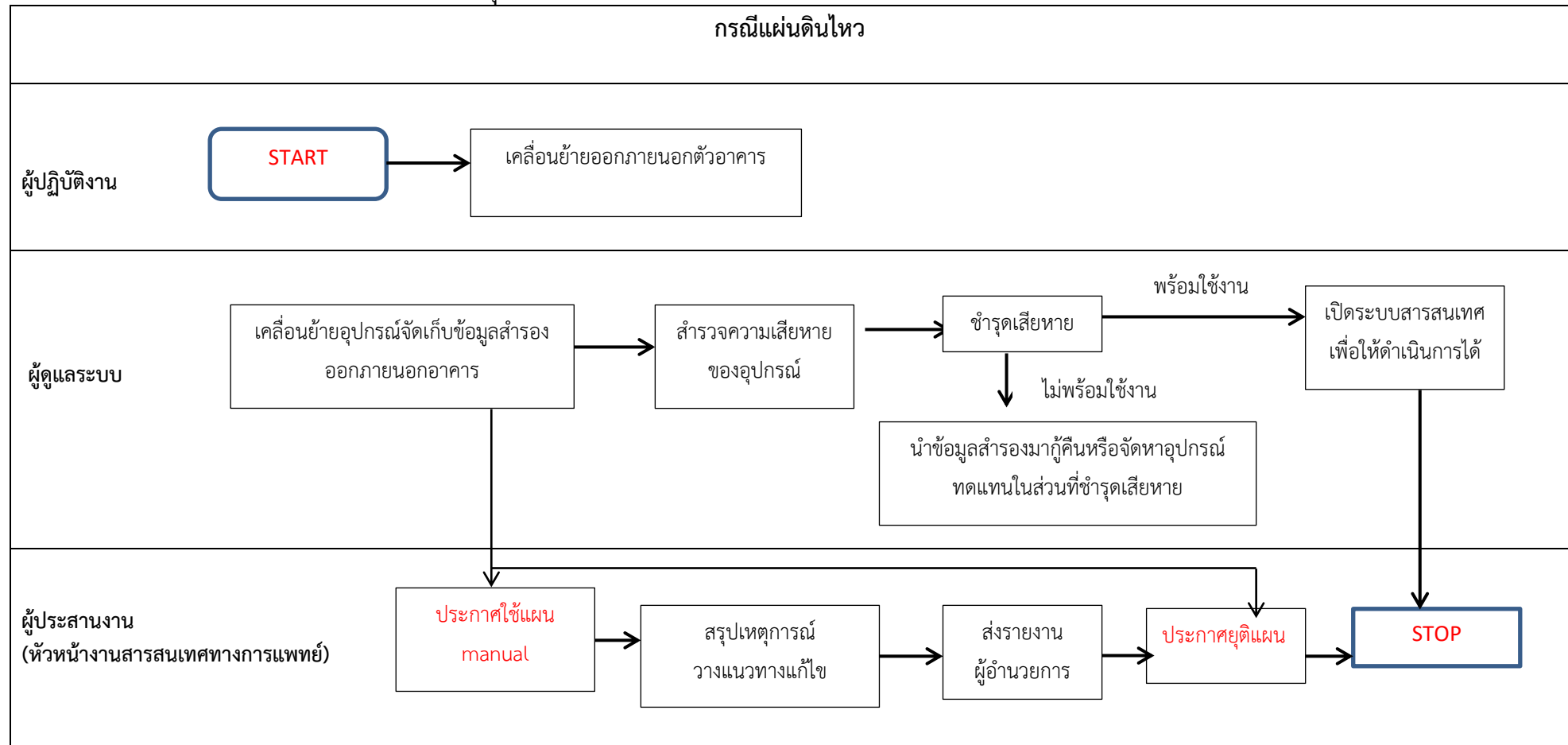
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



4.2.3 กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุดเสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

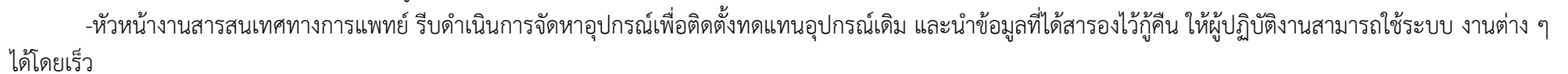


4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

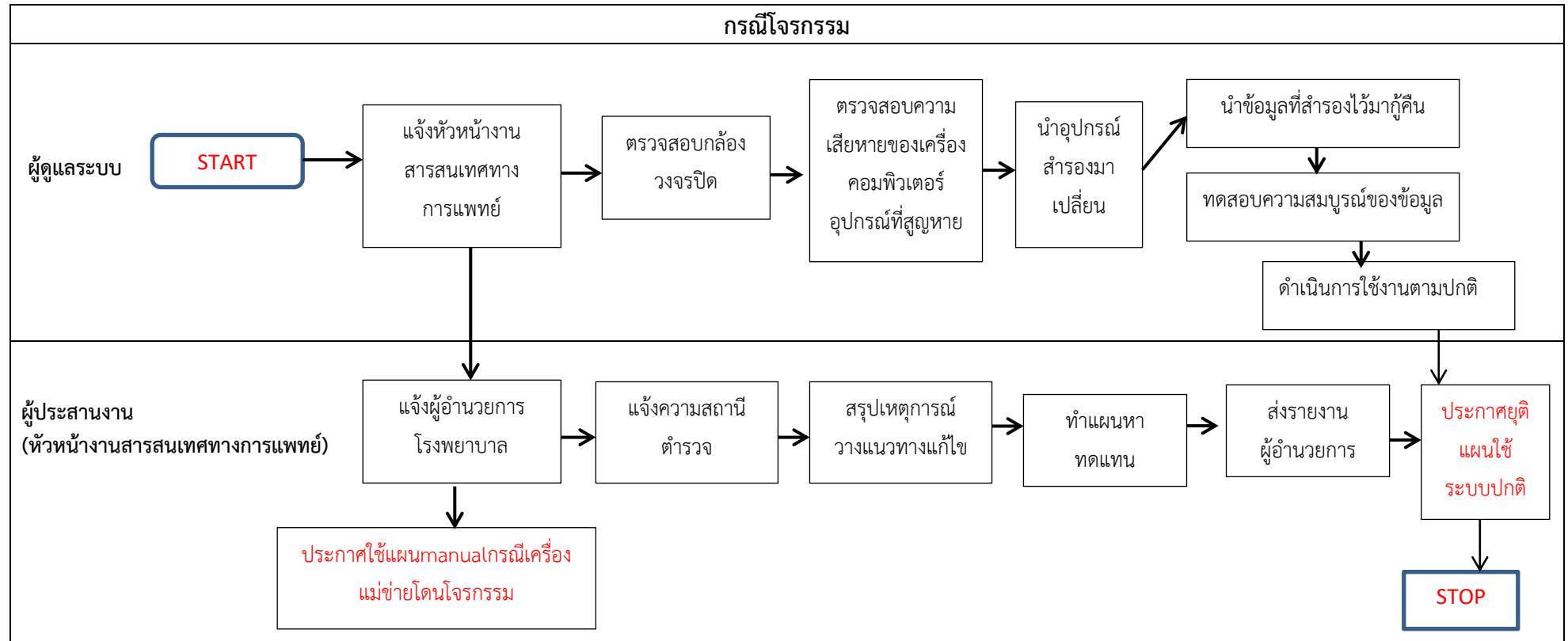
4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งหัวหน้างานสารสนเทศทางการแพทย์ทราบเพื่อรายงานผู้อำนวยการโรงพยาบาลต่อไป

- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและเจ้าหน้าที่เครื่องคอมพิวเตอร์ตรวจสอบความเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบ ความชำรุดเสียหาย ให้ดำเนินการหาอุปกรณ์ทดแทนรับผิดชอบดูแลบำรุงรักษา



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



5. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

1. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

- 1.1. ผู้อำนวยการโรงพยาบาลสมเด็จพระสังฆราชองค์ที่19 ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
- 1.2. ประธานทีมเทคโนโลยีสารสนเทศและเวชระเบียน ดำรงตำแหน่งรองผู้บริหารเทคโนโลยีสารสนเทศ
- 1.3. รองประธานทีมเทคโนโลยีสารสนเทศและเวชระเบียน ดำรงตำแหน่งรองผู้บริหารเทคโนโลยีสารสนเทศ

2. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

- 2.1. นายจิรัฐากรณ์ ชัมพาลี เจ้าพนักงานเภสัชกรรมชำนาญงาน

3. รับผิดชอบการปฏิบัติงานซ่อมบำรุงรักษา สำนวความเสียหาย ได้แก่

- 3.1 นายชัยพร จำปานิธิ เจ้าพนักงานเครื่องคอมพิวเตอร์
- 3.2 นายเฉลิมพล หวังดี เจ้าพนักงานเครื่องคอมพิวเตอร์
- 3.3 นายอภิชาติ ชมบุญ เจ้าพนักงานเครื่องคอมพิวเตอร์

4. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

- 4.1 นางสาวรัชดาพรรณ สารศาลิน พยาบาลวิชาชีพชำนาญการ
- 4.2 นางพัชรจิตร วงษ์สุน พยาบาลวิชาชีพชำนาญการ

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(นางสาวรัชดาพรรณ สารศาลิน)

พยาบาลวิชาชีพชำนาญการ

หัวหน้างานสารสนเทศทางการแพทย์

ตุลาคม 2563