แผนรองรับสถานการณ์ฉุกเฉิน

ที่อาจเกิดขึ้นกับระบบสารสนเทศ โรงพยาบาลตำรวจ

(IT Contingency plan)

จัดทำโดย ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร.

ประจำปี 2557 - 2558

คำนำ

ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ มีความสำคัญยิ่งต่อการบริหารระบบราชการ ซึ่งศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. เป็นหน่วยงานที่รับผิดชอบในการดำเนินการตรวจสอบและควบคุมมาตรฐานการรักษาความปลอดภัยทางเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ และได้ตระหนักถึงการดูแลรักษาระบบสารสนเทศของโรงพยาบาลตำรวจ ให้มีความมั่นคงปลอดภัยและลดความเสี่ยงต่างๆ ที่จะเกิดขึ้นกับระบบสารสนเทศ เพื่อให้ระบบสารสนเทศของโรงพยาบาลตำรวจ สามารถใช้งานได้อย่างมีประสิทธิภาพและประสิทธิผล จึงได้จัดทำแผนแก้ไขปัญหาระบบเทคโนโลยีสารสนเทศ เมื่อเกิดเหตุการณ์ฉุกเฉิน (IT Contingency Plan) ของโรงพยาบาลตำรวจ ปีงบประมาณ พ.ศ. 2557-2558 เพื่อเป็นกรอบแนวทางในการบำรุงรักษา ป้องกันและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงานต่างๆ ภายในโรงพยาบาลตำรวจ

ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร.

สารบัญ

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency plan)
ปีงบประมาณ พ.ศ. 2557-2558

หลักการและเหตุผล

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งาน และความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์การจำเป็นจะต้องการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทสเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

โรงพยาบาลตำรวจได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากระบบเซิฟเวอร์ ระบบเน็ตเวิร์คขัดข้อง ระบบล่มจากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่ต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาลตำรวจ

การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของโรงพยาบาลตำรวจได้ใช้เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอันจะส่งผลกระทบต่อระบบเทคโนโลยีสารเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจมีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างๆ ด้านสารสนเทศ โรงพยาบาลตำรวจ พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

2. ความเสี่ยงด้านการปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติ หรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศโรงพยาบาลตำรวจ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของโรงพยาบาลตำรวจ

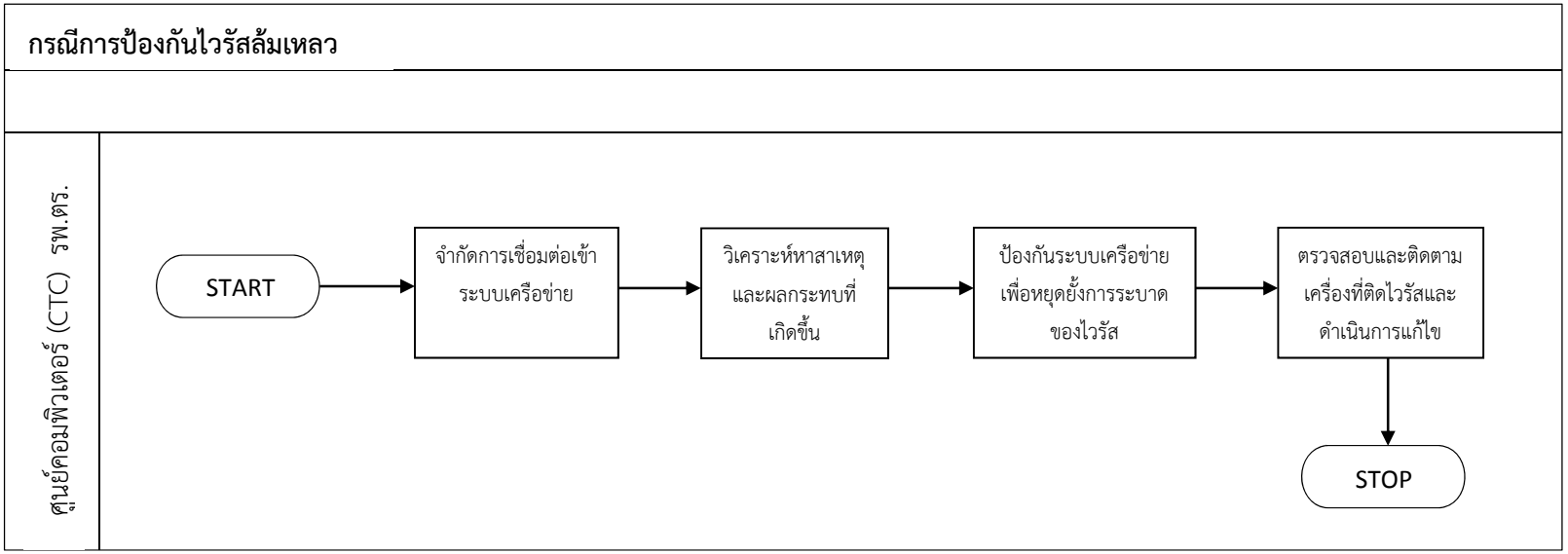
แผนรองรับสถานการณ์ฉุกเฉิน

1. สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

1.1 กรณีการป้องกันไวรัสล้มเหลว ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไขกรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ โอเปเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร. ตามลำดับ
- แจ้งบริษัทภายนอกที่เกี่ยวข้องเพื่อดำเนินการตรวจสอบ เช่น ระบบ PACS LAB และ HIS ฯลฯ

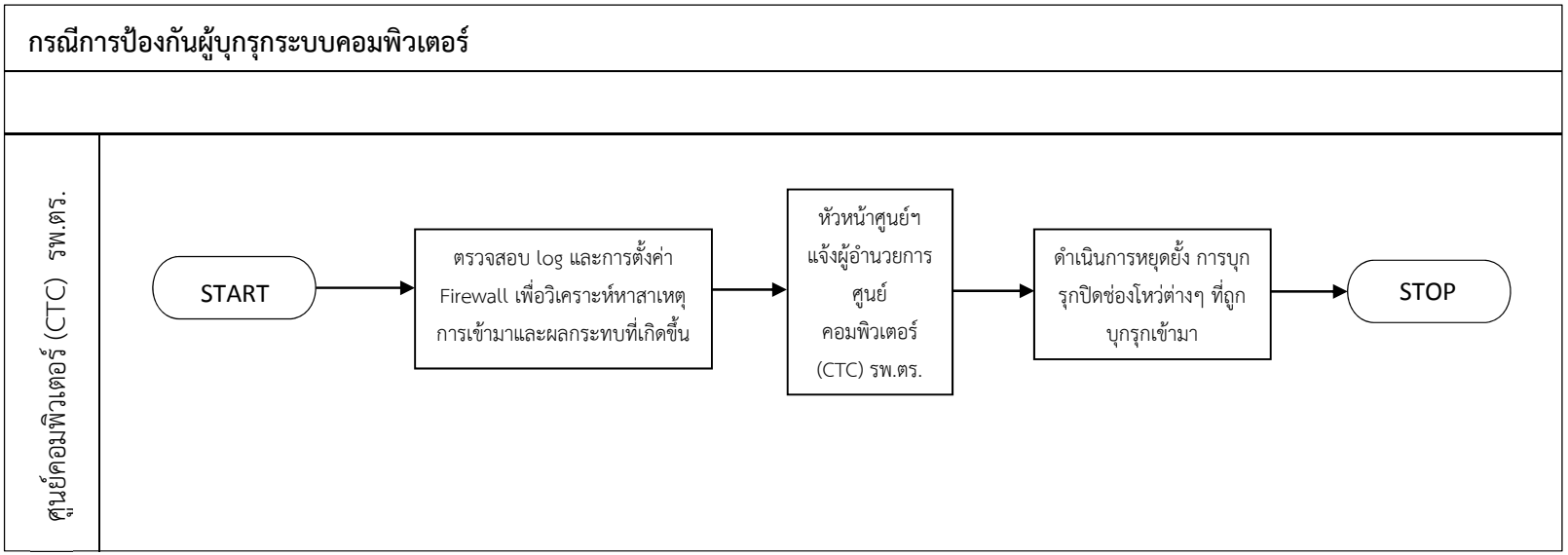
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



1.2 กรณีการป้องกันผู้บุกรุกระบบคอมพิวเตอร์ ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- กรณีที่มีผู้บุกรุก ต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
- หัวหน้าศูนย์คอมพิวเตอร์ รายงาน ผู้อำนวยการศูนย์คอมพิวเตอร์ และรายงาน CIO รพ.ตร. ให้รับทราบ
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่งต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

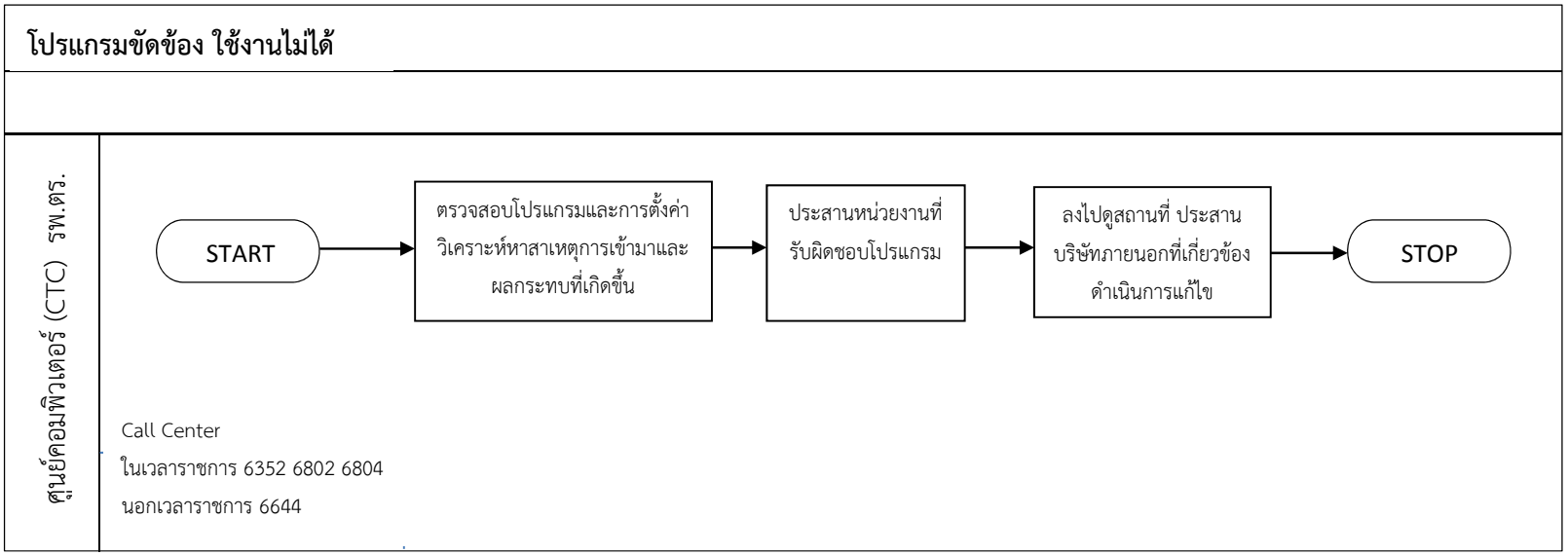
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกระบบคอมพิวเตอร์



1.3 กรณีโปรแกรมบริหารโรงพยาบาลตำรวจขัดข้องไม่สามารถใช้งานได้ ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- ตรวจสอบโปรแกรมและการตั้งค่า วิเคราะห์สาเหตุ และผลกระทบที่อาจจะเกิดขึ้นกับระบบ
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- ลงไปตรวจสอบจุดที่มีปัญหาพร้อมดำเนินการแก้ไข ให้ใช้เวลาน้อยที่สุด
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ
- แจ้งบริษัทภายนอกที่เกี่ยวข้องเพื่อดำเนินการตรวจสอบ เช่น ระบบ PACS LAB และ HIS ฯลฯ

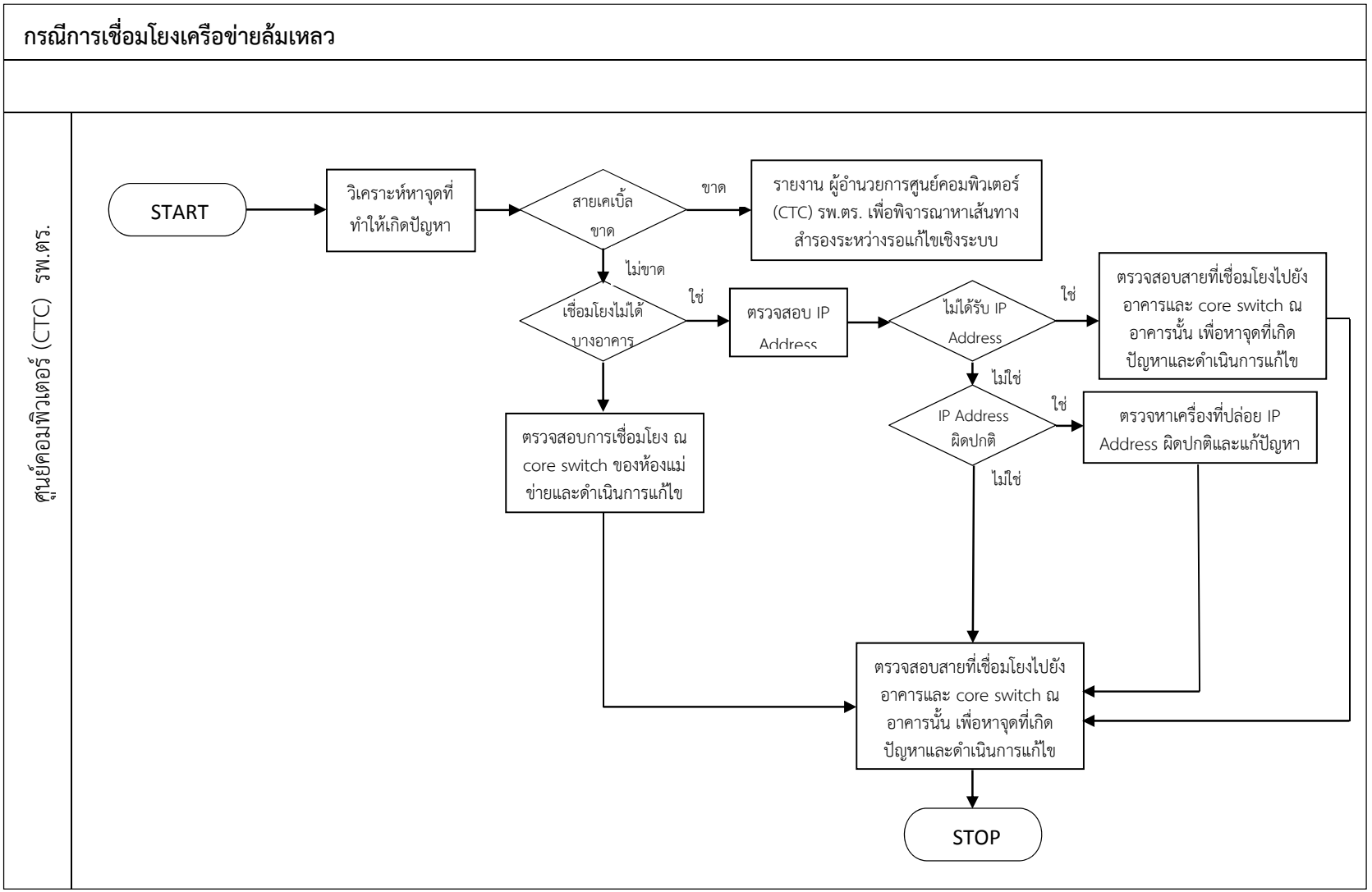
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโปรแกรมระบบบริหารโรงพยาบาลขัดข้อง ใช้งานไม่ได้



1.4 กรณีการเชื่อมโยงเครือข่ายล้มเหลว ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหาหากสายเคเบิ้ลขาด เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- ลงไปตรวจสอบจุดที่มีปัญหาพร้อมดำเนินการแก้ไข ให้ใช้เวลาน้อยที่สุด
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

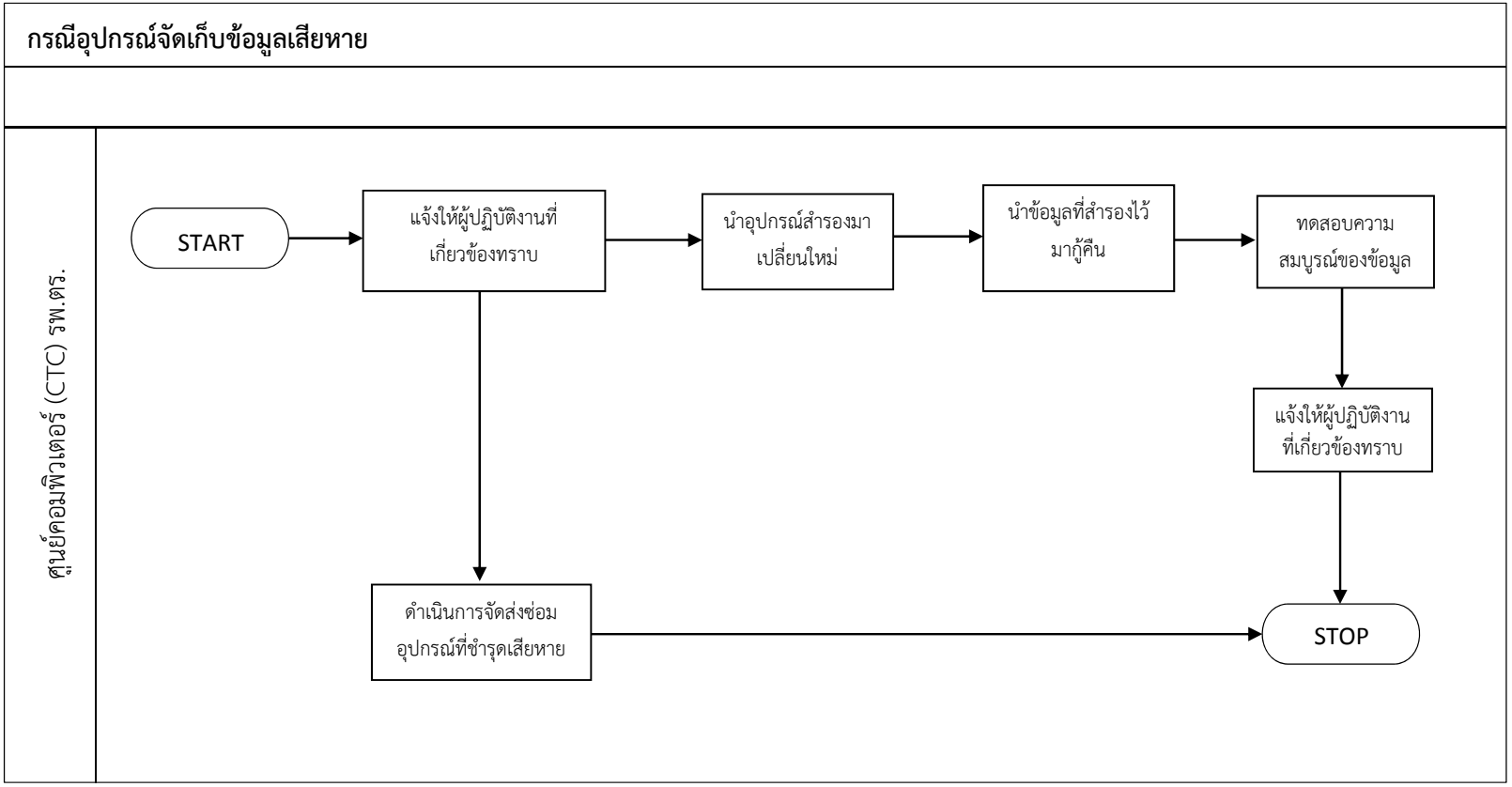
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



1.5 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

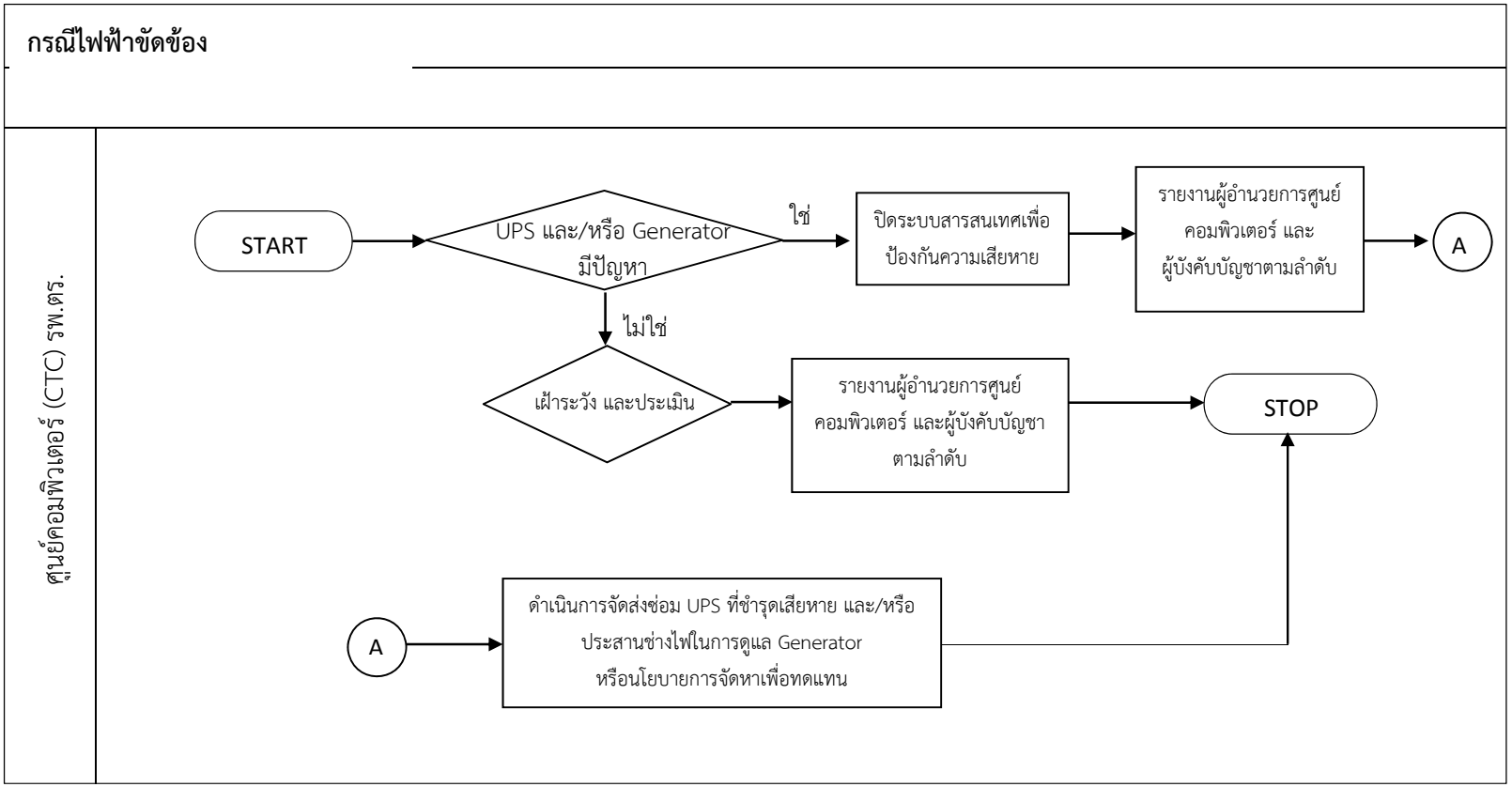
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



1.6 กรณีไฟฟ้าขัดข้อง ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- ระบบฐานข้อมูลสารสนเทศมี UPS และ เครื่อง generator ที่สามารถให้บริการระบบไฟสำรอง
- ประสานเรื่องระบบไฟฟ้ากับห้องช่าง
- ดำเนินการปิดระบบเพื่อป้องกันความเสียหาย ในกรณีที่ระบบสำรองไฟมีปัญหา
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

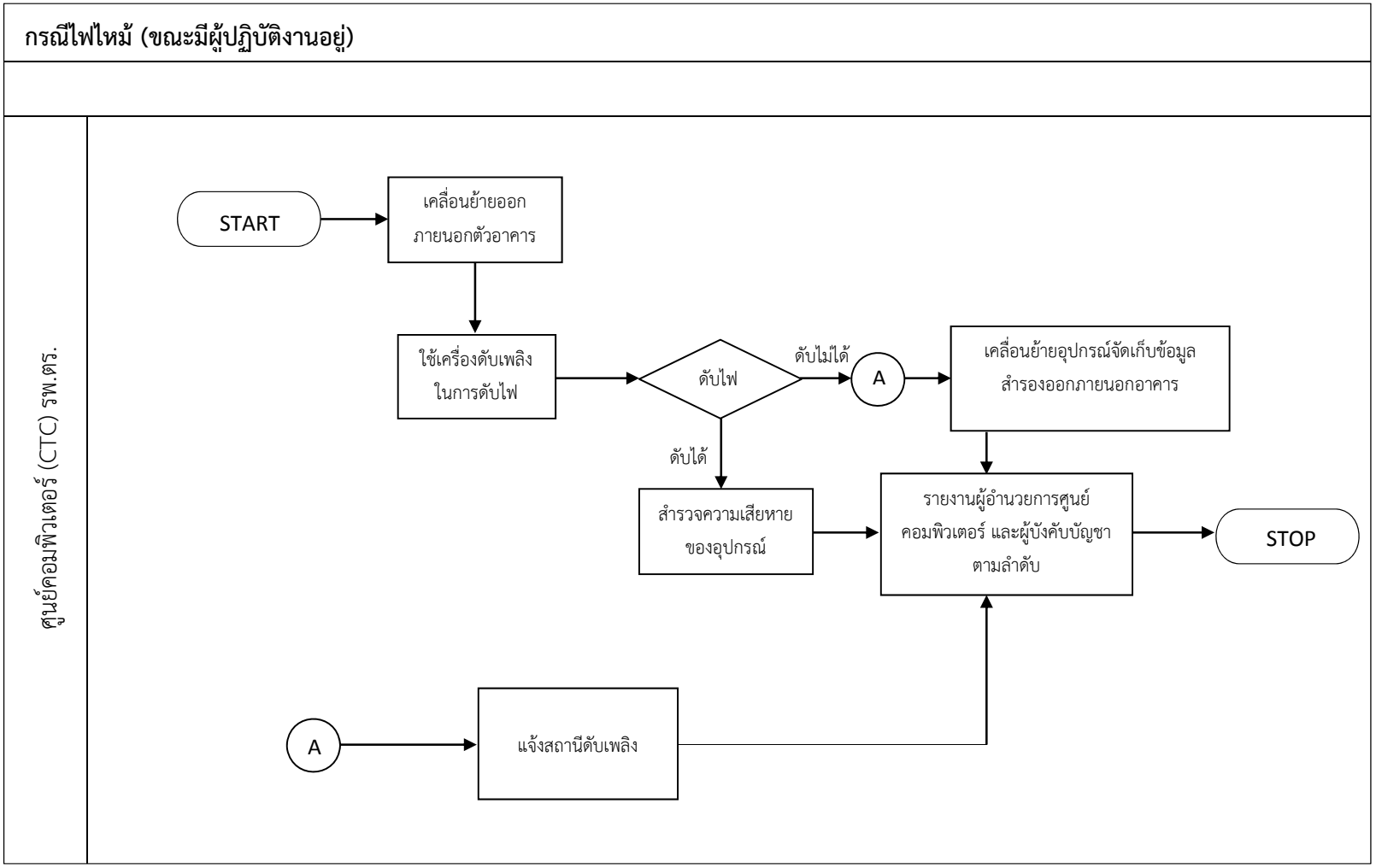


2. สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

2.1 กรณีไฟไหม้ ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคารให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- แจ้งศูนย์ รปภ. โรงพยาบาลตำรวจ
- หากไม่สามารถควบคุมไฟได้ จะต้องเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งศูนย์ปฏิบัติการอาคารและสถานที่และยานพาหนะทันทีโทรแจ้งสถานีดับเพลิง
- หากเกิดไฟไหม้ในขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงาน อย่างสม่ำเสมออย่างน้อยปีละ 2 ครั้ง

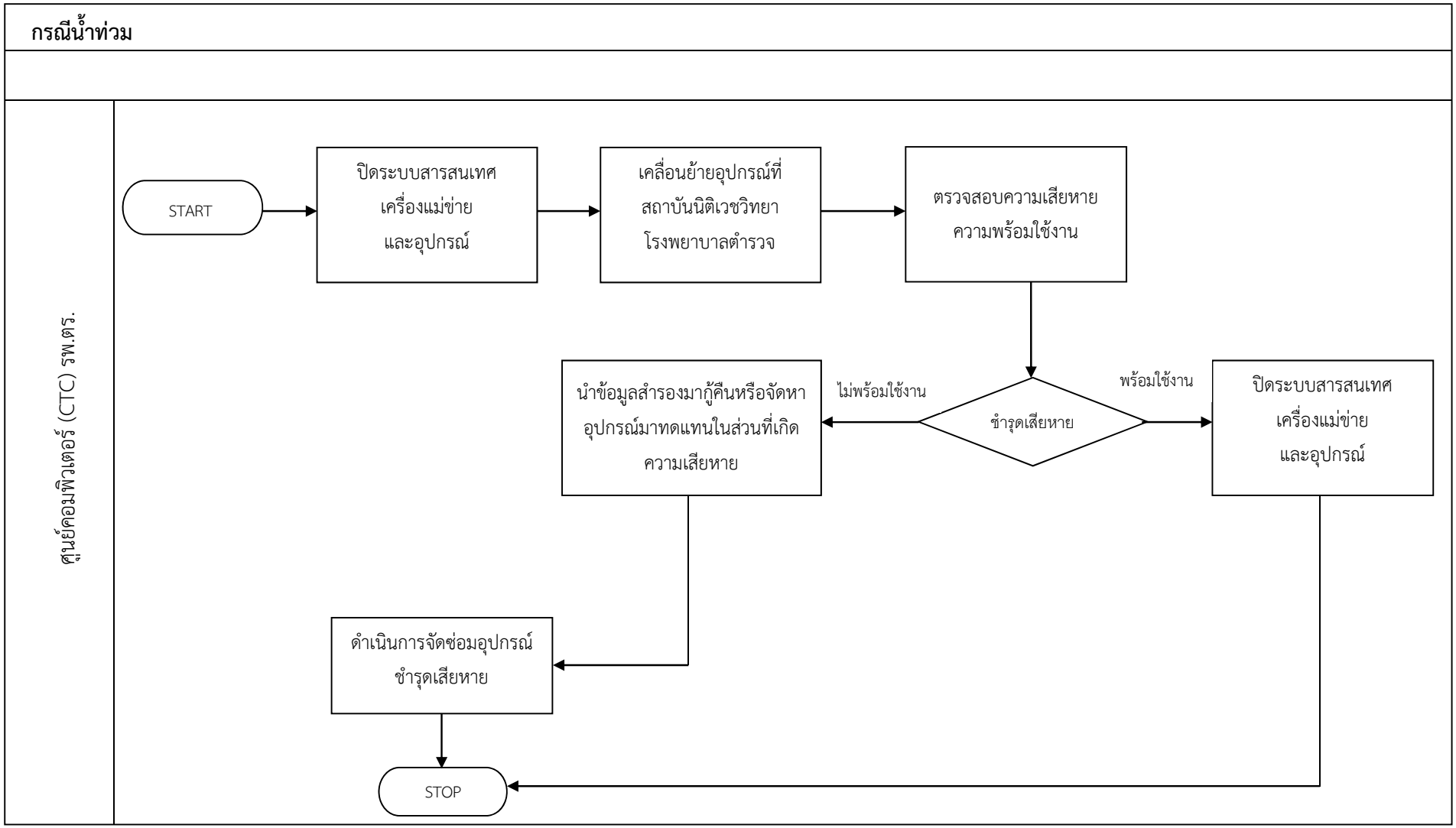
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



2.2 กรณีน้ำท่วม ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- ปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่างๆที่ยังสามารถใช้งานได้ไปติดตั้งที่ห้องแม่ข่ายสำรอง สถาบันนิติเวชวิทยา โรงพยาบาลตำรวจ
- นำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

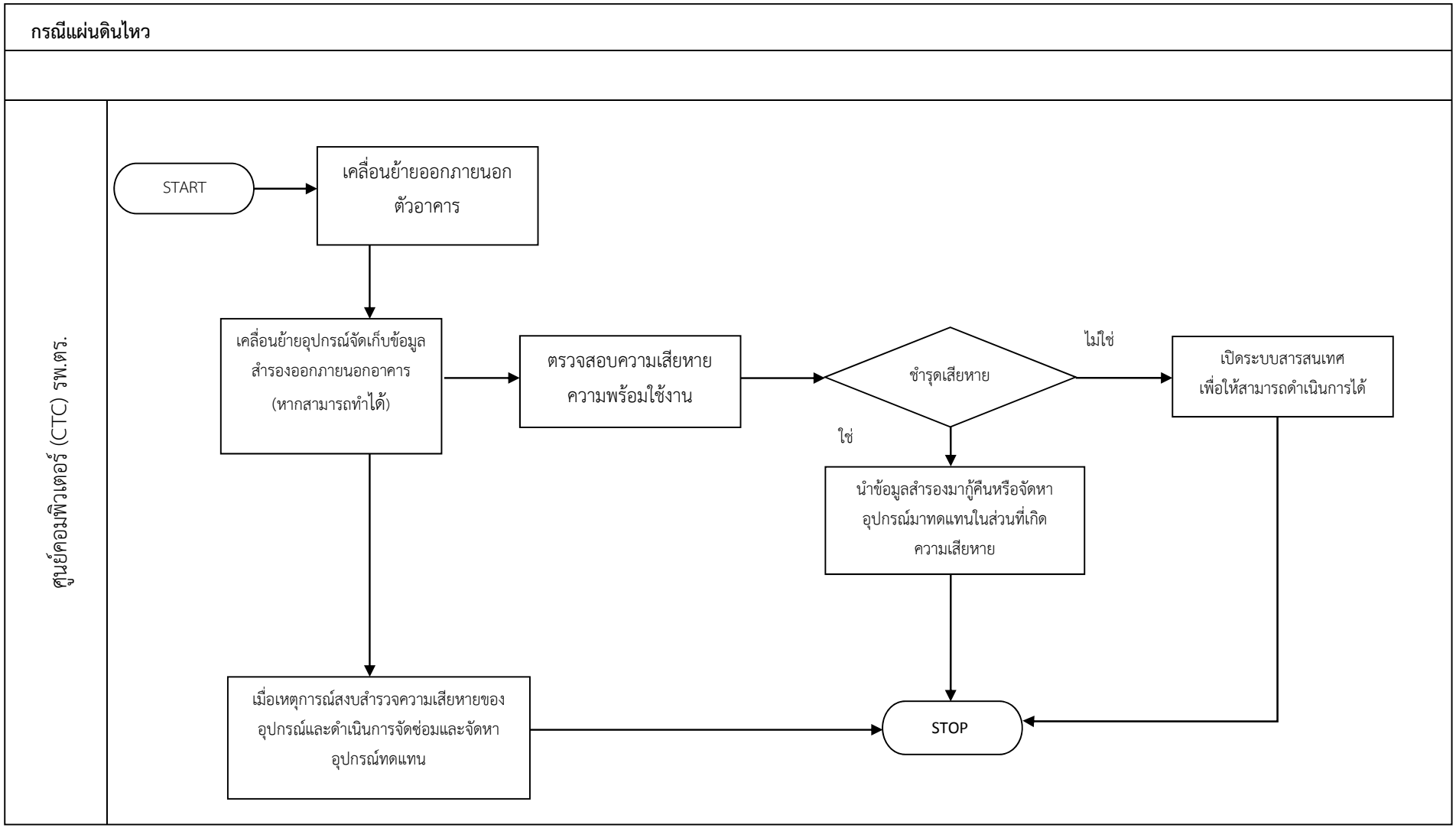
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



2.3 กรณีแผ่นดินไหว ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- นำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

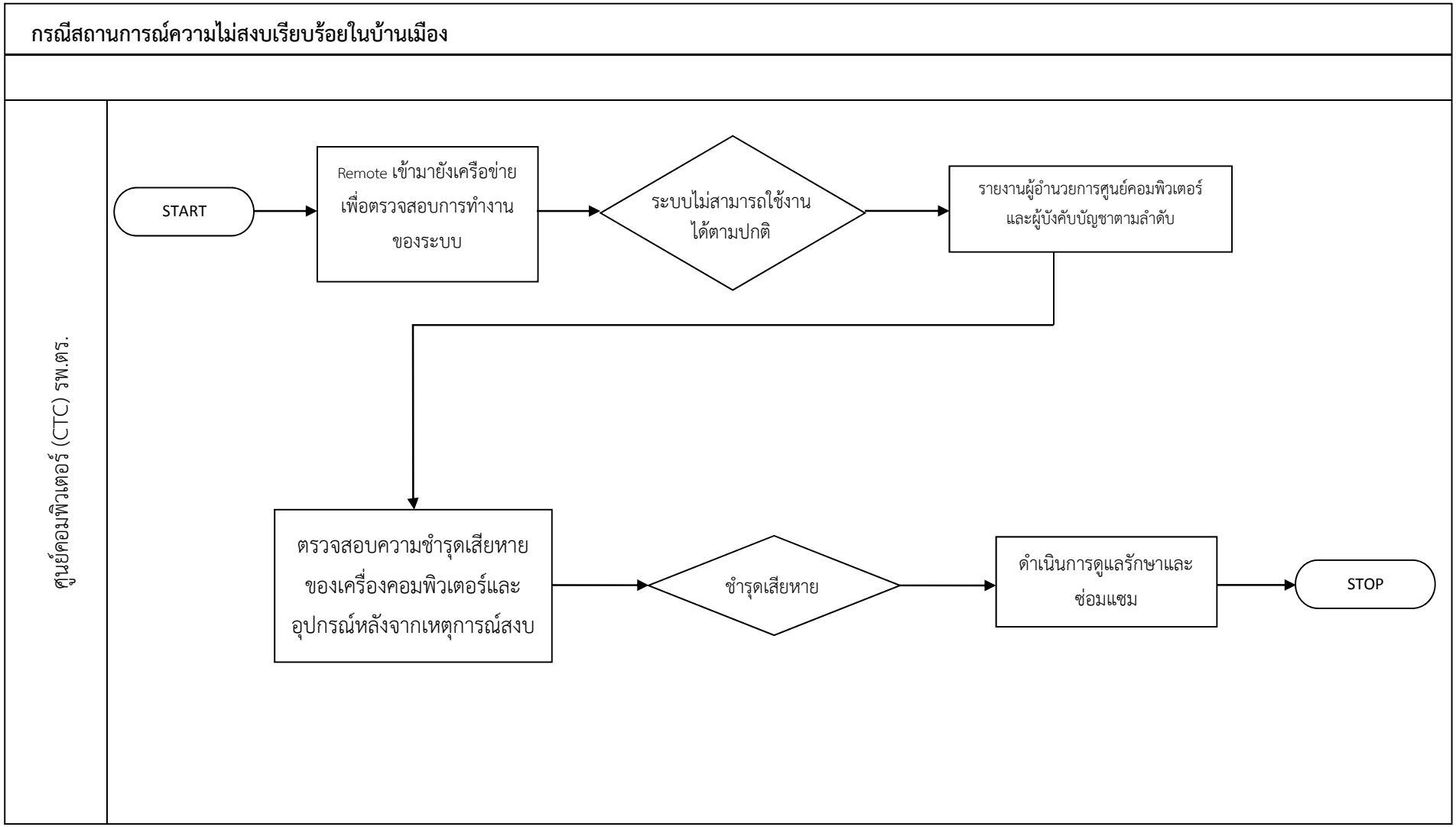


3. สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

3.1 กรณีเกิดสถานการณ์ความสงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ จะดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ
- หลังเหตุการณ์ความไม่สงบ ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ดำเนินการบำรุงรักษาและซ่อมแซมเพื่อให้กลับสู่สภาพปกติโดยเร็วที่สุด

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

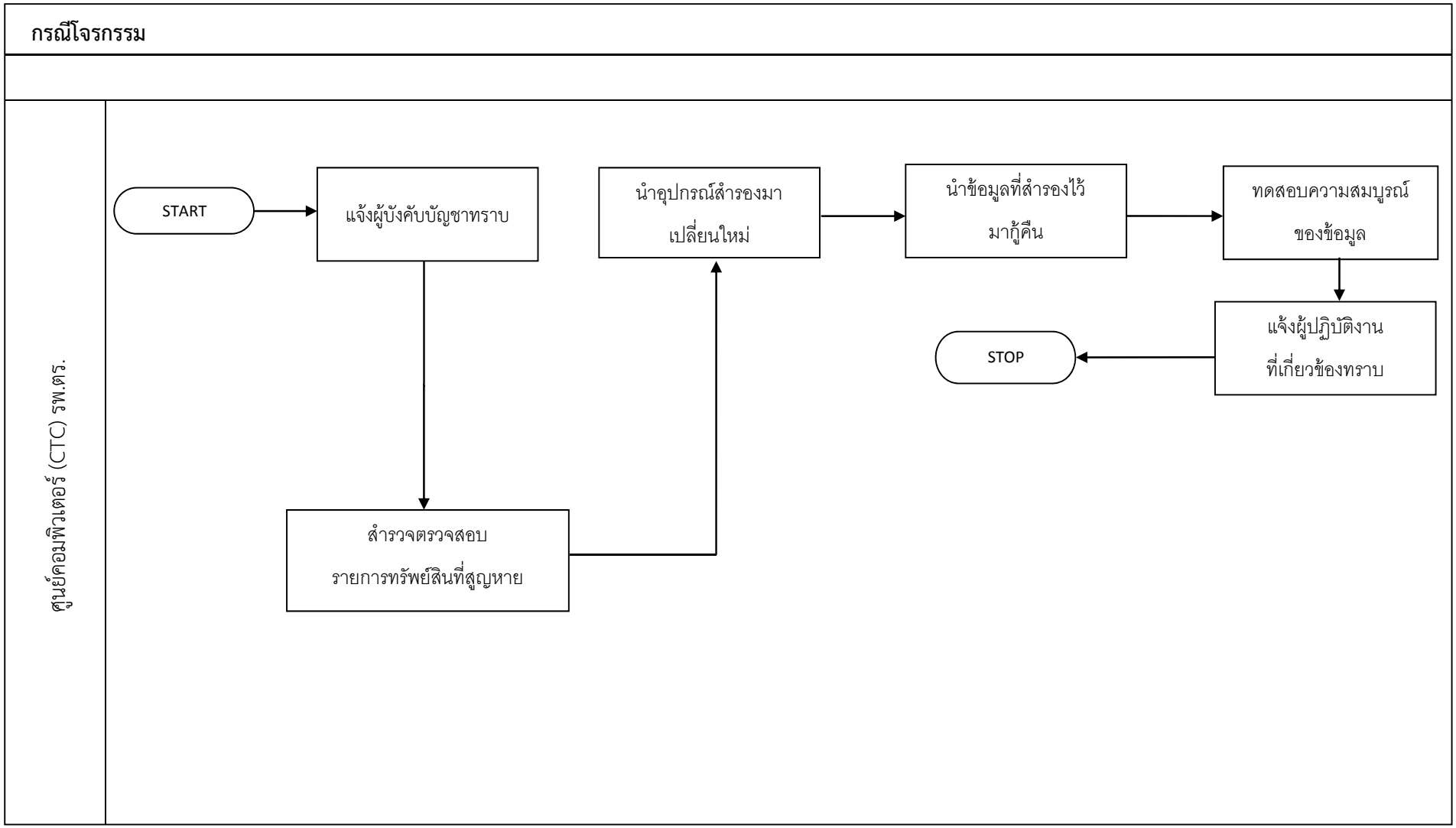


4. สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

4.1 กรณีโจรกรรม ศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. ปฏิบัติดังต่อไปนี้

- แจ้งผู้บังคับบัญชาตามลำดับชั้นให้ทราบโดยด่วน
- สำรวจตรวจรายการทรัพย์สินที่สูญหาย
- แจ้งศูนย์ รปภ. โรงพยาบาลตำรวจ
- หากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
- รีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืนให้ผู้ปฏิบัติงานสามารถใช้งานระบบงานต่างๆ ได้โดยเร็ว
- รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



คู่มือช่างในกรณีที่เกิดเหตุการณ์ระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ ระบบล่ม

1. เจ้าหน้าที่เวร ศูนย์ (call center) 6644 เมื่อได้รับแจ้งเหตุทางโทรศัพท์ ระบบคอมพิวเตอร์มีปัญหาให้รีบบันทึกสาเหตุ หน่วยงานที่แจ้ง เวลาที่ระบบเริ่มมีปัญหา ตรวจสอบโปรแกรมและการตั้งค่าวิเคราะห์สาเหตุว่าเป็นที่ Software, Hardware หรือระบบเครือข่าย Networkและผลกระทบที่อาจจะเกิดขึ้นกับระบบ
2. พื้นที่ตรวจสอบและดำเนินการแก้ไขเบื้องต้น ให้เร็วที่สุด
3. รายงานผู้บังคับบัญชาตามลำดับชั้น ได้แก่ หัวหน้าศูนย์คอมพิวเตอร์ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. CIO รพ.ตร. และ พตร.ตามลำดับ
4. ถ้าหากระบบคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติให้แจ้งเหตุ โอเปอเรเตอร์ กด 9 (02-207-6000) เพื่อประกาศให้ทุกหน่วยงานในสังกัดของโรงพยาบาลตำรวจทราบว่าระบบคอมพิวเตอร์ไม่สามารถใช้การได้ กำลังดำเนินการแก้ไข เพื่อให้หน่วยงานที่ต้องให้บริการกับผู้ป่วยให้บริการ ตามแผนของแต่ละหน่วยงานสำหรับกรณีที่ระบบคอมพิวเตอร์ขัดข้อง
5. ดำเนินการแก้ไขระบบให้กลับสู่สภาพปกติโดยเร็วที่สุด
6. ทำรายงาน และประชุม บุคลากรที่เกี่ยวข้อง เพื่อประเมินเหตุการณ์ที่เกิดขึ้นและวิเคราะห์สาเหตุ การแก้ไข เพื่อไม่ให้เกิดขึ้นในครั้งต่อไป

ผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของเจ้าหน้าที่ศูนย์คอมพิวเตอร์ (CTC) โรงพยาบาลตำรวจ ดังต่อไปนี้

1. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะคำปรึกษาตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบเจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่
   1.1. พล.ต.ต. ทรงชัย สิมะโรจน์ ประธานคณะกรรมการบริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) รพ.ตร. โทร.0813377447
   1.2. พ.ต.อ.วิโรจน์ ลาภไพบูลย์พงศ์ ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. โทร.0863868698
   1.3. พ.ต.อ.หญิง สายวริน ลาภไพบูลย์พงศ์ หัวหน้าศูนย์คอมพิวเตอร์ (CTC) รพ.ตร. โทร 0814851289
2. รับผิดชอบงานด้าน software ได้แก่
   2.1. ว่าที่ ร.ต.ต.หญิง ดาราพร ทองคำ โทร.6352 หรือ 0863971625
   2.2. น.ส.ชณิตา รุจิรากรสกุล โทร.6352 หรือ 0852638323
   2.3. น.ส.จิตรลดา สีสุข โทร.6352 หรือ 0896683300
   2.4. น.ส.รินณารา สายมณี โทร.6352 หรือ 0892328530
3. รับผิดชอบงานฐานข้อมูล แม่ข่าย และ network
   3.1. นายเทียนไชย ทรัพย์ประกอบ โทร.6352 หรือ 0866180524
   3.2. นายสิทธิ์บดี เธียรเล็ก โทร.6352 หรือ 0865631773
   3.3. น.ส.สรัชณ์ภร พนัสพิบูลย์ โทร.6352 หรือ 0859418778
4. รับผิดชอบงานด้าน website
   4.1 ว่าที่ ร.ต.ท. ศุขภฒ สุนนท์ชัย โทร.6352 หรือ 0811452110
   4.2 น.ส.ศรสวรรค์ เสนาะคำ โทร.6352 หรือ 0870111080
5. รับผิดชอบด้าน AV
   5.1 นายทรงศักดิ์ แซ่แต้ โทร.6352 หรือ 0850438418
   5.2 นายภรต สุนทรครุฑ โทร.6352 หรือ 0877159740
6. รับผิดชอบการช่างเทคนิคคอมพิวเตอร์
   6.1 นายชัยวัฒน์ เพียรชอบ โทร.6644 หรือ 0891894708
   6.2 นายสุริยัน ทัศสามี โทร.6644 หรือ 0815654069
   6.3 นายพงษ์ภัทร์ สีสุข โทร.6644 หรือ 0827802005
   6.4 น.ส.ประภาวัลย์ เย็นคงคา โทร.6644 หรือ 0906589743

การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และรายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการแก้ไขในทุกกรณีตามที่ระบุไว้

พ.ต.อ.หญิง ผู้เสนอแผน

(สายวริน ลาภไพบูลย์พงศ์)

หัวหน้าศูนย์คอมพิวเตอร์ (CTC) รพ.ตร.

พ.ต.อ. ผู้ตรวจสอบ

(วิโรจน์ ลาภไพบูลย์พงศ์)

ผู้อำนวยการศูนย์คอมพิวเตอร์ (CTC) รพ.ตร.

พล.ต.ต. ผู้อนุมัติแผน

(ทรงชัย สิมะโรจน์)

รอง พตร./

ประธานคณะกรรมการบริหารคอมพิวเตอร์ (CIO) รพ.ตร.