๒๕๖๖

แผนรองรับสถานการณ์ฉุกเฉิน

(IT Contingency Plan)

สารบัญ

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

๑. บทนำ

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้การบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลาการ ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์การจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

โรงพยาบาลท่ากระดาน ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการบุคลากรทางการแพทย์ และเจ้าหน้าที่ได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรืออาจจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๑. เพื่อแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสานสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของโรงพยาบาลท่ากระดาน

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของโรงพยาบาลท่ากระดาน มีความหลากหลายเช่นภารกิจด้านบริการ การบันทึกผลวินิจฉัย ภารกิจด้านการให้การบริการวิชาการแก่ชุมชน เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาวิธีป้องกันปัญหาและลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่ากระดาน เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์ละตรวจสอบความเสี่ยงต่างๆด้านสารสนเทศ ของโรงพยาบาลท่ากระดาน พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสานสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของโรงพยาบาลท่ากระดาน ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้นเพื่อให้ระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่ากระดาน มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศของโรงพยาบาลท่ากระดาน

๔. แผนรองรับสถานการณ์ฉุกเฉิน

๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

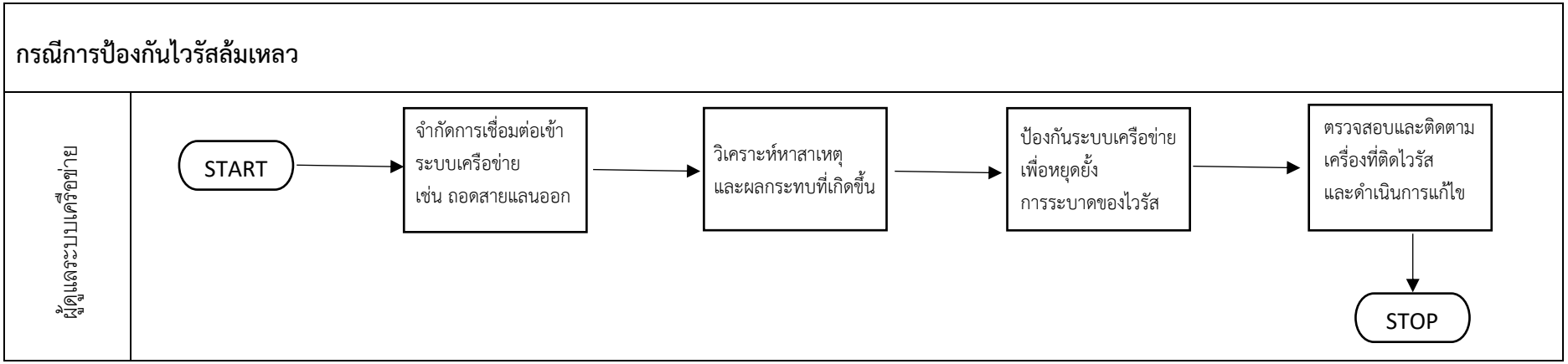
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุให้เจ้าหน้าที่ที่งานเทคโนโลยีสารสนเทศทางการแพทย์ หรือกรณีมีเหตุอันทำให้แผนกเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ งานพัฒนาระบบเครือข่ายและการสื่อสาร จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



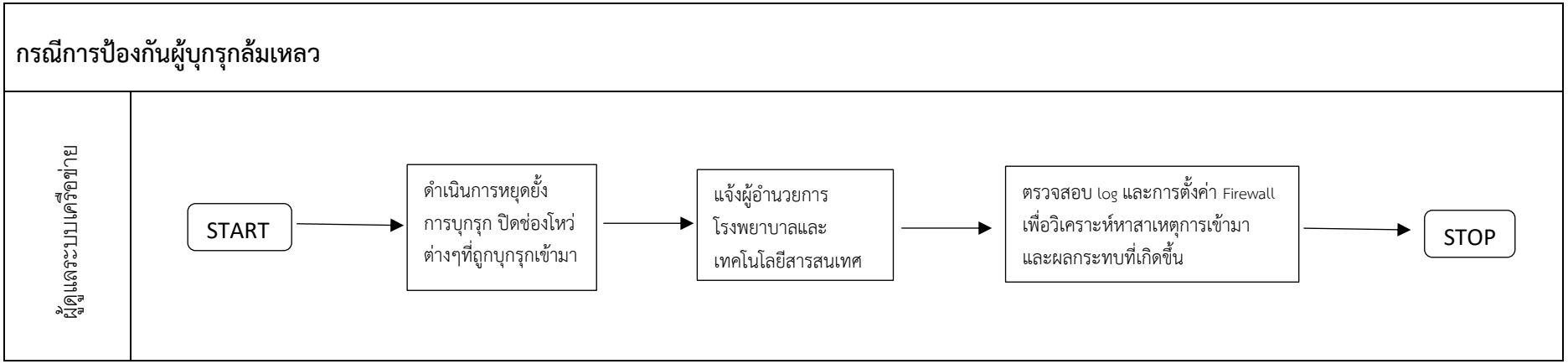
๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบปละผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของFirewall

- ผู้ดูแลระบบแจ้งผู้อำนวยการโรงพยาบาลและเทคโนโลยีสารสนเทศให้ทราบโดยด่วน

- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



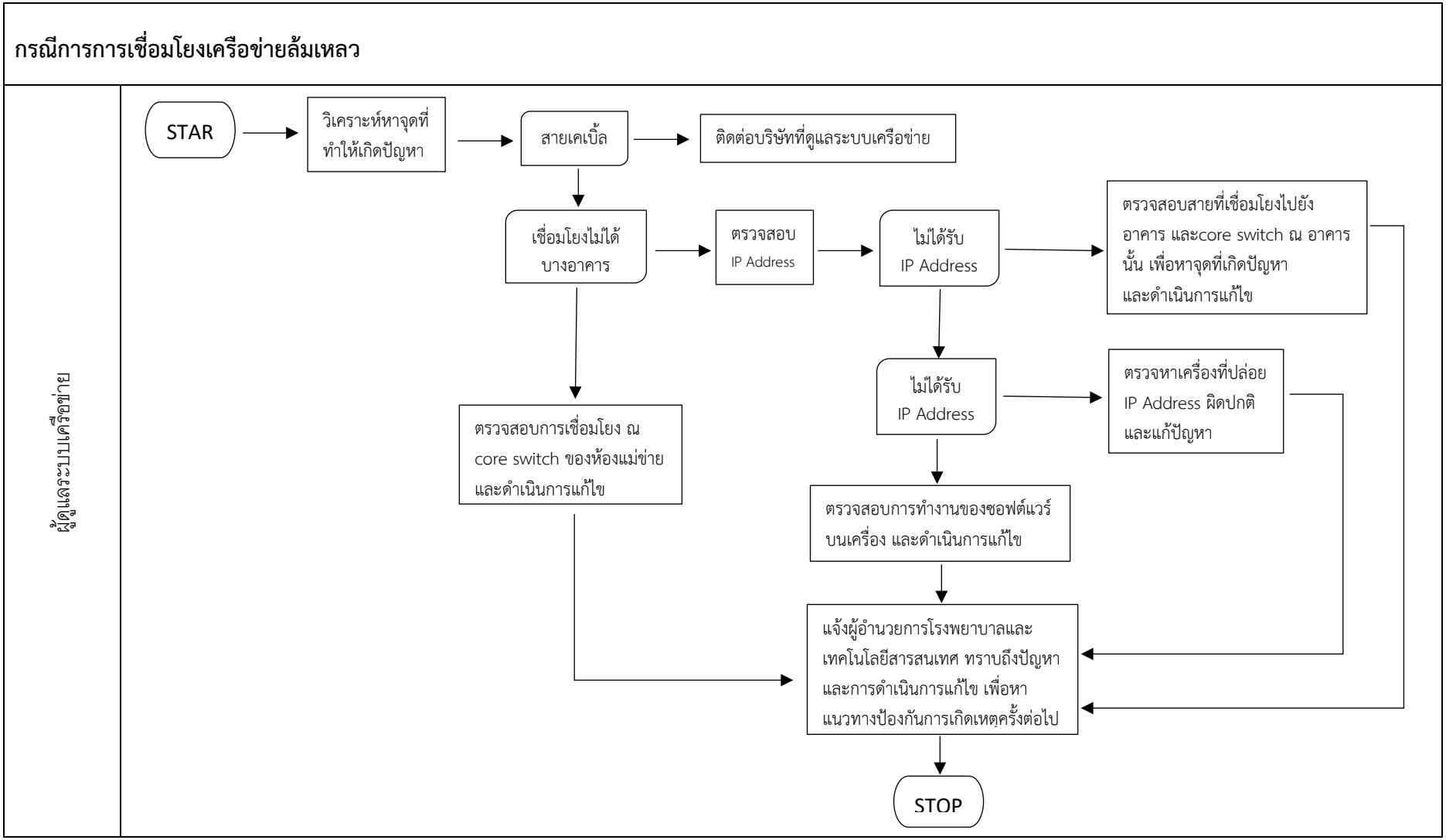
๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดอยู่ ณ อาคารนั้นๆ

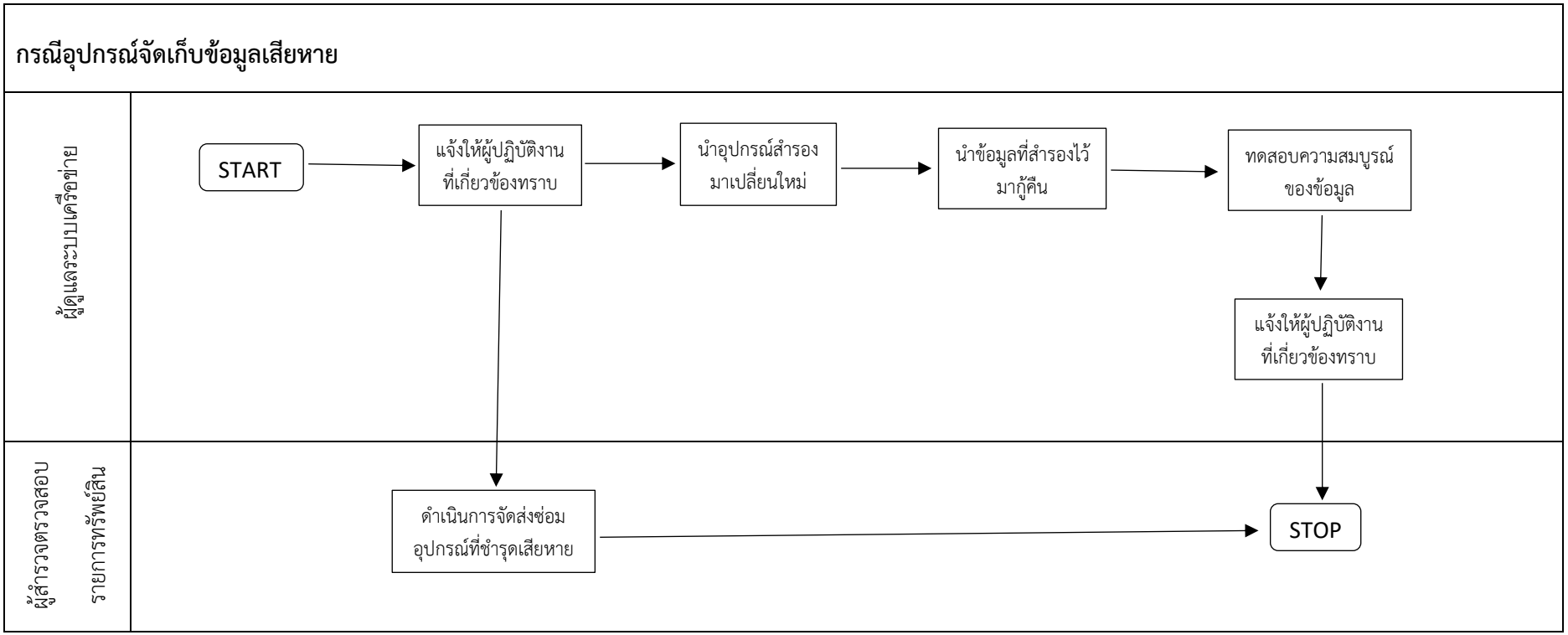
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

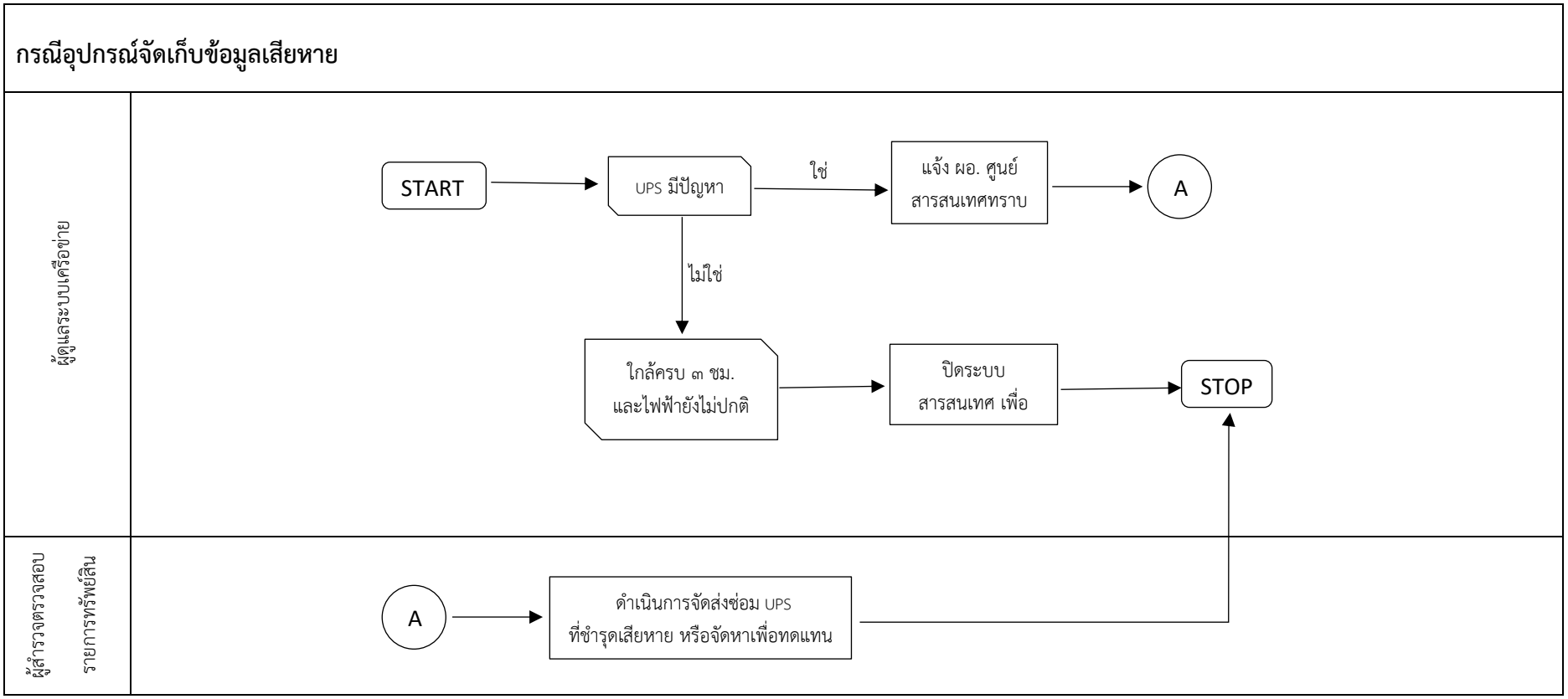
- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



๔.๑.๕ กรณีไฟฟ้าขัดข้อง

- ระบบข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓ ชั่วโมง
- หากใกล้ครบ ๓ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้อำนวยการโรงบาลและเทคโนโลยีสารสนเทศ
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน



๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

๔.๒.๑ กรณีไฟไหม้

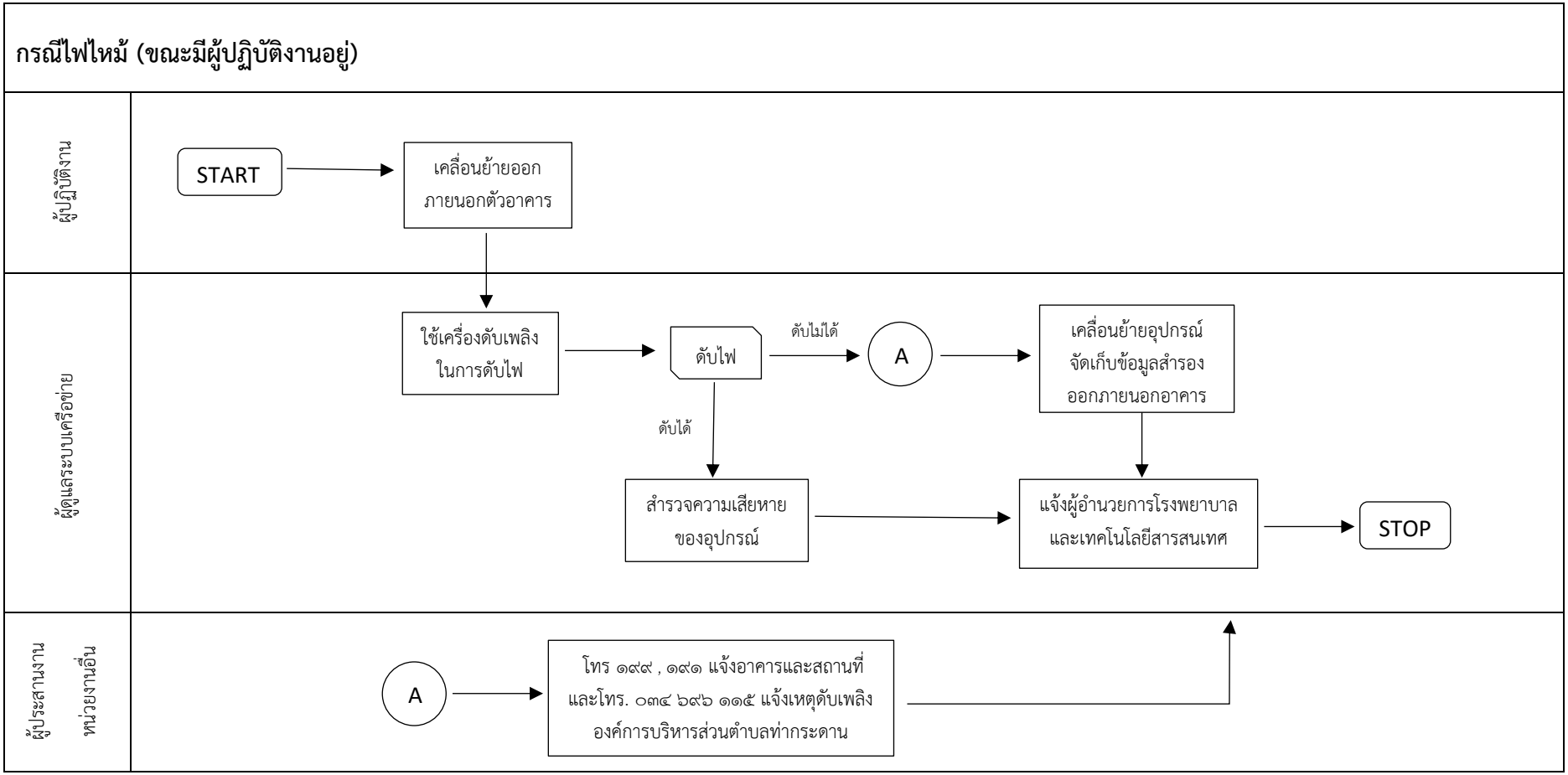
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งอาคารและสถานที่ และยานพาหนะทันที ที่เบอร์๐๓๔ ๖๙๖ ๑๑๘ ต่อ ๑๐๓

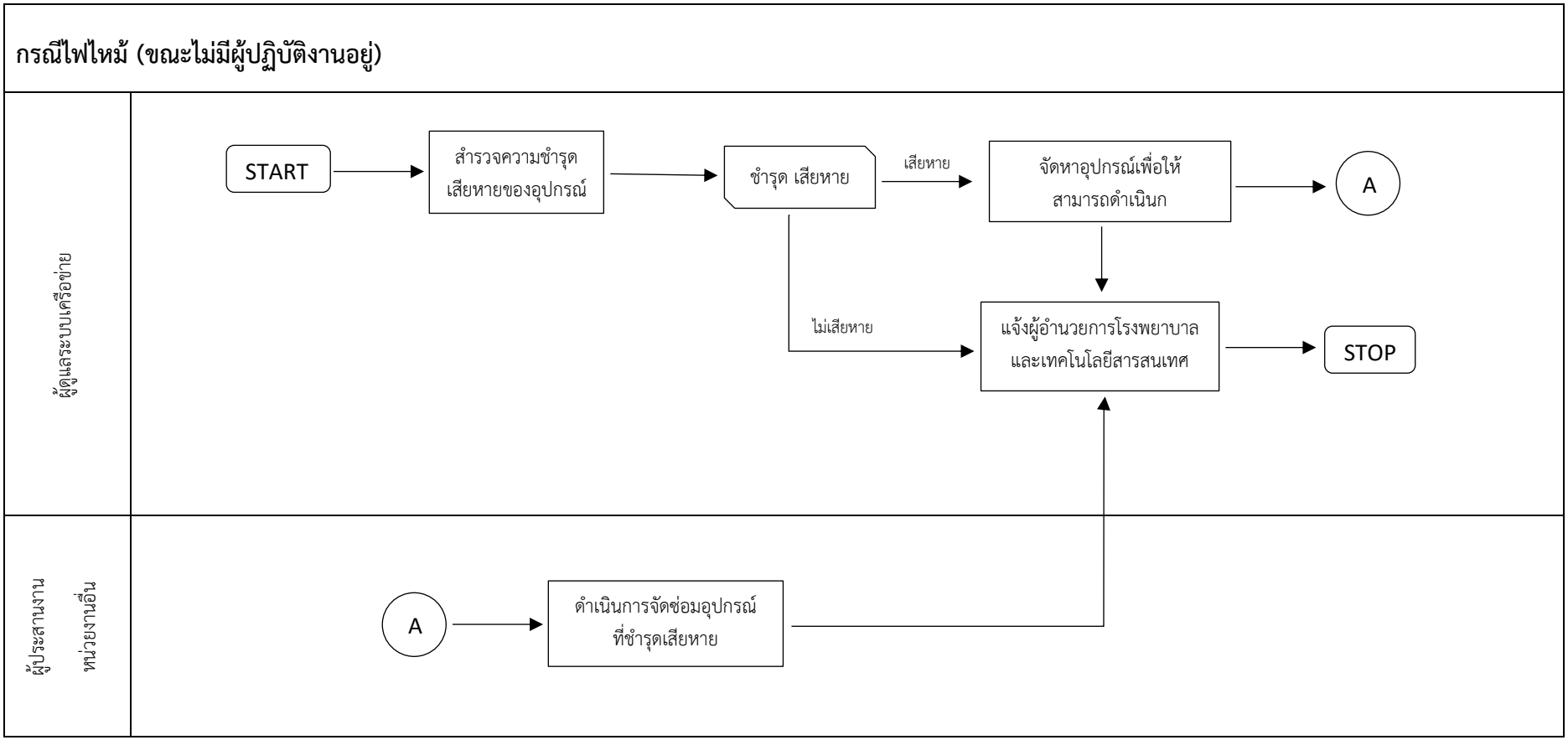
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไหได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๒ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



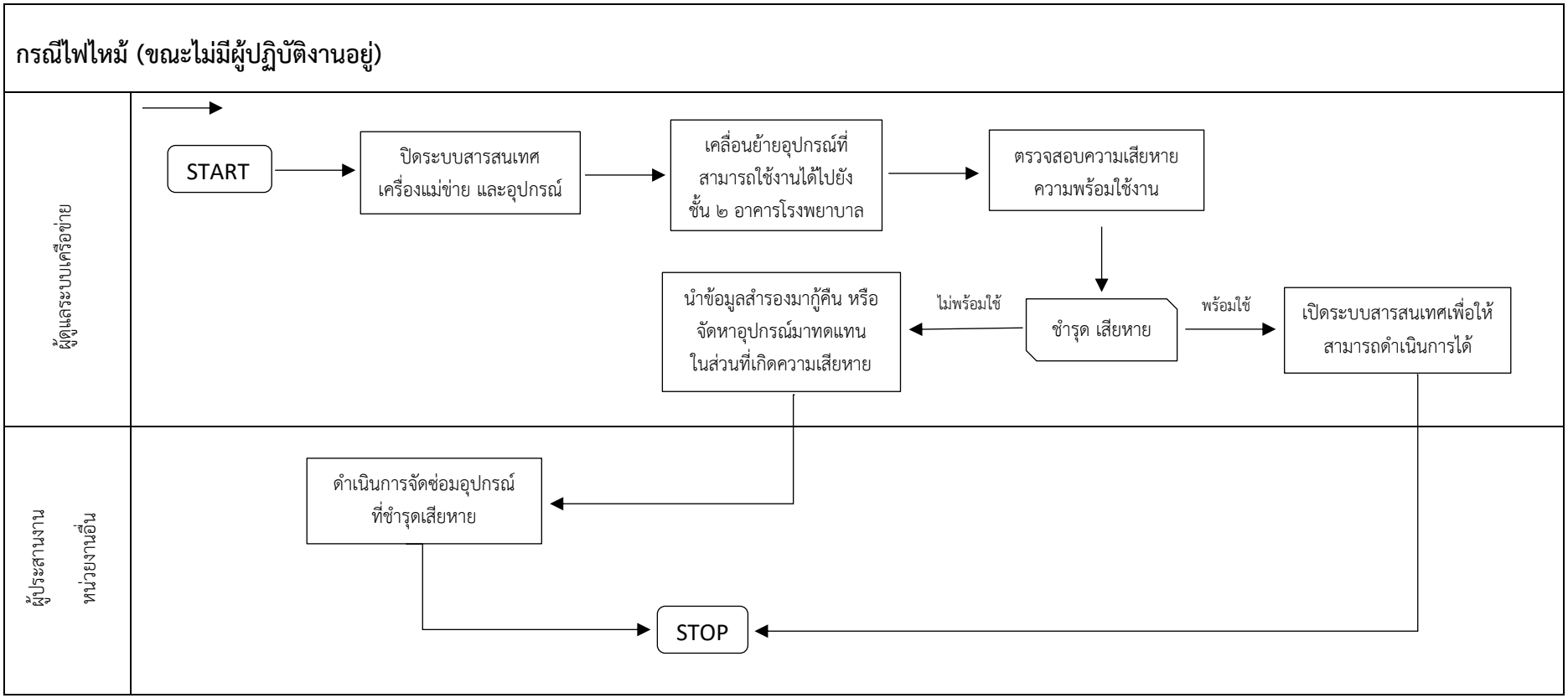
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



๔.๒.๒ กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่างๆที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ชั้น ๒ อาคารโรงพยาบาล
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

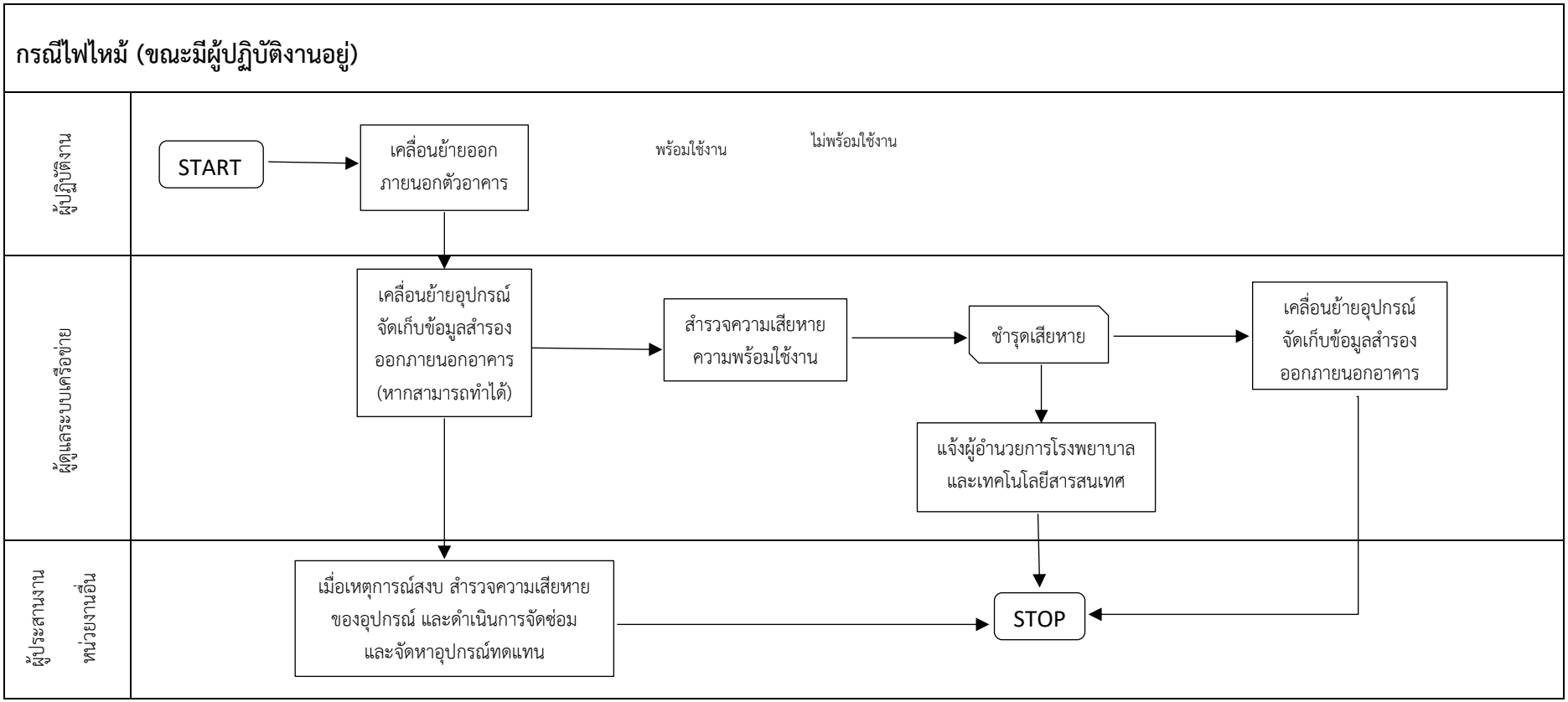
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



๔.๒.๒ กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรองเคลื่อนย้ายไปด้วย หากสามารถทำได้
- เมื่อสถานการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



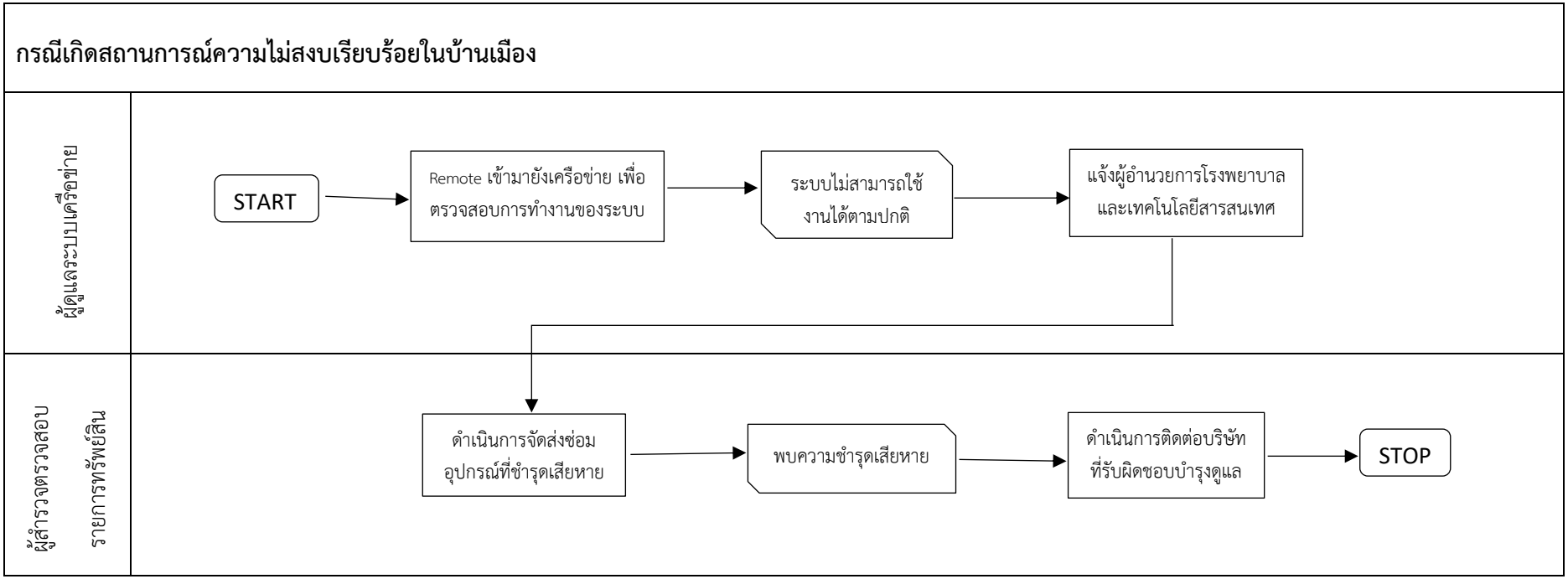
๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๔.๓.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการโรงพยาบาลและเทคโนโลยีสารสนเทศ

- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สิน ตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

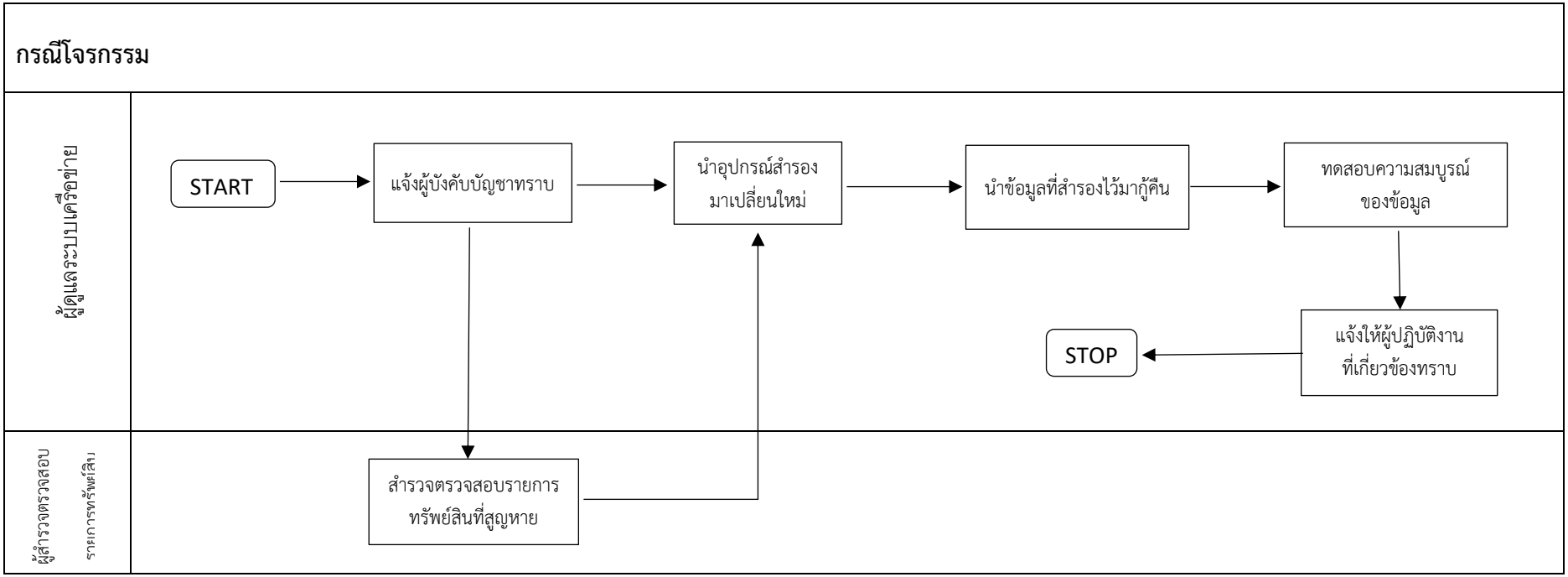


๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

๔.๔.๑ กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบ งานต่างๆได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

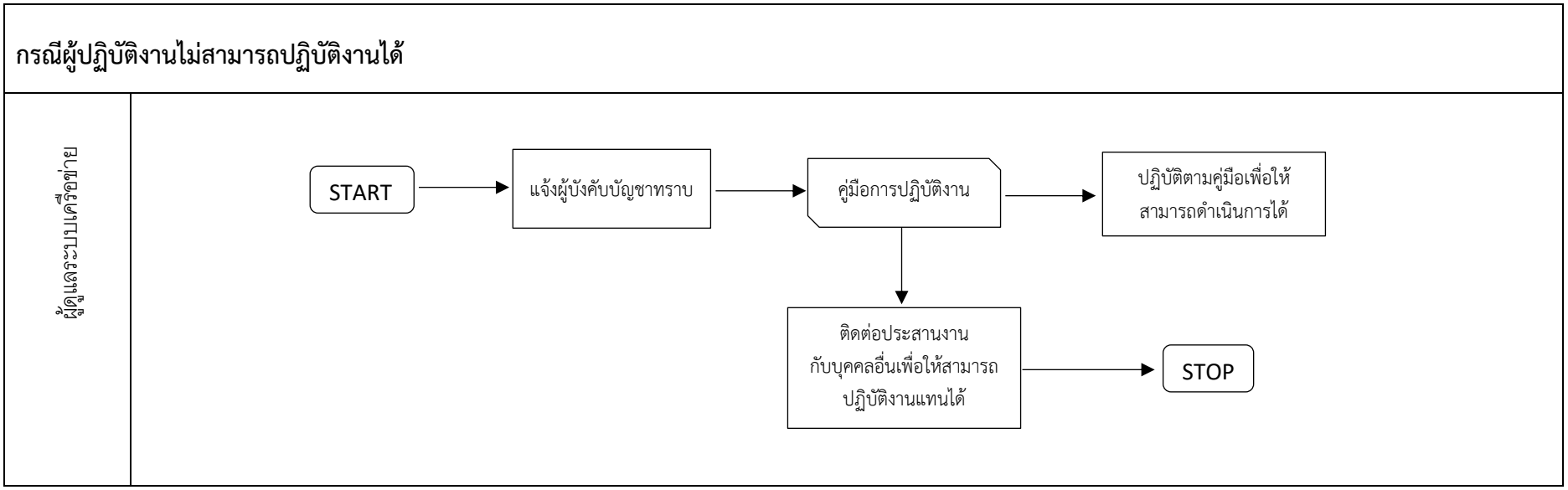


๔.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ

- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้



๕. การกู้คืนระบบกลับสู่สภาพปกติ (Disaster Recovery Plan)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้เร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จ

๔) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

๕) นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้ทีมกู้ระบบร่วมกันก็ระบบกลับมาโดยเร็ว

๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศหน่วยงาน จึงมีแผนจัดทำการแผนสำรองแหล่งข้อมูลที่ไซต์สำรอง เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ โดยแบ่งไซต์ ได้ ๓ ไซต์ คือ

๑. Hot Site เป็นไซต์ที่มีอุปกรณ์และซอฟต์แวร์เหมือนไซต์หลัก มีความพร้อมใช้งานทำให้เวลาในการกู้คืนระบบน้อยแต่จะมีต้นทุนการจัดทำที่สูง

๒. Warm Site เป็นไซต์ที่คล้ายกับ Hot Site แต่อาจจะมีอุปกรณ์ไม่ครบทำให้ความพร้อมใช้งานต่ำกว่า Hot Site ใช้ระยะเวลาในการกู้คืนมากกว่า แต่ต้นทุนราคาการจัดทำน้อยกว่า Hot Site

๓. Cold Site เป็นไซต์ที่มีแต่สถานที่ ไม่มีอุปกรณ์ทั้ง Hardware และ Software ในการกู้คืน มีต้นทุนการจัดทำต่ำ แต่ระยะเวลาในการกู้คืนนาน

๖. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงานได้แก่

๑.๑ ผู้อำนวยการ โรงพยาบาลท่ากระดาน

๑.๒ นักจัดการงานทั่วไป โรงพยาบาลท่ากระดาน

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

๒.๑ นาง กัญจนพร ศรีเพ็ชร นักวิชาการคอมพิวเตอร์

๒.๒ นางสาวฤทัยชนก อัจจิมากาญจน์ เจ้าพนักงานเครื่องคอมพิวเตอร์

แผนการรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการโรงพยาบาลท่ากระดาน เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(นายพิสุทธิ์ จรุงเรืองทรัพย์)

นายแพทย์ชำนาญการ ปฏิบัติหน้าที่

ผู้อำนวยการโรงพยาบาลท่ากระดาน

การดำเนินการบริหารจัดการความเสี่ยง ทีมสารสนเทศโรงพยาบาลท่ากระดาน ปีงบประมาณ 2565

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2565				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
๑.ความเสี่ยงจาก การเกิดไฟไหม้ น้ำท่วม แผ่นดินไหว อาคารถล่ม	ตรวจสอบความพร้อมใช้ของอุปกรณ์ดับเพลิง		✓			๑.ตรวจสอบอุปกรณ์ดับเพลิงถังสีเขียวชนิดฮาโลตรอน ให้เกจ์ความดันพร้อมใช้ ติดตั้งไว้หน้าห้องศูนย์คอมพิวเตอร์ ๒.ติดตั้งเบรกเกอร์ในการตัดไฟฟ้าของระบบ เมื่อไฟฟ้าเกิน รั่ว หรือขัดข้อง
	จัดทำแผนในการ เคลื่อนย้ายอุปกรณ์ ตามลำดับความสำคัญ				✓	๑.ทบทวนลำดับความสำคัญ ในการเคลื่อนย้าย ๒.จัดระบบให้ง่ายต่อการเคลื่อนย้าย สามารถถอดสายสัญญาณต่างๆได้อย่างสะดวกรวดเร็ว
	จัดทำแผนรับสถานการ เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง	←			→	๑.ตรวจสอบสำรวจเส้นทางสม่ำเสมอ และจัดทำเส้นทางสำรอง ๒.ทบทวนกระบวนการ หาวิทยาการและแนวทางใหม่ๆ
๒. ความเสี่ยงจากผู้ใช้งานสารสนเทศขาดความระมัดระวัง และ การตระหนักถึงความสำคัญของความปลอดภัยด้านเทคโนโลยีสารสนเทศ	ฝึกอบรม เผยแพร่ และประชาสัมพันธ์ เรื่องความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ	←			→	๑.จัดทำเอกสารประชาสัมพันธ์ ความมั่งคงปลอดภัยเทคโนโลยีสารสนเทศ แจกให้ทุกหน่วยงานได้รับทราบ
	กำกับดูแลการ ปฏิบัติตามแนว ปฏิบัติด้านการรักษาความมั่งคงปลอดภัย ด้านเทคโนโลยี สารสนเทศอย่างเคร่งครัด	←			→	๑.การออกระเบียบมาตรฐานการเข้าถึง การใช้ข้อมูล การรักษาความลับ ของการใช้ เทคโนโลยีสารสนเทศ ตามระเบียบหรือ พรบ.กฎหมายที่กำหนด ๒.การกำหนดการเข้าถึงข้อมูลสารสนเทศที่จำเป็น
๓. ความเสี่ยงจาก กระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที	แจ้งดำเนินการปรับปรุงของระบบไฟฟ้าสำรองอัตโนมัติ				✓	๑.เมื่อเครื่อง SERVER ปิดลงโดยเครื่องสำรองไฟฟ้าของโรงพยาบาลไม่ทำงาน แจ้งบริหารดำเนินการ
	ตรวจสอบความพร้อมของระบบสำรองไฟฟ้า	←			→	๑.วางแผนจัดซื้อ จัดหาเครื่องสำรองไฟฟ้าให้พอเพียงพ้อมใช้ ๒.ระบบบำรุงรักษาเครื่องสำรองไฟฟ้า บันทึกอายุการใช้งานและความคุ้มค่า

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2565				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
๔.ความเสี่ยงจากการ การถูกบุกรุกโดยผู้ไม่ประสงค์ดี	ตรวจสอบการตั้งค่า ของ Firewall, PS อย่างสม่ำเสมอ	←			→	๑.ศึกษา ตั้งค่า ตรวจสอบการท างานของระบบ fire wall สม่ำเสมอ ๒.อัพเดทการตั้งค่าตามความจำเป็น
	บริหารจัดการระบบ ตรวจสอบการบุกรุก เครือข่ายและติดตามเพื่อปรับปรุงอย่าง สม่ำเสมอ	←			→	๑.ศึกษาเทคโนโลยี การปรับปรุง ความเหมาะสมของอุปกรณ์ fire wall ๒.ตรวจสอบการบุกรุก และหาทางป้องกันอย่างสม่ำเสมอ
	จัดทำแผนจัดซื้อ Firewall ทดแทน				✓	๑.จัดซื้อตามความเหมาะสม คุ้มค่าตามอายุการใช้งาน
	อัพเดท Firmware content ของระบบ Firewall		✓			๑.อัพเดทเฟิร์มแวร์ของระบบ Firewall ให้ทันสมัยอยู่เสมอ
๕.ความเสี่ยงจากการ เชื่อมต่อเครือข่าย อินเทอร์เน็ตล้มเหลว หรือไม่สามารถใช้ งานได้	สำรวจและจัดหาระบบ เครือข่ายอินเทอร์เน็ตสำรองเพื่อเป็นช่องทางให้ระบบอินเทอร์เน็ต ใช้ งานได้อย่างต่อเนื่อง	←			→	๑.จัดทำระบบ Internet สำรอง ด้วยวิธี Load balance ๒.ตรวจสอบการอัพเดทแพ็กเกจอินเตอร์เน็ต เพื่อให้องค์กรใช้ได้อย่างคุ้มค่า ๓.กรณีอินเตอร์เน็ตขัดข้องทั้ง ๒ เส้น จำเป็นต้องยอมรับความเสี่ยง
	ตรวจสอบการเชื่อมต่อเครือข่ายอินเทอร์เน็ต	←			→	๑.สร้างมาตรฐาน ตรวจสอบการเชื่อมต่อ ความเร็ว ของอินเตอร์เน็ตอยู่เสมอ
๖. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉินร้ายแรงมากที่สุด	จัดทำแผนขั้นตอนการอนุมัติ การติดตั้งเพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง				✓	๑.จัดทำแผนจัดซื้อไปอย่างสม่ำเสมอ เพื่อสามารถจัดหาได้อย่างทันเวลา ๒.จัดทำระบบสำรองอุปกรณ์อย่างเพียงพอ เหมาะสม
	จัดทำคู่มือแผนบริหารความต่อเนื่อง (BCP)และแผนกู้คืนระบบ DRP				✓	๑.จัดทำคู่มือ และสามารถเรียกใช้ได้ทันที

ประเภทความเสี่ยง	แนวทางการควบคุม	ปีงบ 2565				มาตรการควบคุม
		Q1	Q2	Q3	Q4	
๗.ความเสี่ยงจากการไม่ได้รับงบประมาณในการบำรุงรักษาระบบสารสนเทศ และระบบคอมพิวเตอร์อย่างต่อเนื่องและเพียงพอ	มีการสำรวจและ รวบรวมความต้องการ อย่างต่อเนื่อง เพื่อการจัดทำงบประมาณใน แต่ละปี		←	→		๑.รวบรวมความต้องการ จัดทำแผนล่วงหน้าในการพิจารณาตามลำดับความสำคัญ ๒.ชี้แจงแนวทางการจัดซื้อ อธิบายการไม่อนุมัติแก่เจ้าหน้าที่และวางแผนการ ดำเนินงานในคราวถัดไป
	มีการหารือ ชี้แจ้งและทำความเข้าใจกับ ผู้บังคับบัญชาในเรื่องงบประมาณที่ต้องการใช้อย่างชัดเจน			✓		๑.มีการวางแผนจัดซื้อ ปรึกษาทำความเข้าใจ สรุปการจัดซื้อและทิศทางที่จะเป็นไป ๒.ออกแบบแผนงานให้สอดคล้องกับนโยบายของผู้บังคับบัญชา
๘. ความเสี่ยงระบบเทคโนโลยีอาจทำให้ เกิดความบกพร่องในการดูแลผู้ป่วย	เมื่อพบเหตุอุบัติการณ์ให้รายงานทุกครั้ง	←			→	๑.บันทึกอุบัติการณ์ ไว้เป็นข้อมูลปรับปรุง พัฒนา ของฝ่ายสารสนเทศ
	ควบคุม ติดตาม ดูแล โดยคณะกรรการความ เสี่ยงรพ.ท่ากระดาน	←			→	๑.ติดตามข้อมูล เก็บประวัติและสถิติ ไว้ปรับปรุงแก้ไข ทุกๆปี ๒.เมื่อมีเหตุระดับรุนแรงให้วางแผนแก้ไขทันที
๙. ความเสี่ยงด้านการการเปิดเผยข้อมูลผู้ป่วย	จัดทำแผนโครงการกระตุ้นผู้ใช้งานให้ ตระหนักในความเสี่ยงของการเปิดเผยข้อมูล หรือแชร์ข้อมูลในสื่อสังคมออนไลน์ ทุกชนิด	←			→	๑.จัดทำสื่อ กระตุ้นเตือน ให้ตระหนักในความเสี่ยงของการเปิดเผยข้อมูล หรือแชร์ข้อมูลในสื่อสังคม ออนไลน์ทุกปี
	ปรับปรุงระเบียบปฏิบัติในการรักษาความ มั่นคงปลอดภัยด้านสารสนเทศของ รพ.				✓	๑.ปรับปรุงระเบียบปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศทุกปี ๒.ศึกษาระเบียบต่างๆอยู่เสมอ เพื่อสร้างมาตรฐานตามหลักสากล
	ประกาศใช้นโยบายเรื่องระเบียบปฏิบัติใน การปฏิบัติการส่งข้อมูลผู้ป่วยทางโปรแกรม LINE	✓				๑.จัดทำนโยบายเรื่องระเบียบปฏิบัติในการปฏิบัติการส่งข้อมูลผู้ป่วยทางด้านต่างๆ และประกาศใช้ในโรงพยาบาล
	เพิ่มกระบวนการให้ผู้ป่วยยินยอมให้เปิดเผย ข้อมูลเพื่อการวินิจฉัยและรักษาในช่องทาง ต่าง ๆ (*ผู้ป่วยในใช้แบบฟอร์ม Informed Consent,ผู้ป่วยนอกใช้ตรายาง)	✓				๑.ประชุมหาข้อตกลง ในการออกแบบฟอร์มให้ผู้รับบริการยินยอมเปิดเผยข้อมูล