



แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan)



กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ

ศูนย์คุณธรรม (องค์การมหาชน)

[illegible]

สารบัญ

เรื่อง	หน้า
1.บทนำ.....	1
2.วัตถุประสงค์.....	1
3.การวิเคราะห์ความเสี่ยง.....	2
4.แผนรองรับสถานการณ์ฉุกเฉิน.....	3
4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค	
4.1.1 กรณีการป้องกันไวรัสล้มเหลว.....	3
4.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว.....	4
4.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว.....	5
4.1.4 กรณีอุปกรณ์หรือคอมพิวเตอร์ขัดข้อง.....	6
4.1.5 กรณีไฟฟ้าขัดข้อง.....	8
4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ	
4.2.1 กรณีไฟไหม้.....	9
4.2.2 กรณีน้ำท่วมหรือน้ำรั่ว.....	12
4.2.3 กรณีแผ่นดินไหว/อาคารถล่ม.....	13
4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง	
4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง.....	14
4.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล	
4.4.1 กรณีโจรกรรม.....	15
4.4.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้.....	16
5.การกำหนดผู้รับผิดชอบ.....	17

แผนรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (IT Contingency plan) ศูนย์คุณธรรม (องค์การมหาชน)

1. บทนำ

ปัจจุบัน ศูนย์คุณธรรม (องค์การมหาชน) มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการในการสนับสนุนการปฏิบัติงานของเจ้าหน้าที่ศูนย์คุณธรรม มากขึ้นประกอบกับการพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งาน อันมีประโยชน์ต่อส่งเสริมและสนับสนุนเสริมด้านคุณธรรมทั้งภายในและภายนอกองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นจำเป็นต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ ศูนย์คุณธรรม (องค์การมหาชน) ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนให้ได้รับความสะดวกมากยิ่งขึ้น ในขณะที่เดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตีจากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการทำงาน ดังนั้น เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีการรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันที่
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

3. การวิเคราะห์ความเสี่ยง

ศูนย์คุณธรรม (องค์การมหาชน) มีการใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนส่งเสริมคุณธรรม ความดีให้เกิดประโยชน์สูงสุด

การวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ศูนย์คุณธรรม (องค์การมหาชน) พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง การถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ไฟฟ้าขัดข้อง เป็นต้น
2. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการทำงานด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของ ศูนย์คุณธรรม (องค์การมหาชน) ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ ศูนย์คุณธรรม (องค์การมหาชน) ให้มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

4. แผนรองรับสถานการณ์ฉุกเฉิน

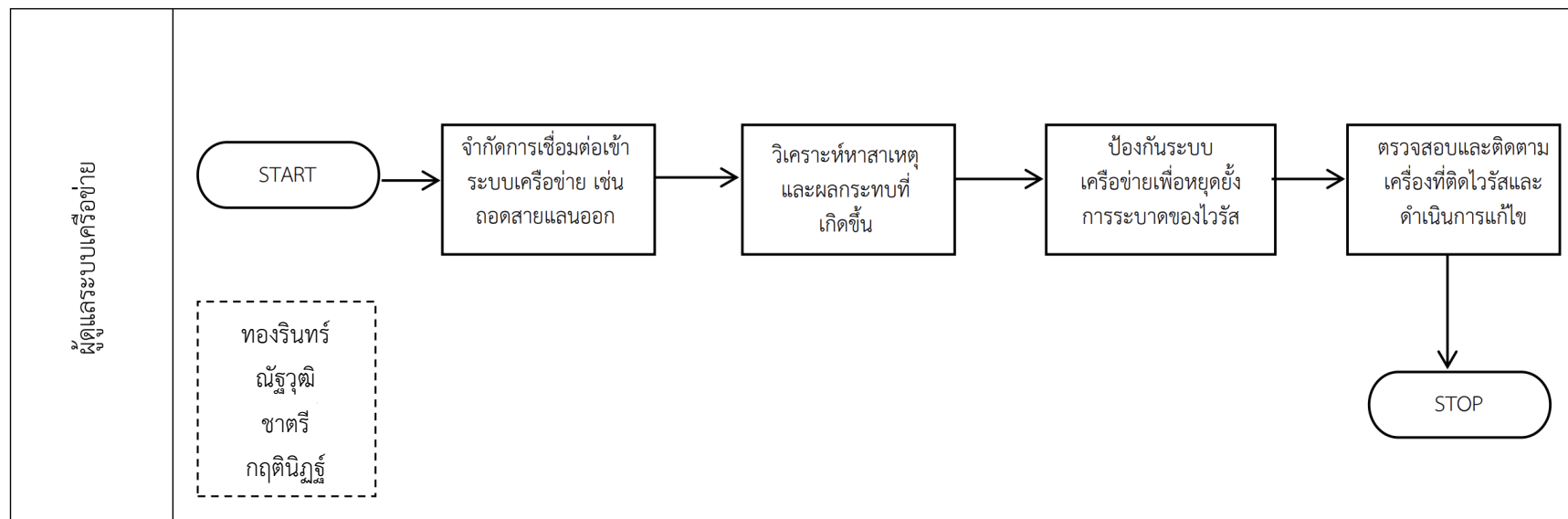
4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

4.1.1 กรณีการป้องกันไวรัสล้นเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าสู่ระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ ทราบ หรือกรณี

มีเหตุอันทำให้งานเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ กลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงาน ทราบ

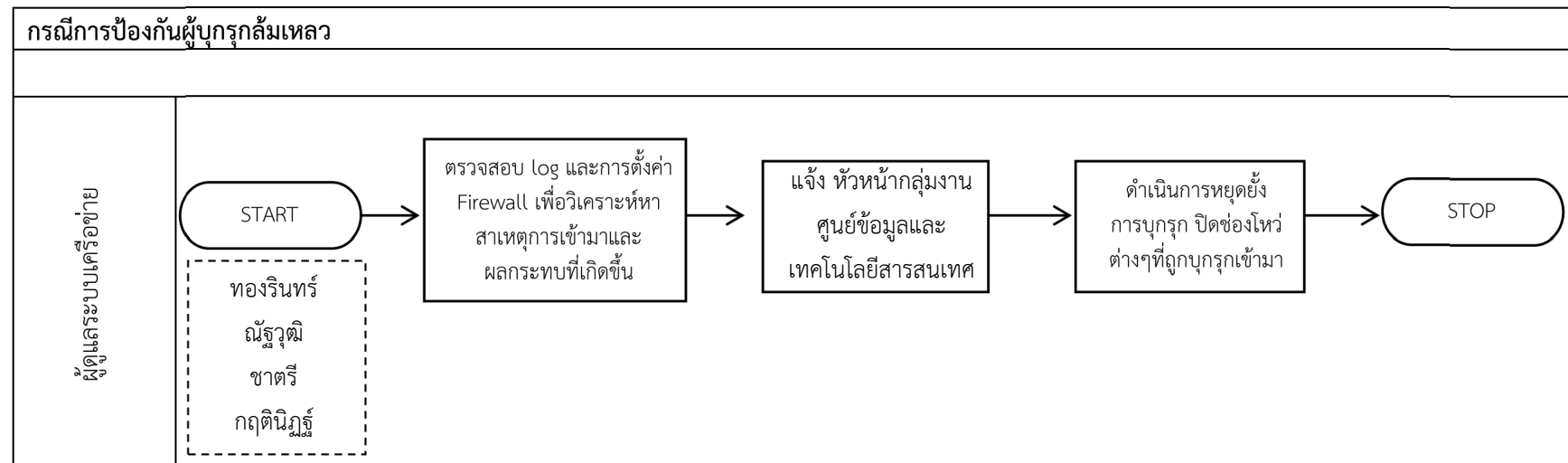
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้นเหลว



4.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

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

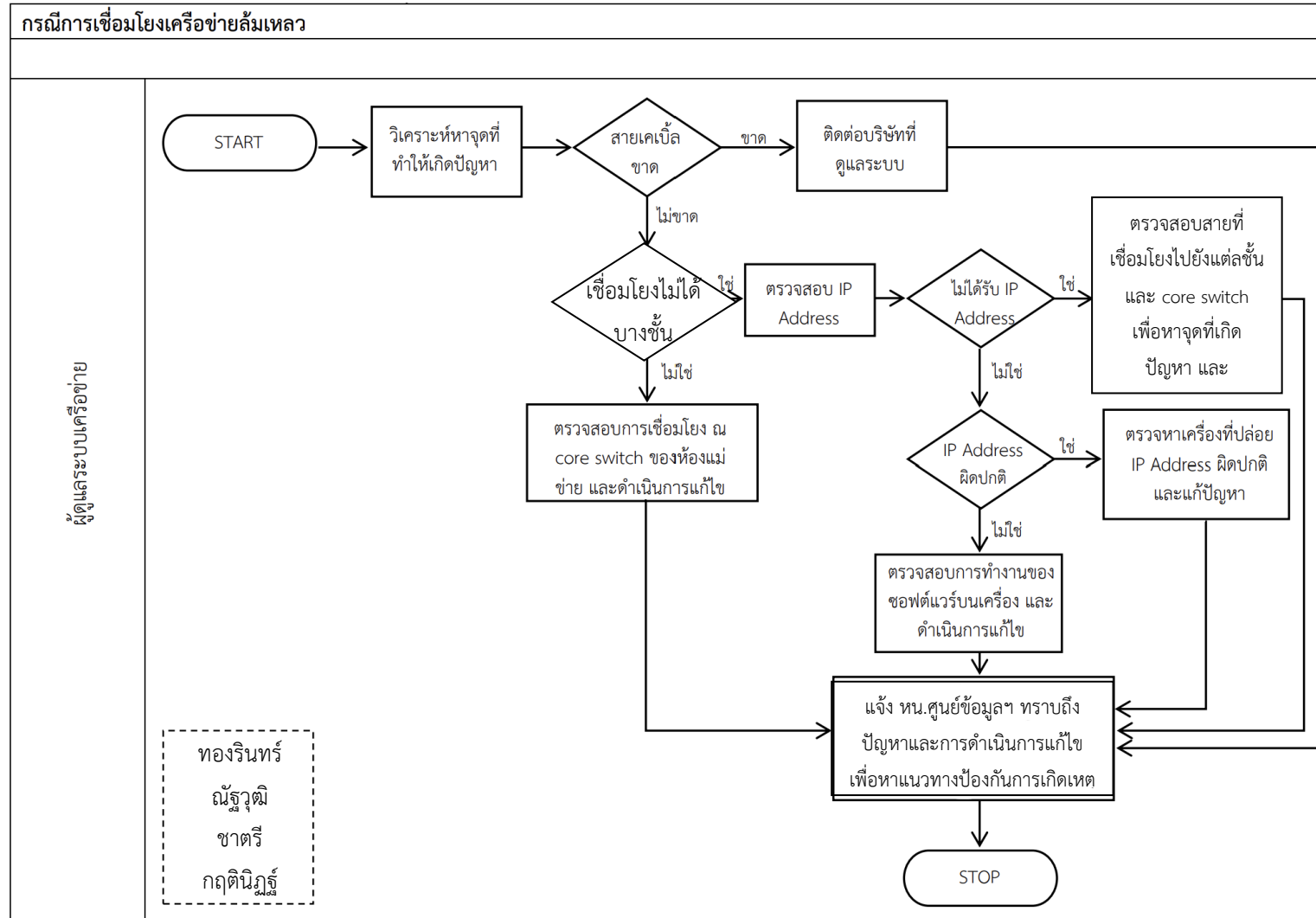
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



4.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รับผิดชอบการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิลขาด ให้รีบแจ้งผู้อำนวยการ/ผู้บริหารสารสนเทศระดับสูงระดับกรม (DCIO) พร้อมติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา เพื่อดำเนินการซ่อมแซมสายเคเบิลให้เสร็จเรียบร้อยโดยเร็ว

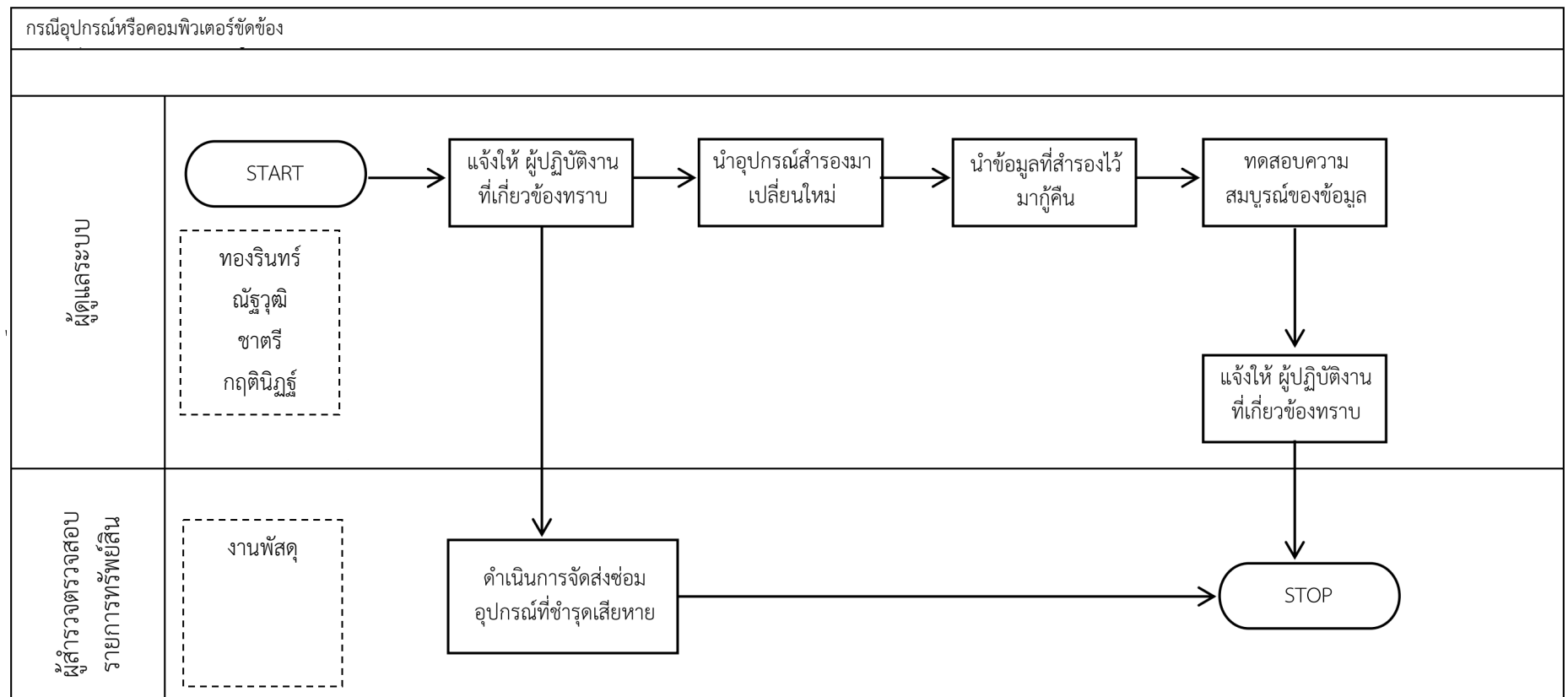
- แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



4.1.4 กรณีอุปกรณ์หรือคอมพิวเตอร์ขัดข้อง

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รับผิดชอบการจัดหาอุปกรณ์มาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

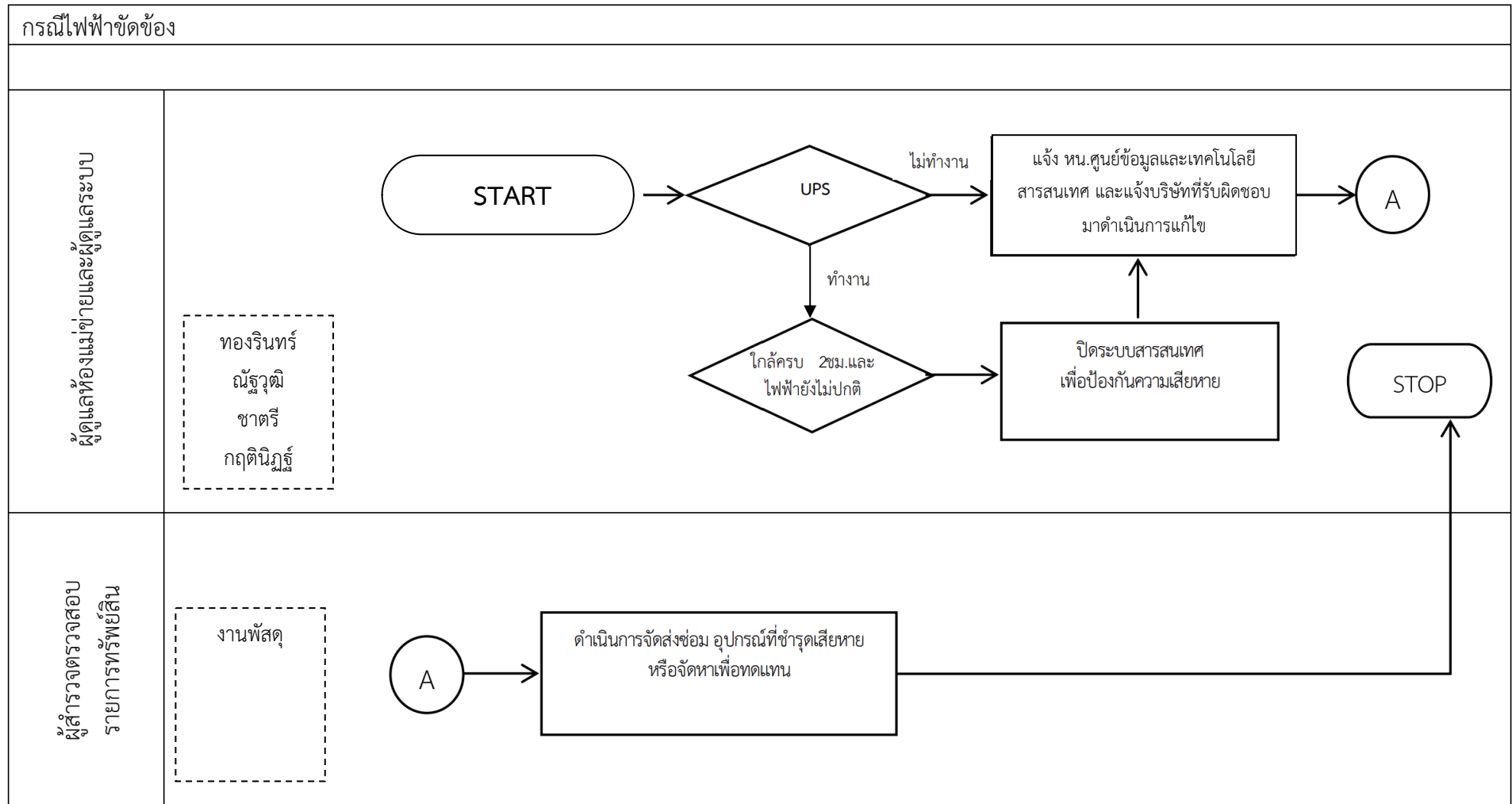
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์หรือคอมพิวเตอร์ขัดข้อง



4.1.5 กรณีไฟฟ้าขัดข้อง

- ศูนย์ข้อมูลและเทคโนโลยีสารสนเทศมี เครื่องสำรองไฟฟ้า (UPS) ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ 2 ชั่วโมง
- หากใกล้ครบ 2 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้ากลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ
- ผู้ดูแลระบบดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งหัวหน้ากลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศและติดต่อบริษัทแลบำรุงรักษา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

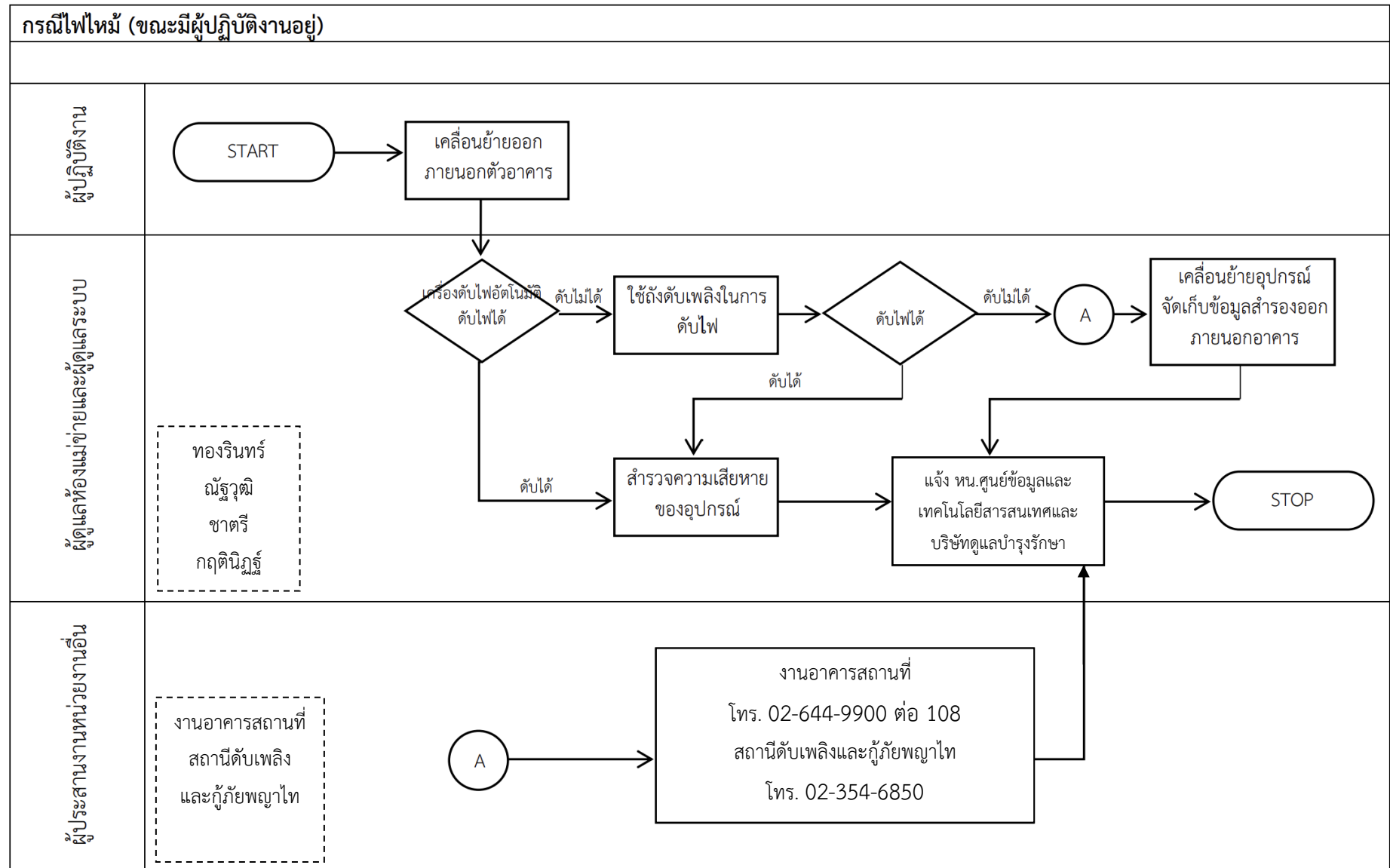


4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

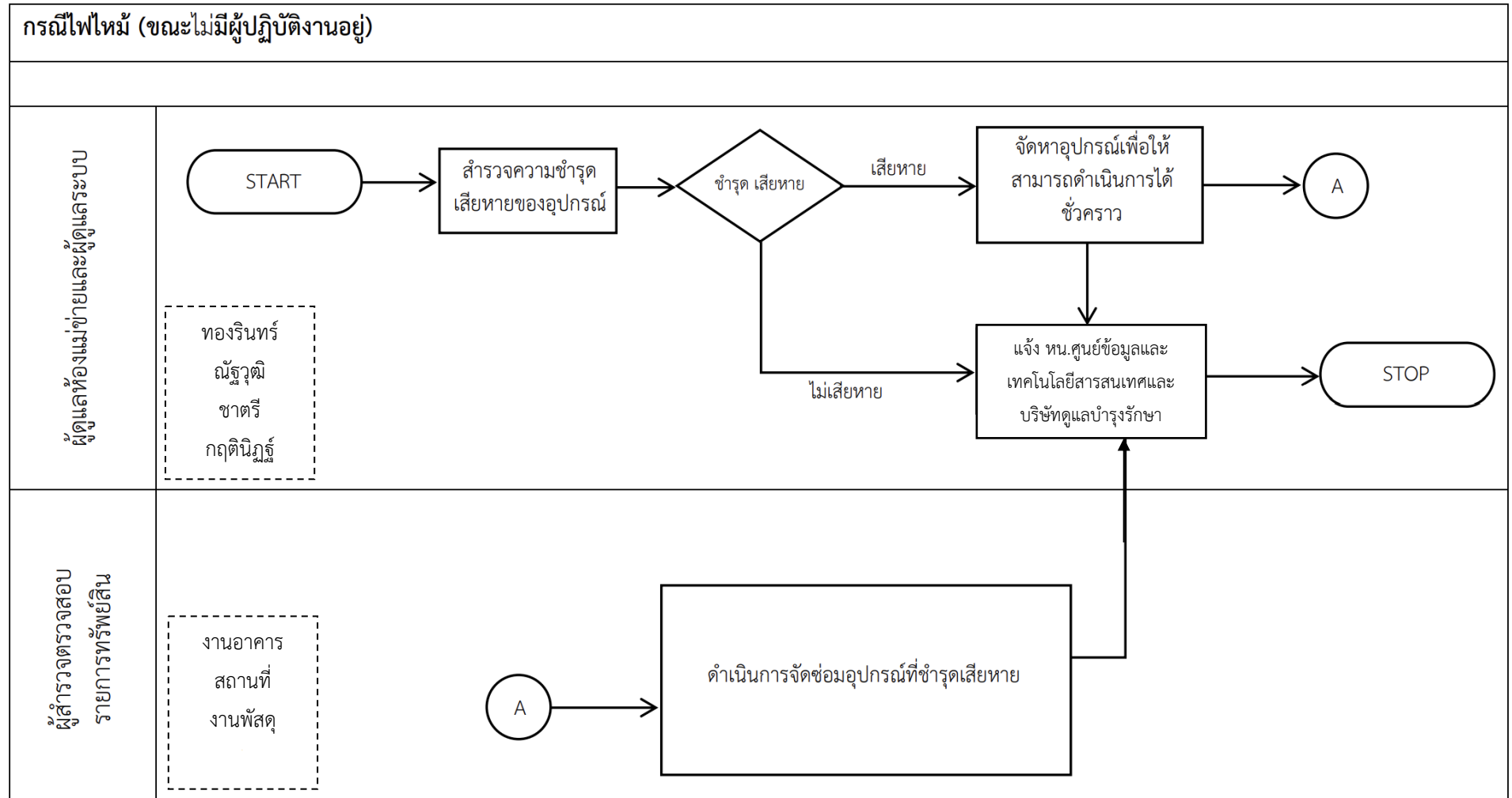
4.2.1 กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้ง งานอาคารสถานที่ หมายเลขโทรศัพท์ศูนย์คุณธรรม โทร. 02-644-9900 ต่อ 108 และโทรแจ้งสถานีดับเพลิงและกู้ภัยพญาไท โทร. 02-354-6850
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และ/หรือ ระบบดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



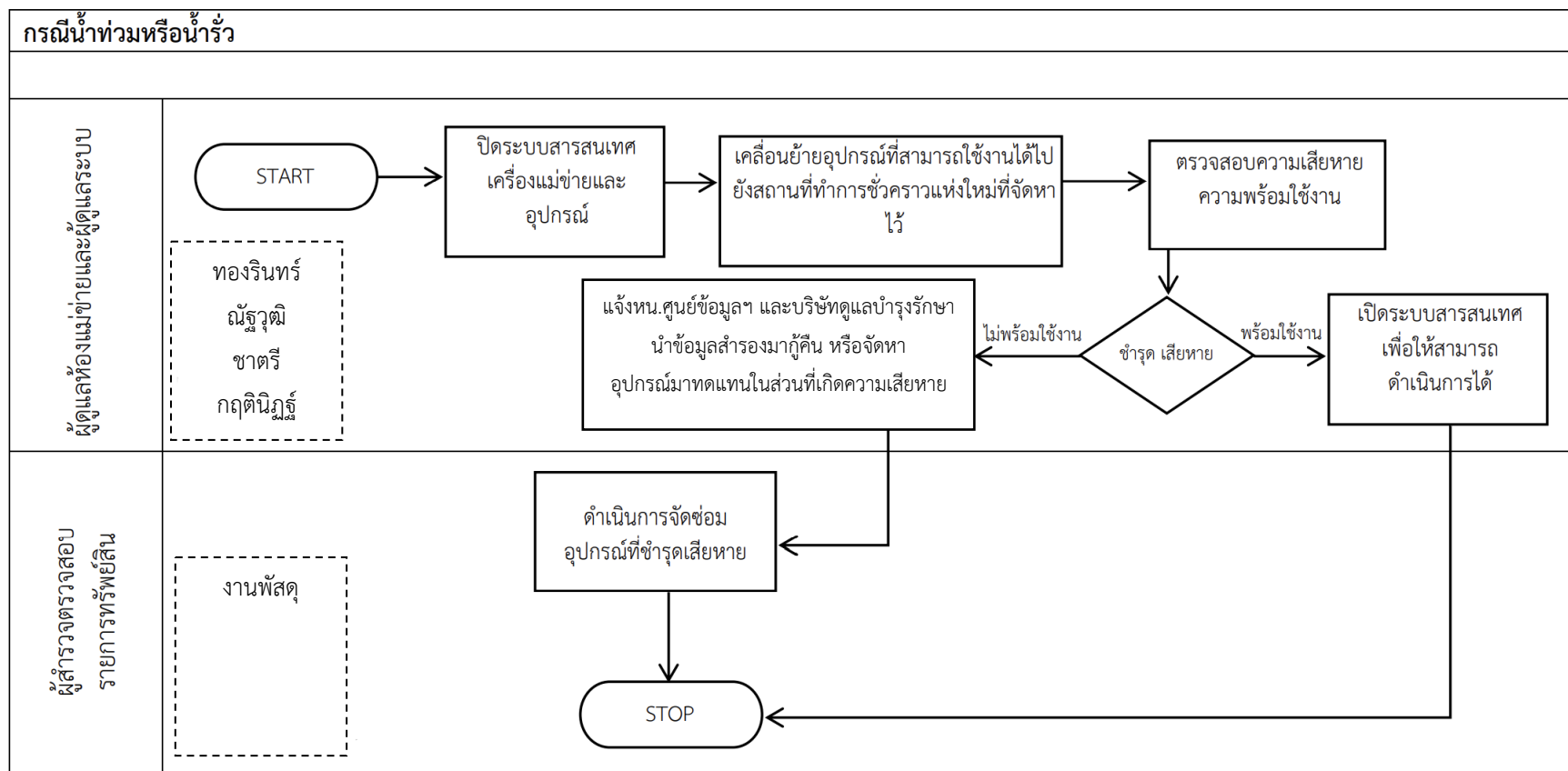
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



4.2.2 กรณีน้ำท่วมหรือน้ำรั่ว

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่างๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ สถานที่ทำการชั่วคราวที่จัดหาไว้ผู้ดูแลระบบนำข้อมูลสำรองเคลื่อนย้ายไปด้วยหากสามารถทำได้
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำนวความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

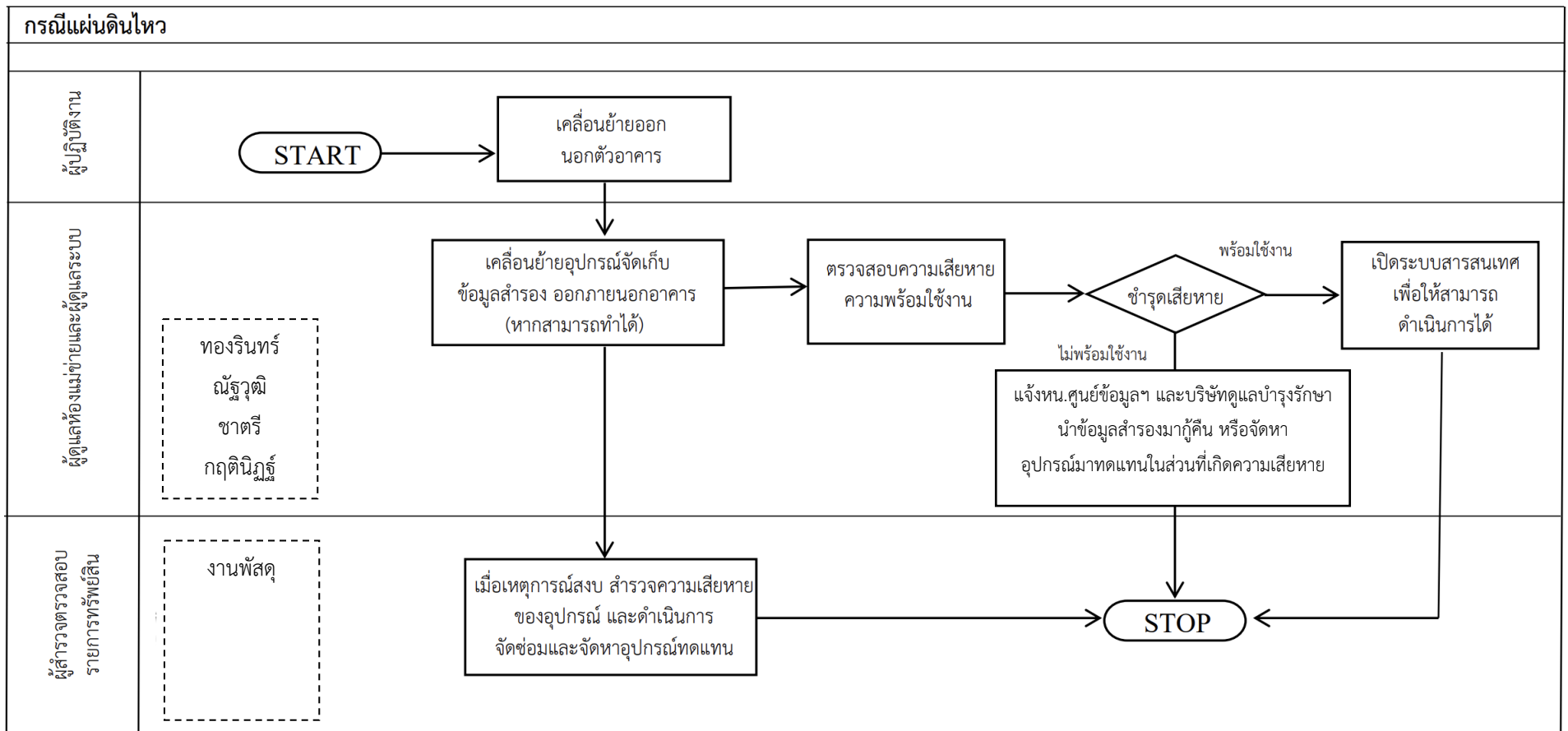
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วมหรือน้ำรั่ว



4.2.3 กรณีแผ่นดินไหว/อาคารถล่ม

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

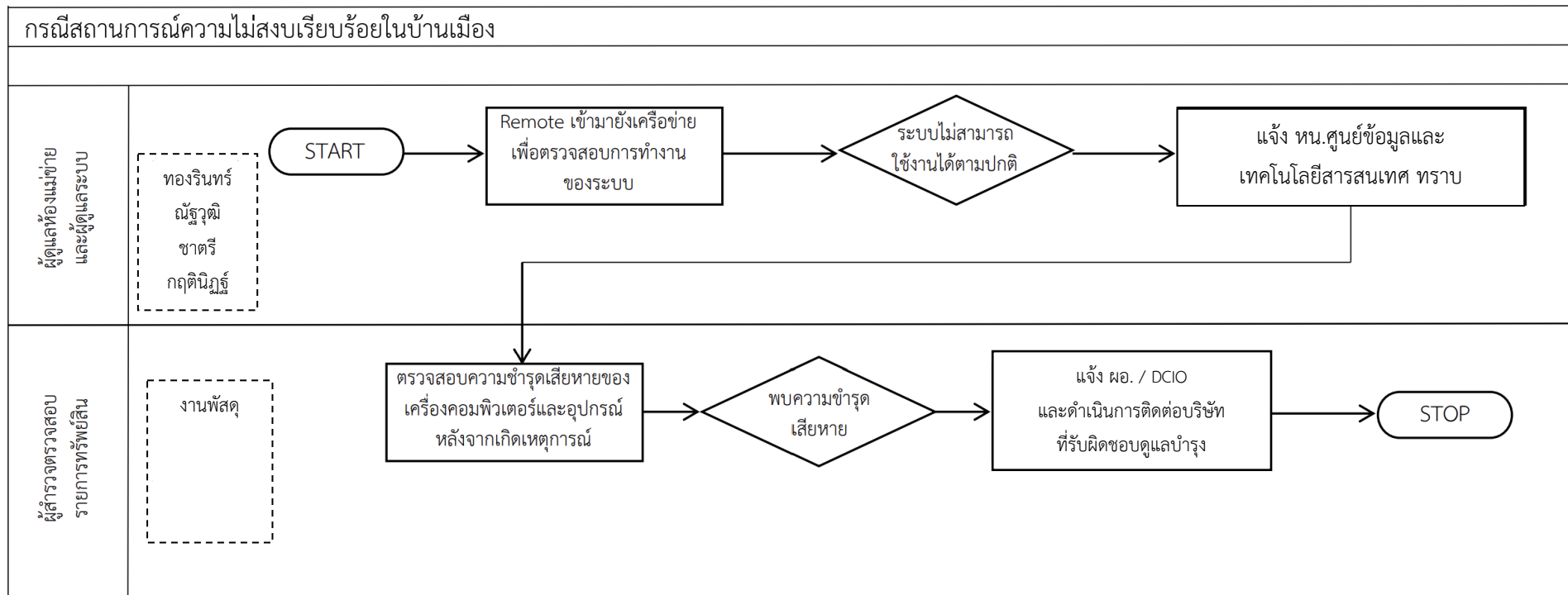


4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งหัวหน้าศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้แจ้งผู้ผู้อำนวยการ/ผู้บริหารสารสนเทศระดับสูงระดับกรม (DCIO) ทราบพร้อมดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษาดำเนินการซ่อมแซมแก้ไขหากจำเป็น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

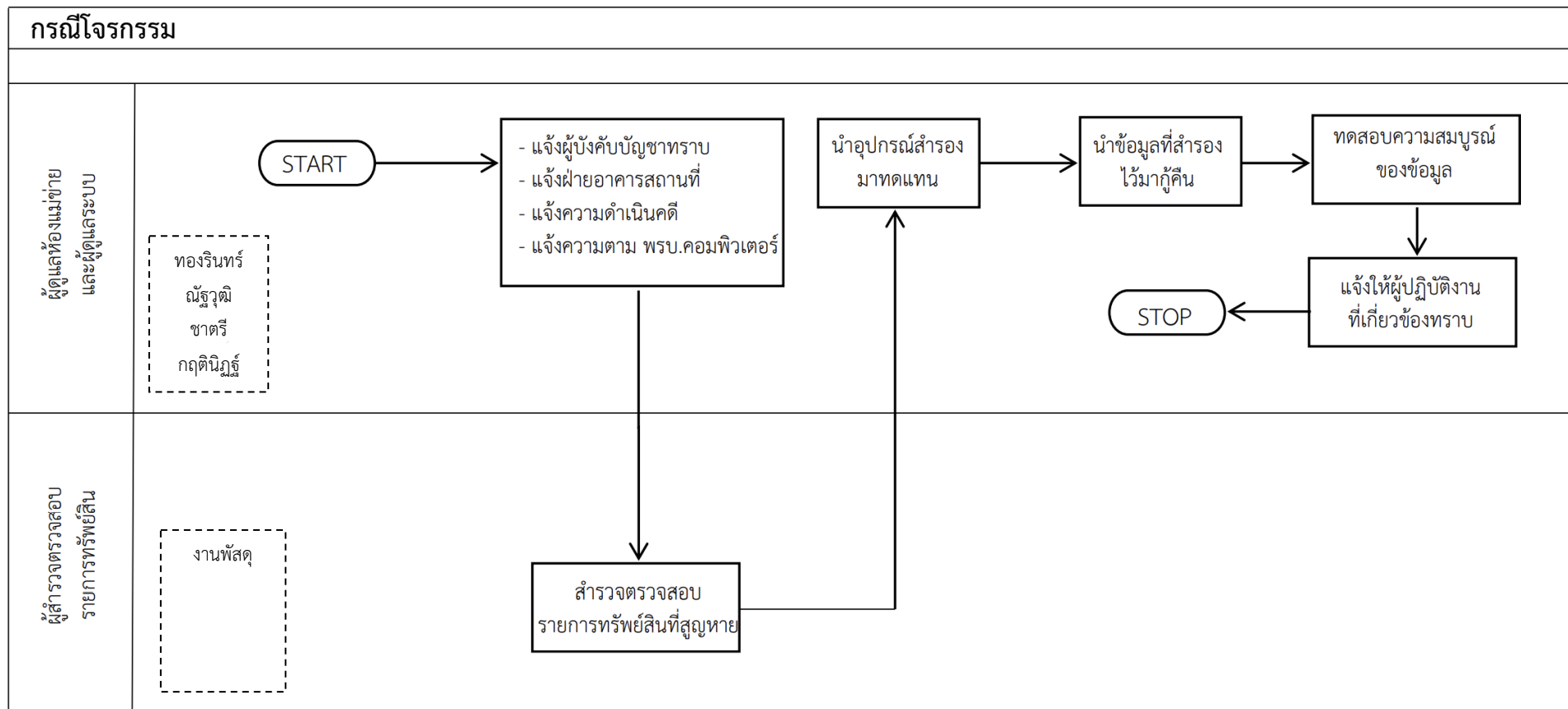


4.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

4.4.1 กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สํารวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆได้โดยเร็ว

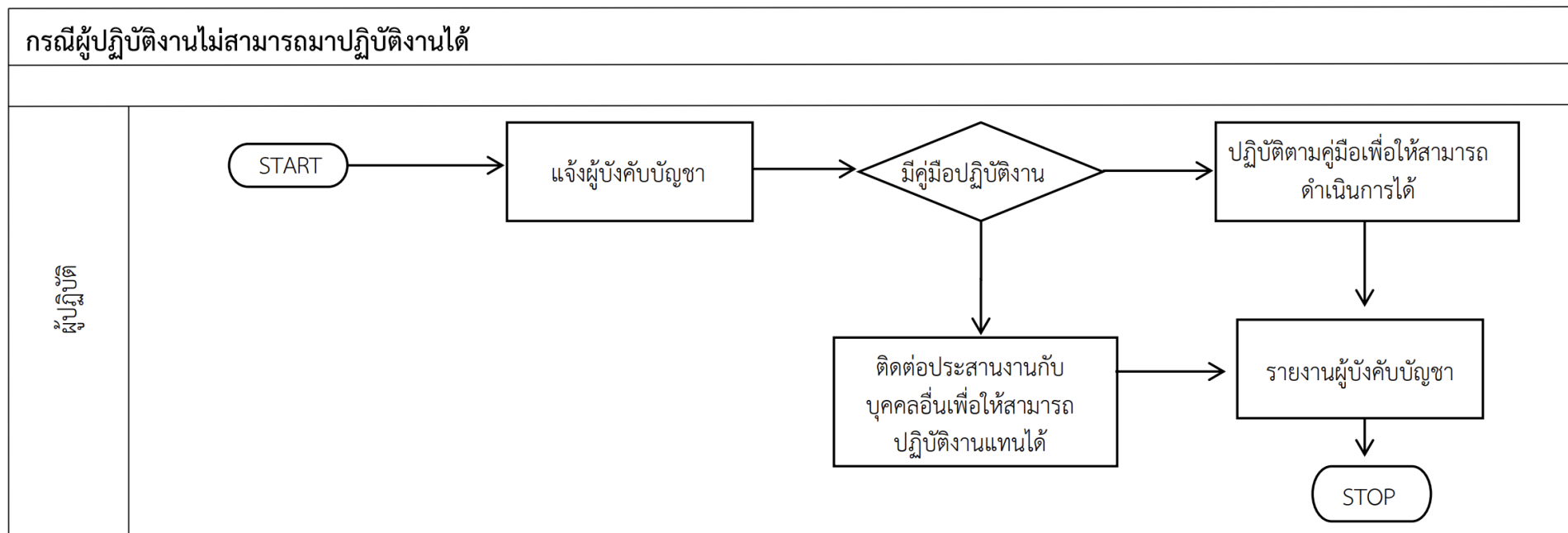
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



4.4.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



5. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

1. ผู้บริหาร รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

1.1 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO) หรือ ผู้จัดการสำนักพัฒนาองค์ความรู้นวัตกรรมและสื่อสารสนเทศ

1.2 หัวหน้ากลุ่มงานศูนย์ข้อมูลและเทคโนโลยีสารสนเทศ

2. ทีมวิศวกรรม รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล (ปรับเปลี่ยนผู้ให้บริการตามการจัดซื้อจัดจ้างตามปีงบประมาณ)

3. ทีมระบบสารสนเทศและฐานข้อมูล รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

3.1 นายชาติรี ดุลยเสนีย์ เจ้าหน้าที่โครงการ

3.2 นายณัฐวุฒิ วศินโกศทรัพย์ เจ้าหน้าที่เทคโนโลยีสารสนเทศ

4. ทีมบริการเทคนิคและการประสานงาน รับผิดชอบการปฏิบัติงานทางเทคนิค และประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

4.1 นายณัฐวุฒิ วศินโกศทรัพย์ เจ้าหน้าที่เทคโนโลยีสารสนเทศ

4.2 นางกฤติณัฐ์ ประสมพลอย นักวิชาการส่งเสริมคุณธรรม

4.3 นายชาติรี ดุลยเสนีย์ เจ้าหน้าที่โครงการ

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากคณะทำงานพัฒนาระบบข้อมูลสารสนเทศและเทคโนโลยีดิจิทัล ศูนย์คุณธรรม (องค์การมหาชน) เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม

มิถุนายน 2567