แผนบริหารความเสี่ยง
เทคโนโลยีสารสนเทศและการสื่อสารจังหวัดพัทลุง

สำนักงานจังหวัดพัทลุง

สารบัญ

หน้า

แผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศและการสื่อสาร

๑. หลักการและเหตุผล

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการและสนับสนุนการปฏิบัติงานมากขึ้นเพื่อความสะดวกในการปฏิบัติงาน อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร การนำเทคโนโลยีสารสนเทศและการสื่อสารมาใช้มากขึ้น ทำให้การใช้ข้อมูลสารสนเทศต่างๆ มีความยึดโยงกับระบบเทคโนโลยีสารสนเทศเป็นสำคัญ ในขณะที่การใช้ระบบเทคโนโลยีฯ ยังมีข้อจำกัดในด้านการรักษาความมั่นคงและความปลอดภัยของข้อมูล จึงจำเป็นต้องมีระบบการจัดเก็บและดูแลรักษาความปลอดภัยของข้อมูลสารสนเทศที่มีประสิทธิภาพ

จังหวัดพัทลุงได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานและให้บริการประชาชนให้ได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากสถานการณ์ภัยพิบัติ เช่น ปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหาอันอาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ รวมทั้งระบบเครือข่าย จังหวัดจึงได้จัดทำแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศเพื่อเป็นกรอบแนวทางในการดูแลรักษา และป้องกันแก้ไขปัญหาอันอาจเกิดขึ้นดังกล่าว

๒. นิยามศัพท์

๒.๑ การบริหารความเสี่ยง หมายถึง การบริหารจัดการและการเก็บรวบรวมข้อมูลอย่างเป็นระบบเพื่อไม่ให้ข้อมูลที่จัดเก็บเกิดการสูญหายอันเนื่องมาจากภัยพิบัติที่เกิดขึ้น

๒.๒ ภัยพิบัติ หมายถึง ภัยที่เกิดจากธรรมชาติและจากการกระทำของมนุษย์ที่มีระดับความรุนแรงและผลกระทบที่ต่างกันไป กล่าวคือ

(๑) ภัยที่เกิดจากธรรมชาติ เป็นภัยที่เกิดจากสภาพทางภูมิศาสตร์และที่ตั้ง ได้แก่ อุทกภัย วาตภัย ภัยหนาว ภัยแล้ง ไฟป่า และแผ่นดินไหว เป็นต้น

(๒) ภัยที่เกิดจากการกระทำของมนุษย์ เป็นภัยที่ปรากฏเป็นรูปธรรมและภัยที่เป็นนามธรรม ได้แก่ อัคคีภัย ภัยจากการคมนาคมขนส่ง ภัยจากการทำงาน ภัยจากสารเคมีและวัตถุอันตราย ภัยจากโรคระบาดสัตว์และพืช รวมทั้งภัยจากเทคโนโลยีอื่นๆ

๒.๓ ระบบสารสนเทศ หมายถึง ระบบข้อมูลข่าวสารที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสาร มาช่วยในการสร้างระบบสารสนเทศเพื่อนำมาใช้ในการวางแผน การบริหารและการพัฒนา ซึ่งมีองค์ประกอบดังนี้

(๑) ระบบคอมพิวเตอร์ (Computer System)

(๒) ระบบสื่อสาร (Communication System)

(๓) ระบบสารสนเทศ (Information System)

๓. วัตถุประสงค์

๑. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและความเสียหายที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศมีประสิทธิภาพสามารถใช้งานได้ตลอดเวลา และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงทีกรณีเกิดภัยคุกคาม

๔.สถานภาพระบบสารสนเทศและการสื่อสารจังหวัดพัทลุง

๔.๑ ระบบสารสนเทศและการสื่อสารจังหวัดพัทลุง ประกอบด้วย

๔.๑.๑ ระบบเครือข่าย

- สัญญาณอินเตอร์เน็ต สำนักงานปลัดกระทรวงมหาดไทย
- สัญญาณอินเตอร์เน็ต GIN (ของกระทรวงเทคโนโลยีสารสนเทศฯ)

๔.๑.๒ ระบบสารสนเทศ

- ระบบฐานข้อมูลศูนย์ข้อมูลกลางกระทรวงมหาดไทยและจังหวัด
- ระบบศูนย์ข้อมูลกลางจังหวัด
- ระบบบริหารงบประมาณและยุทธศาสตร์จังหวัด
- ระบบบริหารงานบุคลากรจังหวัด
- ระบบการให้บริการสัญญาณอินเตอร์เน็ตไร้สาย
- ระบบบริหารจัดการเว็บไซต์/สารสนเทศที่ให้บริการผ่านทางเว็บไซต์จังหวัด

๔.๑.๓ ระบบโทรศัพท์กระทรวงมหาดไทย

๔.๑.๔ ระบบวีดีโอคอนเฟอร์เรนท์ (Video Conference)

๔.๑.๕ ระบบการรักษาความปลอดภัย

๔.๒ ผู้รับบริการระบบสารสนเทศจังหวัดพัทลุง

๔.๒.๑ ส่วนราชการภายในจังหวัด

๔.๒.๒ ประชาชนทั่วไป/ส่วนราชการภายนอกจังหวัด

๔.๓ การรักษาความปลอดภัยระบบสารสนเทศ

๔.๓.๑ ระบบ Firewall & Antivirus ป้องกันการบุกรุกจากภายนอกและภายในเครือข่าย

๔.๓.๒ การกำหนด username & password ในการกำหนดสิทธิในการเข้าถึงข้อมูล

๔.๓.๓ คู่มือควบคุมการปฏิบัติงาน

๔.๓.๔ การสำรองข้อมูล

๔.๓.๕ การกำหนดผู้เก็บรักษากุญแจห้องสื่อสาร

๔.๓.๖ การบำรุงรักษาอุปกรณ์ตามระยะเวลาที่กำหนด

๕.การวิเคราะห์ความเสี่ยงที่อาจเกิดขึ้น

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของจังหวัดพัทลุง พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๕.๑ ความเสี่ยงจากภายนอก

(๑) ความเสี่ยงด้านเทคนิค ที่อาจเกิดจากการถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี การถูกก่อกวนจาก Hacker หรือถูกเจาะทำลายระบบจาก Cracker เป็นความเสี่ยงที่ทำให้ระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ของหน่วยงานเสียหาย

(๒) ผู้ให้บริการระบบเครือข่ายไม่สามารถให้บริการสัญญาณอินเตอร์เน็ตได้ หรือการเชื่อมโยงเครือข่ายล้มเหลว

(๓) ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง การถูกโจรกรรม เป็นต้น

๕.๒ ความเสี่ยงจากภายใน

(๑) ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

(๒) ความเสี่ยงด้านเทคนิค ที่เกิดจากหน่วยงานขาดการบำรุงรักษาเครื่องมือ อุปกรณ์ตลอดจนระบบเครือข่ายภายในหน่วยงาน เครื่องมือ/อุปกรณ์เกิดการชำรุด หรือมีอายุการใช้งานนานเกินไป ไม่พร้อมต่อการใช้งาน

(๓) ความเสี่ยงด้านผู้ปฏิบัติงาน ไม่มีความรู้ความเข้าใจในการใช้งานระบบเทคโนโลยีสารสนเทศอันอาจทำให้ระบบเสียหาย ชำรุด จนไม่สามารถใช้งานได้

เพื่อให้ระบบเทคโนโลยีสารสนเทศของ จังหวัดพัทลุงมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของจังหวัดพัทลุง

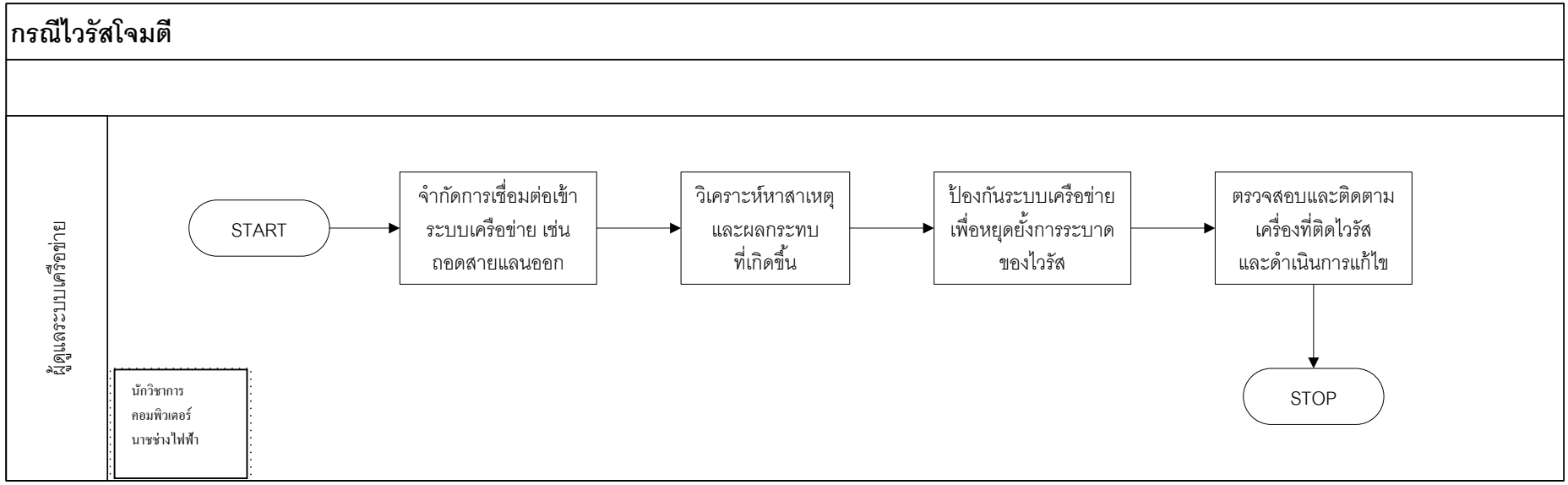
๖. แผนรองรับสถานการณ์ฉุกเฉิน

๖.๑ สถานการณ์ฉุกเฉินที่เกิดจากภายนอกหน่วยงาน

(๑) กรณีไวรัสโจมตี

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่กลุ่มงานข้อมูลสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ระบบสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ สำนักงานจังหวัดจะต้องประกาศให้ทุกหน่วยงานในจังหวัดทราบ

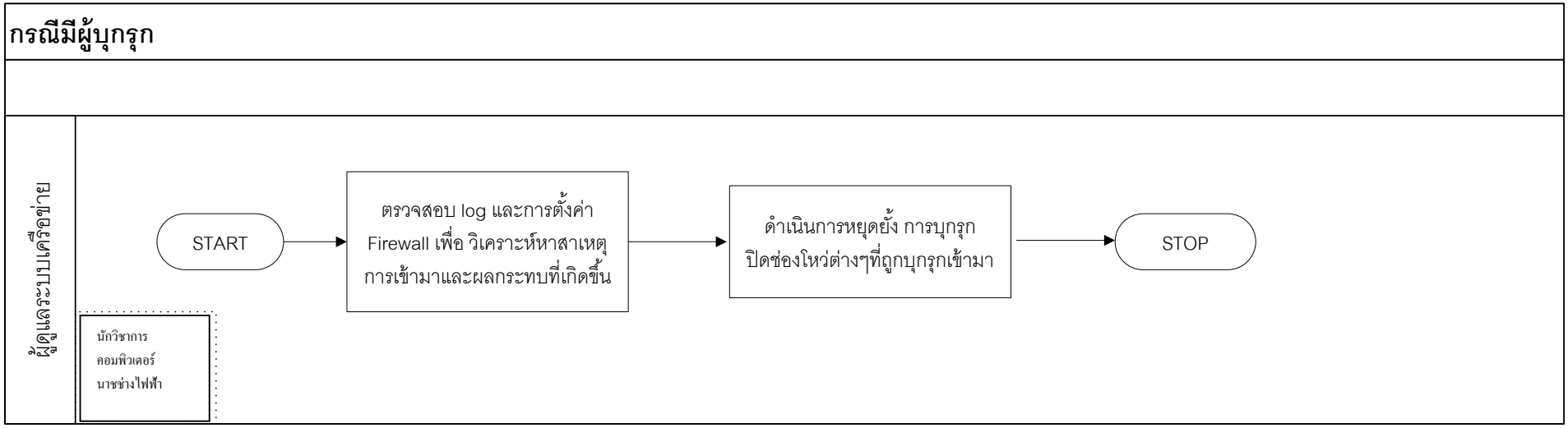
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไวรัสโจมตี



(๒) กรณีมีผู้บุกรุก เช่น Hacker

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

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีมีผู้บุกรุก เช่น Hacker

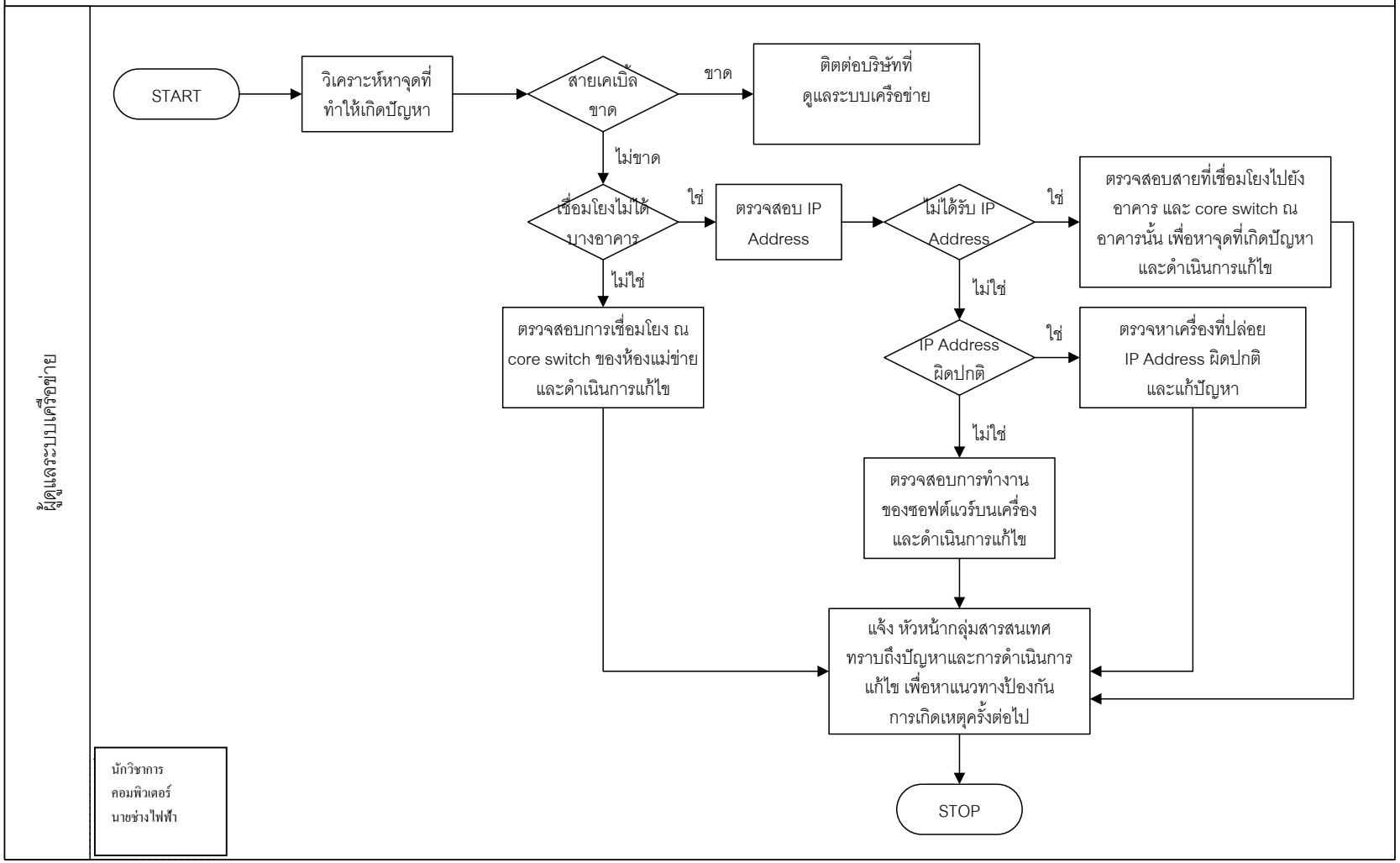


(๓) กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่ายเพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

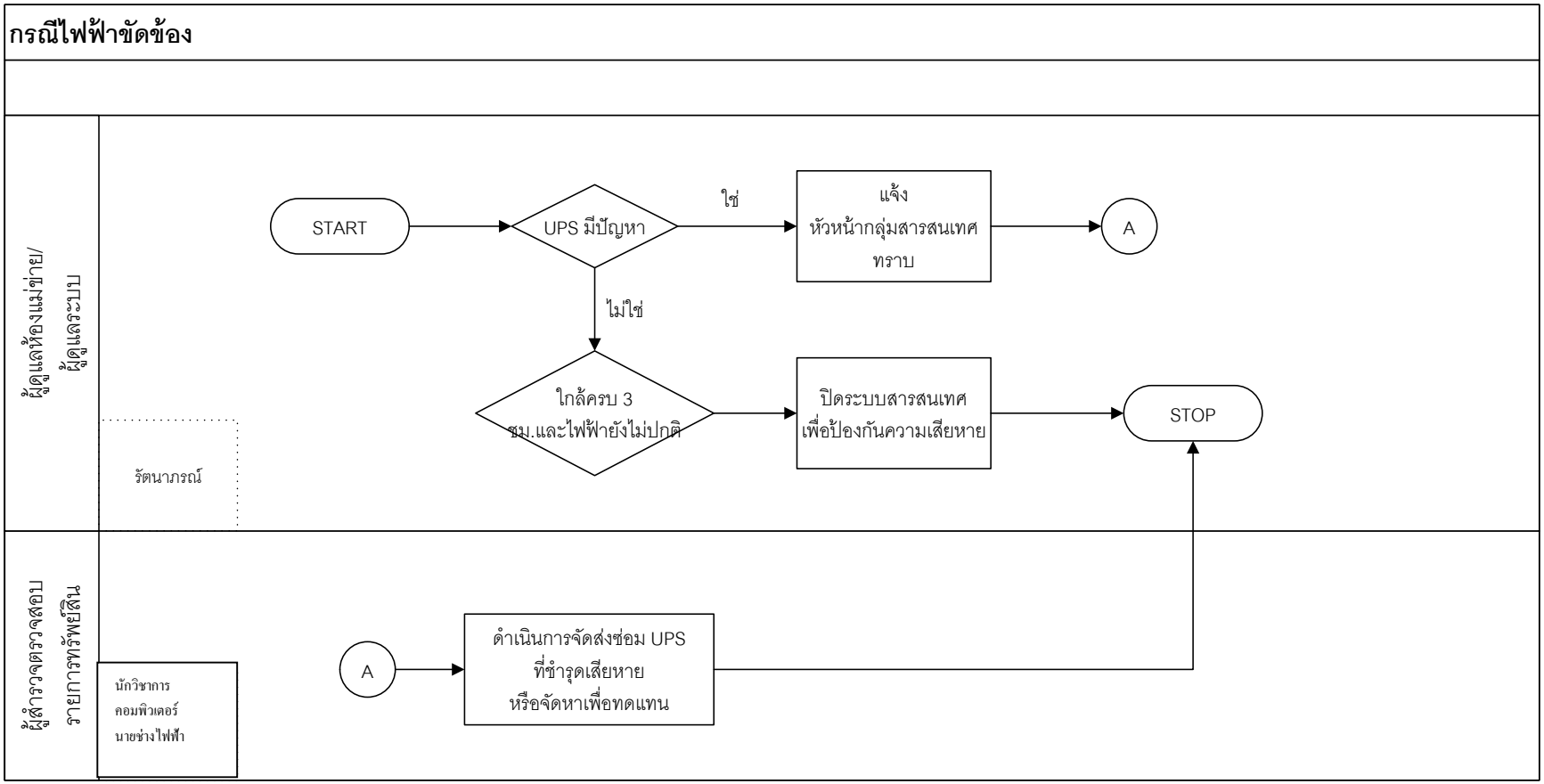
กรณีการเชื่อมโยงเครือข่ายล้มเหลว



(๔) กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมีเครื่องสำรองซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓ ชั่วโมง
- หากใกล้ครบ ๓ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้บังคับบัญชา
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง

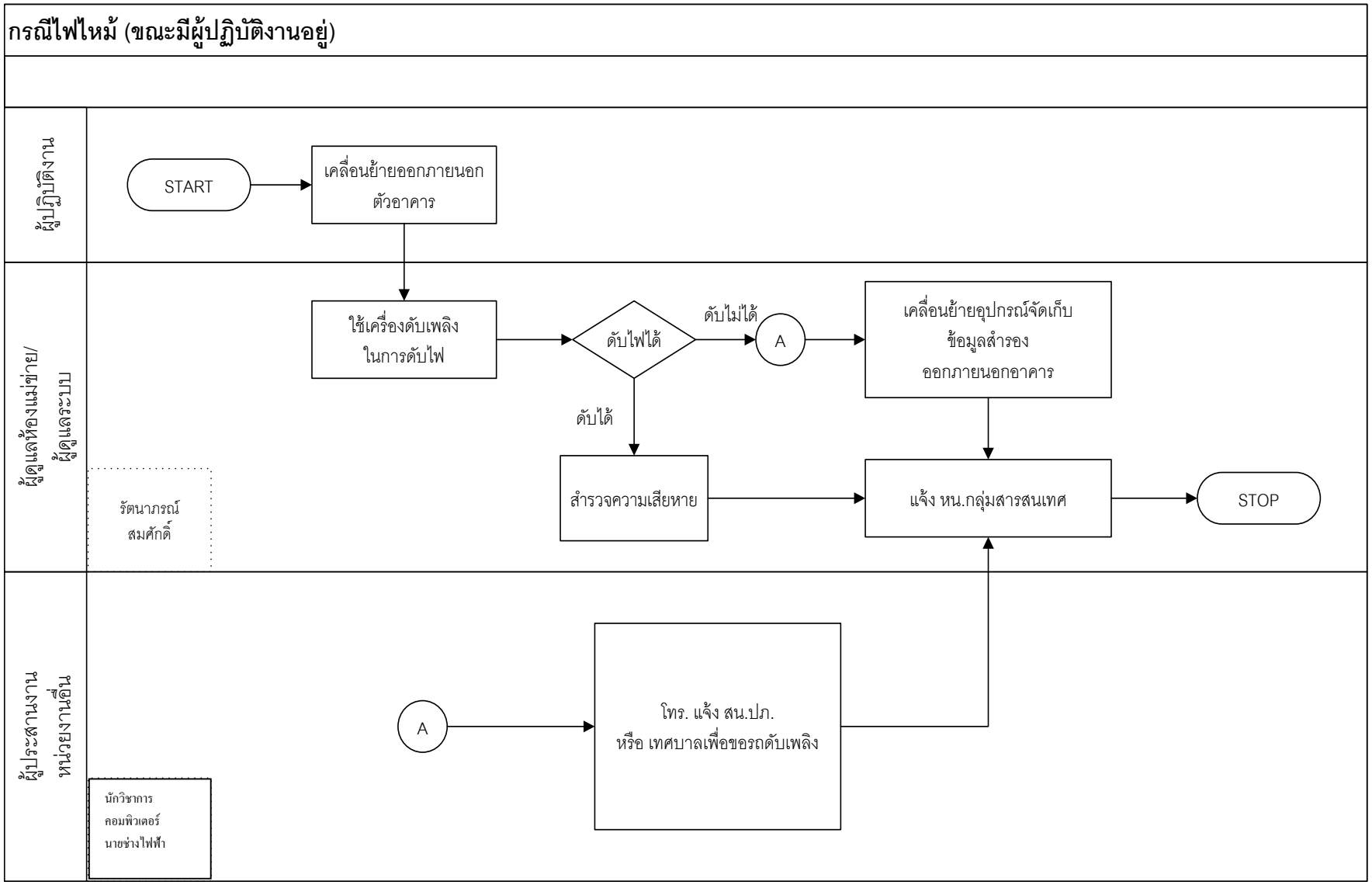


(๕) กรณีไฟไหม้

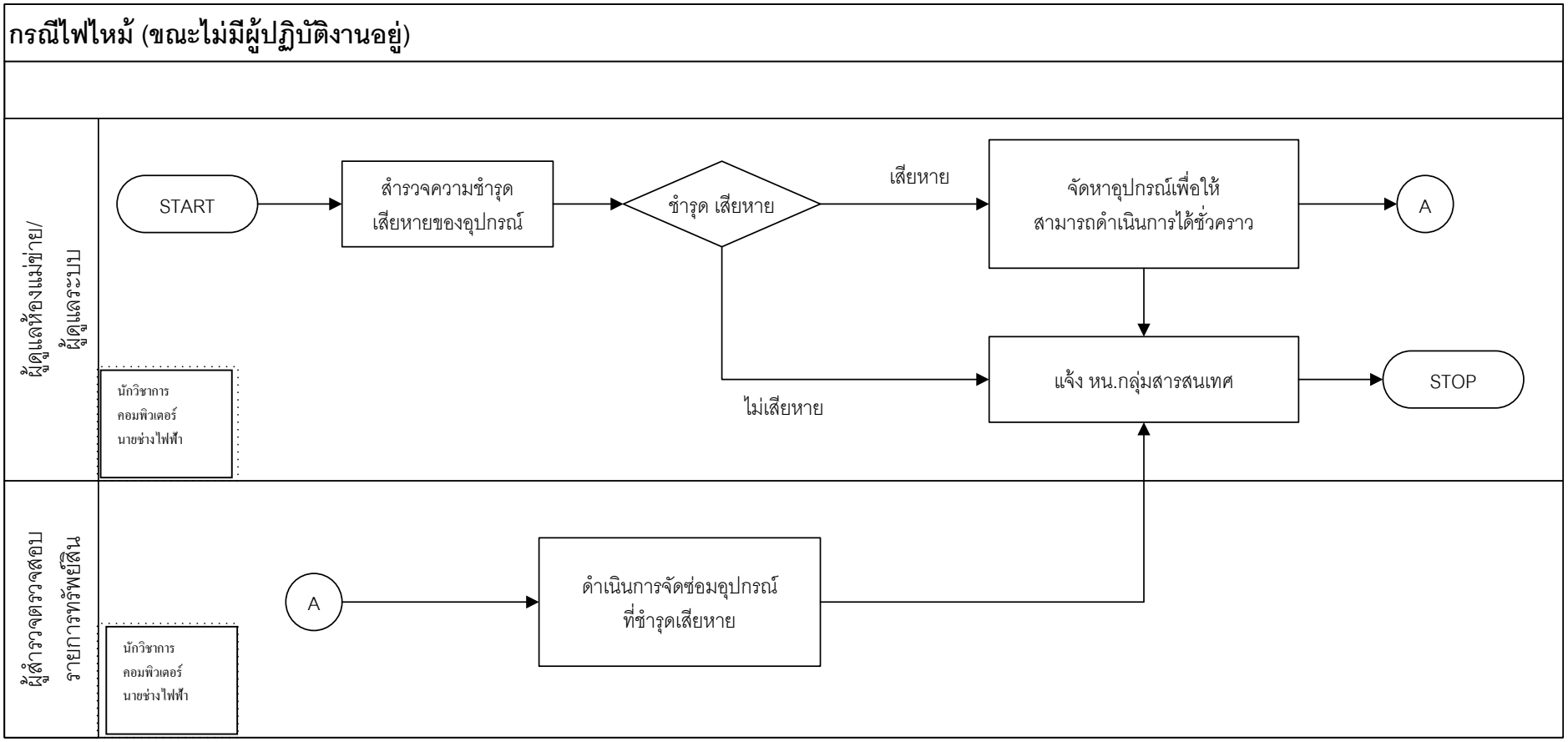
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งศูนย์ปฏิบัติการอาคารและสถานที่และยานพาหนะทันที และโทรแจ้งสำนักงานป้องกันและบรรเทาสาธารณภัย
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๒ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)

กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



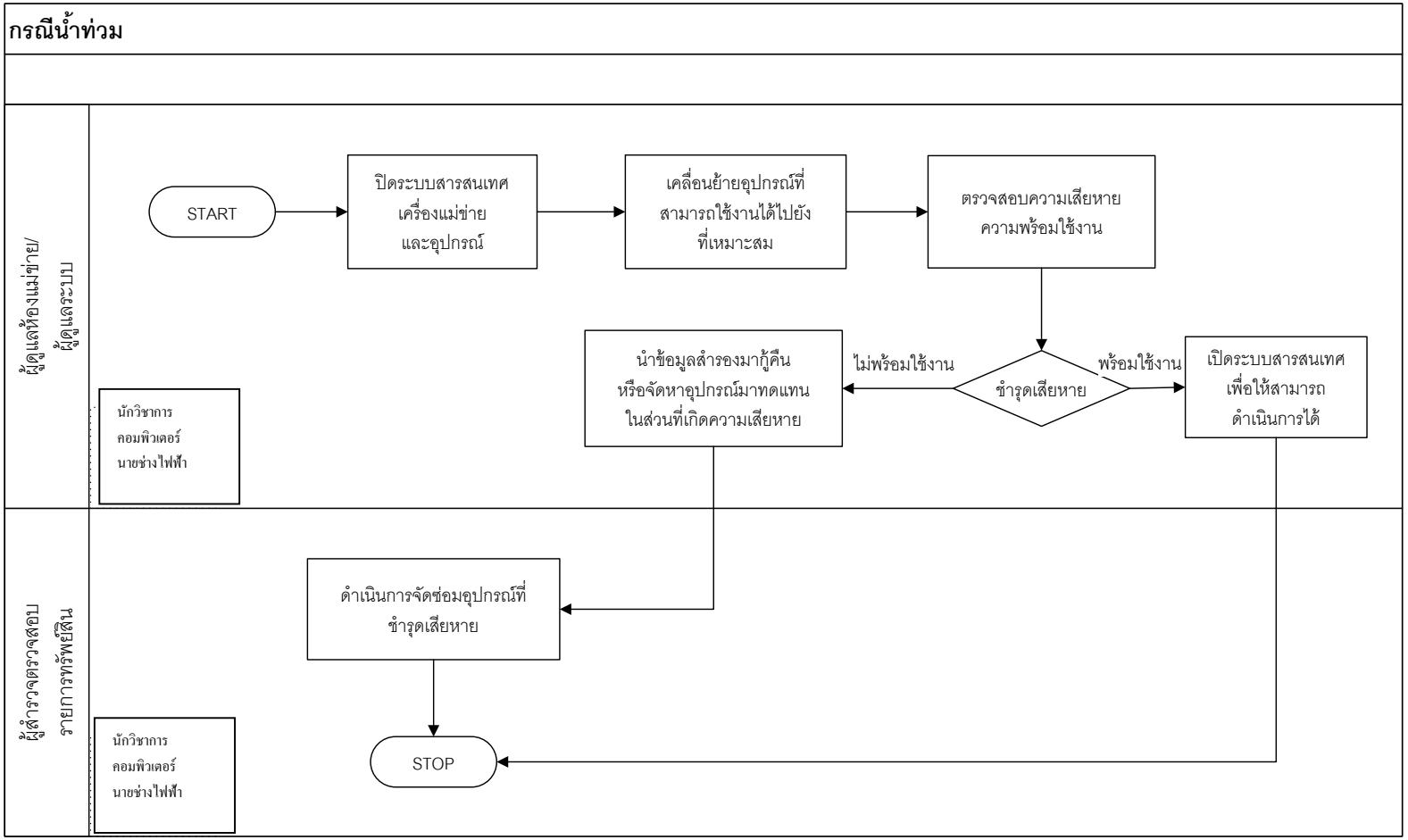
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



(๖) กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ อาคารที่เหมาะสม
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

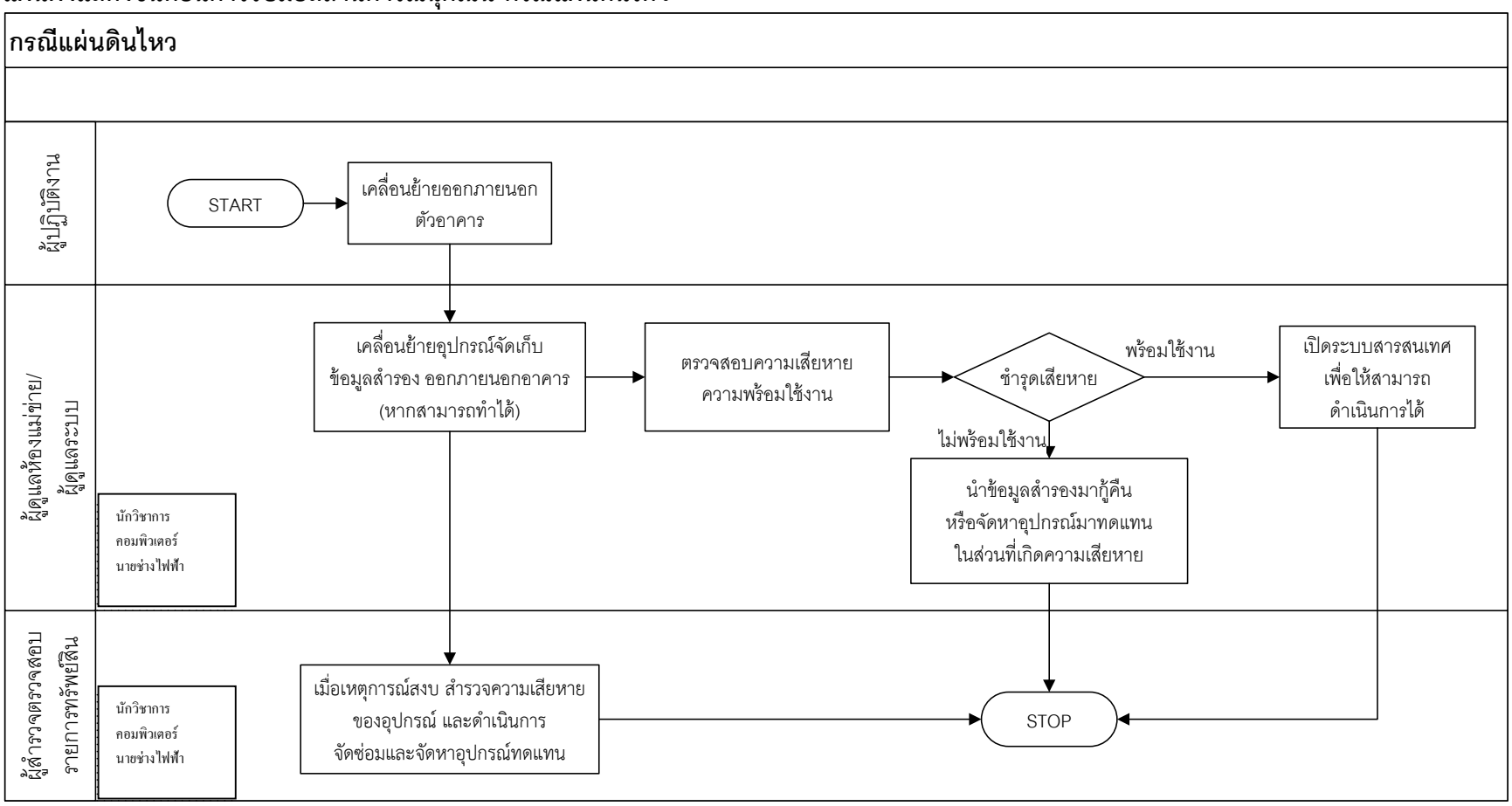
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



(๗) กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

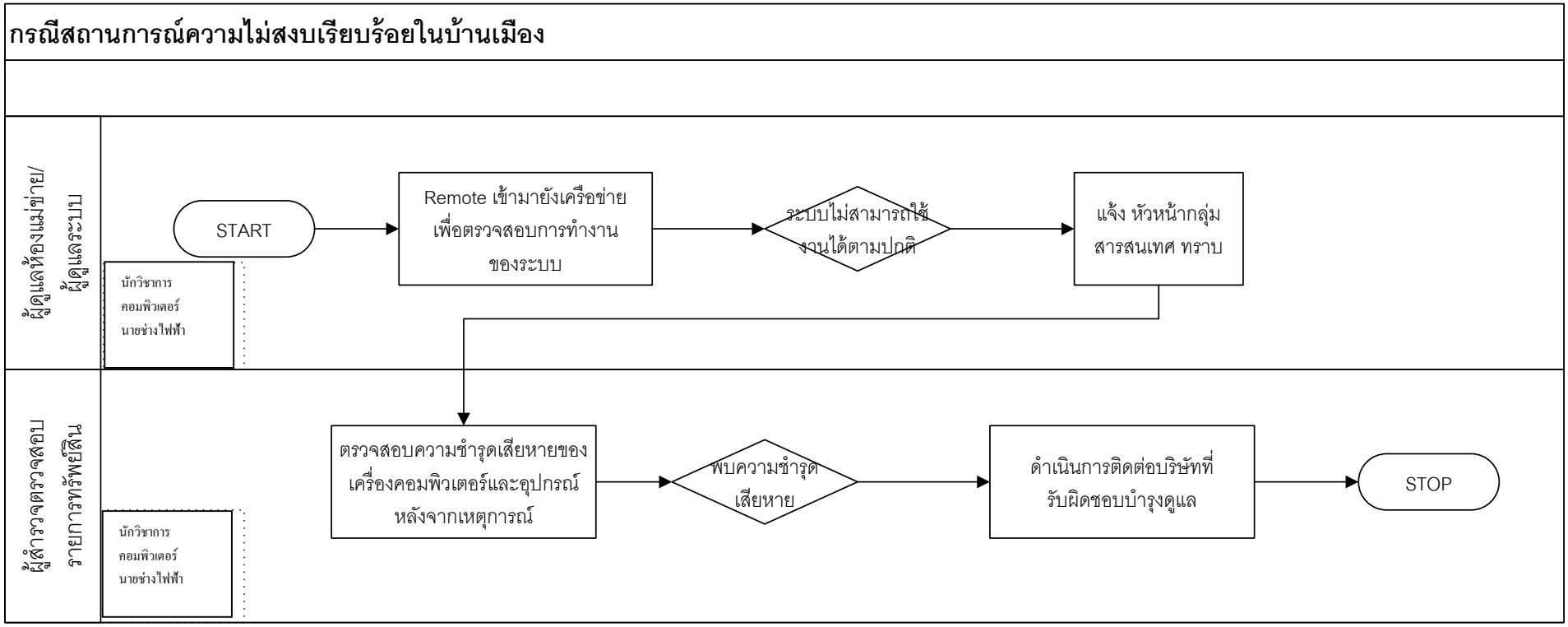
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



(๘) กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้บังคับบัญชาทราบ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

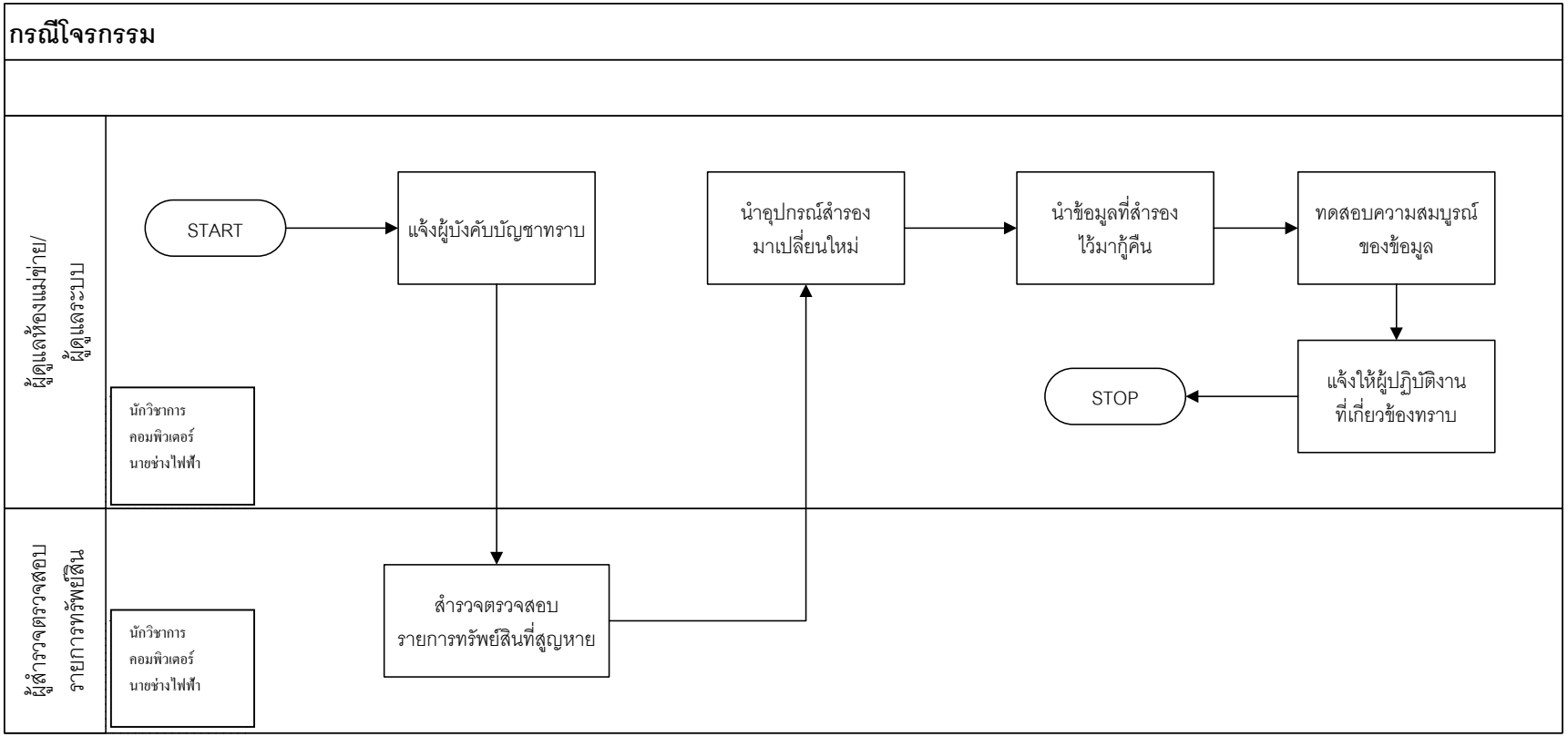
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



(๙) กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

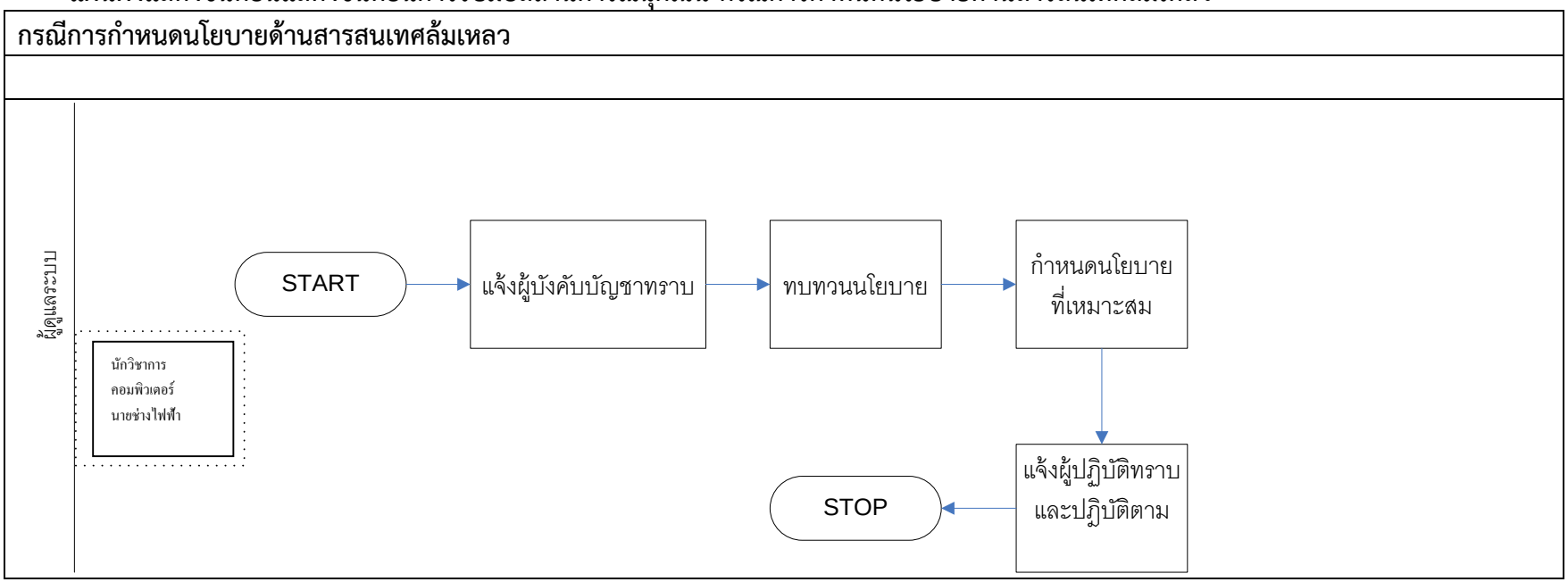


๖.๒ สถานการณ์ฉุกเฉินที่เกิดจากภายในหน่วยงาน

(๑) กรณีการกำหนดนโยบายด้านสารสนเทศล้มเหลว เช่น การวางแผนหรือบริหารจัดการสถานการณ์ที่ไม่คาดคิดผิดพลาด การกำหนดวงเงินงบประมาณในการปรับปรุงหรือพัฒนาระบบไม่เพียงพอ

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบถึงปัญหาและอุปสรรค
- รายงานผู้บริหารเพื่อแก้ไขนโยบายด้านสารสนเทศ

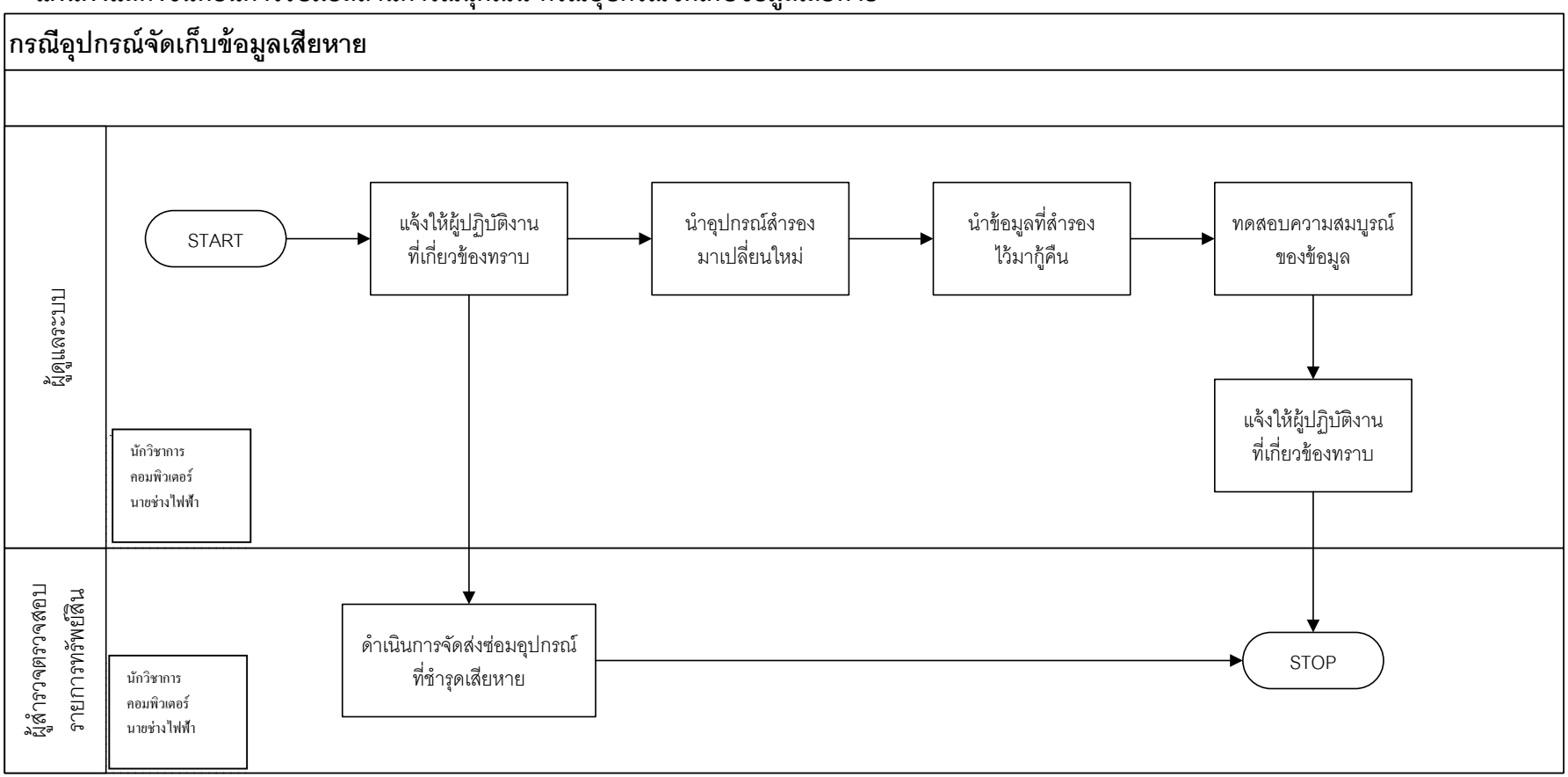
แผนผังแสดงขั้นตอนแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการกำหนดนโยบายด้านสารสนเทศล้มเหลว



(๒) กรณีเครื่องมือ/อุปกรณ์ชำรุดเสียหาย

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

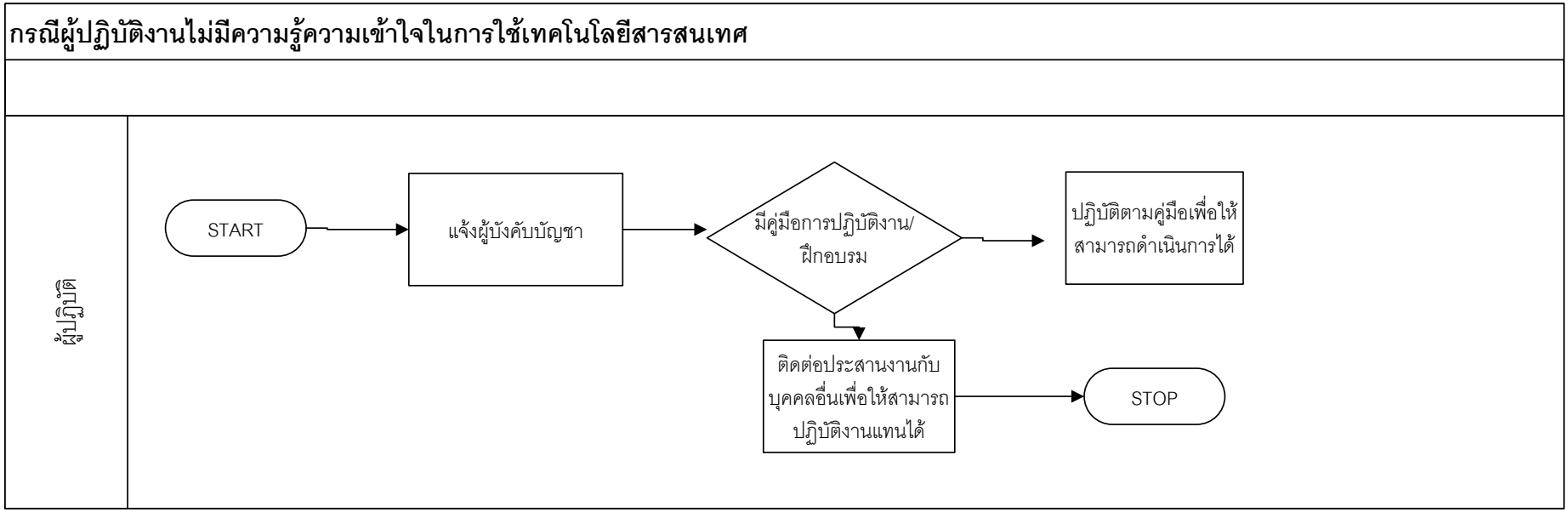
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



(๓) กรณีผู้ปฏิบัติงานไม่มีความรู้ความเข้าใจในการใช้เทคโนโลยีสารสนเทศ

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่มีความรู้ความเข้าใจในการใช้เทคโนโลยีสารสนเทศ



๗. แผนการดำเนินงาน

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๑.การป้องกันไวรัสล้มเหลว/เครื่องคอมพิวเตอร์ถูกไวรัสคอมพิวเตอร์โจมตี	๑. ป้องกันไม่ให้ไวรัสคอมพิวเตอร์โจมตีเครื่องคอมพิวเตอร์ได้	๑. มีการติดตั้งโปรแกรม Nod ๓๒ ป้องกันไวรัสคอมพิวเตอร์ และตั้งเวลาให้ทำการ Update และตรวจสอบไวรัส ภายในเครื่องโดยอัตโนมัติ ๒. มีการกำหนดสิทธิในการเข้าถึงเครื่องคอมพิวเตอร์ ๓.มีการตรวจสอบสถานะ การทำงานของเครื่องทุกสัปดาห์	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น	**๑.** ถอดสาย LAN ๒.กำจัดไวรัสคอมพิวเตอร์ โดยการการสแกน และ Update โปรแกรมสแกนไวรัส ๓.กรณีที่ไวรัสทำลายระบบจนไม่สามารถให้บริการได้ จะทำการล้างระบบเครื่องคอมพิวเตอร์พร้อมติดตั้งระบบปฏิบัติการใหม่และนำข้อมูลที่ Backup ไว้เข้าสู่ระบบ ๔. ทำสำเนาข้อมูลทั้งหมดของระบบไว้ ๓ ชุด แยกเก็บต่างที่ ห้อง POC ๑ ชุด, ห้องสื่อสาร ๑ ชุด, สำนักงานจังหวัด ๑ ชุด ๕. จัดทำคู่มือการติดตั้งระบบใหม่และวิธีการนำเข้าข้อมูล	๑.โปรแกรมป้องกันไวรัสสามารถอัพเดตและตรวจจับไวรัสได้ทุกครั้งที่มีไวรัสมาก่อกวน ๒. สามารถกู้ระบบและข้อมูลภายในเวลา ๑ ชม. หลังจากตรวจพบ	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๒.การป้องกันการบุกรุกจากผู้ประสงค์ร้าย (Hacker)	๑.จัดทำระบบเก็บข้อมูลจราจรคอมพิวเตอร์(log) ตาม พ.ร.บ.กระทำความผิดทางคอมพิวเตอร์ ๒. ติดตั้งระบบ Firewall	๑.ติดตั้งระบบ log file เพื่อตรวจสอบสิทธิการเข้าใช้บริการระบบ ๒.ติดตั้ง Firewall	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น	๑.วิเคราะห์สาเหตุของการเข้ามาในระบบและผลความเสียหาย โดยตรวจสอบจาก log file ๒.ยับการการบุกรุก ปิดช่องโหว่ต่าง ๆ	ตรวจสอบ log file และยับยั้งการบุกรุกได้	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น
๓. การเชื่อมโยงเครือข่ายล้มเหลว	๑.มีระบบเครือข่ายสำรอง	๑. เดินสายสัญญาณระบบเครือข่ายประกอบด้วย เครือข่ายของ สป.มท. และเครือข่าย GIN ๒.ติดตั้งระบบสัญญาณอินเตอร์ไร้สาย	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น	๑.วิเคราะห์หาจุดที่ทำให้เกิดปัญหา ๒.หากสายเคเบิ้ลขาดให้ติดต่อบริษัทซ่อมแซมสายเคเบิ้ล	สามารถใช้ระบบสำรองทดแทนระบบเดิม และแก้ไขระบบเดิมให้แล้วเสร็จภายในเวลาที่เหมาะสม	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๔.กรณีไฟฟ้าขัดข้อง	๑.จัดหาเครื่องสำรองไฟ	๑.ติดตั้งเครื่องสำรองไฟสำหรับเครื่องแม่ข่ายและอุปกรณ์ที่จำเป็นต้องทำงานได้ ๒๔ ชม.	นายสมศักดิ์ รักชูชื่น	๑.ให้เครื่องสำรองไฟทำงานและหากเกิน ๑ ชม.แจ้งผู้บังคับทราบ พร้อมปิดระบบเพื่อป้องกันความเสียหาย ๒.ซ่อมบำรุงเครื่องสำรองไฟอย่างสม่ำเสมอ	สามารถแก้ไขปัญหาที่เกิดขึ้นได้อย่างทันท่วงที	นายสมศักดิ์ รักชูชื่น
๕.กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงาน)	๑.ติดตั้งถังดับเพลิง	๑.ติดตั้งถังดับเพลิงพร้อมซักซ้อมการดับเพลิงและการเคลื่อนย้าย	นายสุพจน์ พรหมมาศ นายสมศักดิ์ รักชูชื่น	๑.เคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกอาคาร พร้อมแจ้งผู้บังคับบัญชาและดับไฟไปพร้อม ๆ กัน	สามารถเคลื่อนย้ายอุปกรณ์ได้ทันท่วงที	นายสุพจน์ พรหมมาศ นายสมศักดิ์ รักชูชื่น

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๖.กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงาน)	๑.สำรองข้อมูลนอกอาคาร	๑.สำรองข้อมูลไว้นอกอาคาร	๑.นายสมศักดิ์ แก้วเกลี้ยง ๒.นายสมศักดิ์ รักชูชื่น	๑.สำรวจความเสียหายของอุปกรณ์ ๒.จัดหาอุปกรณ์เพื่อให้สามารถดำเนินการได้ชั่วคราว ๓.กู้ข้อมูล/นำข้อมูลที่สำรองไว้มาติดตั้งกับระบบชั่วคราว ๔.ซ่อมบำรุงและจัดหาทดแทน	สามารถดำเนินการได้ทันท่วงที	๑.นายสมศักดิ์ แก้วเกลี้ยง นักวิชาการคอมพิวเตอร์ ๒.นายสมศักดิ์
๗.กรณีน้ำท่วม	๑.ติดตามเฝ้าระวังสถานการณ์น้ำอย่างต่อเนื่องเพื่อเตรียมความพร้อมในการเคลื่อนย้ายอุปกรณ์	๑.จัดเจ้าหน้าที่เฝ้าระวังสถานการณ์อย่างต่อเนื่อง	นายสุพจน์ พรหมมาศ นายสมศักดิ์ รักชูชื่น	๑.ปิดระบบและเคลื่อนย้ายอุปกรณ์ไปยังอาคารที่เหมาะสม ๒.สำรวจความเสียหายและซ่อมแซมอุปกรณ์ที่ชำรุด	สามารถเคลื่อนย้ายอุปกรณ์ได้ทันท่วงที	นายสุพจน์ พรหมมาศ นายสมศักดิ์รักชูชื่น

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๘.กรณีแผ่นดินไหว	๑.รีบเคลื่อนย้ายอุปกรณ์ออกนอกอาคาร	๑.กำหนดลำดับความสำคัญของอุปกรณ์ในการเคลื่อนย้าย	นายสุพจน์ พรหมมาศ	๑.เคลื่อนย้ายอุปกรณ์พร้อมข้อมูลสำรองออกนอกอาคาร ๒.เมื่อเหตุการณ์สงบตรวจสอบความเสียหาย ๓.ดำเนินการแก้ไข	สามารถย้ายอุปกรณ์ที่จำเป็นได้ทันท่วงที	นายสมศักดิ์ รักชูชื่น
๙.กรณีเกิดความไม่สงบเรียบร้อยในบ้านเมือง	๑. Remote เข้ามาตรวจสอบการทำงานของระบบ	๑.มอบหมายผู้ดูแลระบบดำเนินการ Remote	นายสมศักดิ์ แก้วเกลี้ยง	๑.กรณีไม่สามารถเข้าไปปฏิบัติหน้าที่ได้ให้Remoteเข้ามาตรวจสอบการทำงานของระบบ ๒.กรณีเหตุการณ์สงบแล้วให้สำรวจความเสียหายแจ้งผู้บังคับบัญชาทราบ	สามารถรักษาอุปกรณ์และข้อมูลต่าง ๆ ไว้ได้มากกว่าร้อยละ ๘๐	นายสมศักดิ์ แก้วเกลี้ยง
๑๐.กรณีโจรกรรม	๑.กำหนดสิทธิในการเข้าห้องสื่อสาร	๑.มอบหมายเจ้าหน้าที่ดูแลรักษาห้องสื่อสาร	นายสมศักดิ์ รักชูชื่น	๑.แจ้งผู้บังคับบัญชาทราบ ๒.ตรวจสอบทรัพย์สินและจัดหาทดแทน	สามารถจัดหาอุปกรณ์ทดแทนได้ทันเวลา	นายสมศักดิ์ รักชูชื่น

ภัยพิบัติ	แผนการดำเนินงาน					
	แผนการป้องกัน			แผนการแก้ไข		
	แผน/การควบคุม	ผลการดำเนินงาน	ผู้รับผิดชอบ	แผน/การแก้ไข	เป้าหมาย	ผู้รับผิดชอบ
๑๑.กรณีการกำหนดนโยบายด้านสารสนเทศล้มเหลว	๑.ทบทวนนโยบายด้านสารสนเทศอย่างต่อเนื่อง	ปรับปรุงแผนบริหารความเสี่ยงอย่างต่อเนื่อง	นายสมศักดิ์ แก้วเกลี้ยง	๑.แจ้งผู้บังคับบัญชาทราบ ๒.กำหนดนโยบายด้านสารสนเทศที่เหมาะสม	๑.มีนโยบายด้านสารสนเทศที่เหมาะสมและทันสมัย	นายสมศักดิ์ แก้วเกลี้ยง
๑๒.กรณีอุปกรณ์ในหน่วยงานขาดการบำรุงรักษา/ชำรุด	๑.มีการตรวจสอบอุปกรณ์และซ่อมบำรุงอุปกรณ์อย่างต่อเนื่อง ๒.จัดวงเงินงบประมาณในการซ่อมบำรุงอุปกรณ์หรือซื้อทดแทนของเดิมที่ชำรุด	๑.มีการตรวจสอบอุปกรณ์เป็นประจำทุกสัปดาห์ ๒.ซ่อมบำรุงอุปกรณ์อย่างสม่ำเสมอ	นายสมศักดิ์ รักชูชื่น นายสมศักดิ์ แก้วเกลี้ยนง	๑.แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ ๒. รีบดำเนินการจัดหาอุปกรณ์ ๓.จัดวงเงินงบประมาณอย่างเหมาะสม	๑.อุปกรณ์พร้อมใช้งานตลอดเวลา	นายสมศักดิ์ รักชูชื่น นายสมศักดิ์ แก้วเกลี้ยง
๑๓.เจ้าหน้าที่ขาดความรู้ในการใช้งานระบบสารสนเทศ	๑.จัดอบรมให้ความรู้แก่บุคลกรในหน่วยงาน ๒.จัดทำคู่มือการใช้งานระบบสารสนเทศ	๑.มีการจัดอบรมความรู้ด้านสารสนเทศ ๒.มีการถ่ายทอดองค์ความรู้	นายสมศักดิ์ แก้วเกลี้ยง	๑.รายงานผู้บังคับบัญชาทราบ ๒.จัดทำคู่มือการใช้งานระบบสารสนเทศ	๑.เจ้าหน้าที่มีความรู้ในการใช้งานระบบสามารถปฏิบัติงานได้อย่างมีประสิทธิภาพ	นายสมศักดิ์ แก้วเกลี้ยง

เจ้าหน้าที่/หน่วยงานที่เกี่ยวข้อง

ที่	เจ้าหน้าที่ผู้รับผิดชอบตามแผนบริหารความเสี่ยง	ความรับผิดขอบ	เบอร์ติดต่อ
บุคลากรปฏิบัติงานภายในจังหวัด			
๑	นายกู้เกียรติวงศ์กระพันธุ์ ผู้ว่าราชการจังหวัดพัทลุง	สนับสนุนและมอบนโยบายในการการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	ที่ทำงาน ๐-๗๔๖๑-๓๐๑๒ มือถือ ๐๘-๙๒๐๓๐๔๖๗
๒	นายฉัตรชัย อุสาหะ รองผู้ว่าราชการจังหวัดพัทลุง	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงประจำจังหวัด (CIO)	ที่ทำงาน ๐-๗๔๖๑-๑๕๙๓ มือถือ ๐๘-๙๒๐๓-๑๗๔๖
๓	นายอภิชาติ สาราบรรณ์ หัวหน้าสำนักงานจังหวัดพัทลุง	สนับสนุนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามแผนบริหารความเสี่ยง	ที่ทำงาน ๐-๗๔๖๑-๔๐๖๒ มือถือ ๐๘-๙๒๐๓๔๒๔๖
๔	นางณัฏฐ์วรัตถ์ จิณรัฐ	สนับสนุนการปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามแผนบริหารความเสี่ยง	ที่ทำงาน ๐-๗๔๖๑-๓๔๐๙ มือถือ ๐๘-๙๒๐๓๔๒๔๙
๕	นายสมศักดิ์ แก้วเกลี้ยง นักวิชาการคอมพิวเตอร์ชำนาญการ	๑.การรักษาความปลอดภัยการใช้งานเทคโนโลยีสารสนเทศ (Security) ๒.การสนับสนุน ให้ความรู้และแก้ไขปัญหาด้าน Software ๓.การปฏิบัติงานด้านระบบเครือข่ายอินเตอร์เน็ต ๔.การปฏิบัติงานด้านการพัฒนาระบบ (Software Developer) ๕.ปฏิบัติงานด้านการจัดทำแผนปฏิบัติงานด้านสารสนเทศและการประสานงานทั่วไป	ที่ทำงาน ๐-๗๔๖๑-๓๔๐๙ มือถือ ๐๘-๑๕๙๓-๙๑๓๕
๖	นายสมศักดิ์ รักชูชื่น นายช่างไฟฟ้าปฏิบัติการ	๑.การปฏิบัติงานด้านระบบเครือข่ายอินเตอร์เน็ต ๒.ปฏิบัติงานด้านการรักษาความมั่นคง ปลอดภัยของระบบ ๓.ปฏิบัติงานด้านระบบสื่อสาร	ที่ทำงาน ๐-๗๔๖๑๓๔๐๙ มือถือ ๐๘-๙๐๓๓-๒๕๐๑

		๔. การปฏิบัติงานด้านการดูแลและแก้ไขปัญหาการใช้งานเบื้องต้นในระบบสารสนเทศและการประสานงานตามภารกิจทั่วไป	
หน่วยงานประสานที่เกี่ยวข้อง			
๑	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงมหาดไทย		
	๑.๑ กลุ่มพัฒนาและมาตรฐานระบบสารสนเทศและการสื่อสาร	Security ระบบความปลอดภัยของอุปกรณ์คอมพิวเตอร์	โทรศัพท์ ๐-๒๒๘๑-๑๕๖ สายด่วน ๕๑๔๒๙
	๑.๒ กลุ่มพัฒนาทรัพยากรบุคคลด้านเทคโนโลยีสารสนเทศและการสื่อสาร	การฝึกอบรมบุคลากร	โทรศัพท์ ๐-๒๒๘๑-๑๕๖๔ สายด่วน ๕๑๔๒๘
	๑.๓ กลุ่มพัฒนาเทคโนโลยีสารสนเทศ		โทรศัพท์ ๐-๒๒๒๖-๐๕๐๖ สายด่วน ๕๐๔๗๖
	๑.๔ กลุ่มพัฒนาระบบงานสารสนเทศ	Software Website ระบบภายในต่าง ๆ	โทรศัพท์ ๐๒-๒๖๙๗-๙๙๐๙ สายด่วน ๕๑๑๓๙
	๑.๕ ส่วนติดตามและประเมินผลด้านสารสนเทศและการสื่อสาร		โทรศัพท์ ๐-๒๖๙๗-๙๙๒๔ สายด่วน ๕๑๑๒๔
	๑.๖ ส่วนโครงสร้างพื้นฐานด้านสารสนเทศและการสื่อสาร	Internet Network	โทรศัพท์ ๐-๒๒๘๒-๖๕๘๒ สายด่วน ๕๑๔๕๐
	๑.๗ ส่วนเทคโนโลยีการสื่อสาร	VCS	โทรศัพท์ ๐-๒๒๘๒-๖๕๘๕
๒	บริษัทซิตี้ วาไรตี้ คอร์เปอเรชั่น จำกัด	Hosting / Serserver	โทรศัพท์ ๐-๗๔๕๕-๙๓๐๔ มือถือ ๐๘-๖๔๗๐๒๔๕
๓	บริษัท TOT จำกัด มหาชน	ระบบเครือข่าย GIN	โทรศัพท์ ๐-๗๔๘๒-๙๙๙๙ มือถือ ๐๘-๑๔๑๘-๐๐๓๐
๔	การไฟฟ้าส่วนภูมิภาคจังหวัดพัทลุง	ระบบไฟฟ้าศาลากลางจังหวัด	โทรศัพท์ ๐-๑๔๖๗-๑๕๘๗ มือถือ ๐๘-๐๕๔๓-๑๑๑๖
๕	การประปาส่วนภูมิภาค สาขาพัทลุง	ระบบประปาศาลากลางจังหวัด	โทรศัพท์ ๐-๗๔๖๑-๓๑๖๗ มือถือ ๘-๑๕๔๐-๖๑๙๑

๘. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑ ผู้ว่าราชการจังหวัดพัทลุง

๑.๒ รองผู้ว่าราชการจังหวัดพัทลุง ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ประจำจังหวัด

๑.๓ หัวหน้าสำนักงานจังหวัดพัทลุง

๑.๔ ผู้อำนวยการกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัด

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

๒.๑. นักวิชาการคอมพิวเตอร์

๒.๒. นายช่างไฟฟ้า

๓. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๓.๑ นักวิชาการคอมพิวเตอร์

ทั้งนี้ ให้ผู้อำนวยการกลุ่มงานยุทธศาสตร์และข้อมูลเพื่อการพัฒนาจังหวัดเป็นผู้บัญชาการเบื้องต้นในการควบคุมดูแลด้านระบบข้อมูลสารสนเทศของส่วนราชการ/หน่วยงานประจำจังหวัดพัทลุงและประสานงานให้เป็นไปตามแผนฯ หากมีปัญหาอุปสรรคหรือข้อขัดข้องใดเกิดขึ้นให้รายงานผู้บังคับบัญชาได้ทราบตามลำดับชั้นต่อไป

(ลงชื่อ) ผู้เสนอแผน

(นายอภิชาติ สาราบรรณ์)
หัวหน้าสำนักงานจังหวัดพัทลุง

(ลงชื่อ) ผู้เห็นชอบแผน

(นายฉัตรชัย อุสาหะ)
รองผู้ว่าราชการจังหวัดพัทลุง

(ลงชื่อ) ผู้อนุมัติแผน

(นายกู้เกียรติ วงศ์กระพันธุ์)
ผู้ว่าราชการจังหวัดพัทลุง