แผนผัง/ขั้นตอน
การรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)

กลุ่มงานคอมพิวเตอร์และการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท.

แผนผัง/ขั้นตอน
การรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)

กลุ่มงานคอมพิวเตอร์และการสื่อสาร

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท.

สารบัญ

หน้า

๑. บทนำ ๑
๒. วัตถุประสงค์ ๑
๓. การวิเคราะห์ความเสี่ยง ๒
๔. แผนรองรับสถานการณ์ฉุกเฉิน ๓
๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค
๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว ๓
๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว ๔
๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว ๕
๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่ายเสียหาย ๖
๔.๑.๕ กรณีไฟฟ้าขัดข้อง ๗
๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ
๔.๒.๑ กรณีไฟไหม้ ๘
๔.๒.๒ กรณีแผ่นดินไหว/อาคารถล่ม ๑๐
๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรง
๔.๓.๑ กรณีเกิดโรคระบาดร้ายแรงเป็นเหตุให้ไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งได้ ๑๑
๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง
๔.๔.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง ๑๓
๔.๕ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล
๔.๕.๑ กรณีโจรกรรม ๑๕
๔.๕.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้ ๑๖
๔.๕.๓ กรณีหน่วยงานนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารร้องขอการใช้งาน ผ่านระบบเครือข่ายเสมือน (Virtual Private Network : VPN) ๑๗
๔.๕.๔ กรณีหน่วยงานนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารร้องขอการแก้ไข ปัญหาการใช้งานระบบสารบรรณอิเล็กทรอนิกส์ ๑๘
๕. การกำหนดผู้รับผิดชอบ ๑๙

แผนผัง/ขั้นตอนการรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

๑. บทนำ

ปัจจุบันหน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศ เพื่อความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผน พัฒนา และบริหารจัดการองค์กร รวมถึงการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และการให้บริการเจ้าหน้าที่รวมไปถึงประชาชน ให้สะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี โดยไวรัสคอมพิวเตอร์ บุคลากรรวมถึงผู้มาติดต่อ ปัญหาระบบไฟฟ้า อัคคีภัย หรือปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงาน เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

๓. การวิเคราะห์ความเสี่ยง

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. มีการนำเทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาใช้ในการปฏิบัติงานให้เกิดประโยชน์สูงสุด

การวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. พบว่าประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง การถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ไฟฟ้าขัดข้อง เป็นต้น

๒. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงาน ป.ป.ท. ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ สำนักงาน ป.ป.ท. มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๔. แผนรองรับสถานการณ์ฉุกเฉิน

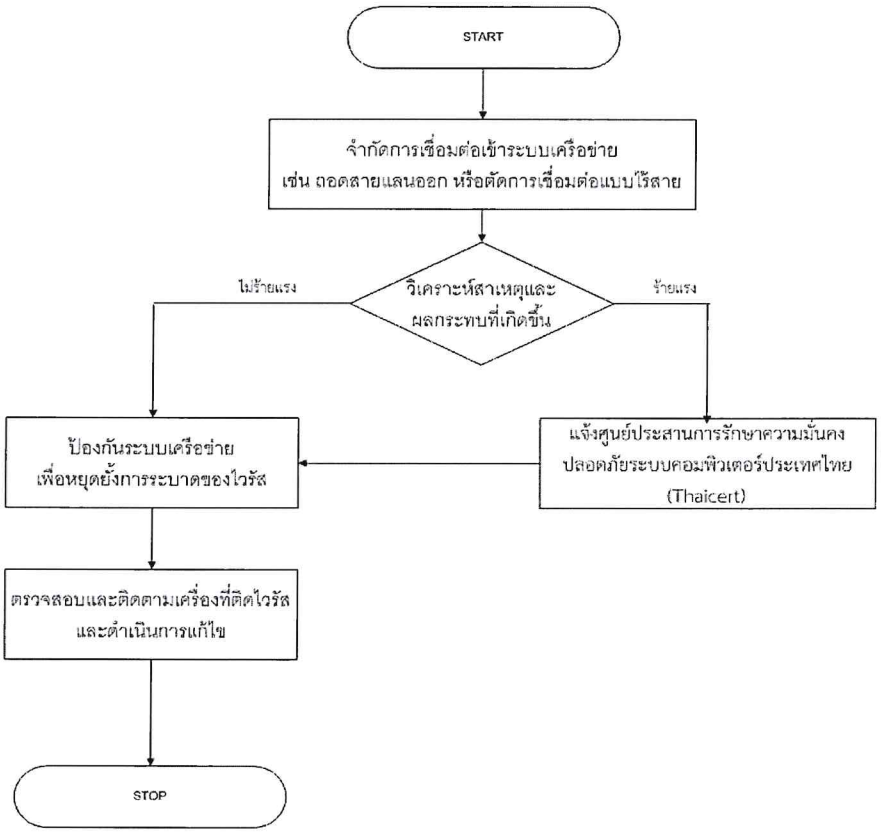
๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้มีการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
  - กรณีไม่ร้ายแรง :
    - ➢ ดำเนินการแก้ไขเพื่อป้องกันการแพร่กระจายของไวรัสคอมพิวเตอร์
  - กรณีร้ายแรง :
    - ➢ แจ้งศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งประเทศไทย (Thaicert)
    - ➢ ดำเนินการแก้ไขเพื่อป้องกันการแพร่กระจายของไวรัสคอมพิวเตอร์ตามคำแนะนำของ (Thaicert)
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสเพื่อป้องกันไม่ให้เกิดปัญหาอีก
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่กลุ่มงานคอมพิวเตอร์และการสื่อสาร หรือกรณีมีเหตุอันทำให้งานเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ กลุ่มงานคอมพิวเตอร์และการสื่อสารจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว

ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร

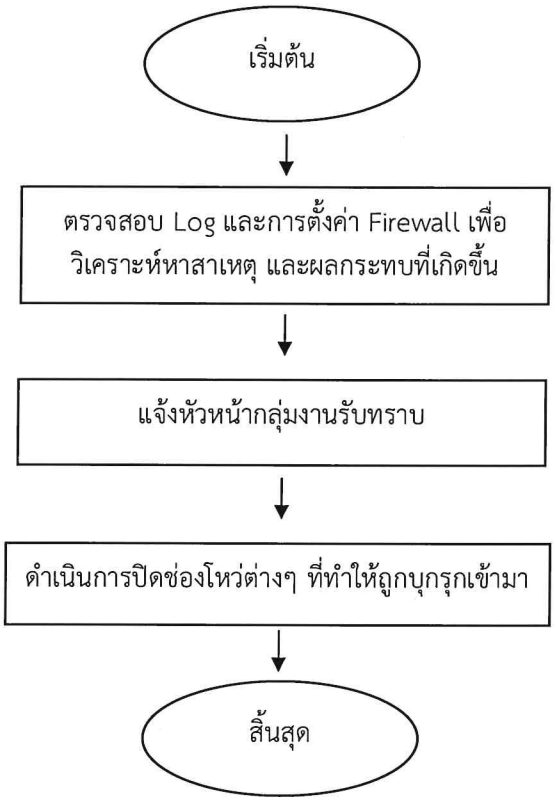


๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งหัวหน้ากลุ่มงานรับทราบ
- ดำเนินการ ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว

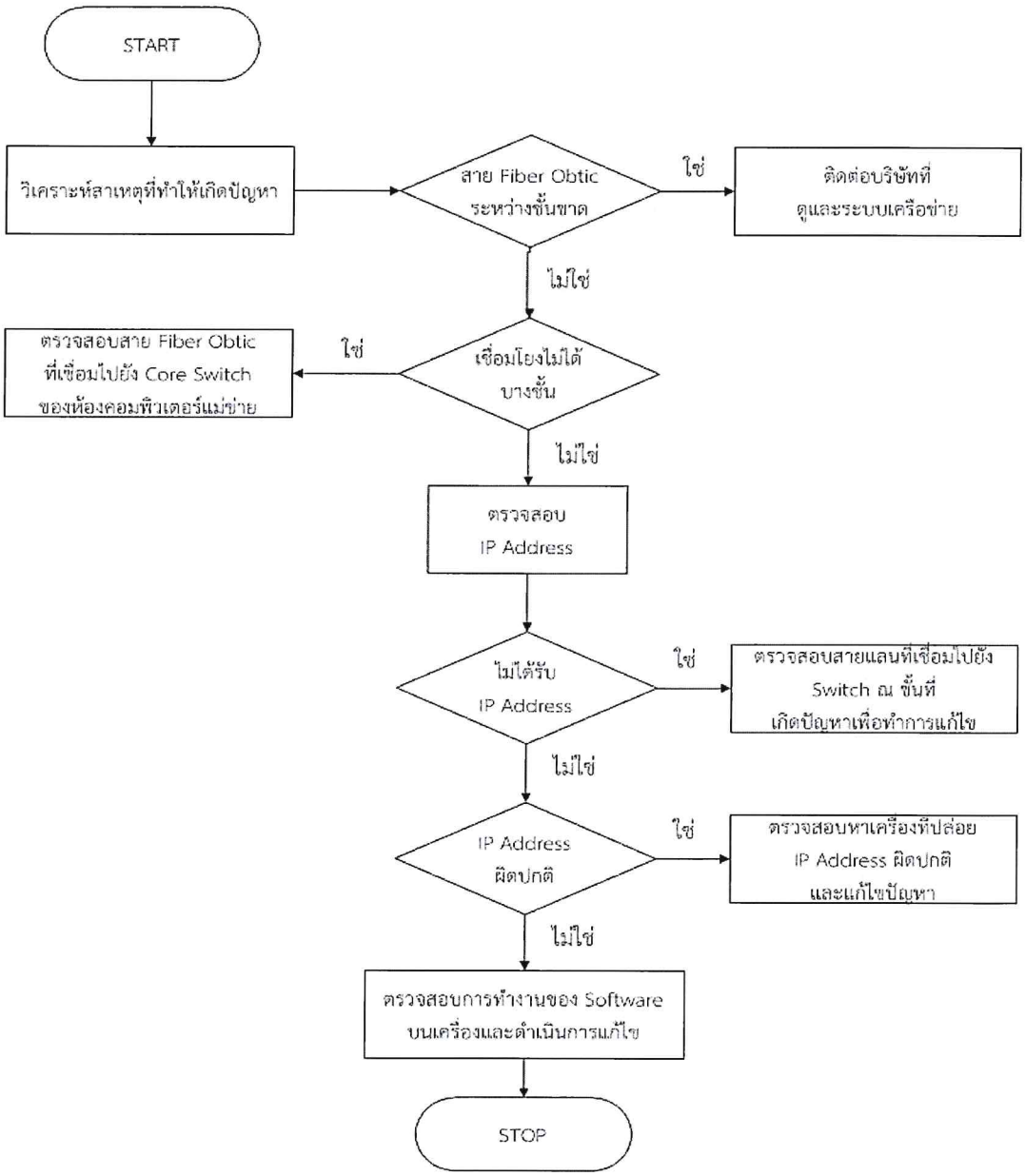
ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร



๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาด ให้รีบแจ้งผู้บริหารพร้อมติดต่อบริษัทฯ ภายนอก เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางชั้น ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังชั้นที่เกิดปัญหาและ Switch ที่ติดตั้งอยู่ชั้นนั้นๆ

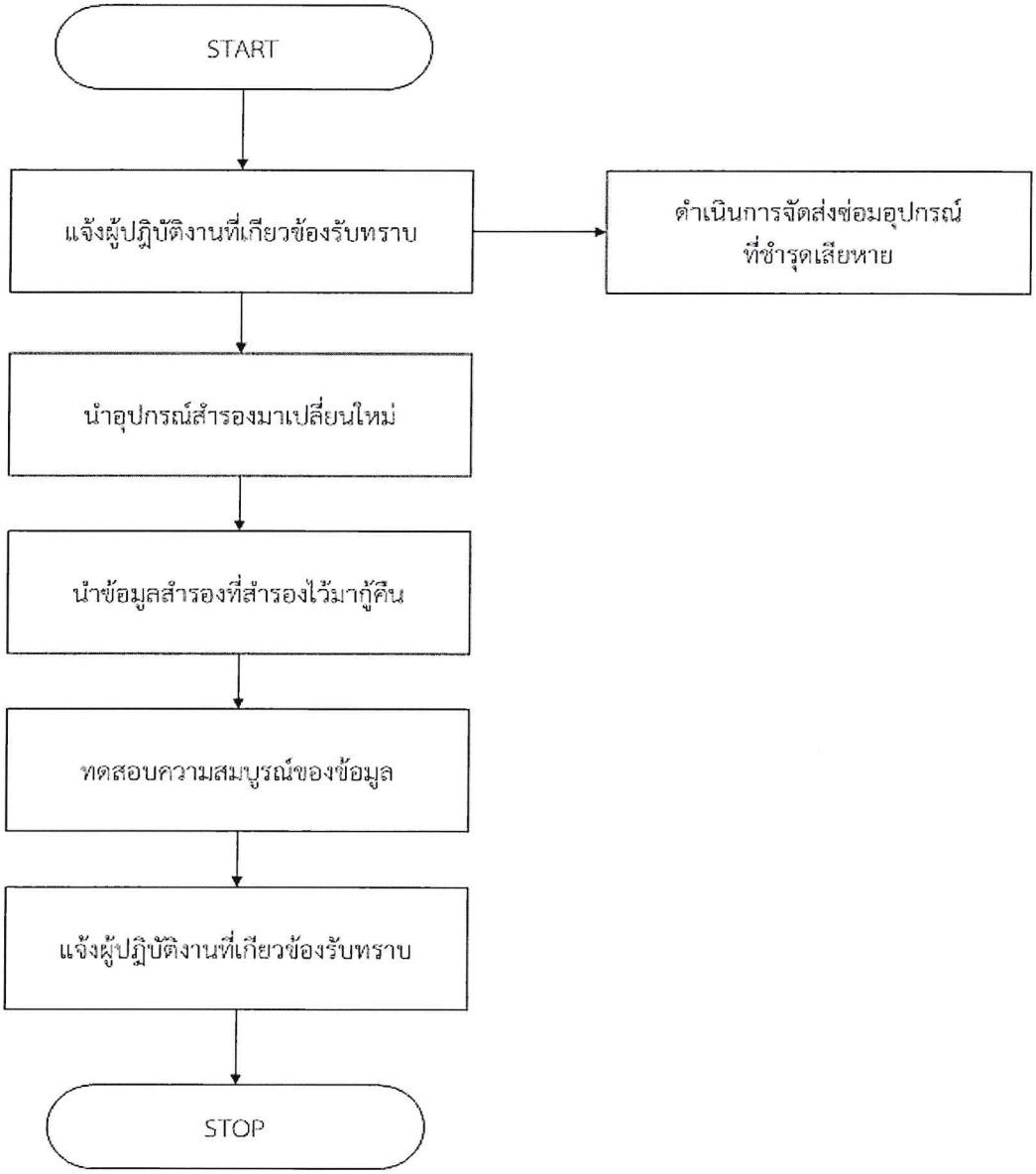
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว
ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร



๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย (Server) เสียหาย

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์มาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

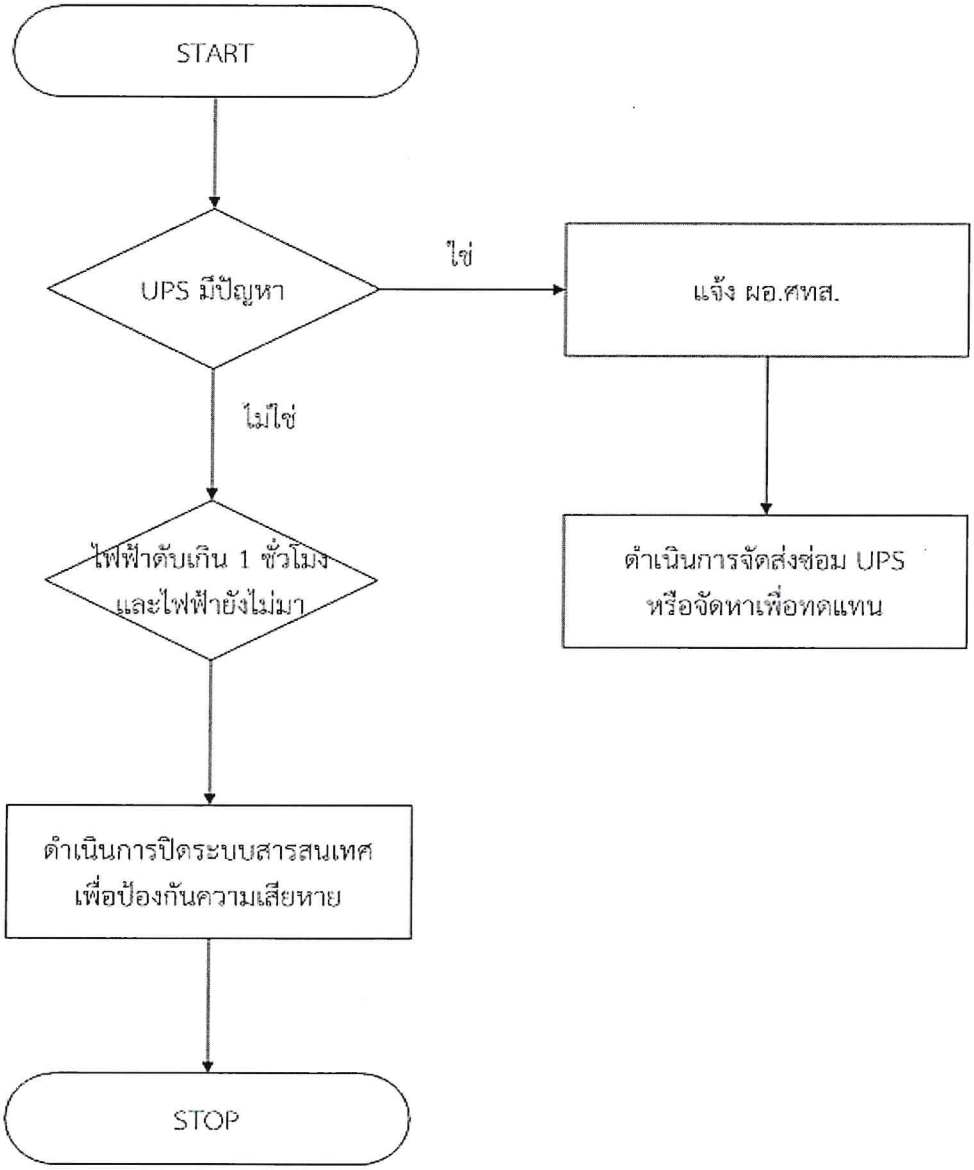
แผนแผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน
กรณีอุปกรณ์จัดเก็บข้อมูลในเครื่องคอมพิวเตอร์แม่ข่าย (Server) เสียหาย
ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร
และกลุ่มงานบริหารเทคโนโลยีสารสนเทศ



๔.๑.๕ กรณีไฟฟ้าขัดข้อง

- ระบบสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ ๑ ชั่วโมง
- หากใกล้ครบ ๑ ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้างานเทคโนโลยีสารสนเทศ
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว
ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร

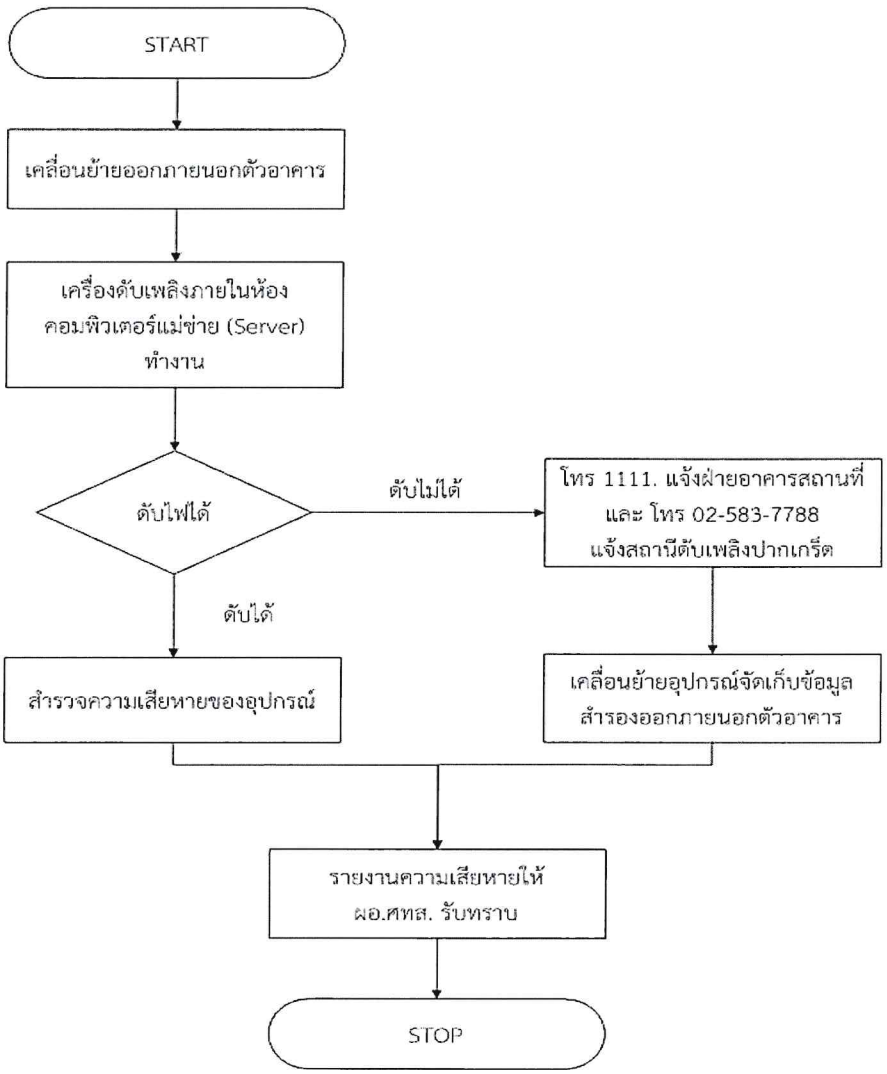


๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

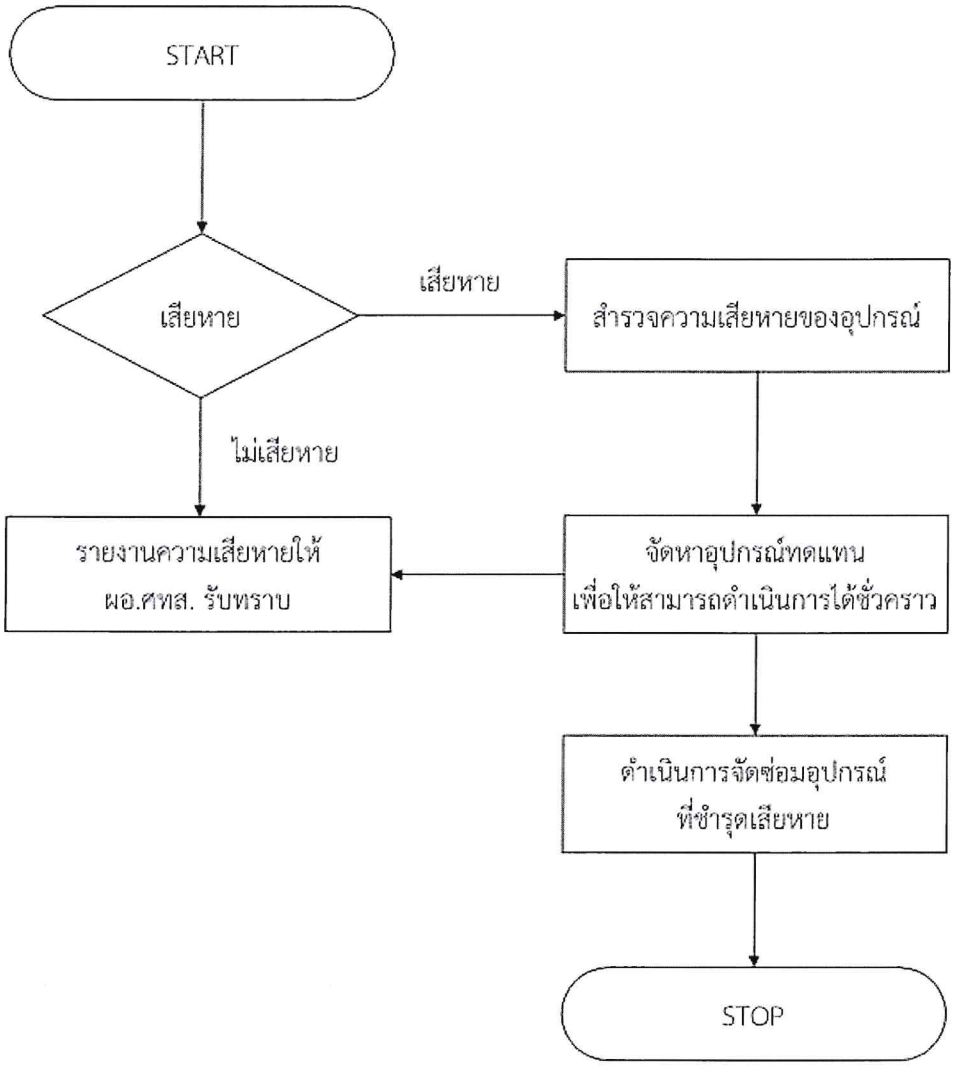
๔.๒.๑ กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่เพื่อดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้งงานอาคารและสถานที่ ที่ โทร. ๑๑๑๑ และโทรแจ้งสถานีดับเพลิงปากเกร็ด โทร. ๐-๒๕๘๓-๗๗๘๘
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ - ๒ ครั้ง

แผนแผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



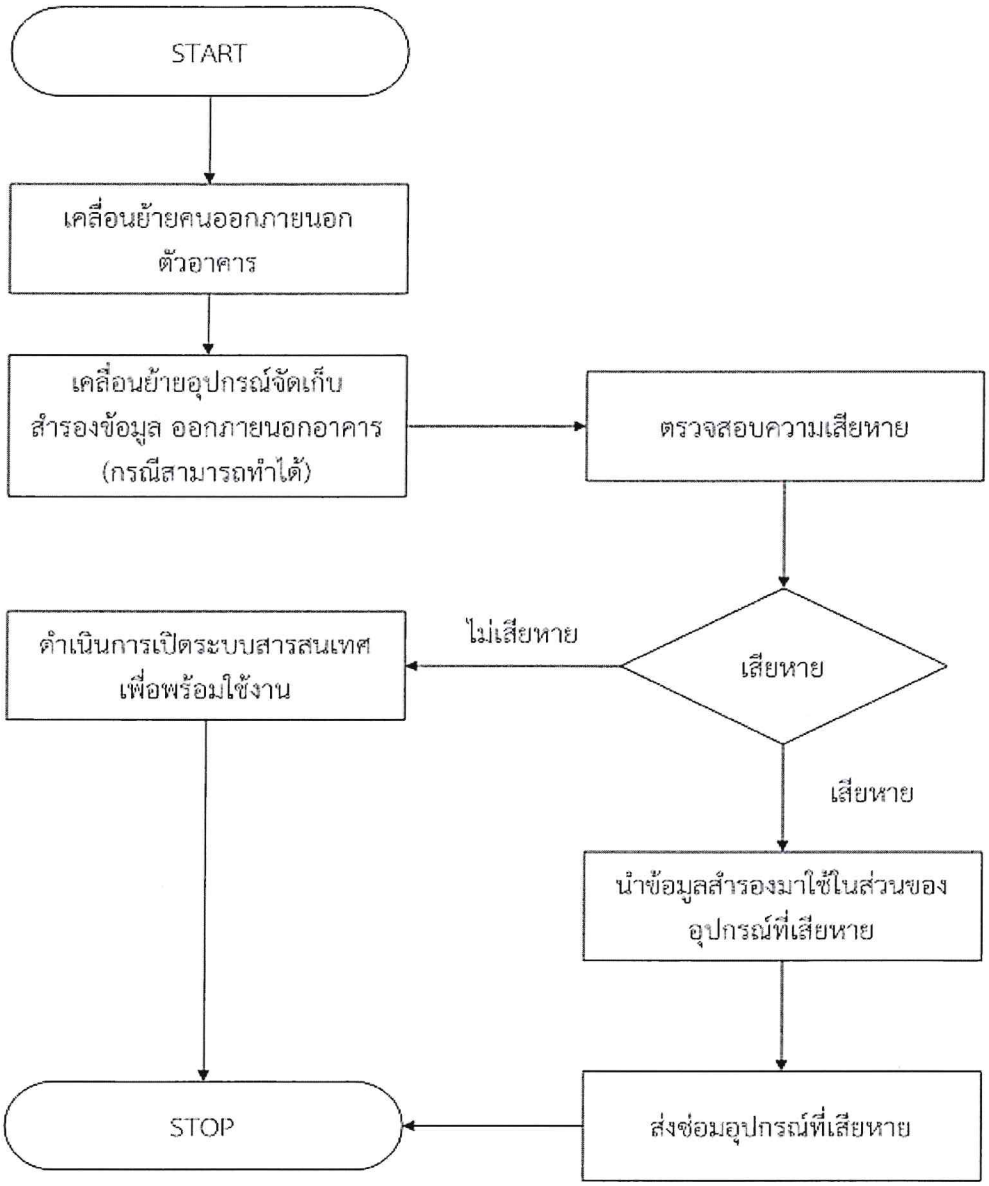
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



๔.๒.๒ กรณีแผ่นดินไหว/อาคารถล่ม

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

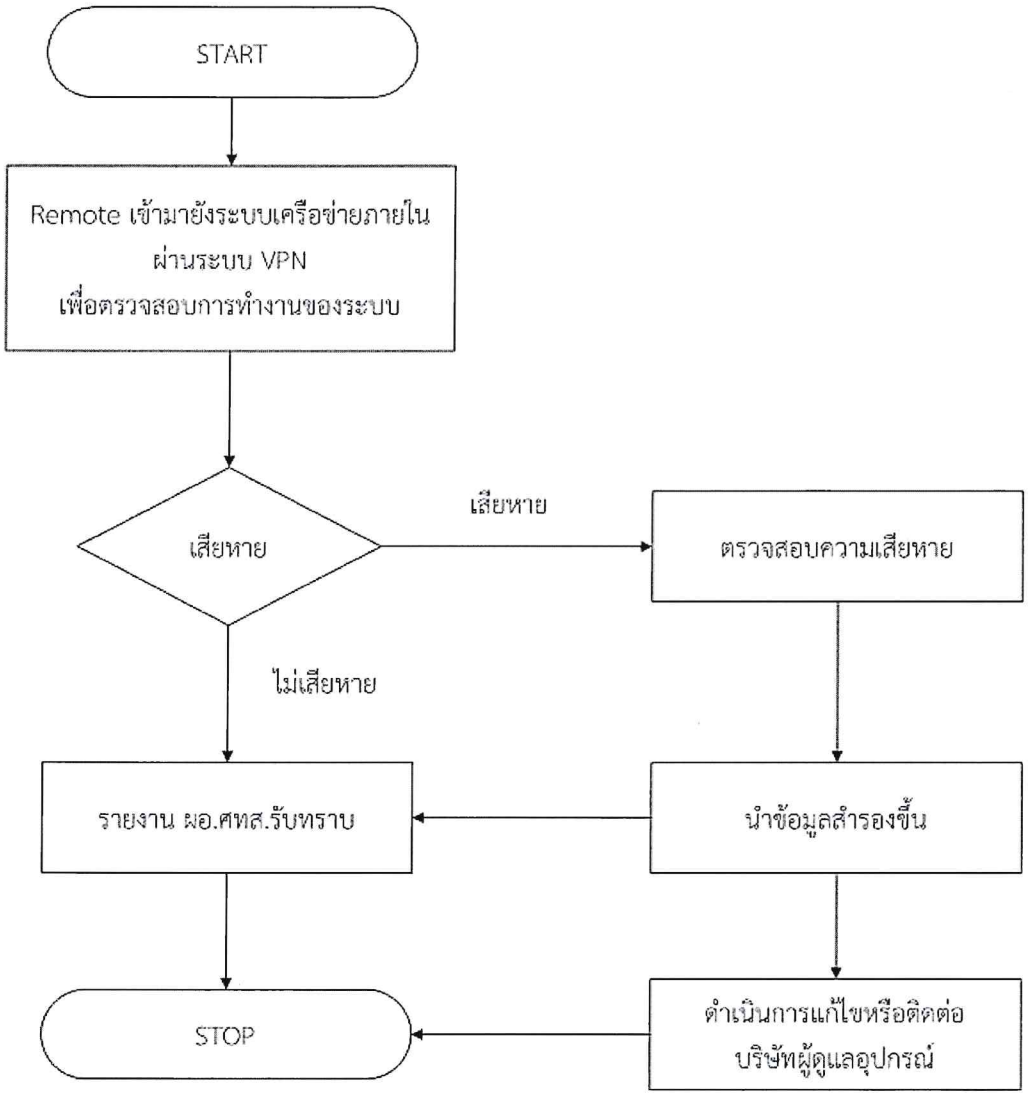


๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรง

๔.๓.๑ กรณีเกิดโรคระบาดร้ายแรงเป็นเหตุให้ไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งได้

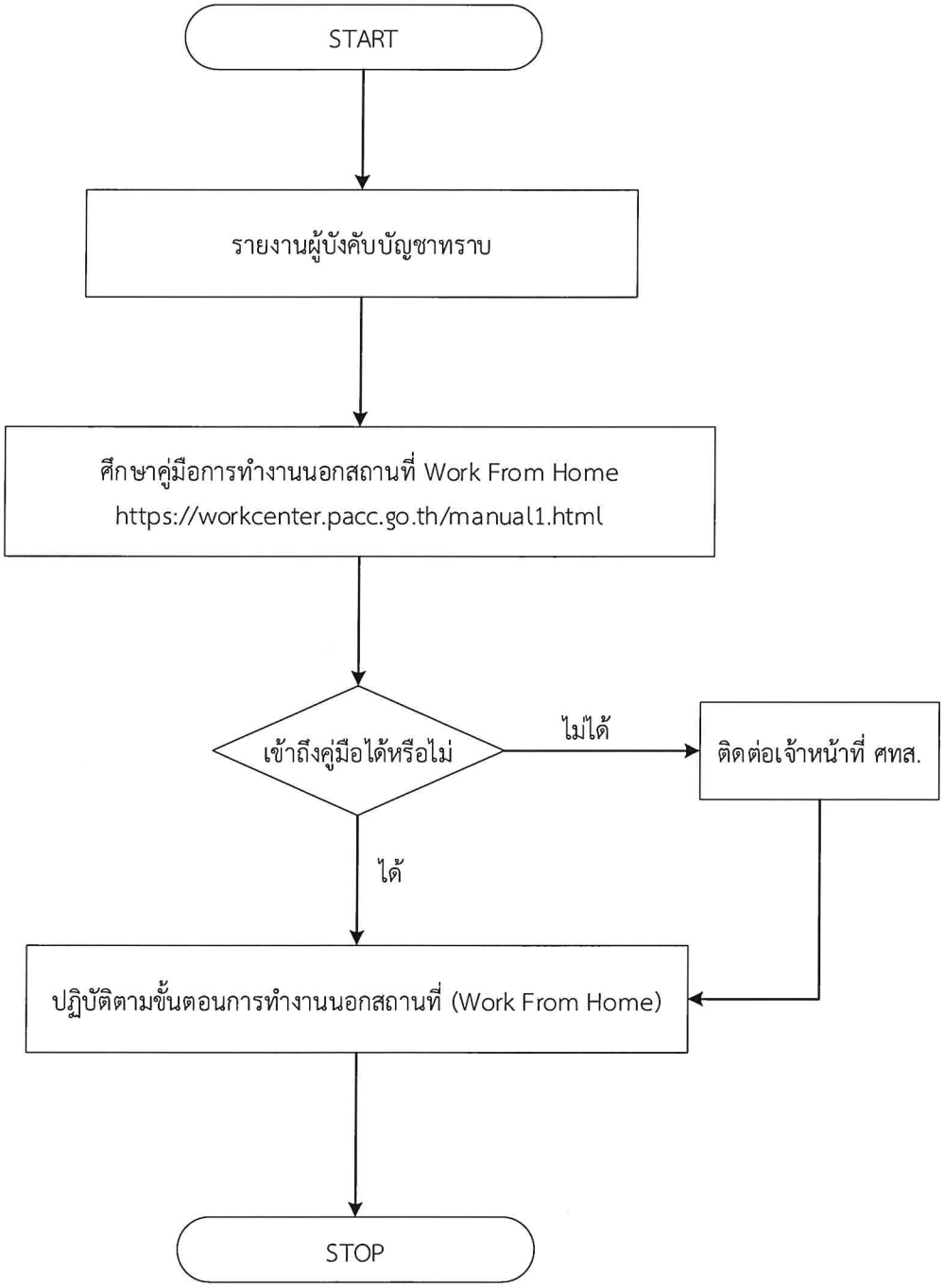
- กรณีที่เจ้าหน้าที่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งสำนักงานได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรง
กรณีที่เจ้าหน้าที่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งสำนักงานได้
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



- กรณีที่เจ้าหน้าที่ ป.ป.ท. ส่วนอื่นๆ ไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งสำนักงานได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินที่เกิดจากโรคระบาดร้ายแรง
กรณีที่เจ้าหน้าที่ ป.ป.ท. ส่วนอื่น ๆ ไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งสำนักงานได้
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๔.๔.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

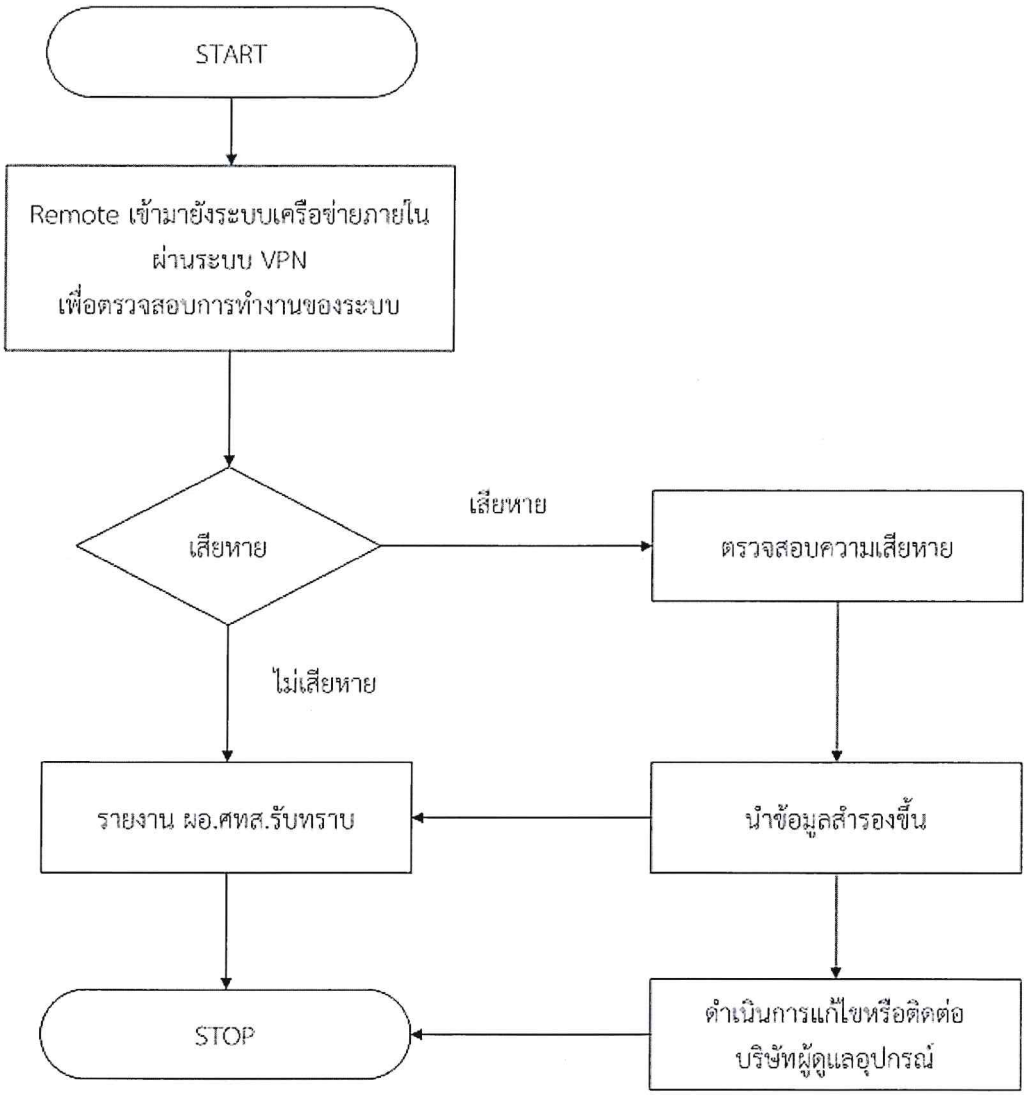
สำหรับเจ้าหน้าที่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้ง ผอ.ศทส. รับทราบ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้แจ้งผู้บริหารทราบพร้อมดำเนินการติดต่อบริษัทภายนอกดำเนินการซ่อมแซมแก้ไขหากจำเป็น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีความไม่สงบเรียบร้อย (ม็อบ)

สำหรับเจ้าหน้าที่ในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

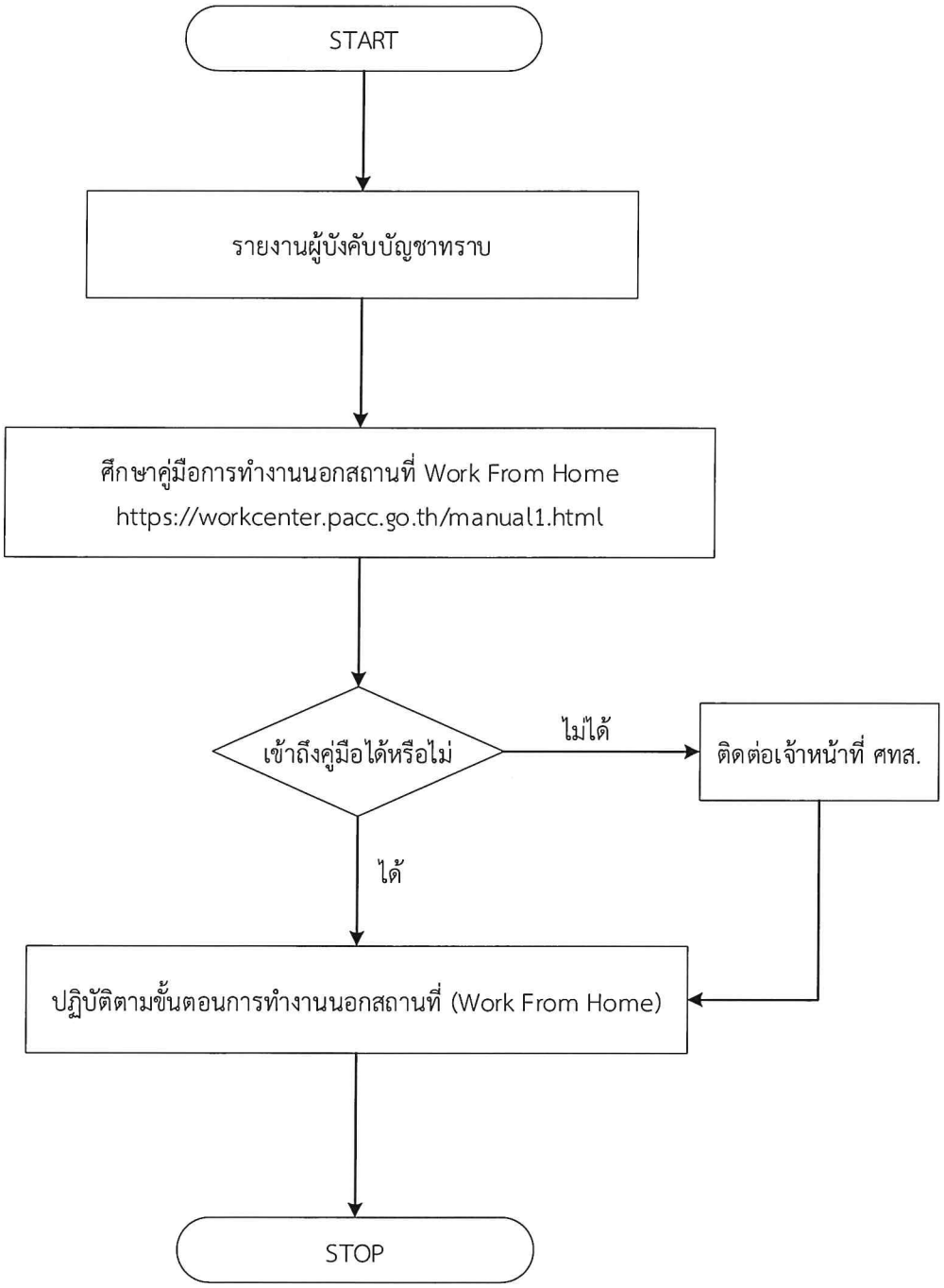
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



สำหรับเจ้าหน้าที่ ป.ป.ท. ในส่วนอื่นๆ

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในที่ตั้งสำนักงานได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีความไม่สงบเรียบร้อย (ม๊อบ)
สำหรับเจ้าหน้าที่ ป.ป.ท. ในส่วนอื่นๆ
ผู้รับผิดชอบในการดำเนินการ : สำหรับเจ้าหน้าที่ ป.ป.ท. ในส่วนอื่นๆ



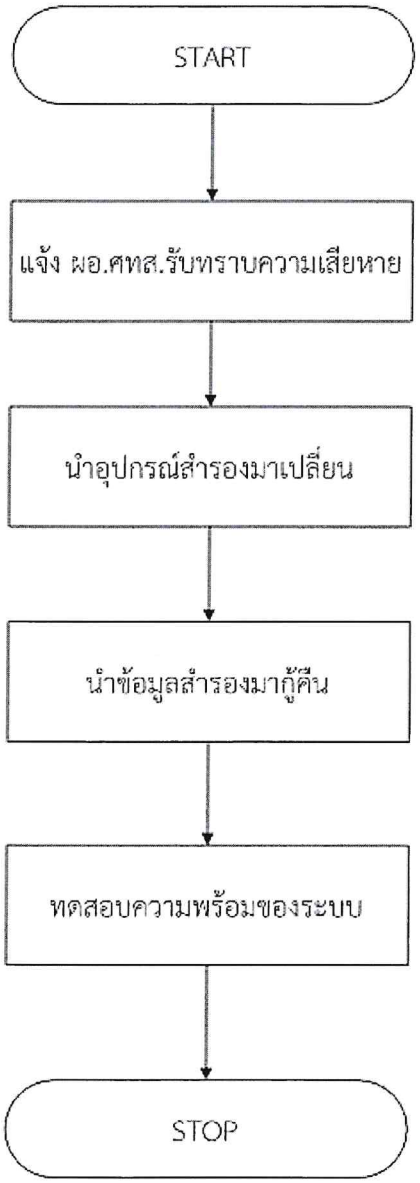
๔.๕ สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

๔.๕.๑ กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

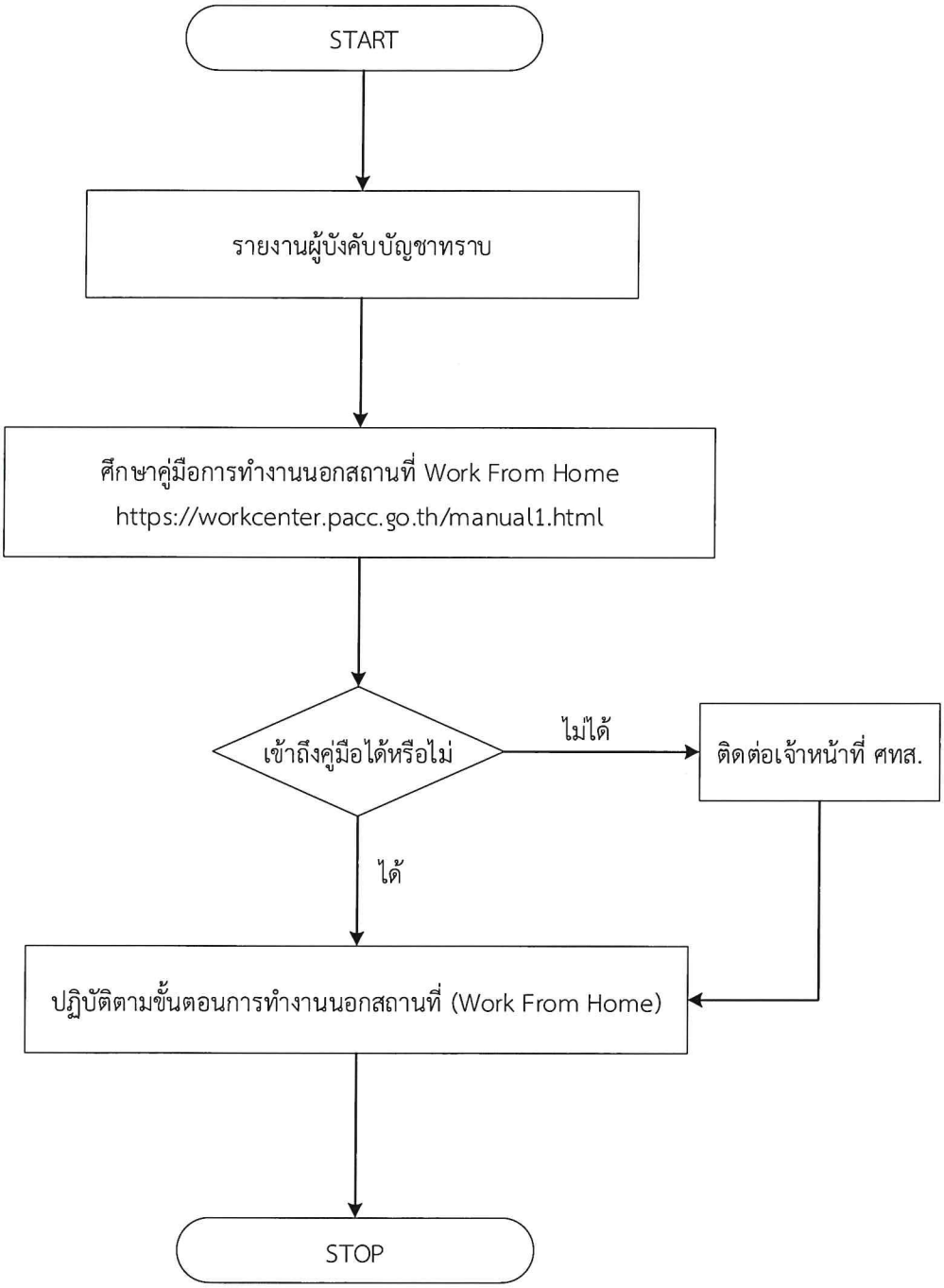
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



๔.๕.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

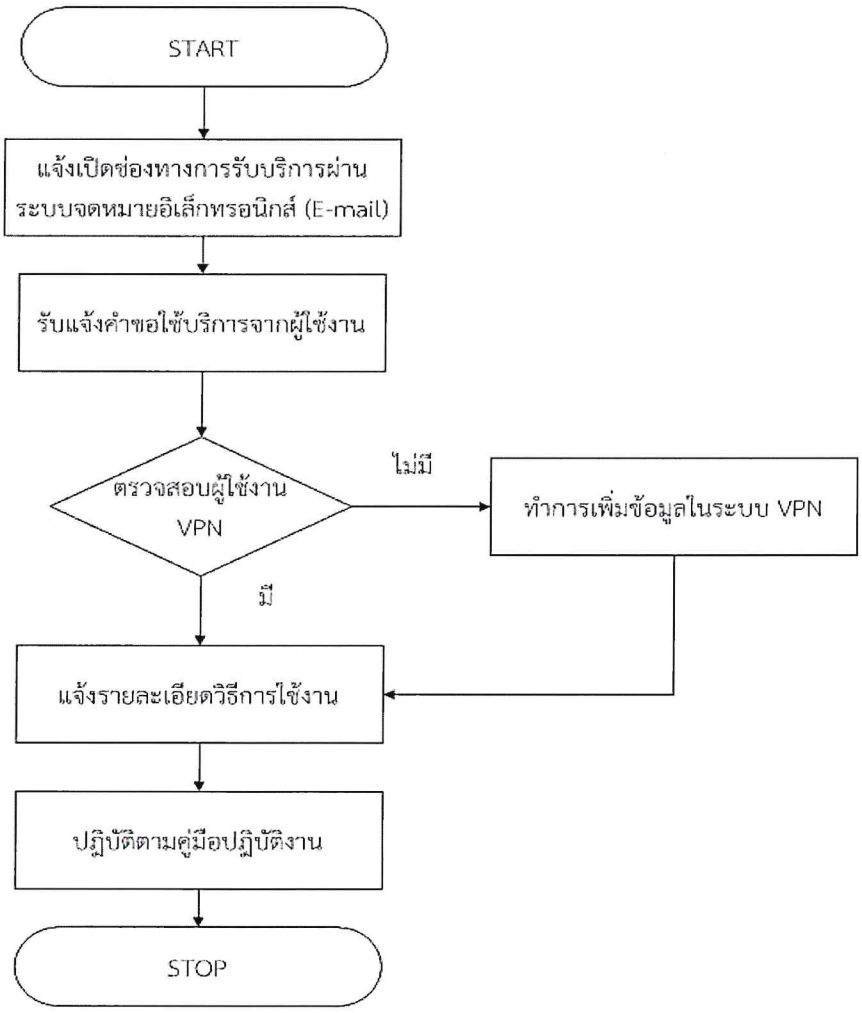
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้
ผู้รับผิดชอบในการดำเนินการ : เจ้าหน้าที่ทุกคนในศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



๔.๕.๓ **กรณีหน่วยงานนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารร้องขอการใช้งานผ่านระบบเครือข่ายเสมือน (Virtual Private Network: VPN) (กรณีไม่สามารถปฏิบัติงานภายในที่ตั้งได้)**

- รับคำร้องขอใช้บริการผ่านระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- ตรวจสอบข้อมูลผู้ขอใช้บริการ
- แจ้งรายละเอียดและข้อกำหนดในการเข้าใช้งานระบบเครือข่ายเสมือน (Virtual Private Network : VPN) ผ่านทางระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- จัดส่งคู่มือการปฏิบัติงาน (Workflow) ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-mail)

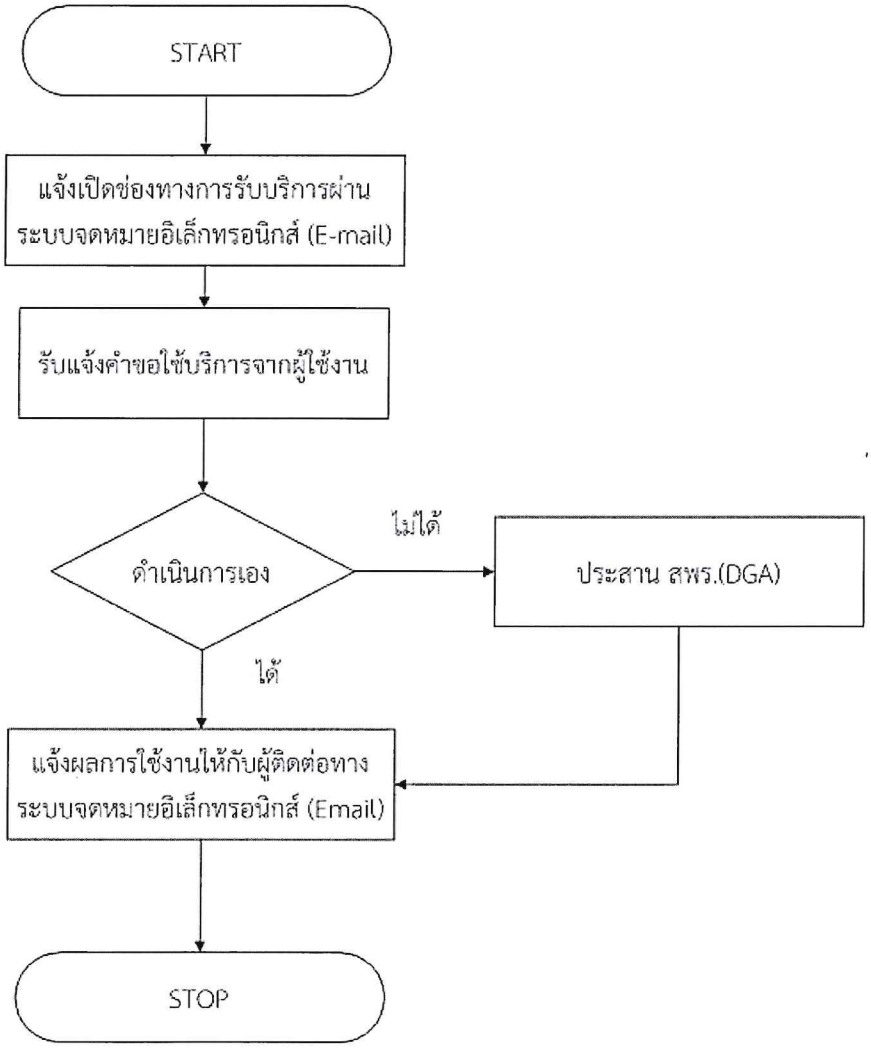
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีหน่วยงานภายในร้องขอการใช้งานผ่านระบบเครือข่ายเสมือน (Virtual Private Network : VPN)
ผู้รับผิดชอบในการดำเนินการ : กลุ่มงานคอมพิวเตอร์และการสื่อสาร



๔.๕.๔ กรณีหน่วยงานนอกศูนย์เทคโนโลยีสารสนเทศและการสื่อสารร้องขอการแก้ไขปัญหาการใช้งานระบบสารบรรณอิเล็กทรอนิกส์ (กรณีไม่สามารถปฏิบัติงานภายในที่ตั้งได้)

- แจ้งเปิดช่องทางการรับบริการผ่านระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- รับคำร้องขอใช้บริการผ่านระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- ดำเนินการแก้ไขปัญหา
- แจ้งผลการดำเนินการ ผ่านทางจดหมายอิเล็กทรอนิกส์ (E-mail)

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีหน่วยงานภายในร้องขอการแก้ไขปัญหาระบบสารบรรณ
ผู้รับผิดชอบในการดำเนินการ : ฝ่ายบริหารทั่วไป



๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

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

๑.๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

๑.๒. ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. กลุ่มงานคอมพิวเตอร์และการสื่อสาร รับผิดชอบการปฏิบัติงานระบบเครือข่ายและห้องแม่ข่าย ได้แก่

๒.๑ นายมรุต อาภาอดุล	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๒.๒ นายพชฎ ศริพันธุ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๒.๓ นางสาวตรียภรณ์ กองอ้น	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๒.๔ นายอานันท์ มากบัวแก้ว	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๓. กลุ่มงานบริหารเทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

๓.๑ นายนักสิทธิ์ อึ่งสกุล	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๓.๒ นางสาวณัฐกฤตา วงษ์สายตา	นักวิชาการคอมพิวเตอร์ชำนาญการ
๓.๓ นางสาวอรวรรณ ผดุงเกียรติ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๓.๔ นายศรนรินทร์ วุมิเฟย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๔. ทีมบริการเทคนิค รับผิดชอบการปฏิบัติงานทางเทคนิค ได้แก่

๔.๑ นายมรุต อาภาอดุล	นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ
๔.๒ นายพชฎ ศริพันธุ์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๔.๓ นายวิกร แก้วกำไร	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

๕. ฝ่ายบริหารทั่วไปและทีมงานประสานงาน รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๕.๑ นางสาวพรทิพย์ อยู่สุข	นักจัดการงานทั่วไปชำนาญการ
๕.๒ นางสาวอรวรรณ ผดุงเกียรติ	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๕.๓ นางสาวตรียภรณ์ กองอ้น	นักวิชาการคอมพิวเตอร์ปฏิบัติการ

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) ของสำนักงาน ป.ป.ท. เพื่อให้เจ้าหน้าที่สำนักงาน ป.ป.ท. ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(นายภูมิวิศาล เกษมศุข)
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)