แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

๑. บทนำ

กรมตรวจบัญชีสหกรณ์ ได้นำเทคโนโลยีสารสนเทศมาช่วยในการปฏิบัติงานตามภารกิจหลัก โดยดำเนินการตรวจสอบบัญชีสหกรณ์และกลุ่มเกษตรกรตามกฎหมายว่าด้วยสหกรณ์และกฎหมายอื่นที่เกี่ยวข้อง กำหนดระบบบัญชีและมาตรฐานการสอบบัญชีให้เหมาะสมกับธุรกิจของสหกรณ์และกลุ่มเกษตรกร ถ่ายทอดความรู้และส่งเสริมการจัดทำบัญชีให้แก่สหกรณ์ กลุ่มเกษตรกร กลุ่มอาชีพ วิสาหกิจชุมชน กลุ่มเป้าหมายตามโครงการพระราชดำริ เกษตรกร และประชาชนทั่วไป และภารกิจสนับสนุนของหน่วยงาน เช่น เว็บไซต์หน่วยงาน (www.cad.go.th) ระบบจดหมายอิเล็กทรอนิกส์ (E-mail) ระบบสารสนเทศ (Intranet) ระบบแผนและผลการปฏิบัติงาน ระบบเชื่อมโยงฐานข้อมูล GFMIS ระบบฐานข้อมูลส่วนบุคคลกรมตรวจบัญชีสหกรณ์ ระบบควบคุมคุณภาพงานสอบบัญชีด้วยระบบกระดาษทำการอิเล็กทรอนิกส์ (EWP/RISK) ระบบสารบรรณอิเล็กทรอนิกส์ (Docflow) โปรแกรมระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS) ระบบสารสนเทศทางการเงินของสหกรณ์และกลุ่มเกษตรกร Online (Version ๓.๐) ระบบควบคุมคุณภาพงานสอบบัญชีด้วยกระดาษทำการอิเล็กทรอนิกส์ ระบบนวัตกรรมเพื่อสร้างข้อมูลที่มีคุณค่า (Smart๔M) ระบบบริการข้อมูลสารสนเทศทางการเงินของสหกรณ์ และกลุ่มเกษตรกร (Web Service) ข้อมูลเชิงวิเคราะห์เศรษฐกิจของสหกรณ์ และกลุ่มเกษตรกร และระบบฐานข้อมูลสารสนเทศทางการเงินของสหกรณ์ออมทรัพย์ (ธนาคารแห่งประเทศไทย) เป็นต้น เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น

กรมตรวจบัญชีสหกรณ์ ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ ซึ่งจำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่าง ๆ อันอาจจะเกิดขึ้นกับระบบสารสนเทศ จึงได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษา และป้องกันแก้ไขปัญหาอันอาจส่งผลกระทบต่อระบบเครือข่ายคอมพิวเตอร์ อุปกรณ์เครือข่าย เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศและฐานข้อมูล ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศและฐานข้อมูลของเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๒.๕ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบสารสนเทศและฐานข้อมูลของกรมตรวจบัญชีสหกรณ์

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของกรมตรวจบัญชีสหกรณ์มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศของกรมตรวจบัญชีสหกรณ์ พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ อาจเกิดถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกต่อกวนจากผู้ไม่ประสงค์ดี (Cracker) เจาะทำลายระบบ เป็นต้น

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศหรือใช้ข้อมูลต่าง ๆ ของกรมตรวจบัญชีสหกรณ์เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินในพื้นที่ของหน่วยงานหรือภายในหน่วยงาน ด้วยเหตุการณ์ต่อไปนี้

๓.๑ อุทกภัย
๓.๒ อัคคีภัย
๓.๓ ชุมนุมประท้วง/จลาจล
๓.๔ ไฟฟ้าขัดข้อง
๓.๕ การก่อการร้าย
๓.๖ ภัยคุกคามทางคอมพิวเตอร์ (Cyber Attack)
๓.๗ โรคระบาดต่อเนื่อง

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์ ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมกรมตรวจบัญชีสหกรณ์มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมตรวจบัญชีสหกรณ์

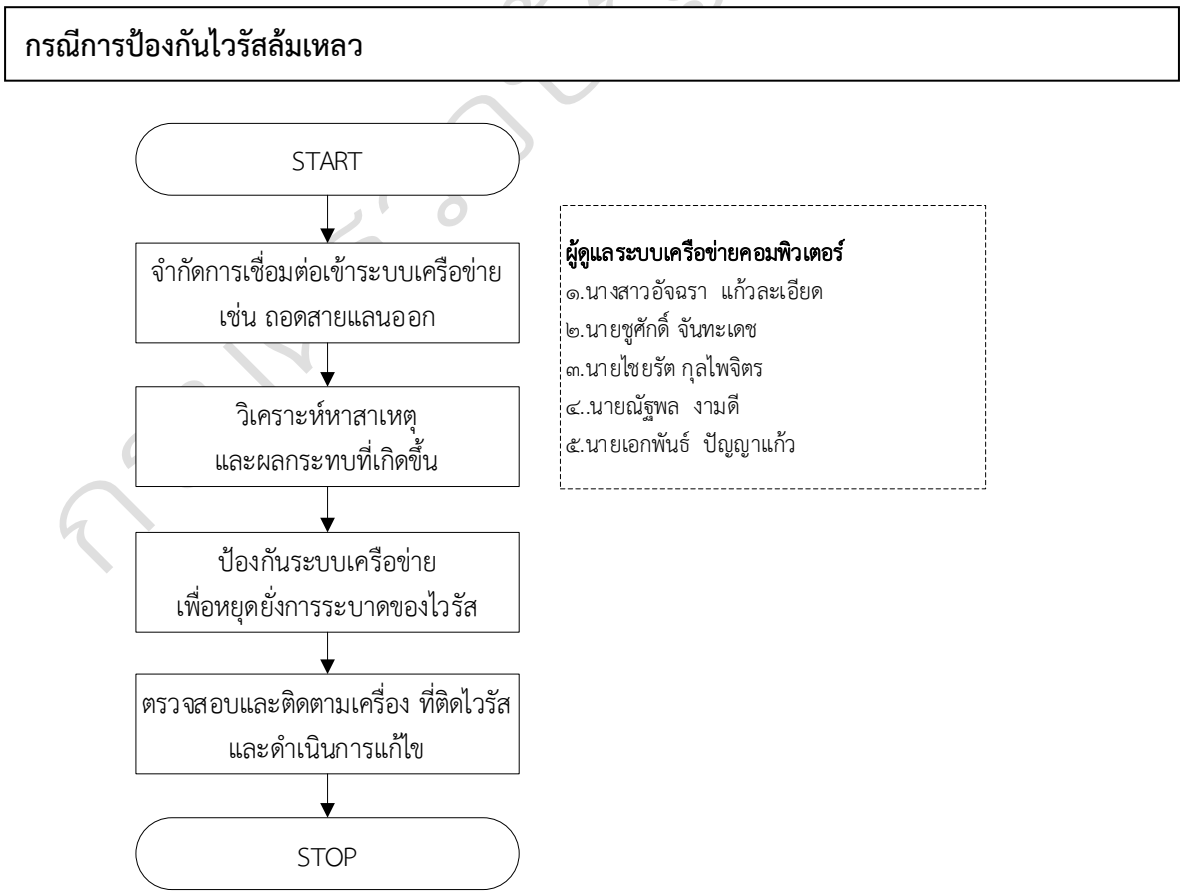
๔. แผนรองรับสถานการณ์ฉุกเฉิน

๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุกับเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ หรือกรณีมีเหตุอันทำให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ไม่สามารถดำเนินการให้บริการด้านระบบเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว

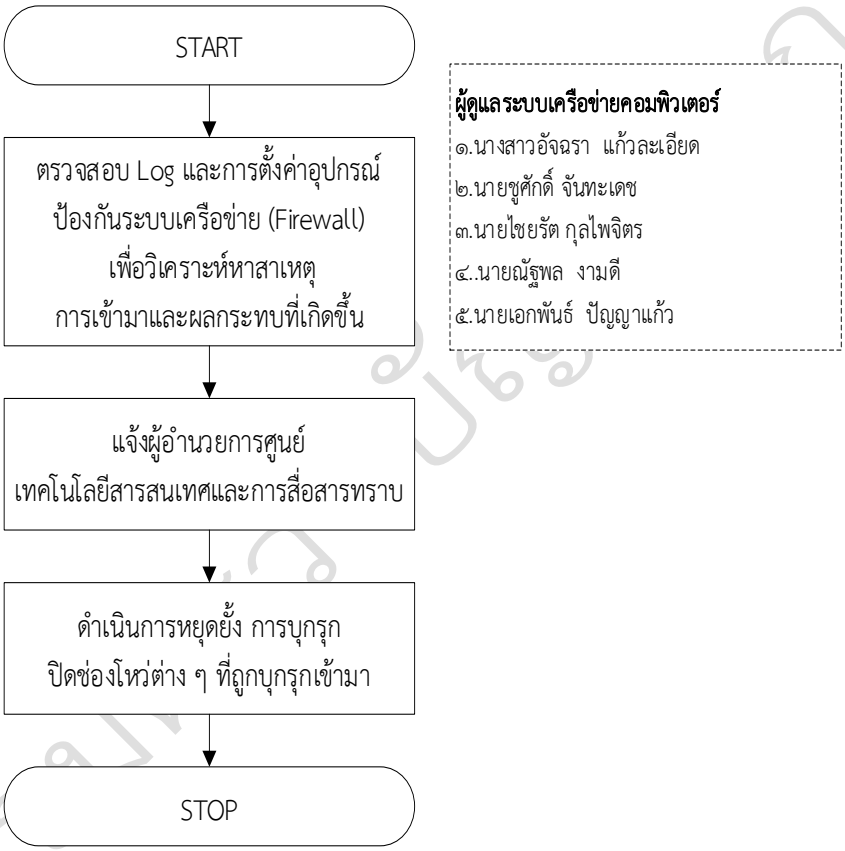


๔.๑.๒. กรณีการป้องกันผู้บุกรุก

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของอุปกรณ์ป้องกันระบบเครือข่าย (Firewall)
- ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุก

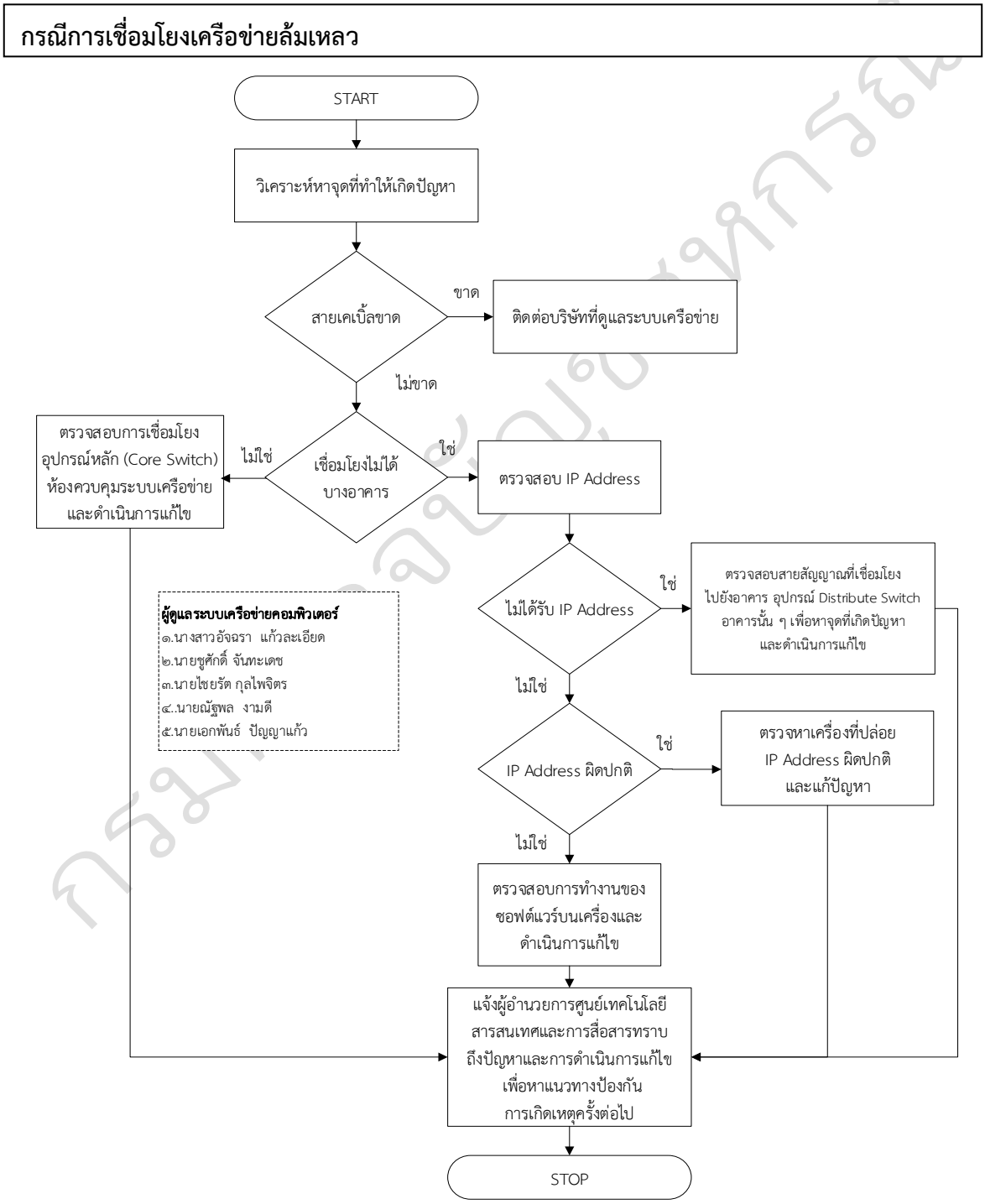
กรณีการป้องกันผู้บุกรุก



๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายเคเบิ้ลขาดให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะอาคาร ให้ดำเนินการตรวจสอบสายสัญญาณที่เชื่อมต่อไปยังอาคาร อุปกรณ์ Core Switch และ Distribute Switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

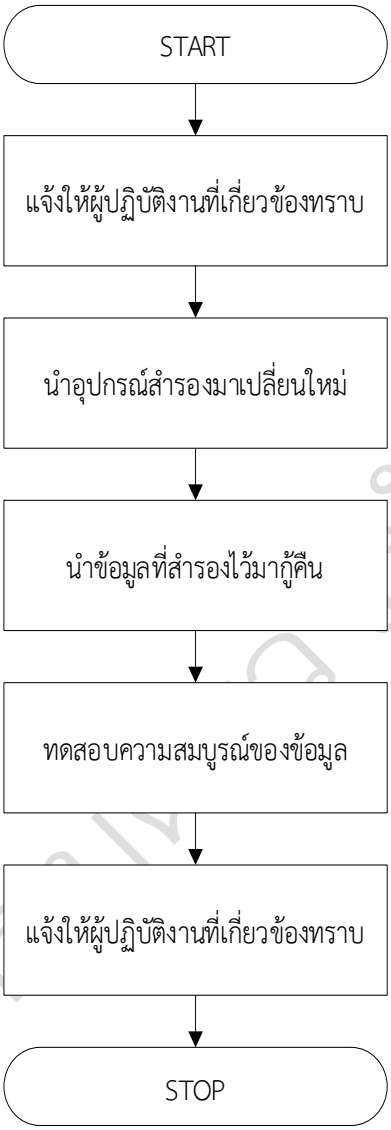


๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

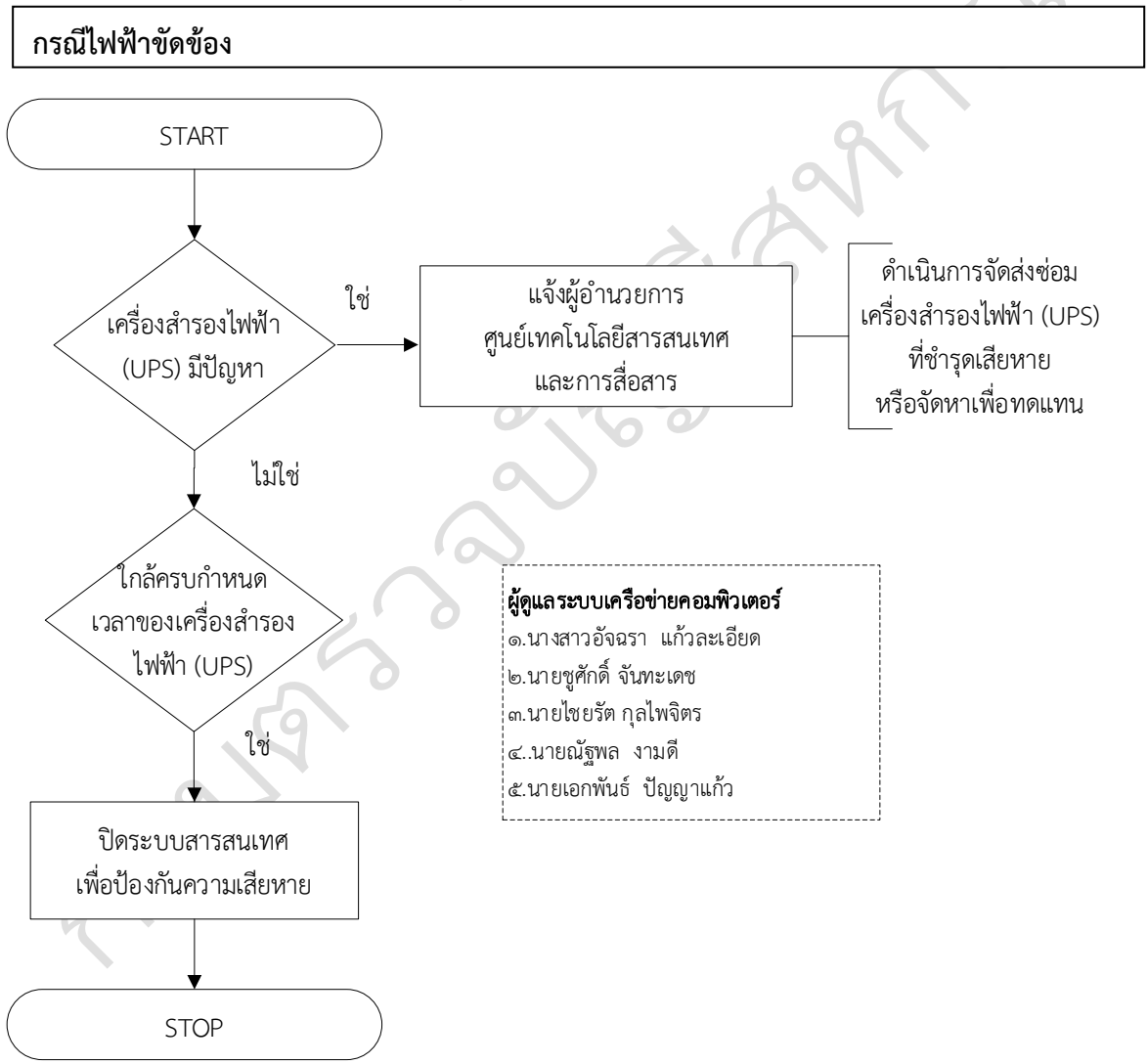


ผู้ดูแลระบบเครือข่าย
คุณอัจฉรา แก้วละเอียด
คุณชูศักดิ์ จันทะเดช
คุณปรียาภา ขำคม
คุณนิชนันท์ อินทะแสง
คุณไชยรัต กุลไพจิตร
คุณณัฐพล งามดี
เอกพันธ์ ปัญญาแก้ว
กลุ่มพัฒนาระบบสารสนเทศและฐานข้อมูล
คุณภักดี ตาติยะ
กลุ่มพัฒนาระบบตรวจสอบบัญชีคอมพิวเตอร์
คุณเพ็ญผกา น้อยศิริ
กลุ่มตรวจสอบข้อมูลและบริการสารสนเทศ
คุณจันทร์เพ็ญ ฐานบัญชา
กลุ่มพัฒนาระบบบัญชีคอมพิวเตอร์
คุณปัทมา พุฒวันเพ็ญ
กลุ่มวิเคราะห์และวัดผลทางการเงิน
คุณวัลดี แก้วพรหม

๔.๑.๕ กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมีเครื่องสำรองไฟฟ้า (UPS) ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓๐ นาที
- หากใกล้ครบ ๓๐ นาทีแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้นหรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

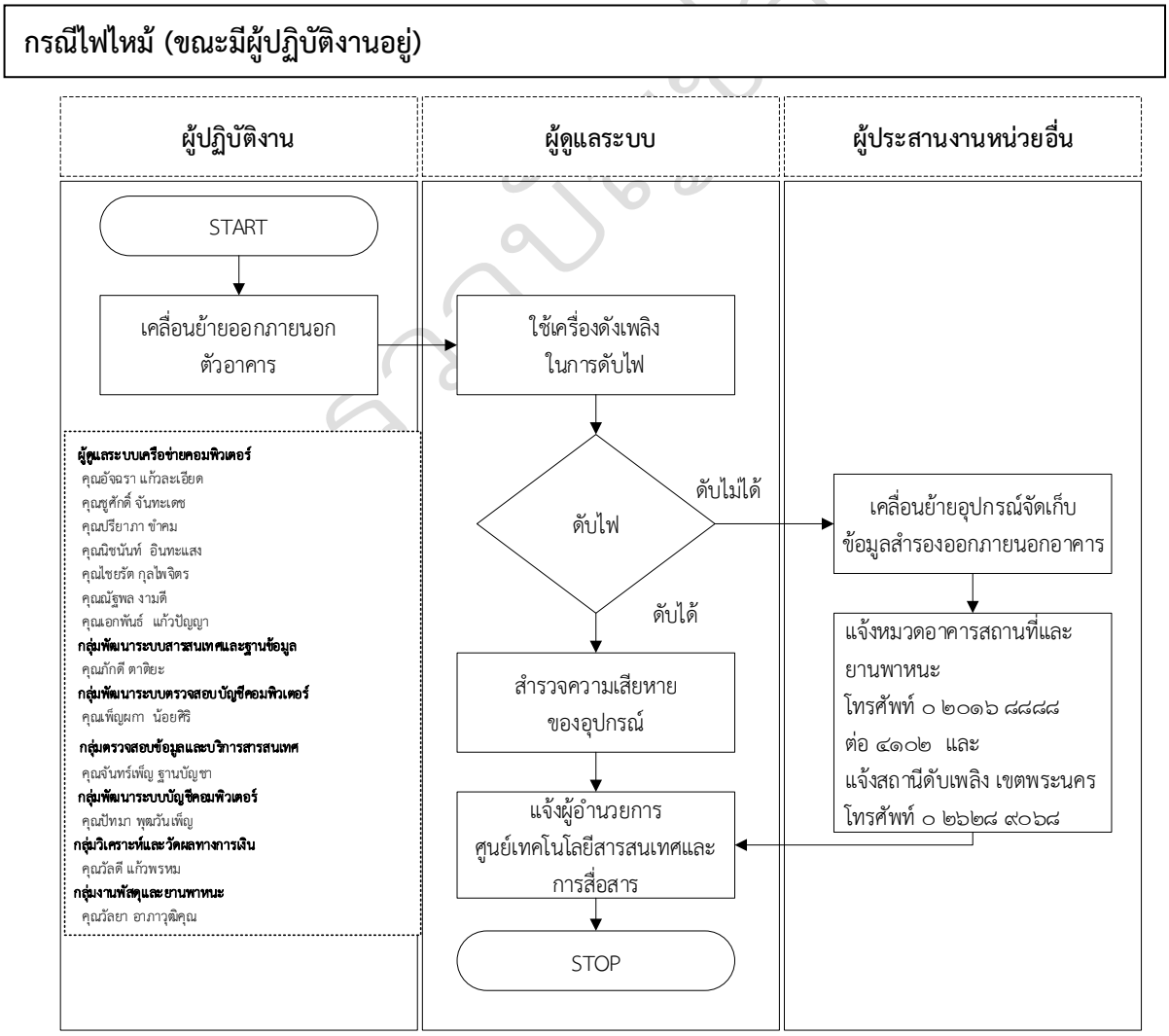


๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

๔.๒.๑ กรณีไฟไหม้

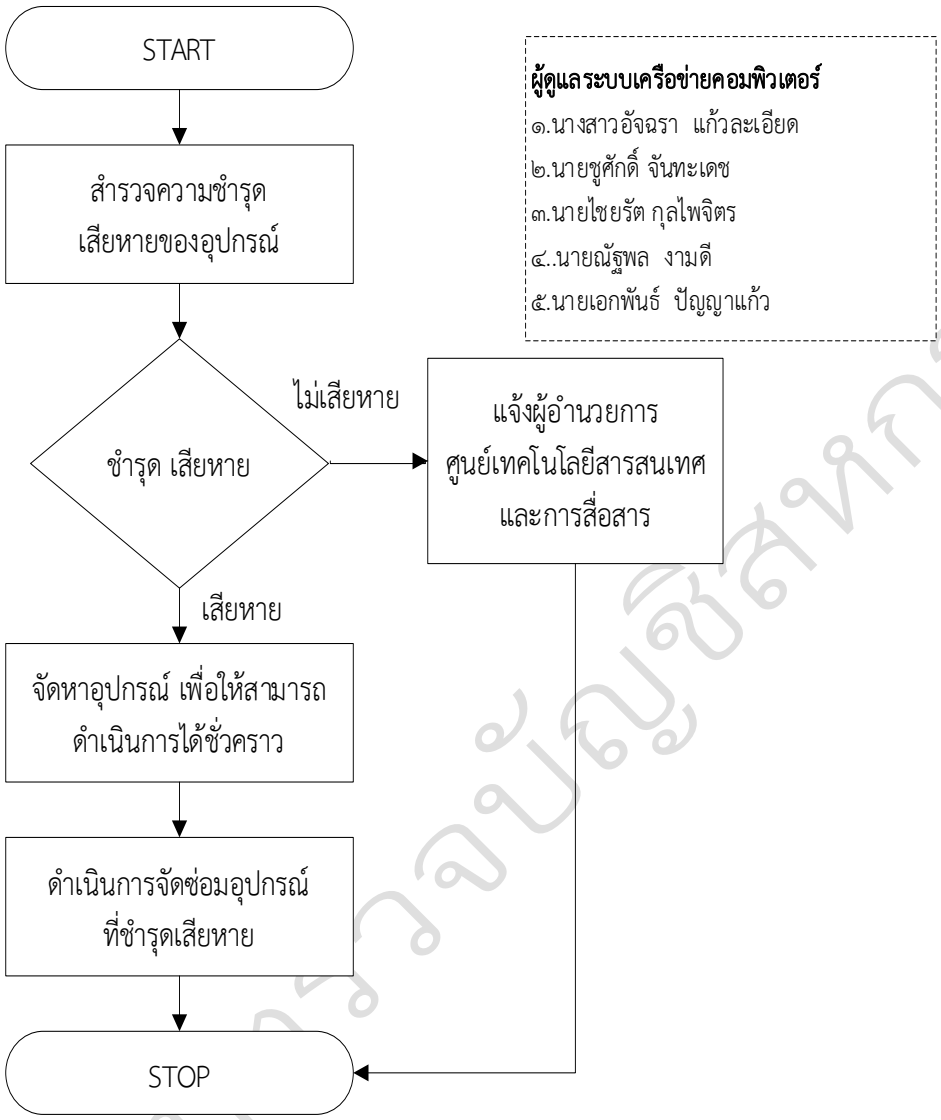
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งหมวดอาคารสถานที่และยานพาหนะทันที โทรศัพท์ ๐ ๒๐๑๖ ๘๘๘๘ ต่อ ๔๑๐๒ และแจ้งสถานีดับเพลิง โทรศัพท์ ๐ ๒๖๒๘ ๙๐๖๘
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)

กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)

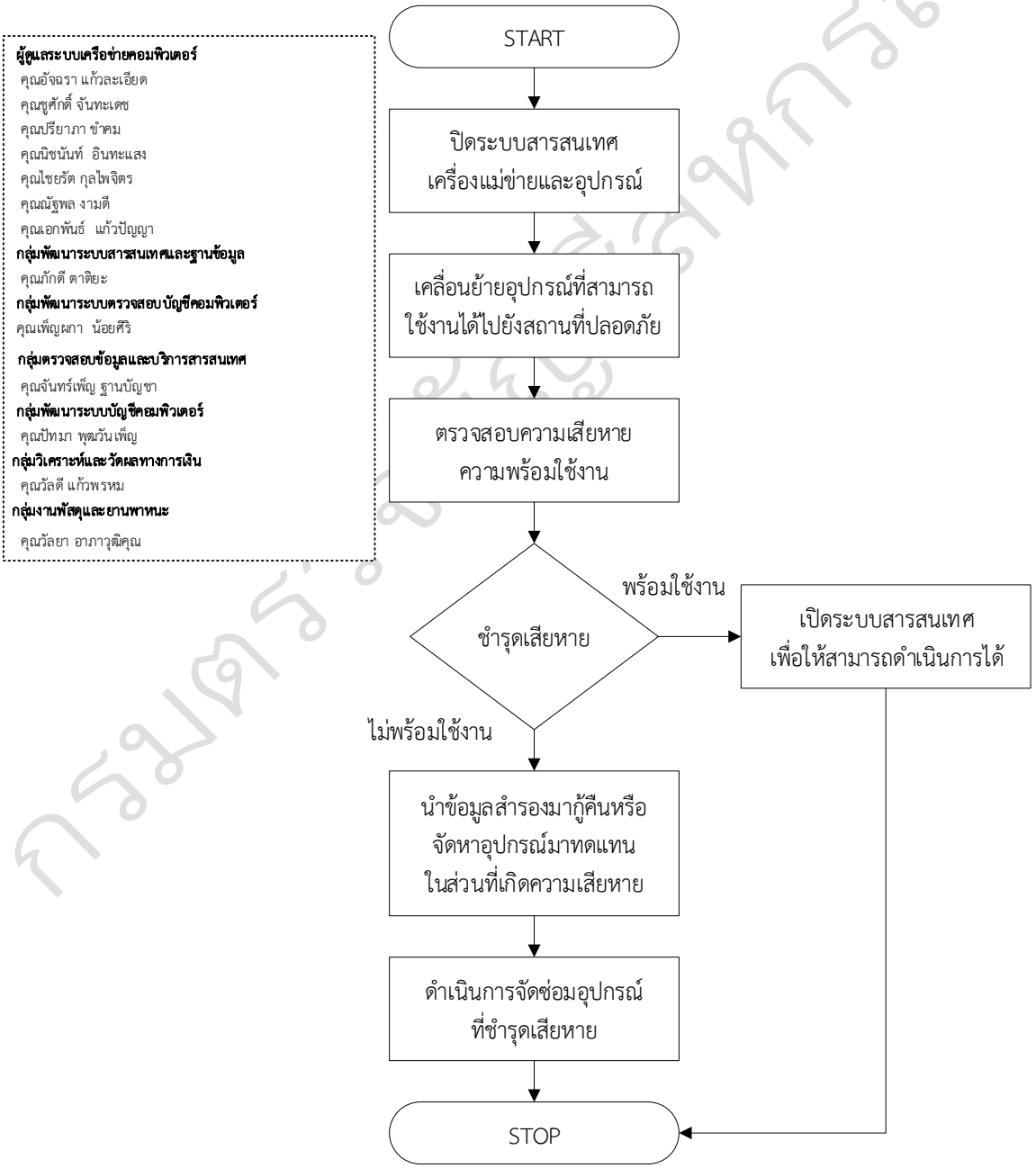


๔.๒.๒ กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปยังที่ปลอดภัย
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม

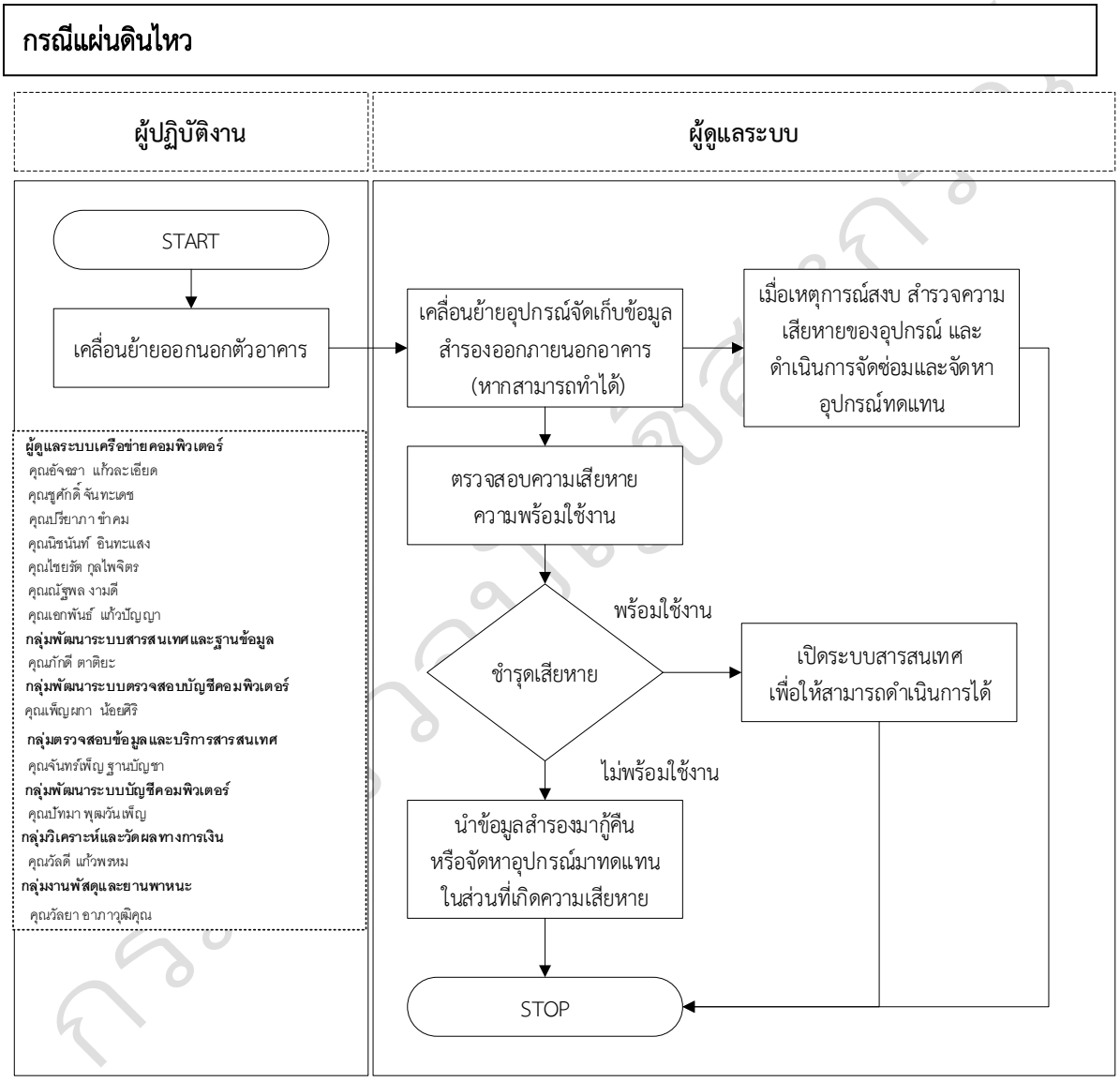
กรณีน้ำท่วม



๔.๒.๓ กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไข เพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

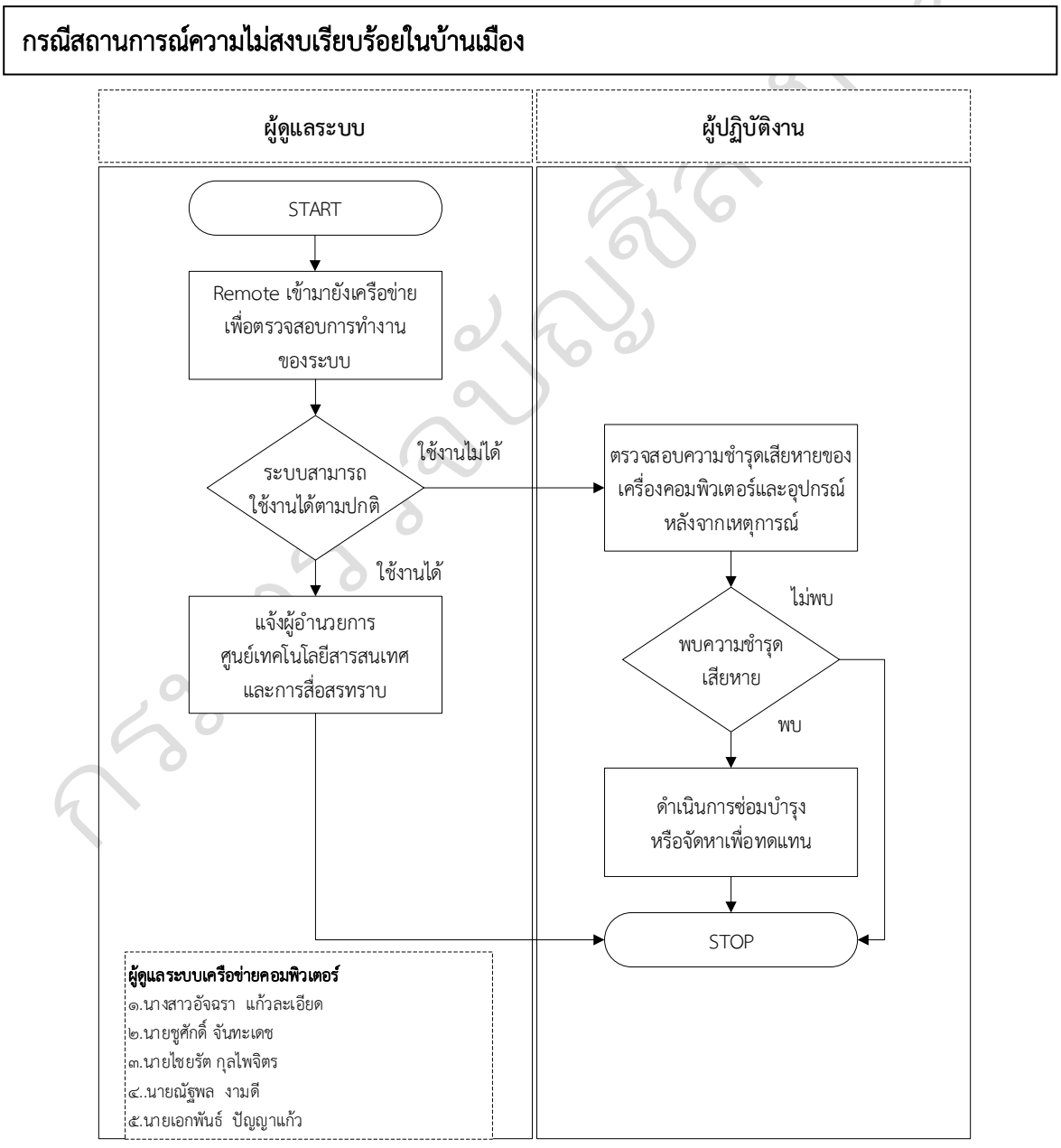


๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๔.๓.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามา เพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบชำรุด เสียหายซึ่งอาจได้รับเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์คงวามไม่สงบเรียบร้อยในบ้านเมือง



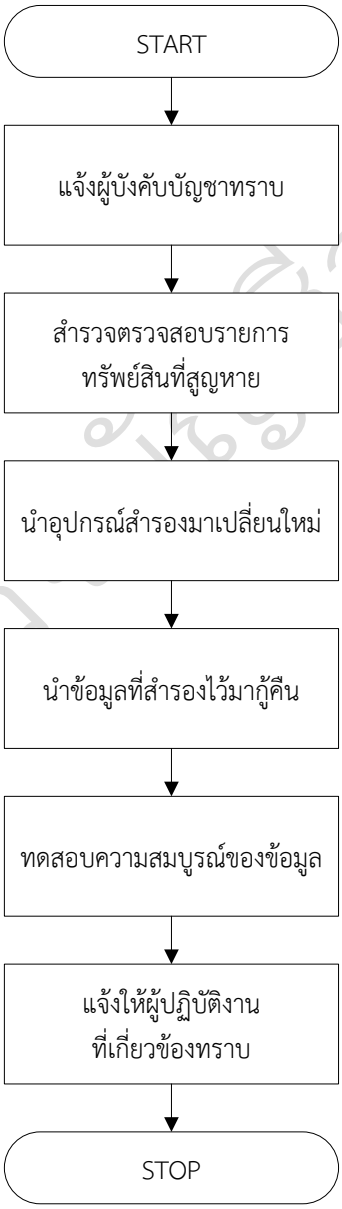
๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

๔.๔.๑ กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

กรณีโจรกรรม

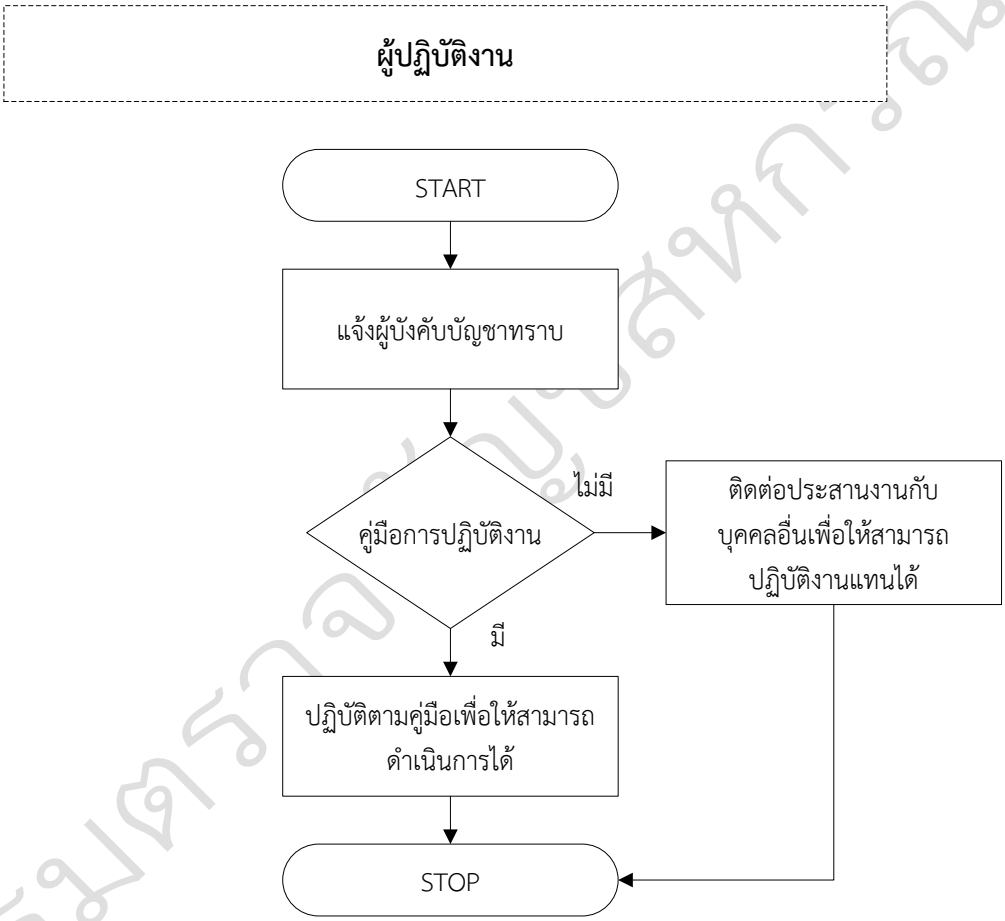


๔.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงาน

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดตามประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑ นางรพีพร กลั่นเนียม ตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO)

๑.๒ นางสาวกนกพรรณ ชำนาญกิจ ตำแหน่งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องควบคุมระบบเครือข่าย (Server) ได้แก่

๒.๑	นางสาวอัจฉรา แก้วละเอียด	ผู้อำนวยการกลุ่มระบบเครือข่ายคอมพิวเตอร์
๒.๒	นายชูศักดิ์ จันทะเดช	นักวิชาการคอมพิวเตอร์ชำนาญการ
๒.๓	นายไชยรัต กุลไพจิตร	นักวิชาการคอมพิวเตอร์
๒.๔	นายณัฐพล งามดี	นักวิชาการคอมพิวเตอร์
๒.๕	นายเอกพันธ์ แก้วปัญญา	นักวิชาการคอมพิวเตอร์

๓. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๓.๑	นางสาวสิริวรรณ คูหาสวัสดิ์	ผู้อำนวยการสำนักบริหารกลาง
๓.๒	นางสาววัลยา อาภาวุฒิคุณ	หัวหน้ากลุ่มงานพัสดุและยานพาหนะ
๓.๓	นางสาวภักดี ตาติยะ	ผู้อำนวยการกลุ่มพัฒนาระบบสารสนเทศและฐานข้อมูล
๓.๔	นางสาวเพ็ญผกา น้อยศิริ	รักษาการแทนผู้อำนวยการกลุ่มพัฒนาระบบตรวจสอบบัญชีคอมพิวเตอร์
๓.๕	นางสาวจันทร์เพ็ญ ฐานบัญชา	รักษาการแทนผู้อำนวยการกลุ่มตรวจสอบข้อมูลและบริการสารสนเทศ
๓.๖	นางวัลดี แก้วพรหม	ผู้อำนวยการกลุ่มวิเคราะห์ข้อมูลทางการเงิน
๓.๗	นางสาวปัทมา พุฒวันเพ็ญ	ผู้อำนวยการกลุ่มพัฒนาระบบบัญชีคอมพิวเตอร์
๓.๘	นางสาวปรียาภา ขำคม	นักวิชาการคอมพิวเตอร์ชำนาญการ
๓.๙	นางสาวนิชนันท์ อินทะแสง	นักวิชาการคอมพิวเตอร์ปฏิบัติการ
