แผนรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)
พ.ศ. ๒๕๖๒ - ๒๕๖๕

กรมบังคับคดี

สารบัญ

หน้า

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

๑. บทนำ

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์การจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

กรมบังคับคดีได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมบังคับคดี

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของกรมบังคับคดีมีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหาและลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมบังคับคดีเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างด้านสารสนเทศ ของกรมบังคับคดี พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของกรมเกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมบังคับคดีดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ กรมบังคับคดีมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมบังคับคดี

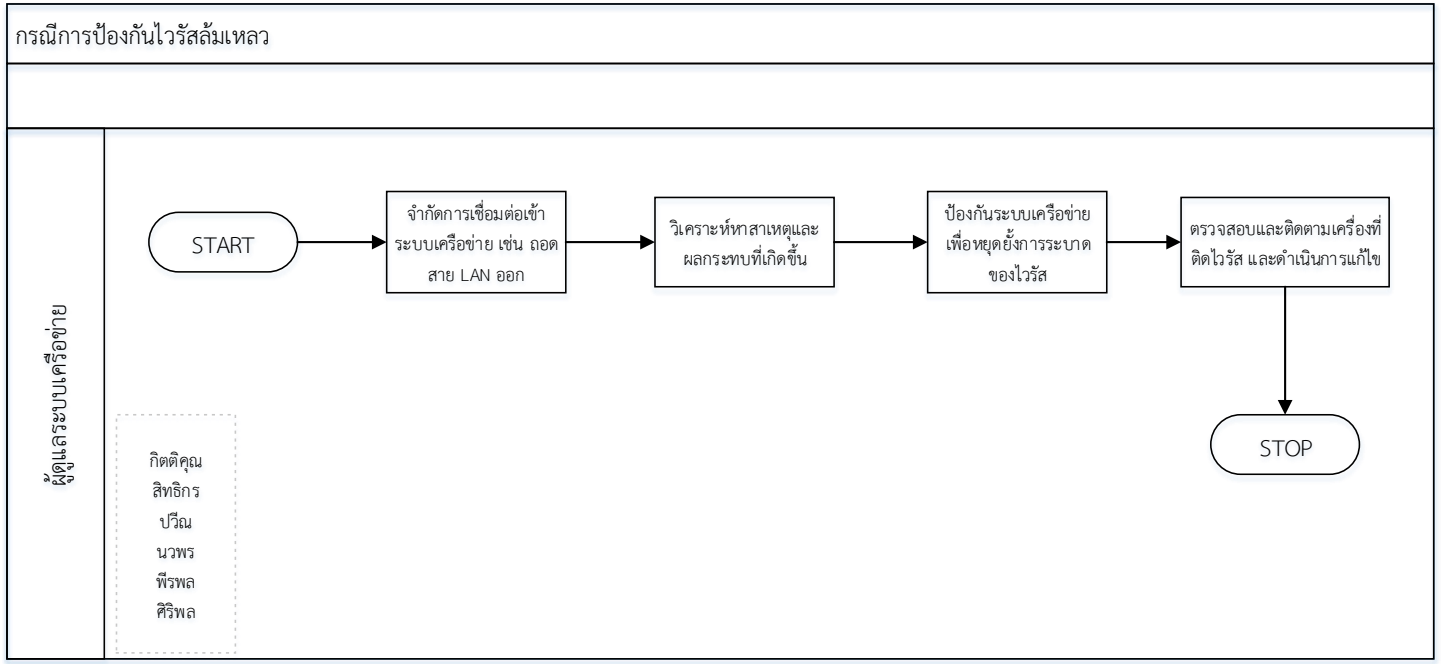
๔. แผนรองรับสถานการณ์ฉุกเฉิน

๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ศูนย์สารสนเทศทราบ หรือกรณีมีเหตุอันทำให้ศูนย์สารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์สารสนเทศจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

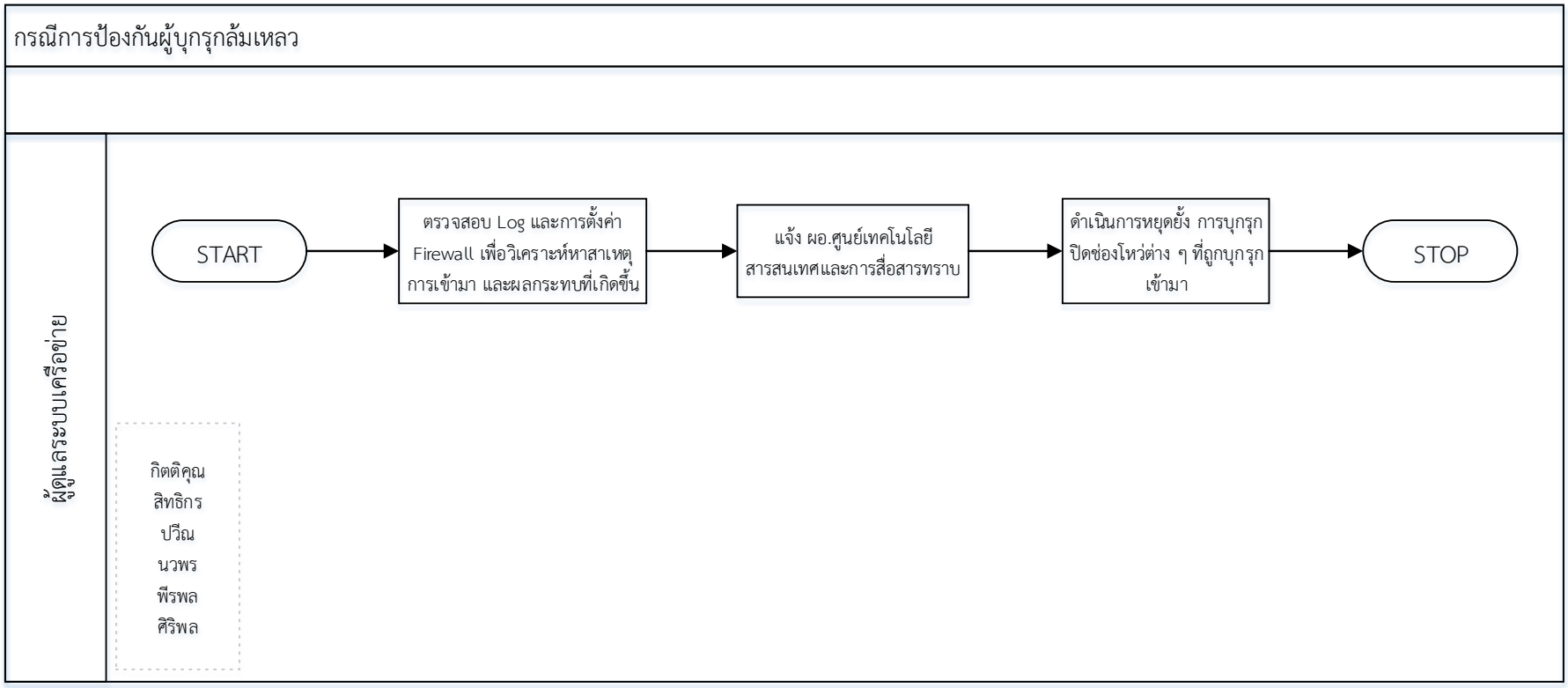
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

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

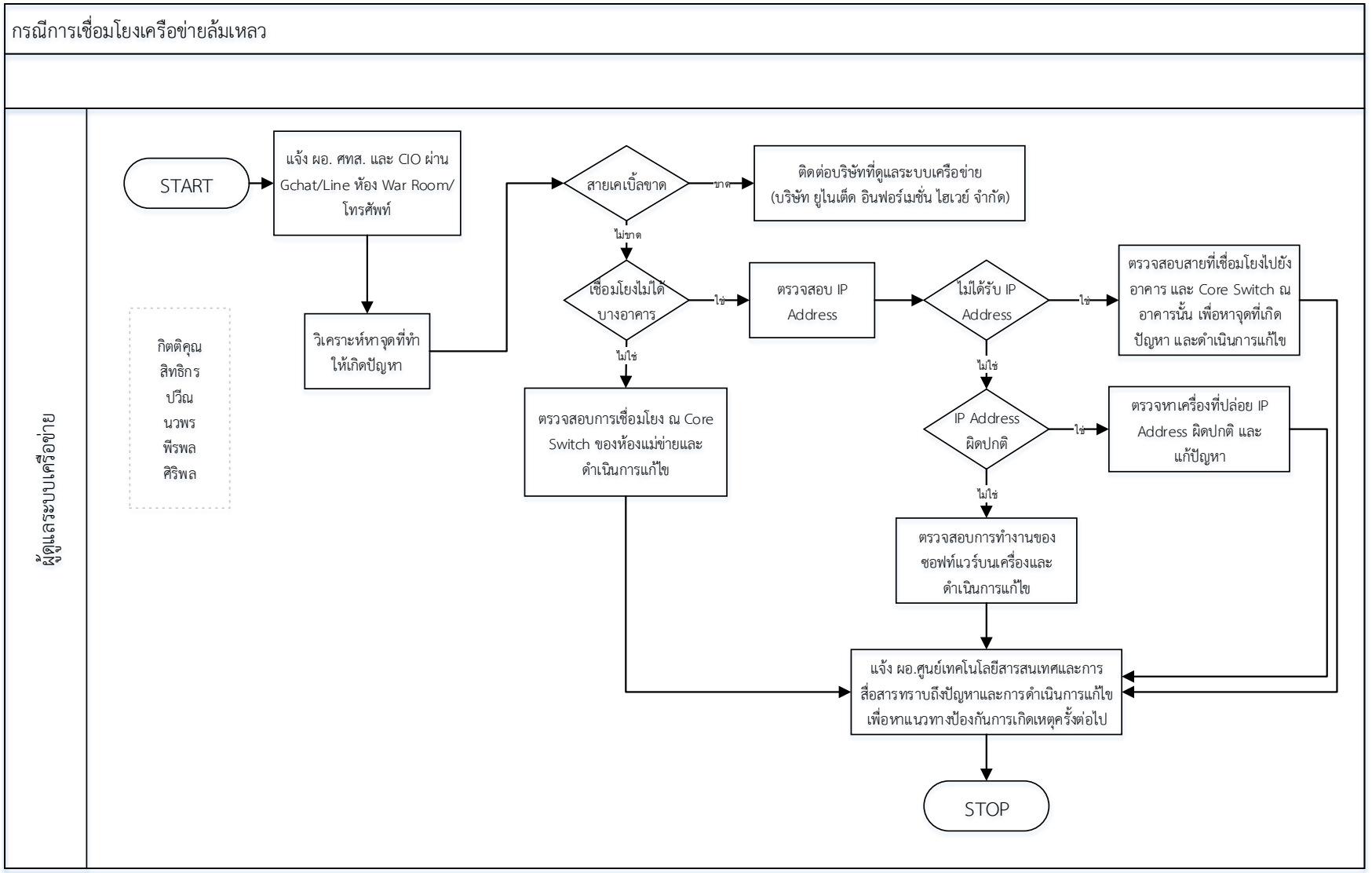
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- ทำการตรวจสอบและนำ Link Backup ใช้งานแทน
- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย (บริษัท อินเทอร์เน็ต อินฟอร์เมชั่น ไฮเวย์ จำกัด) เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ

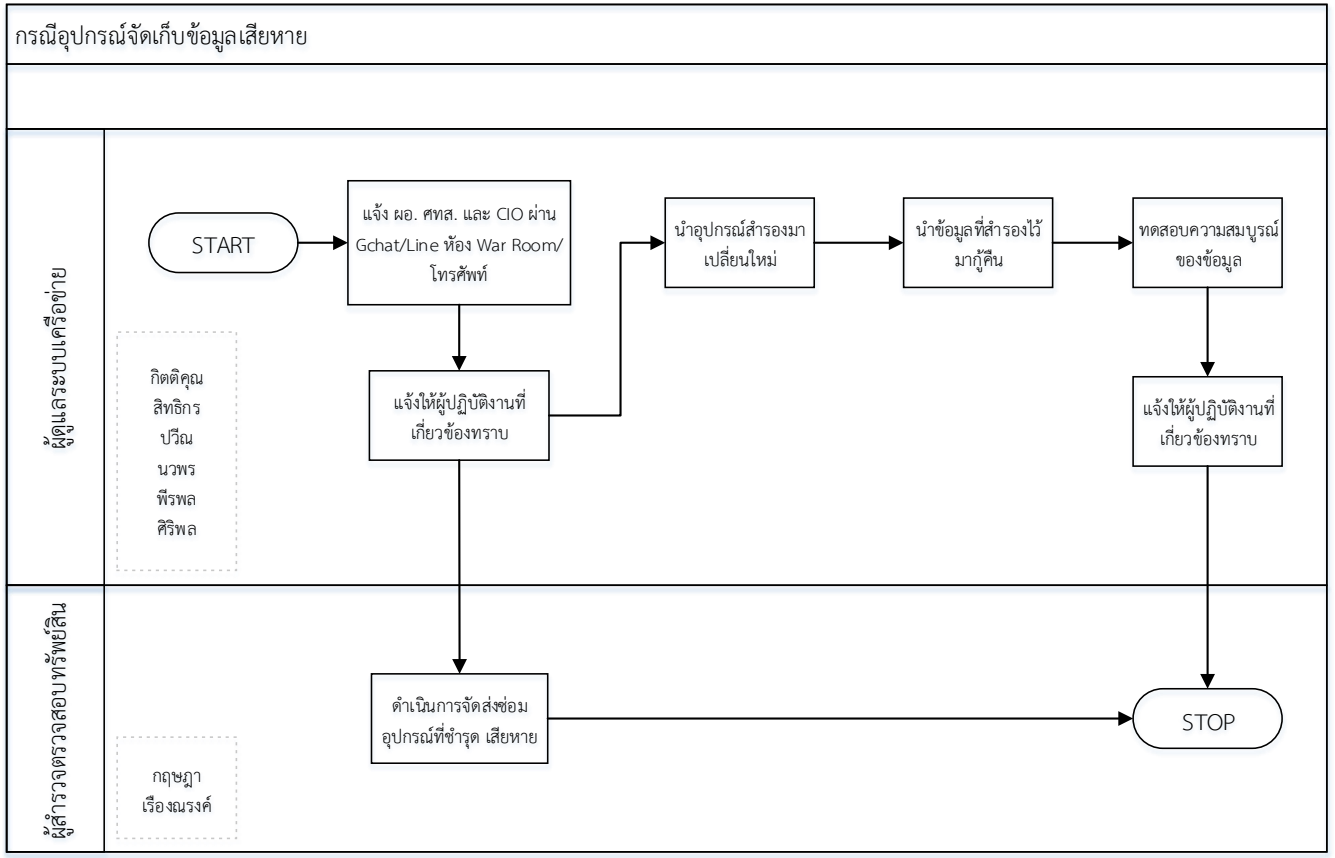
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว


กรณีการเชื่อมโยงเครือข่ายล้มเหลว
ผู้ดูแลระบบเครือข่าย
START
แจ้ง ผอ. ศทส. และ CIO ผ่าน Gchat/Line ห้อง War Room/ โทรศัพท์
กิตติคุณ
สิทธิกร
ปวีณ
นวพร
พีรพล
ศิริพล
วิเคราะห์หาจุดที่ทำให้เกิดปัญหา
สายเคเบิ้ลขาด
ขาด
ติดต่อบริษัทที่ดูแลระบบเครือข่าย (บริษัท ยูไนเต็ด อินฟอร์เมชั่น ไฮเวย์ จำกัด)
ไม่ขาด
เชื่อมโยงไม่ได้บางอาคาร
ใช่
ตรวจสอบ IP Address
ไม่ใช่
ตรวจสอบการเชื่อมโยง ณ Core Switch ของห้องแม่ข่ายและดำเนินการแก้ไข
ไม่ได้รับ IP Address
ใช่
ตรวจสอบสายที่เชื่อมโยงไปยังอาคาร และ Core Switch ณ อาคารนั้น เพื่อหาจุดที่เกิดปัญหา และดำเนินการแก้ไข
ไม่ใช่
IP Address ผิดปกติ
ใช่
ตรวจหาเครื่องที่ปล่อย IP Address ผิดปกติ และแก้ปัญหา
ไม่ใช่
ตรวจสอบการทำงานของซอฟท์แวร์บนเครื่องและดำเนินการแก้ไข
แจ้ง ผอ.ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบถึงปัญหาและการดำเนินการแก้ไข เพื่อหาแนวทางป้องกันการเกิดเหตุครั้งต่อไป
STOP

๔.๑.๔ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

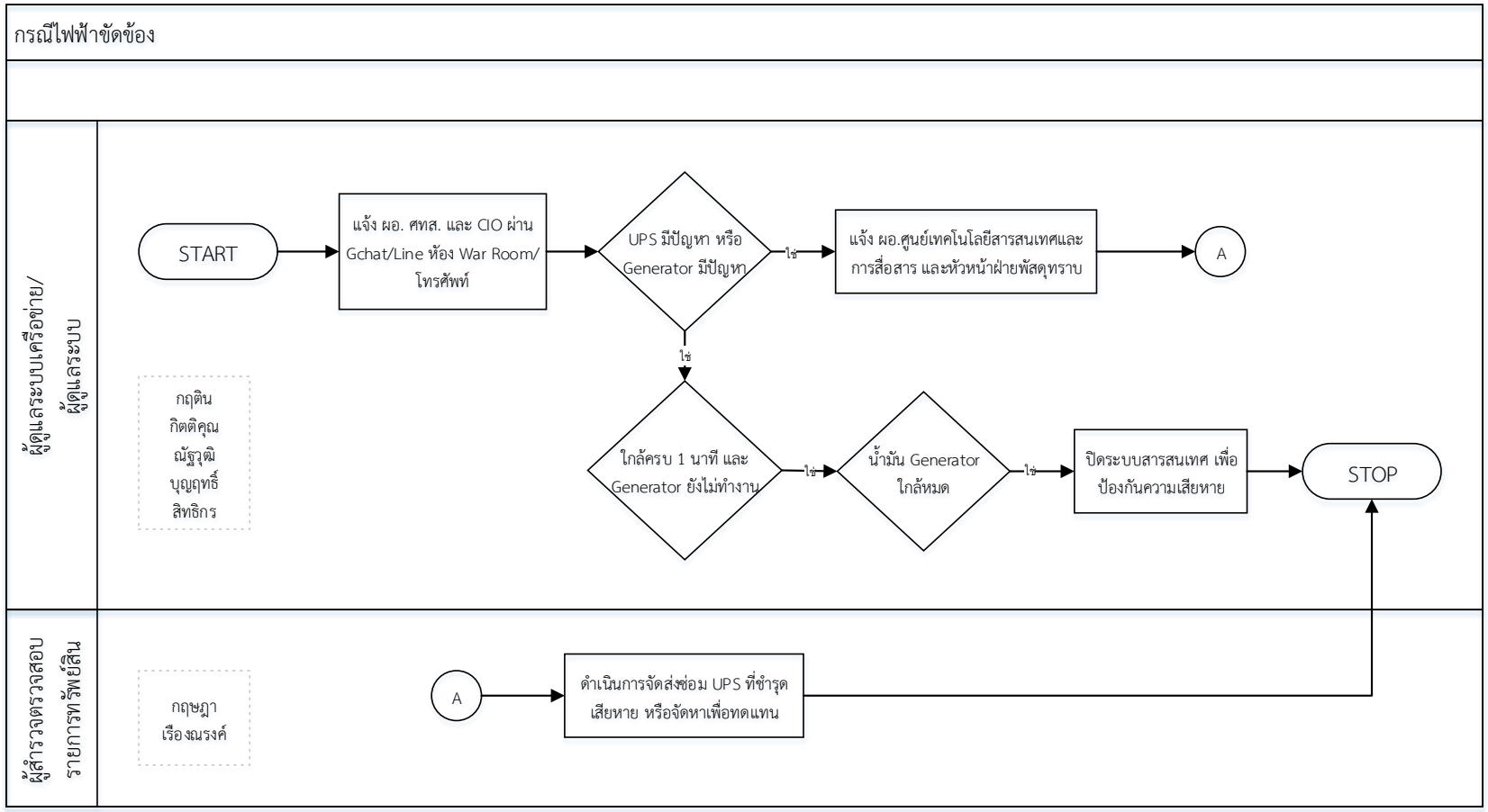
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



๔.๑.๕ กรณีไฟฟ้าขัดข้อง

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- ระบบฐานข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ ๓๐ นาที โดยเมื่อไฟดับระบบ Generator จะทำงานภายใน ๑ นาที
- หากใกล้ครบ ๑ นาทีแล้ว ระบบ Generator ยังไม่ทำงาน ให้มีการแจ้งเตือนไปยังผู้อำนวยการศูนย์สารสนเทศ เพื่อประสานไปยังหัวหน้าฝ่ายพัสดุ เพื่อตรวจสอบระบบ Generator
- หากระบบ Generator ทำงานแล้วให้แจ้งหัวหน้าฝ่ายพัสดุส่งเจ้าหน้าที่ตรวจสอบน้ำมัน
- หากกรณีน้ำมันของระบบ Generator ใกล้หมด ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

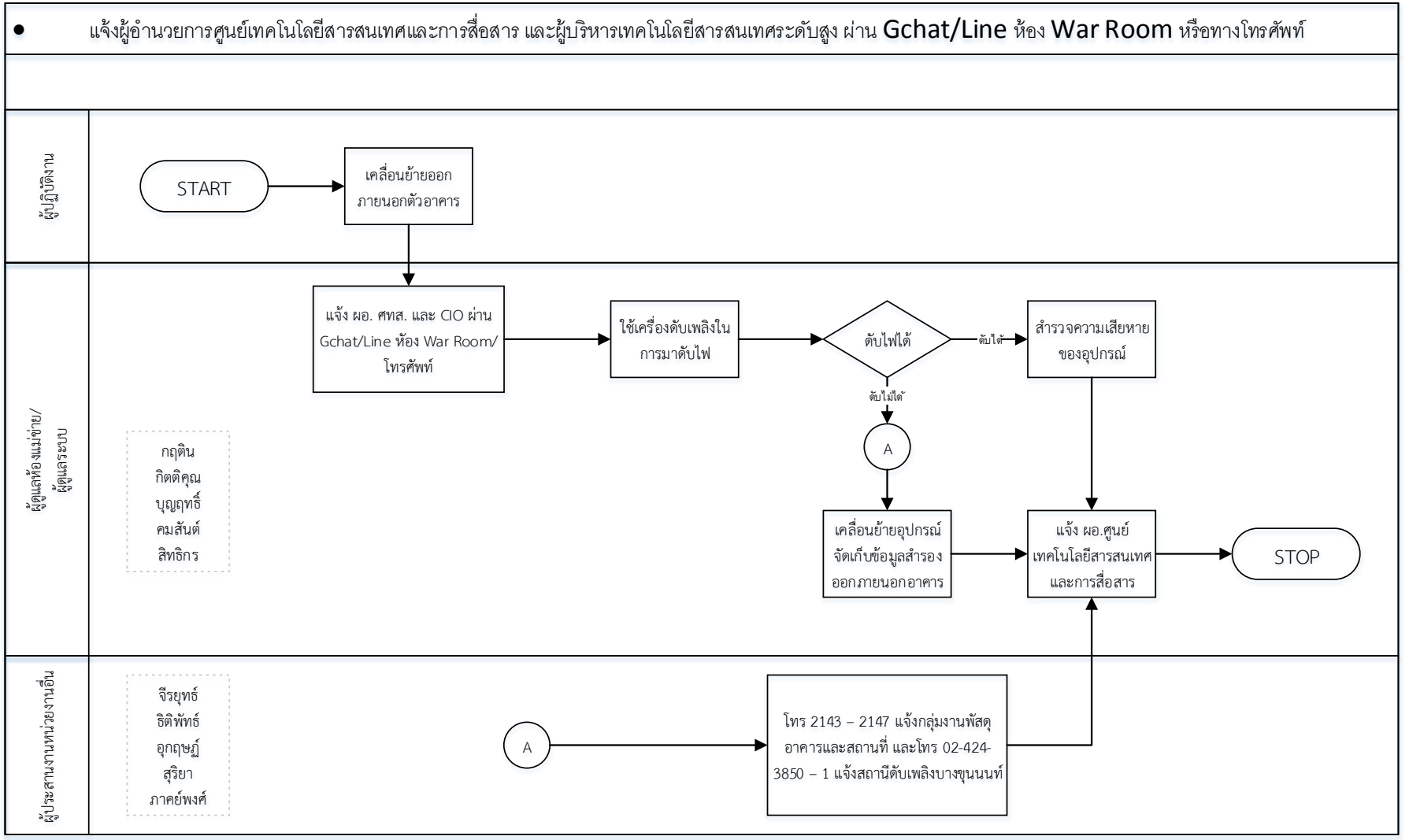

กรณีไฟฟ้าขัดข้อง
ผู้ดูแลระบบเครือข่าย/ ผู้ดูแลระบบ
START
แจ้ง ผอ. ศทส. และ CIO ผ่าน Gchat/Line ห้อง War Room/ โทรศัพท์
UPS มีปัญหา หรือ Generator มีปัญหา
ใช่
แจ้ง ผอ.ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และหัวหน้าฝ่ายพัสดุทราบ
A
ใช่
กฤติน กิตติคุณ ณัฐวุฒิ บุญฤทธิ์ สิทธิกร
ใกล้ครบ 1 นาที และ Generator ยังไม่ทำงาน
ใช่
น้ำมัน Generator ใกล้หมด
ใช่
ปิดระบบสารสนเทศ เพื่อป้องกันความเสียหาย
STOP
ผู้สำรวจตรวจสอบรายการทรัพย์สิน
กฤษฎา เรืองณรงค์
A
ดำเนินการจัดส่งซ่อม UPS ที่ชำรุดเสียหาย หรือจัดหาเพื่อทดแทน

๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

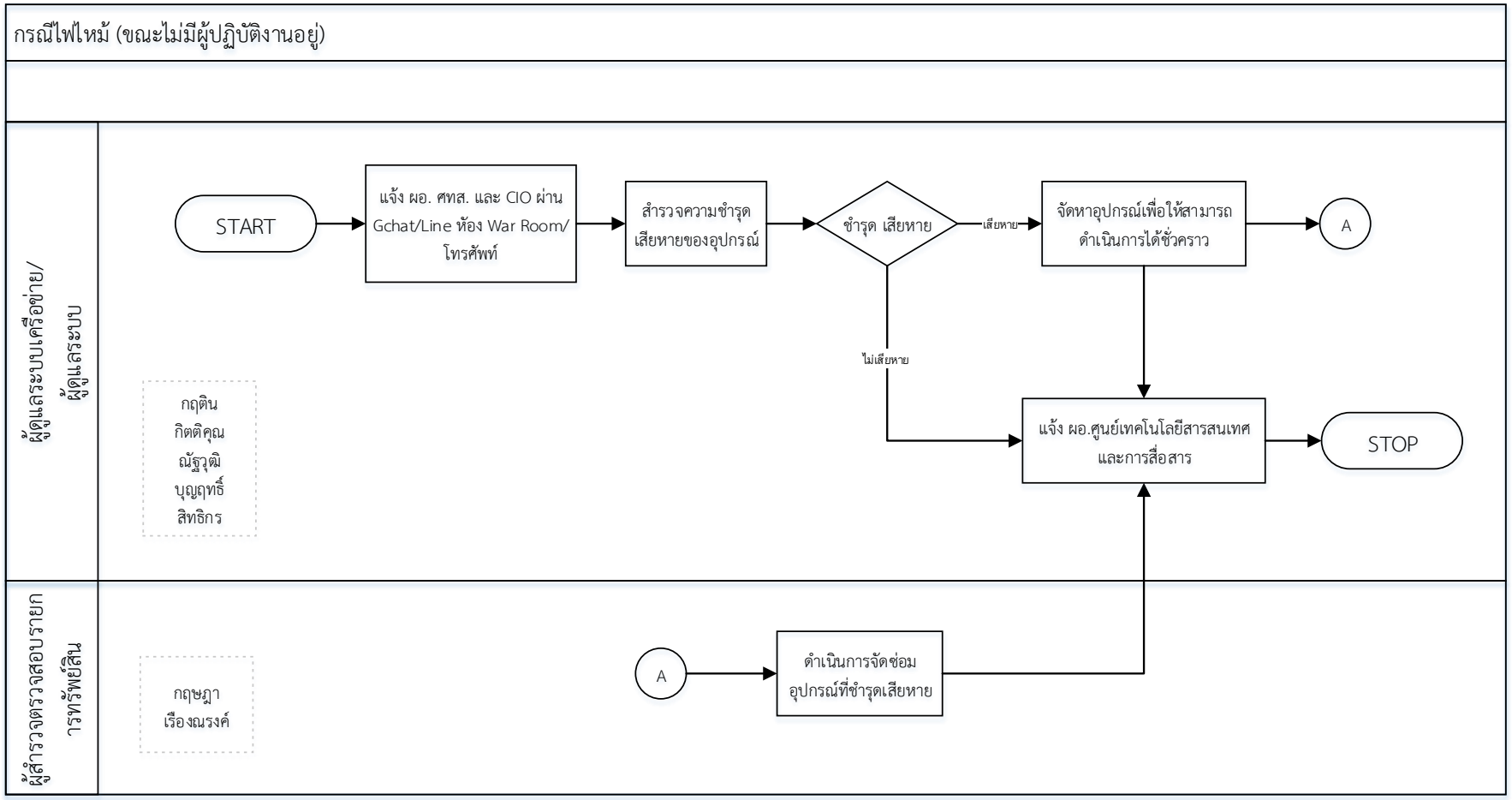
๔.๒.๑ กรณีไฟไหม้

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งฝ่ายพัสดุ กองบริหารการคลัง ที่ดูแลอาคารและสถานที่และยานพาหนะทันที ที่เบอร์ ๒๑๔๓ ถึง ๒๑๔๗ และโทรแจ้งสถานีดับเพลิง บางขุนนนท์ ที่เบอร์ ๐๒ ๔๒๔-๓๘๕๐-๑
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๒ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



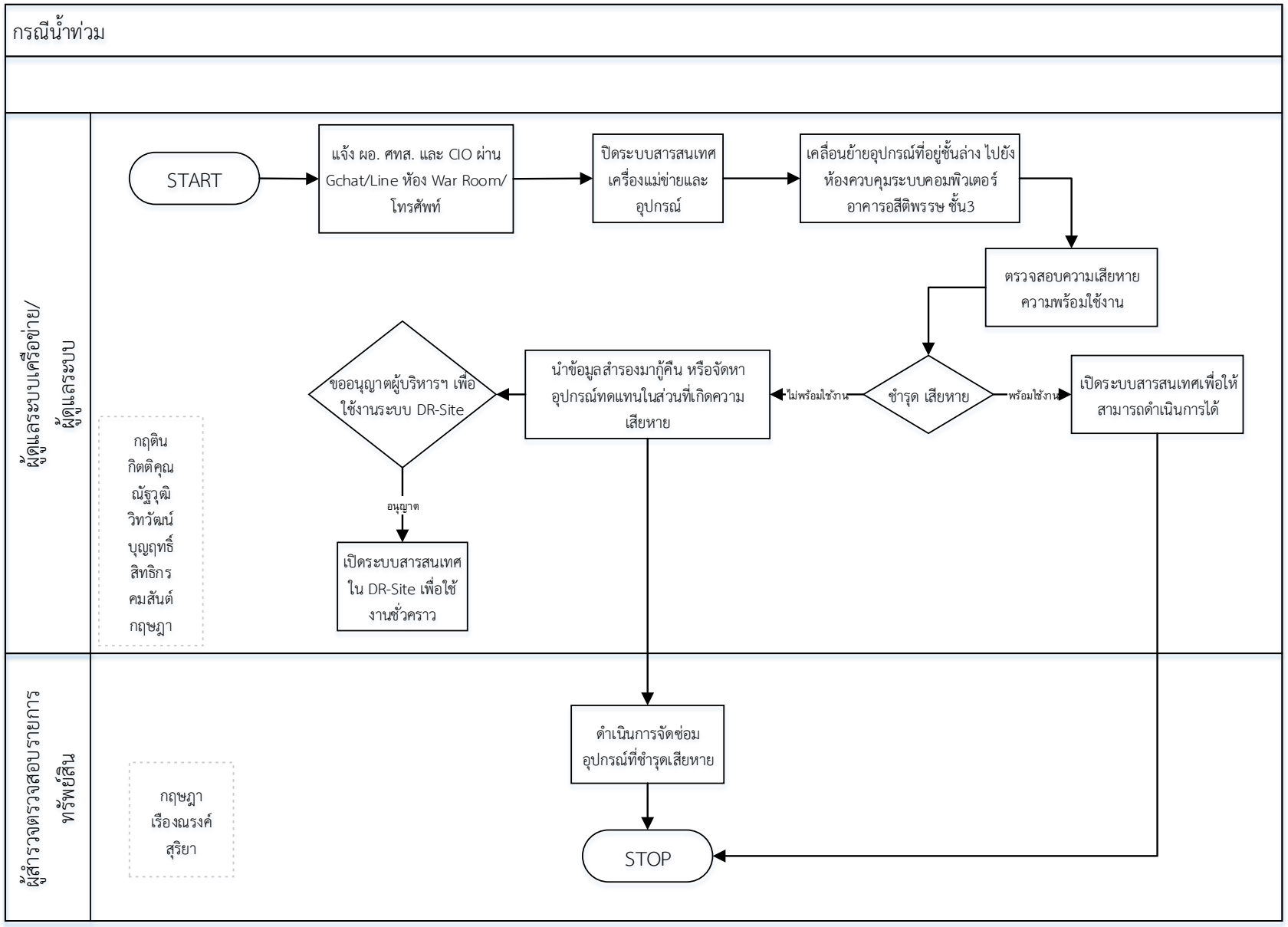
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



๔.๒.๒ กรณีน้ำท่วม

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายเคลื่อนย้ายอุปกรณ์ที่อยู่ชั้นล่างไปยังห้องควบคุมระบบคอมพิวเตอร์อาคารอสีติพรรษ ชั้น ๓
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย หรือระหว่างรอแก้ไขอุปกรณ์ ให้ขออนุญาตผู้บริหาร เพื่อย้ายระบบไปยัง Dr-site ที่กระทรวงยุติธรรม
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

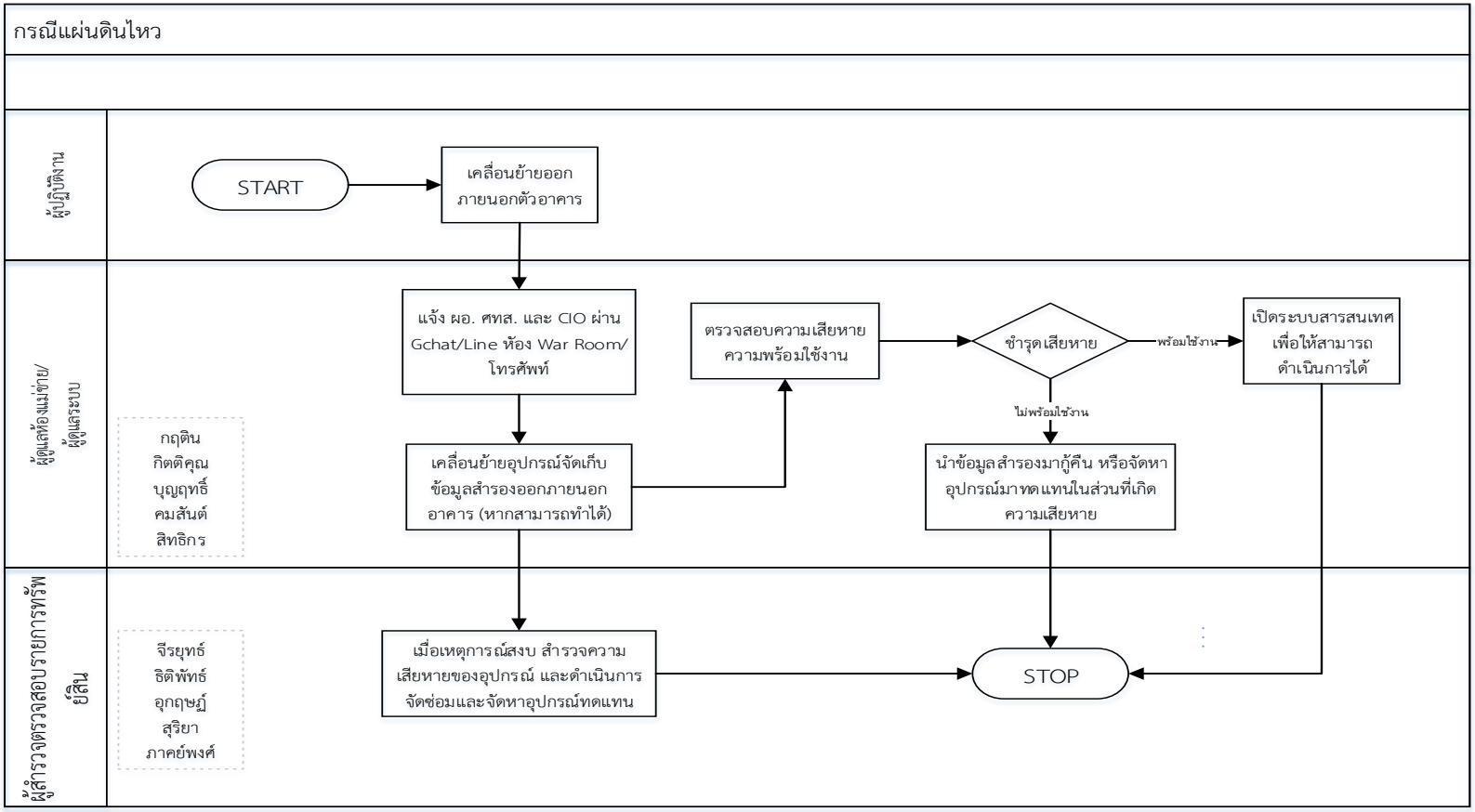
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม


กรณีน้ำท่วม
ผู้ดูแลระบบเครือข่าย/ผู้ดูแลระบบ
START
แจ้ง ผอ. ศทส. และ CIO ผ่าน Gchat/Line ห้อง War Room/ โทรศัพท์
ปิดระบบสารสนเทศ เครื่องแม่ข่ายและ อุปกรณ์
เคลื่อนย้ายอุปกรณ์ที่อยู่ชั้นล่าง ไปยัง ห้องควบคุมระบบคอมพิวเตอร์ อาคารอสีติพรรษ ชั้น3
ตรวจสอบความเสียหาย ความพร้อมใช้งาน
ชำรุด เสียหาย
ไม่พร้อมใช้งาน
พร้อมใช้งาน
นำข้อมูลสำรองมากู้คืน หรือจัดหา อุปกรณ์ทดแทนในส่วนที่เกิดความ เสียหาย
เปิดระบบสารสนเทศเพื่อให้ สามารถดำเนินการได้
ขออนุญาตผู้บริหารฯ เพื่อ ใช้งานระบบ DR-Site
อนุญาต
เปิดระบบสารสนเทศ ใน DR-Site เพื่อใช้ งานชั่วคราว
กฤติน กิตติคุณ ณัฐวุฒิ วิทวัฒน์ บุญฤทธิ์ สิทธิกร คมสันต์ กฤษฎา
ผู้สำรวจตรวจสอบรายการทรัพย์สิน
ดำเนินการจัดซ่อม อุปกรณ์ที่ชำรุดเสียหาย
STOP
กฤษฎา เรืองณรงค์ สุริยา

๔.๒.๓ กรณีแผ่นดินไหว

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

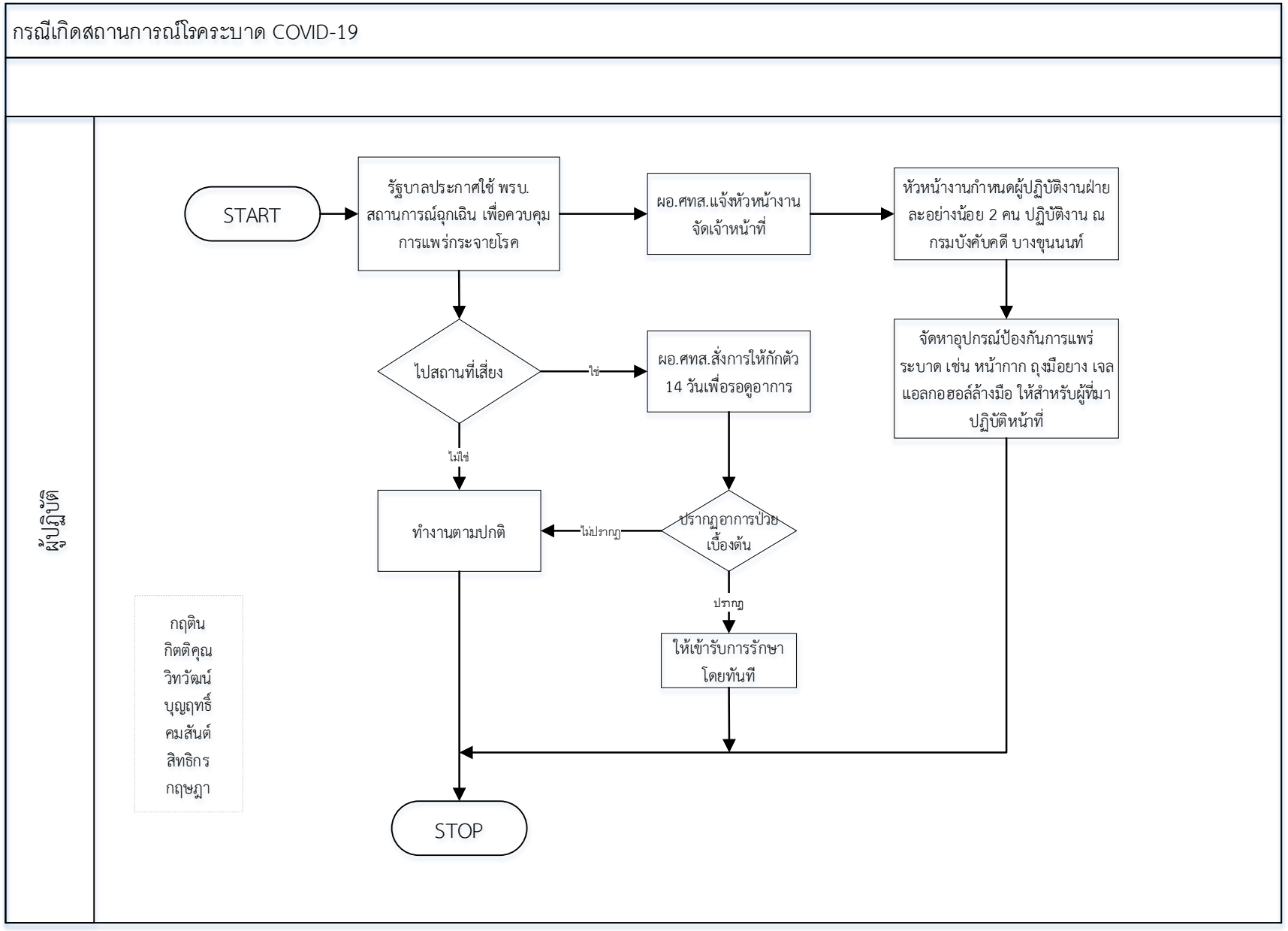

กรณีแผ่นดินไหว
ผู้ปฏิบัติงาน
START
เคลื่อนย้ายออก ภายนอกตัวอาคาร
ผู้ดูแลห้องแม่ข่าย/ ผู้ดูแลระบบ
แจ้ง ผอ. ศทส. และ CIO ผ่าน Gchat/Line ห้อง War Room/ โทรศัพท์
ตรวจสอบความเสียหาย ความพร้อมใช้งาน
ชำรุดเสียหาย
พร้อมใช้งาน
เปิดระบบสารสนเทศ เพื่อให้สามารถ ดำเนินการได้
ไม่พร้อมใช้งาน
กฤติน
กิตติคุณ
บุญฤทธิ์
คมสันต์
สิทธิกร
เคลื่อนย้ายอุปกรณ์จัดเก็บ ข้อมูลสำรองออกภายนอก อาคาร (หากสามารถทำได้)
นำข้อมูลสำรองมากู้คืน หรือจัดหา อุปกรณ์มาทดแทนในส่วนที่เกิด ความเสียหาย
ผู้สำรวจตรวจสอบรายการทรัพย์สิน
จีรยุทธ์
ธิติพัทธ์
อุกฤษฏ์
สุริยา
ภาคย์พงศ์
เมื่อเหตุการณ์สงบ สำรวจความ เสียหายของอุปกรณ์ และดำเนินการ จัดซ่อมและจัดหาอุปกรณ์ทดแทน
STOP

๔.๒.๔ กรณีเกิดสถานการณ์โรคระบาด COVID-๑๙

- หลีกเลี่ยงการเดินทางไปยังพื้นที่เสี่ยง
- ตรวจสอบการเดินทางไปนอกสถานที่ของเจ้าหน้าที่ศูนย์ฯ
- หากพบว่าเจ้าหน้าที่ได้เดินทางไปยังสถานที่ที่มีข่าวการระบาดของโรค ให้แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์ ให้มีคำสั่งกักตัว ณ ที่พักอาศัยเป็นเวลา ๑๔ วันเพื่อรอดูอาการ
- กรณีไม่พบอาการผิดปกติใด ๆ เมื่อครบกำหนดเวลาแล้ว ให้เจ้าหน้าที่ผู้นั้นกลับมาทำงานตามปกติ
- กรณีมีอาการผิดปกติเกิดขึ้น เช่น มีไข้สูงอุณหภูมิเกินกว่า ๓๗ องศาขึ้นไป ไอมีเสมหะนานเกิน ๑ สัปดาห์ หายใจติดขัดไม่สะดวก มีอาการปอดอักเสบหรือปอดบวม ให้เจ้าหน้าที่เข้ารับการรักษาในโรงพยาบาลทันที
- ติดตามข่าวการระบาดของโรคอย่างใกล้ชิด

หากมีการประกาศอย่างเป็นทางการแล้วว่ามีการระบาดเกิดขึ้น

- จัดสรรเจ้าหน้าที่ผู้รับผิดชอบฝ่ายละ ๒ คนเป็นอย่างน้อย ให้มาปฏิบัติงาน ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อเป็นผู้ประสานงานหลักในเรื่องต่าง ๆ เพื่อลดความเสี่ยงในการแพร่ระบาดของโรค
- ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะจัดหาอุปกรณ์ป้องกันการแพร่ระบาด เช่น หน้ากาก ถุงมือยาง เจลแอลกอฮอล์ล้างมือ ให้สำหรับผู้ที่มาปฏิบัติหน้าที่
- เจ้าหน้าที่ผู้มาปฏิบัติงานให้ปฏิบัติตามแนวทางการป้องกันการแพร่กระจายเชื้ออย่างเคร่งครัด

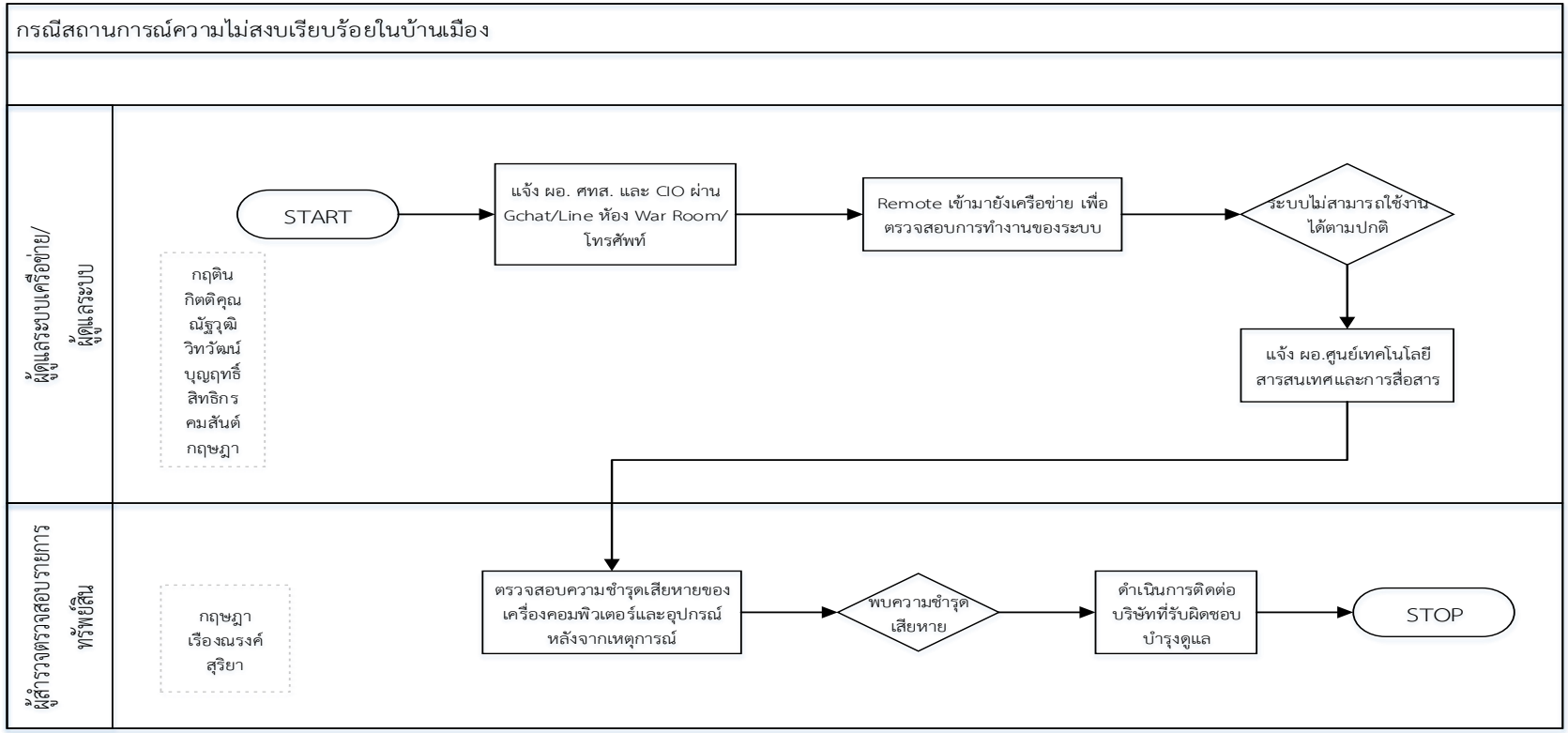

กรณีเกิดสถานการณ์โรคระบาด COVID-19
ผู้ปฏิบัติ
START
รัฐบาลประกาศใช้ พรบ. สถานการณ์ฉุกเฉิน เพื่อควบคุมการแพร่กระจายโรค
ผอ.ศทส.แจ้งหัวหน้างานจัดเจ้าหน้าที่
หัวหน้างานกำหนดผู้ปฏิบัติงานฝ่ายละอย่างน้อย 2 คน ปฏิบัติงาน ณ กรมบังคับคดี บางขุนนนท์
ไปสถานที่เสี่ยง
ใช่
ผอ.ศทส.สั่งการให้กักตัว 14 วันเพื่อรอดูอาการ
จัดหาอุปกรณ์ป้องกันการแพร่ระบาด เช่น หน้ากาก ถุงมือยาง เจลแอลกอฮอล์ล้างมือ ให้สำหรับผู้ที่มาปฏิบัติหน้าที่
ไม่ใช่
ทำงานตามปกติ
ไม่ปรากฏ
ปรากฏอาการป่วยเบื้องต้น
ปรากฏ
ให้เข้ารับการรักษาโดยทันที
STOP
กฤติน
กิตติคุณ
วิทวัฒน์
บุญฤทธิ์
คมสันต์
สิทธิกร
กฤษฎา

๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๔.๓.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการศูนย์สารสนเทศทราบ
- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

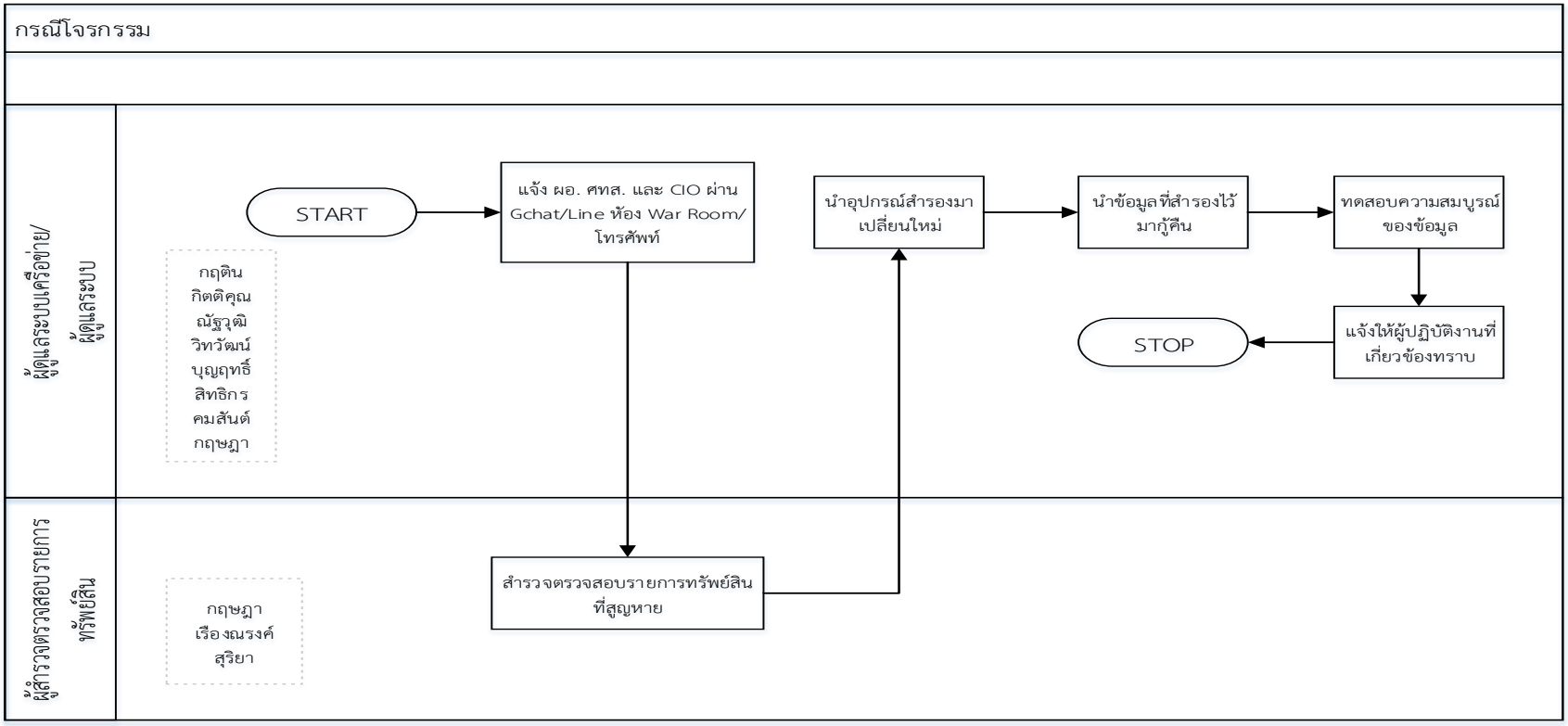


๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

๔.๔.๑ กรณีโจรกรรม

- แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผ่าน Gchat/Line ห้อง War Room หรือทางโทรศัพท์
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆได้โดยเร็ว

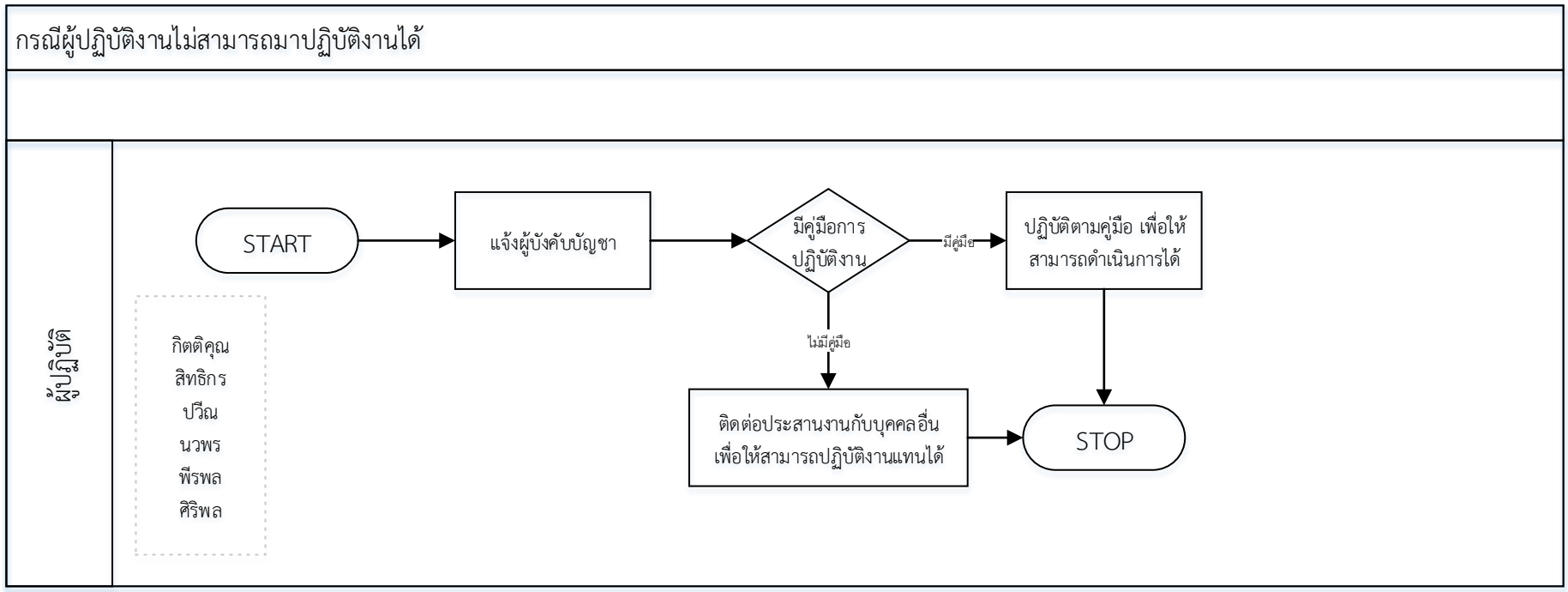
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



๔.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



๕. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑ รองอธิบดีกรมบังคับคดี ที่ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ประจำกรม

๑.๒ นางสาวอรอุมา เก่งทางดี ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

๒. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

๒.๑ นายกฤติน สุขสด นักวิชาการคอมพิวเตอร์ชำนาญการ
๒.๒ นายกิตติคุณ จาดเจริญ นักวิชาการคอมพิวเตอร์ชำนาญการ
๒.๓ นายวิทวัฒน์ ศรีไพร นักวิชาการคอมพิวเตอร์ชำนาญการ
๒.๔ นายณัฐวุฒิ แป้นน้อย นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๒.๕ นายสิทธิกร ศิวะอางกูร เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๒.๖ นายบุญฤทธิ์ ฮอนกัม เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๒.๗ นายคมสันต์ รอดสำราญ เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๒.๘ นายปวีณ แตงสมุทร นักวิชาการคอมพิวเตอร์
๒.๙ นายพีรพล ธานี นักวิชาการคอมพิวเตอร์
๒.๑๐ นายศิริพล อภิรักษ์โภไคย เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๒.๑๑ นายอดิศร สินก่อเกียรติ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์

๓. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๓.๑ นายจีรยุทธ นาคหล่อ นักวิชาการคอมพิวเตอร์
๓.๒ นายธิติพัทธ์ ล้ำเลิศ นักวิชาการคอมพิวเตอร์
๓.๓ นายอุกฤษฏ์ ชัยศรี นักวิชาการคอมพิวเตอร์
๓.๔ นายสุริยา ลี้พานุวงศ์ นักวิชาการคอมพิวเตอร์
๓.๕ นายภาคย์พงศ์ แย้มชมสวน นักจัดการงานทั่วไป

๔. รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน ได้แก่

๔.๑ นายกฤติน สุขสด นักวิชาการคอมพิวเตอร์ชำนาญการ
๔.๒ นายกิตติคุณ จาดเจริญ นักวิชาการคอมพิวเตอร์ชำนาญการ
๔.๓ นายวิทวัฒน์ ศรีไพร นักวิชาการคอมพิวเตอร์ชำนาญการ
๔.๔ นายณัฐวุฒิ แป้นน้อย นักวิชาการคอมพิวเตอร์ปฏิบัติการ
๔.๕ นายสิทธิกร ศิวะอางกูร เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๖ นายบุญฤทธิ์ ฮอนกัม เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๗ นายคมสันต์ รอดสำราญ เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๘ นายกฤษฎา เส็งเล็ก นักวิชาการคอมพิวเตอร์
๔.๙ นายจีรยุทธ นาคหล่อ นักวิชาการคอมพิวเตอร์
๔.๑๐ นายธิติพัทธ์ ล้ำเลิศ นักวิชาการคอมพิวเตอร์
๔.๑๑ นายอุกฤษฏ์ ชัยศรี นักวิชาการคอมพิวเตอร์

๔.๑๒ นางสาวนวพร ชัยสุขสังข์ นักวิชาการคอมพิวเตอร์
๔.๑๓ นายปวีณ แตงสมุทร นักวิชาการคอมพิวเตอร์
๔.๑๔ นางสาววิไลลักษณ์ คำสกุล นักวิชาการคอมพิวเตอร์
๔.๑๕ นายสุริยา ลี้พานุวงศ์ นักวิชาการคอมพิวเตอร์
๔.๑๖ นายศิริพล อภิรักษ์โภไคย เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๑๗ นายธีรชัย วงศ์อนุสรณ์ นักวิชาการคอมพิวเตอร์
๔.๑๘ นายพีรพล ธานี นักวิชาการคอมพิวเตอร์
๔.๑๙ นายเรืองณรงค์ แสนสุทธิ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๒๐ นายอดิศร สินก่อเกียรติ์ เจ้าหน้าที่ระบบงานคอมพิวเตอร์
๔.๒๑ นางสาวมนตรากาล สดรัมย์ นักวิชาการคอมพิวเตอร์
๔.๒๒ นางสาวพรรณราย ปวนปินตา นักวิชาการคอมพิวเตอร์
๔.๒๓ นายสุริยะ วิภาศินนท์ นักวิชาการคอมพิวเตอร์
๔.๒๔ นางสาวณัฏฐกุลฉัตร จุ้ยประเสริฐ นักวิชาการคอมพิวเตอร์
๔.๒๕ นายภาคย์พงศ์ แย้มชมสวน นักจัดการงานทั่วไป
๔.๒๖ นางปัฐน์ธนวันต์ อยู่สนิท เจ้าพนักงานธุรการปฏิบัติงาน
๔.๒๗ นางสาวนงค์เยาว์ โฮทองหลาง เจ้าหน้าที่ธุรการ
๔.๒๘ นางสาวชไมพร แจ้งไธสง เจ้าพนักงานธุรการ
๔.๒๙ นางสาวรัญชนา เข็มทอง เจ้าพนักงานธุรการ

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ของ กรมบังคับคดี เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(นางสาวปนัดดา สินธุวิสุทธ์)
รองอธิบดีกรมบังคับคดี
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง