สารบัญ

หน้า

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

1. บทนำ

ปัจจุบัน มหาวิทยาลัยได้นำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้ งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์การ การบริหารจัดการองค์การ และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นองค์การจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

สำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏนครราชสีมาได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ
3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของมหาวิทยาลัย

3. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของสำนักคอมพิวเตอร์ มหาวิทยาลัยราชภัฏนครราชสีมามีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงต่างด้านสารสนเทศ พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือ และอุปกรณ์ อาจถูกโจมตีจากไวรัสหรือโปแกรมประสงค์ร้าย การถูกก่อกวนจาก Hacker การถูกเจาะทำลายระบบจาก Cracker เป็นต้น

2. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

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

4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยต่อไป

4. แผนรองรับสถานการณ์ฉุกเฉิน

4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

4.1.1 กรณีการป้องกันไวรัสล้มเหลว

1 กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

2 วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

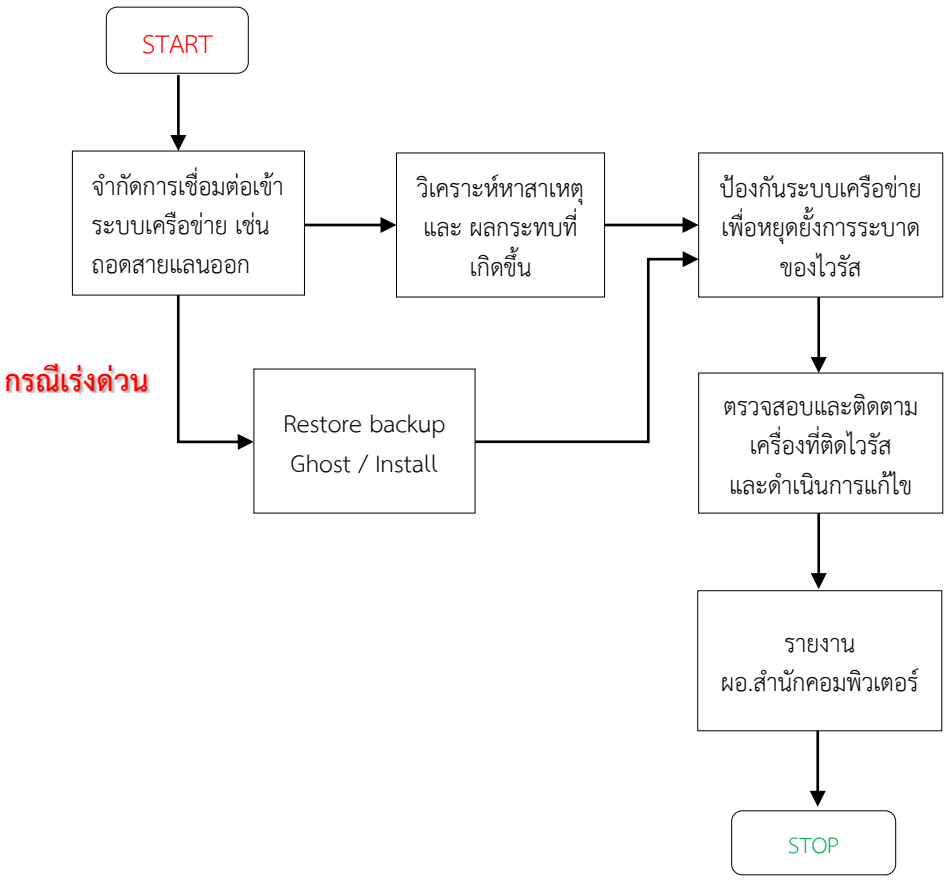
3 ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

4 ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

5 กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ทราบหรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ สำนักคอมพิวเตอร์จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว

ผู้ดำเนินการ ผู้ดูแลระบบเครือข่าย

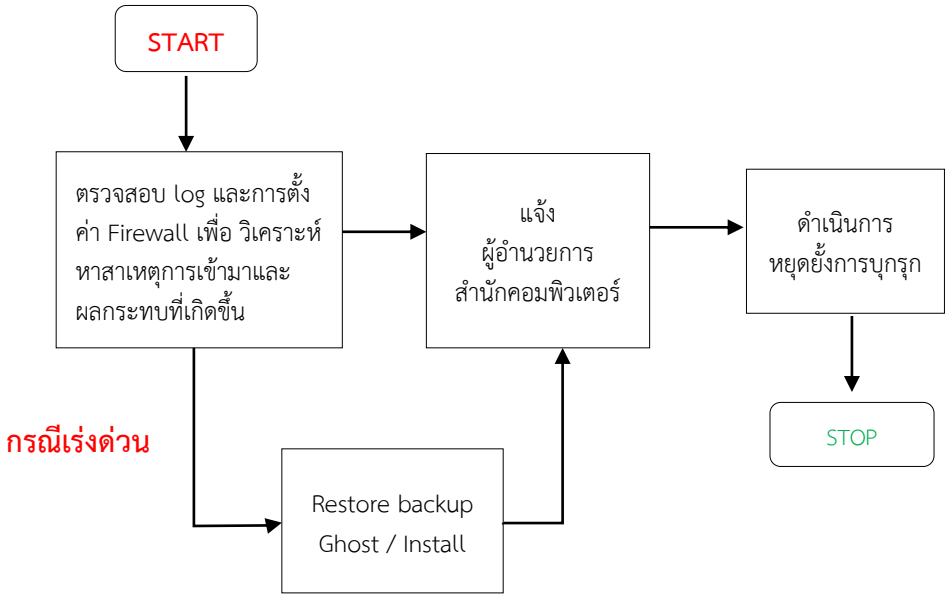


4.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

1 กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
2 ผู้ดูแลระบบแจ้งผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยด่วน
3 ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว

ผู้ดำเนินการ ผู้ดูแลระบบเครือข่าย

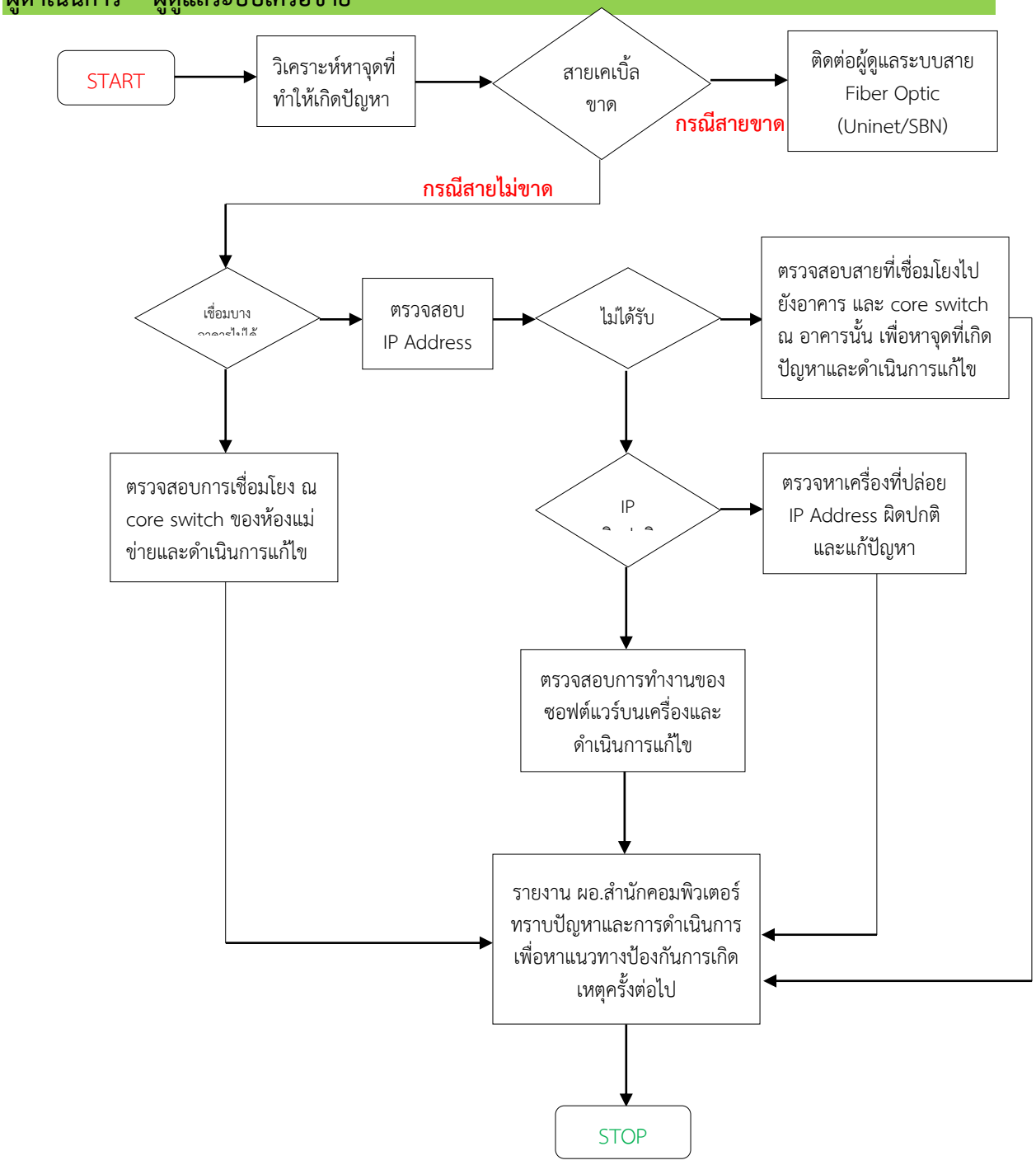


4.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

1 ดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
2 หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว
3 หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ switch ที่ติดตั้งอยู่ ณ อาคารนั้น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

ผู้ดำเนินการ ผู้ดูแลระบบเครือข่าย

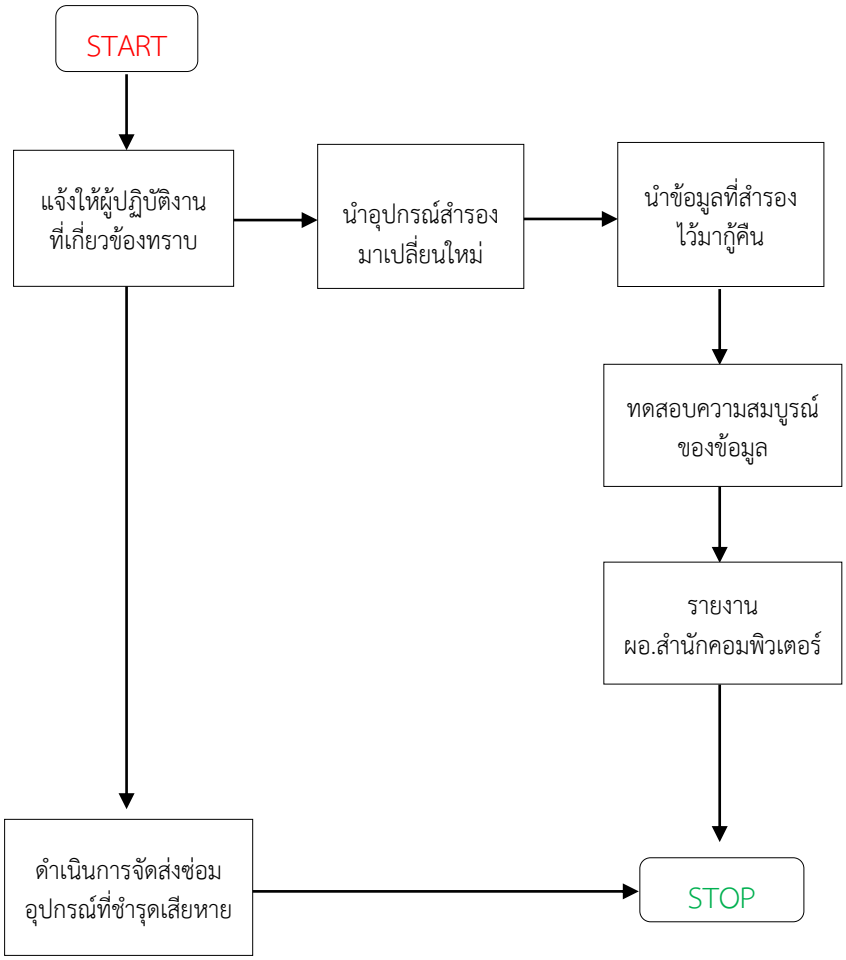


4.1.4 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

1 แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
2 รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
3 ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

ผู้ดำเนินการ ผู้ดูแลระบบสารสนเทศเพื่อการบริหาร



4.1.5 กรณีไฟฟ้าขัดข้อง

1 ระบบฐานข้อมูลสารสนเทศต้องมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 15 นาที

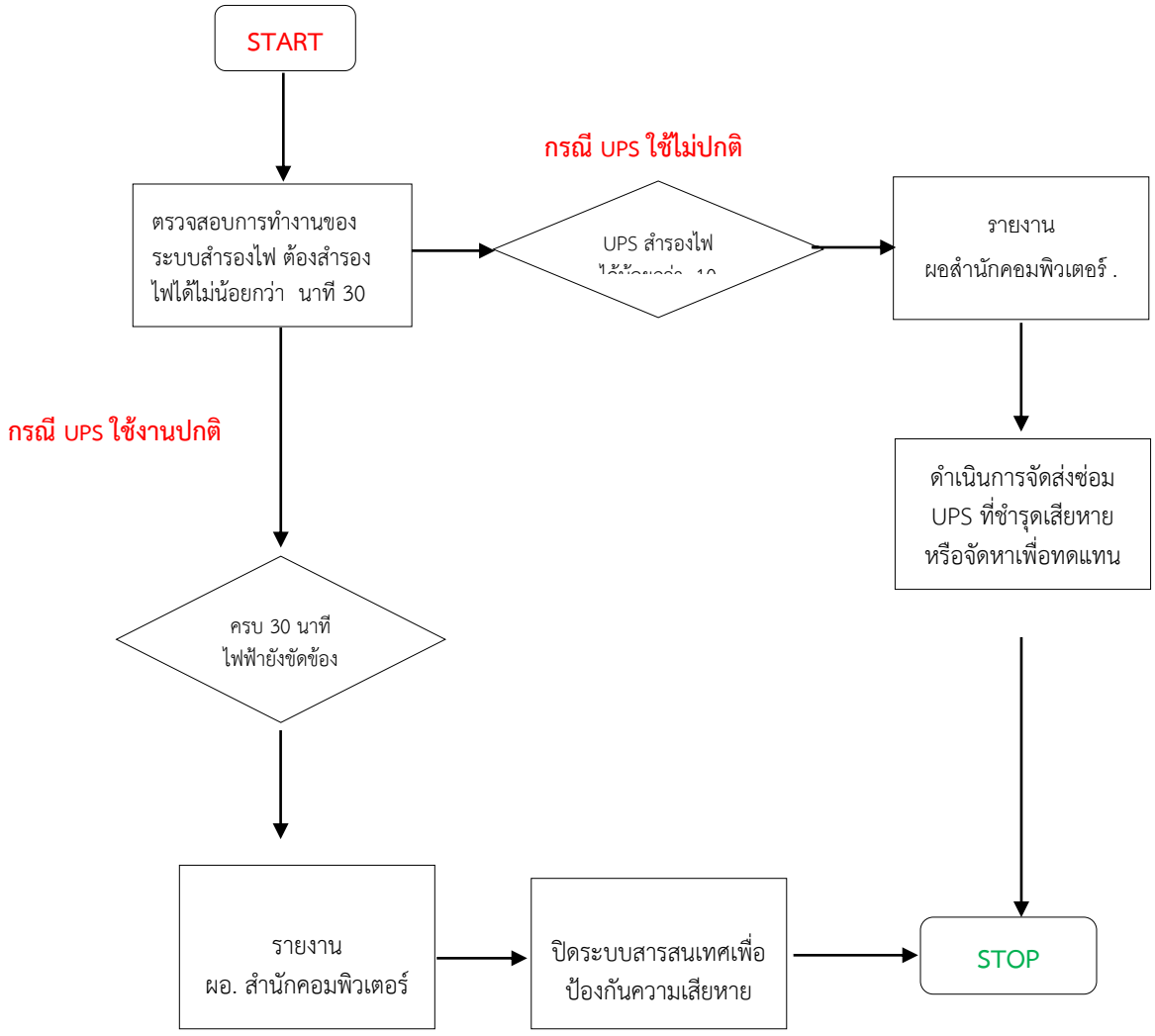
2 หากใกล้ครบ 15 นาทีแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งผู้อำนวยการสำนักคอมพิวเตอร์

3 ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย

4 หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง

ผู้ดำเนินการ ทุกกลุ่มงาน



4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

4.2.1 กรณีไฟไหม้

1 หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

2 หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกอาคาร ผู้ติดต่อประสานงานโทรแจ้ง

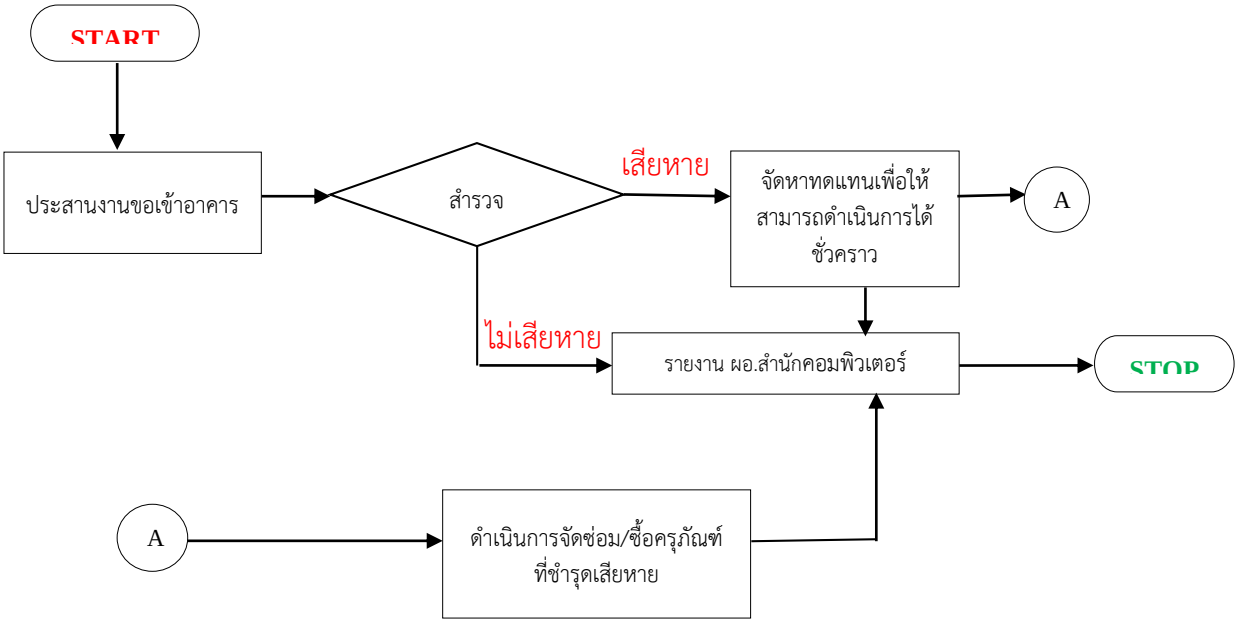
งานรักษาความปลอดภัย ที่เบอร์ 1617
งานอาคารและสถานที่ ที่เบอร์ 1611 และ 1661
งานยานพาหนะ ที่เบอร์ 1613 และ 1624
โทรแจ้งสถานีดับเพลิง ที่เบอร์ 0-4424-2222 (เมืองนครราชสีมา)
0-4492-2585 (บ้านเกาะ)

3 หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

4 อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

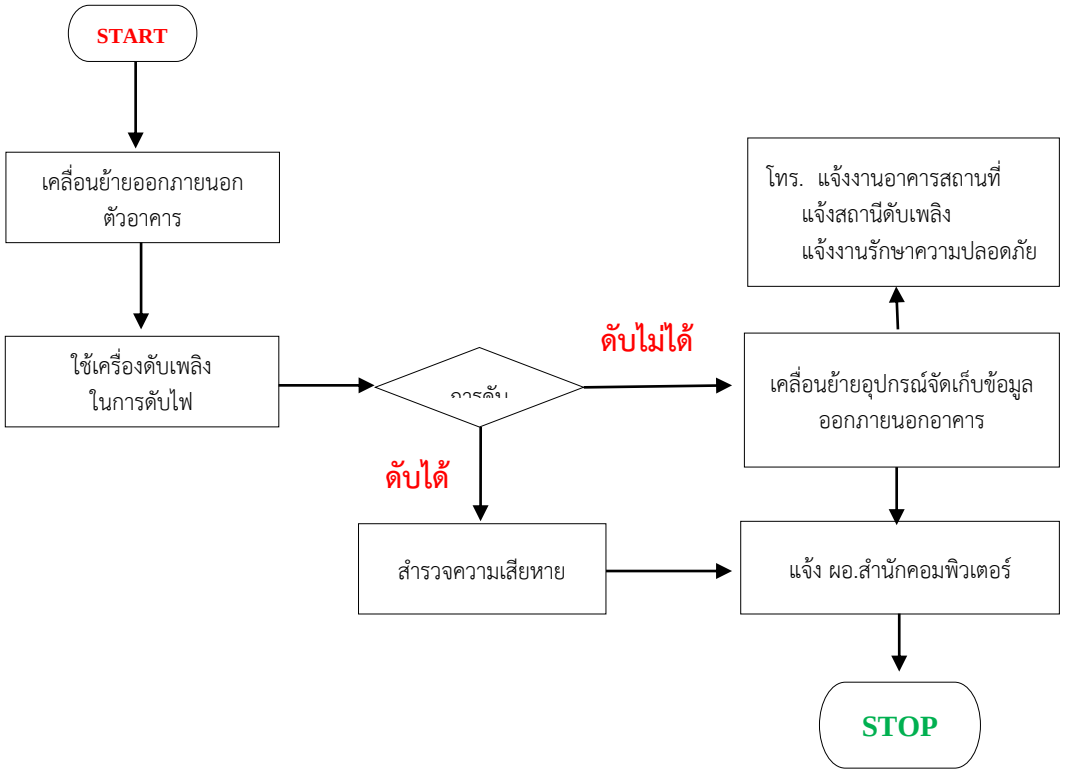
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)

ผู้ดำเนินการ ทุกกลุ่มงาน



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)

ผู้ดำเนินการ ทุกกลุ่มงาน

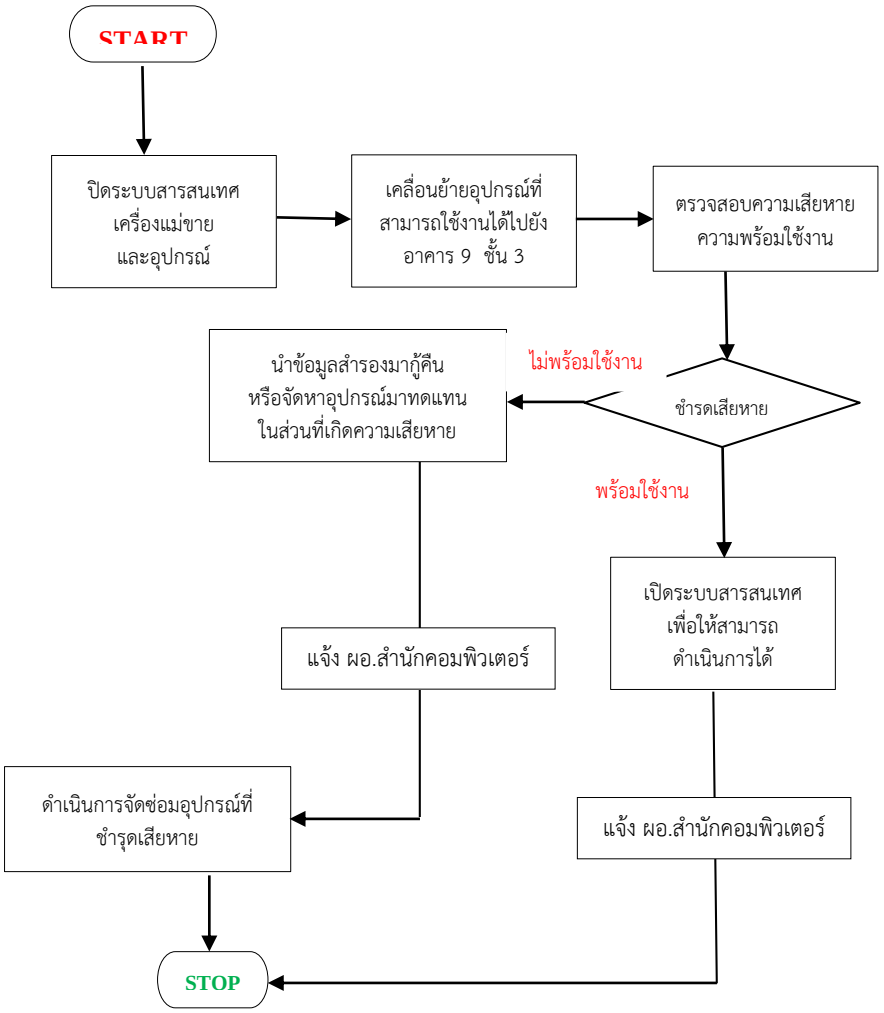


4.2.2 กรณีน้ำท่วม

1 ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ชั้น 3 อาคาร 9
2 ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
3 ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุดเสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม

ผู้ดำเนินการ ทุกกลุ่มงาน

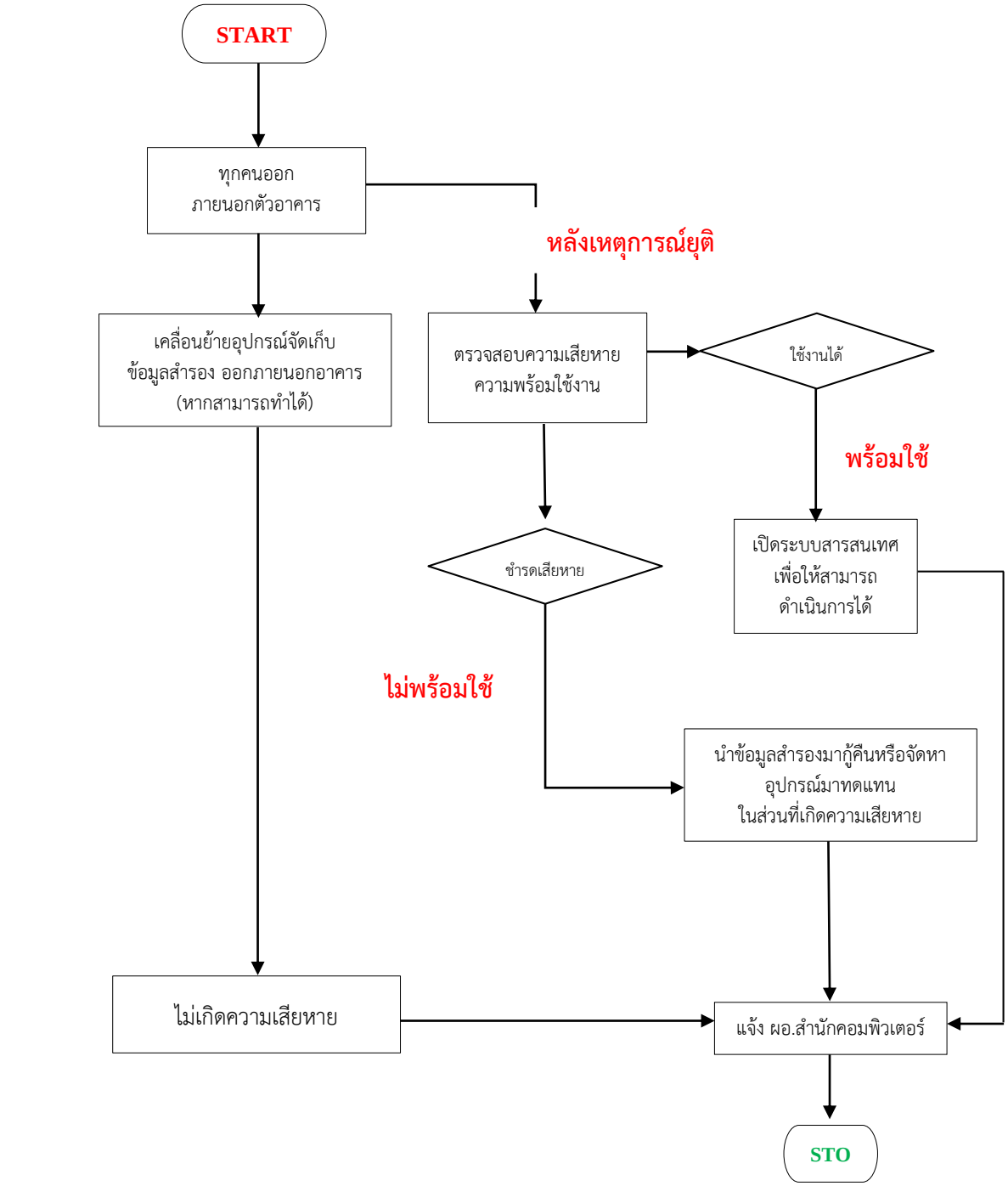


4.2.3 กรณีแผ่นดินไหว

1 ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
2 ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
3 เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว

ผู้ดำเนินการ ทุกกลุ่มงาน



4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

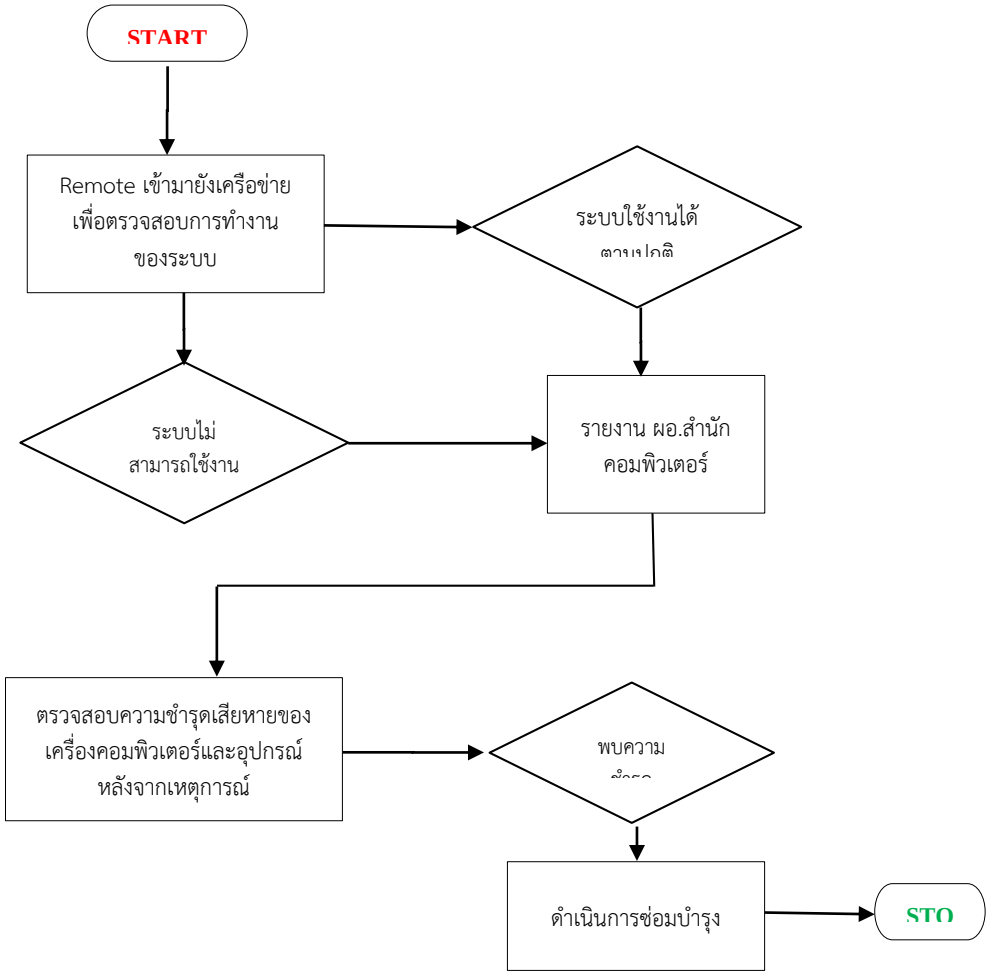
4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อย

กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อย เช่น การก่อการร้าย การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบต้อง Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งผู้อำนวยการสำนักคอมพิวเตอร์ทราบ

หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดความไม่สงบเรียบร้อย

ผู้ดำเนินการ ทุกกลุ่มงาน



4.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

4.4.1 กรณีโจรกรรม

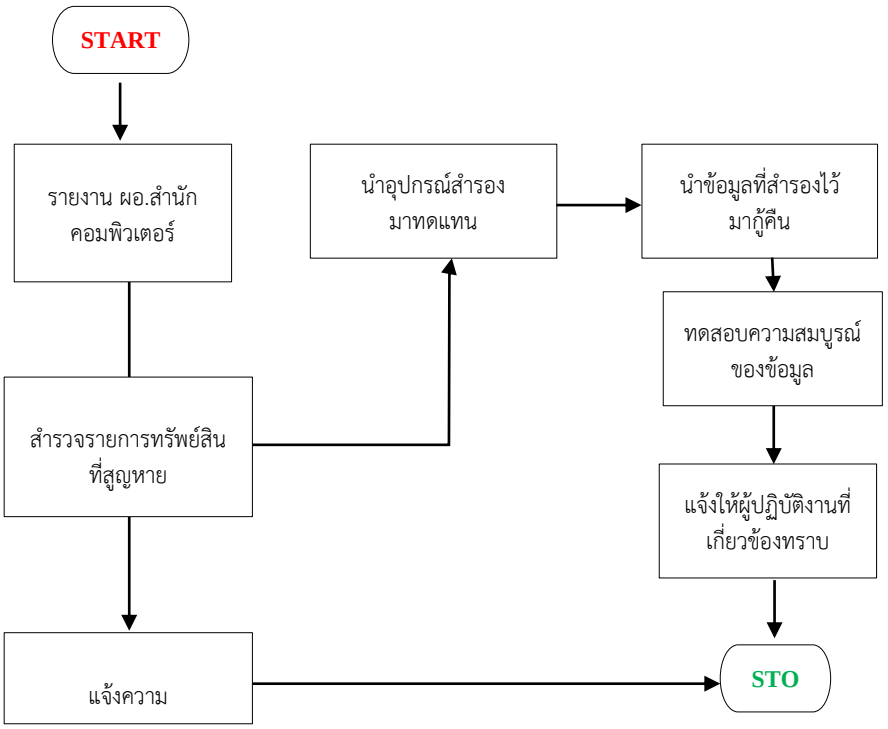
1 ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

2 สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

3 ผู้ดูแลระบบบริบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

ผู้ดำเนินการ ทุกกลุ่มงาน



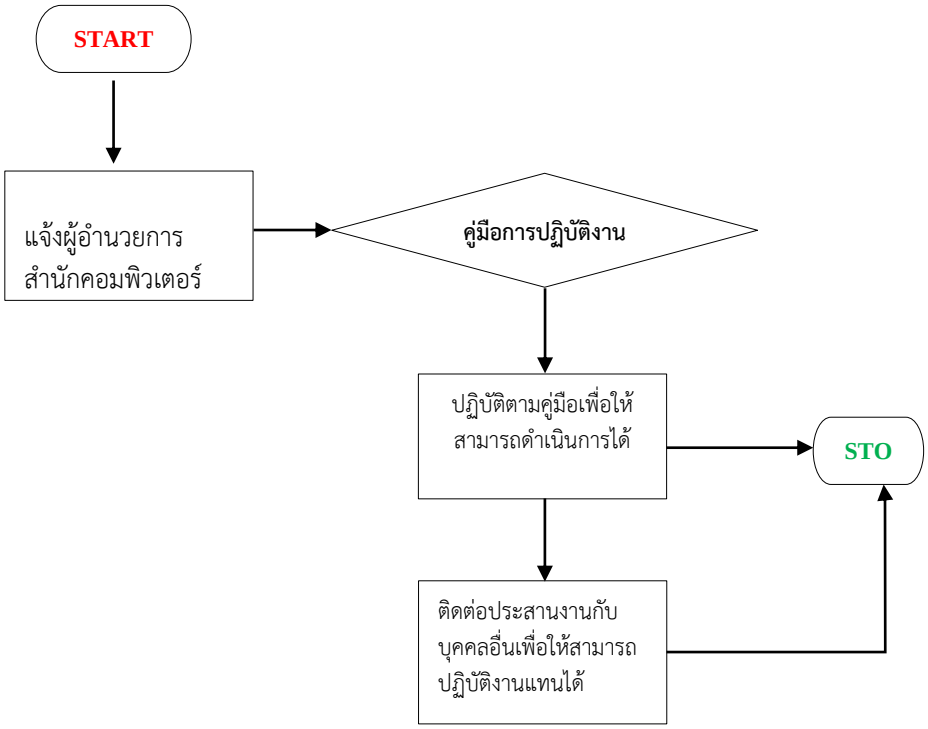
4.4.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

1 แจ้งผู้บังคับบัญชาทราบ

2 ปฏิบัติตามคู่มือการดำเนินการ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

ผู้ดำเนินการ ทุกกลุ่มงาน



5. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

1 รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

1.1. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

1.2. ผศ.เปรมวิทย์ ท่อแก้ว ผู้อำนวยการสำนักคอมพิวเตอร์

2. งานบริหารทั่วไป

2.1 ดร.สิริลักษณ์ โปร่งสันเทียะ รองผู้อำนวยการสำนักคอมพิวเตอร์

2.1 ผู้ดูแลงานบริหารสำนักงาน รับผิดชอบงานการทำรายงานผลการทำงาน การประกันคุณภาพ และตรวจสอบรายการสินทรัพย์ ได้แก่

1 ผศ.ศันสนีย์ เลี้ยงพานิชย์ หัวหน้าสำนักงานสำนักผู้อำนวยการสำนักคอมพิวเตอร์

2 นางธัญทิพย์ พรหมมณี ผู้ปฏิบัติงานบริหาร

3 นายปริญญา กาจสันเทียะ นักวิชาการคอมพิวเตอร์

3 กลุ่มงานฝึกอบรมและบริการ

3.1 ผศ.ดร.สายสุนีย์ จับโจร รองผู้อำนวยการสำนักคอมพิวเตอร์

3.2 ผู้ดูแลงานคอมพิวเตอร์กราฟิก รับผิดชอบงานคอมพิวเตอร์กราฟิก ได้แก่

1 นางสาวสมพิศ คำทองพะเนาว์ หัวหน้างานคอมพิวเตอร์กราฟิก

2 นายสราวุฒิ พงศ์ณัฐกรณ์ นักวิชาการช่างศิลป์

3.3 ผู้ดูแลงานฝึกอบรมและบริการวิชาการ รับผิดชอบงานงานฝึกอบรมและบริการวิชาการ ได้แก่

1 นายวีรพล ปุ้ยกระโทก หัวหน้างานฝึกอบรมและบริการวิชาการ

2 นางสาวรุ่งนภา สวัสดี นักวิชาการคอมพิวเตอร์

3 นายจตุรงค์ กอแก้ว นักวิชาการคอมพิวเตอร์

3.4 ผู้ดูแลงานห้องปฏิบัติการและซ่อมบำรุงคอมพิวเตอร์ รับผิดชอบห้องปฏิบัติการและซ่อมบำรุงคอมพิวเตอร์ ได้แก่

1 นายศราวุฒิ ผาละศรี นักวิชาการคอมพิวเตอร์

2 นายวัชรพล พิลาสมบัติ นักวิชาการคอมพิวเตอร์

3 นายจักรรวี แสงจันทร์ นักวิชาการคอมพิวเตอร์

4 กลุ่มงานพัฒนาระบบสารสนเทศและเครือข่าย

4.1 นายอเนก มหาสมุทร รองผู้อำนวยการสำนักคอมพิวเตอร์

4.2 ผู้ดูแลงานระบบเครือข่าย รับผิดชอบงานระบบเครือข่าย ได้แก่

1. นายอนุพงศ์ โพธิ หัวหน้างานระบบเครือข่าย

2. นายอภิเชฐ แปลสันเทียะ นักวิชาการคอมพิวเตอร์

4.3 ผู้ดูแลงานระบบสารสนเทศเพื่อการบริหาร รับผิดชอบงานสารสนเทศเพื่อการบริหาร การสำรองข้อมูล ได้แก่

1 นางสาวพิชามญชุ์ สินลาลับ หัวหน้างานสารสนเทศเพื่อการบริหาร
2 นายฉัตรดนัย พยักฆพงษ์ นักวิชาการคอมพิวเตอร์
3 นายนัฏศักร แป้นเงิน นักวิชาการคอมพิวเตอร์
4 นายพลธร สุขกิจ นักวิชาการคอมพิวเตอร์

4.4 ผู้ดูแลงานพัฒนาเว็บไซต์ รับผิดชอบการบำรุงรักษาและพัฒนาเว็บไซต์ ได้แก่

1 นายสุภพ โก่งกระโทก หัวหน้างานพัฒนาเว็บไซต์
2 นางสาวนันทนี ศรีแสงจันทร์ นักวิชาการคอมพิวเตอร์