แผนรองรับสถานการณ์ฉุกเฉิน

(IT Contingency Plan)

สำนักงานสาธารณสุขจังหวัดพิจิตร

พ.ศ. 2566

สารบัญ

แผนรองรับสถานการณ์ฉุกเฉิน
(IT Contingency plan)

1. บทนำ

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กรและการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัยและมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

สำนักงานสาธารณสุขจังหวัดพิจิตร ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหาจึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

3. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศของสำนักงานสาธารณสุขจังหวัดพิจิตร

3. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของสำนักงานสาธารณสุขจังหวัดพิจิตรมีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดพิจิตร เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

/จากการวิเคราะห์...

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของสำนักงานสาธารณสุขจังหวัดพิจิตร พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker เป็นต้น

2. ความเสี่ยงด้านบุคคล เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ ของสำนักงานสาธารณสุขจังหวัดพิจิตร เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

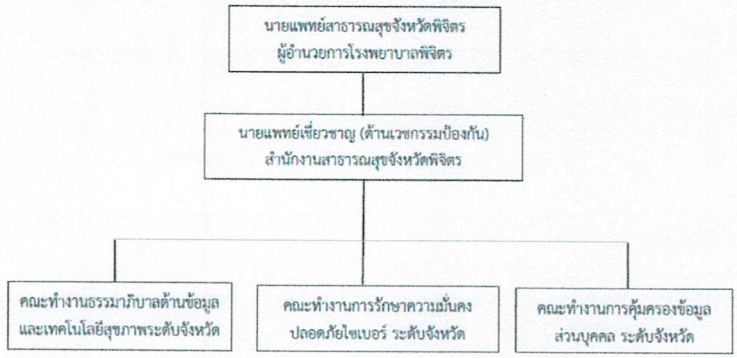
3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม อัคคีภัย การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของสำนักงานสาธารณสุขจังหวัดพิจิตร ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดพิจิตร มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักงานสาธารณสุขจังหวัดพิจิตร

4. โครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

ตามที่กระทรวงสาธารณสุขมีนโยบายมุ่งเน้น ประจำปีงบประมาณ พ.ศ. ๒๕๖๕ ประเด็นธรรมาภิบาลการพัฒนาระบบเทคโนโลยีสารสนเทศ (ICT) เป็นศูนย์ข้อมูลกลางด้านสุขภาพของประชาชน ซึ่งการดำเนินงานให้ศูนย์ข้อมูลกลางด้านสุขภาพของประชาชนมีประสิทธิภาพและมีความมั่นคงปลอดภัยทางไซเบอร์ พร้อมให้บริการข้อมูลสุขภาพส่วนบุคคลแก่ประชาชนผู้เป็นเจ้าของข้อมูลและใช้ข้อมูลสุขภาพในการส่งเสริมการปรับพฤติกรรมสุขภาพด้วยการให้ความรู้สุขภาพ (Heatth Literacy) ผ่านระบบดิจิทัล สำนักงานสาธารณสุขจังหวัดพิจิตร จึงจัดทำโครงสร้างการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ โดยมีคณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพ คณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์ และคณะทำงานการคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด



/4.1 คณะทำงาน...

4.1 คณะทำงานธรรมาภิบาลด้านข้อมูลและเทคโนโลยีสุขภาพระดับจังหวัด

หน้าที่และอำนาจ

1. นำนโยบายจากส่วนกลางไปสู่การปฏิบัติ และกำกับติดตาม ช่วยเหลือและแก้ปัญหาการดำเนินงาน ดังนี้

1.1 ด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security)

1.2 การคุ้มครองข้อมูลส่วนบุคคล (PDPA)

1.3 การเชื่อมโยงข้อมูลระหว่างระบบสถานพยาบาลและผู้รับบริการ ผ่าน HIS gateway

1.4 โครงการ 3-Refer

1.5 คุณภาพระบบเทคโนโลยีสารสนเทศโรงพยาบาล (HA IT)

1.6 IPD Paperless

2. กำหนดแนวทางและกำกับติดตาม การใช้ประโยชน์ข้อมูลสุขภาพส่วนบุคคลร่วมกันได้อย่างไร้รอยต่อภายใต้กฎหมายที่เกี่ยวข้อง การรับส่งข้อมูลตามมาตรฐานที่ตกลงร่วมกัน และการนำข้อมูลสุขภาพไปใช้ประโยชน์ในการให้บริการแก่ประชาชนในรูปแบบต่างๆ อย่างมีธรรมาภิบาลข้อมูล (Data Governance) ให้สอดคล้องกับแนวทางจากส่วนกลาง และจัดให้มีการประชุมนำเสนอปัญหาอุปสรรคและผลการดำเนินงานในที่ประชุมผู้บริหารระดับจังหวัดเป็นประจำ

3 ให้คำปรึกษาแนะนำ ช่วยเหลือและแก้ปัญหาการดำเนินงานด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) การคุ้มครองข้อมูลส่วนบุคคล (PDPA) ให้แก่หน่วยงานในสังกัดสำนักงานสาธารณสุขจังหวัดพิจิตร

4.2 คณะทำงานการรักษาความมั่นคงปลอดภัยไซเบอร์ระดับจังหวัด

หน้าที่และอำนาจ

1. ดูแลรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ ให้มีประสิทธิภาพยิ่งขึ้น

2. กำหนดมาตรการในการป้องกัน รับมือ และลดความเสี่ยงจากการบุกรุกโจมตีไซเบอร์ที่อาจส่งผลกระทบต่อความมั่นคงหน่วยงาน

4.3 คณะทำงานการคุ้มครองข้อมูลส่วนบุคคลระดับจังหวัด

หน้าที่และอำนาจ

1. ให้คำแนะนำแก่ผู้ควบคุมข้อมูลหรือผู้ประมวลผลข้อมูลส่วนบุคคล

2. ตรวจสอบและการดำเนินการเกี่ยวกับการเก็บรวบรวม ใช้ และเปิดเผยข้อมูลของผู้ควบคุมข้อมูลและผู้ประมวลผลข้อมูล

3. รักษาความลับข้อมูลส่วนบุคคล

4. กรณีมีปัญหาการเก็บรวบรวม ใช้ เปิดเผยข้อมูล เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลจะประสานงานและให้ความร่วมมือกับสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลในการจัดการปัญหาต่างๆ

/5.แผนรองรับ...

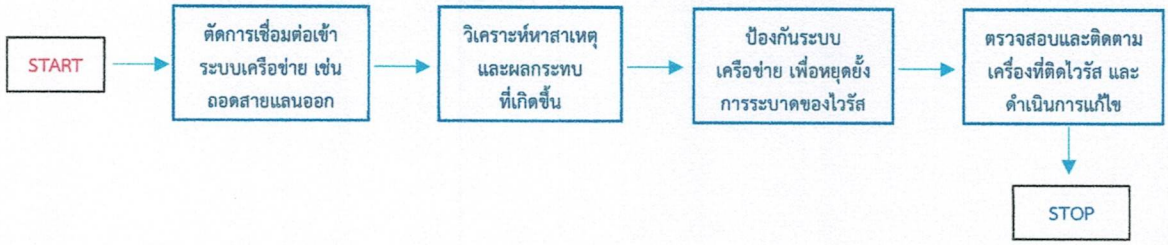
5. แผนรองรับสถานการณ์ฉุกเฉิน

5.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

5.1.1 กรณีการป้องกันไวรัสล้มเหลว

- กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการตัดการเชื่อมต่อเข้าระบบเครือข่าย
- วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส
- ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข
- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่ผู้ดูแลระบบทราบ หรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ผู้ดูแลระบบจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

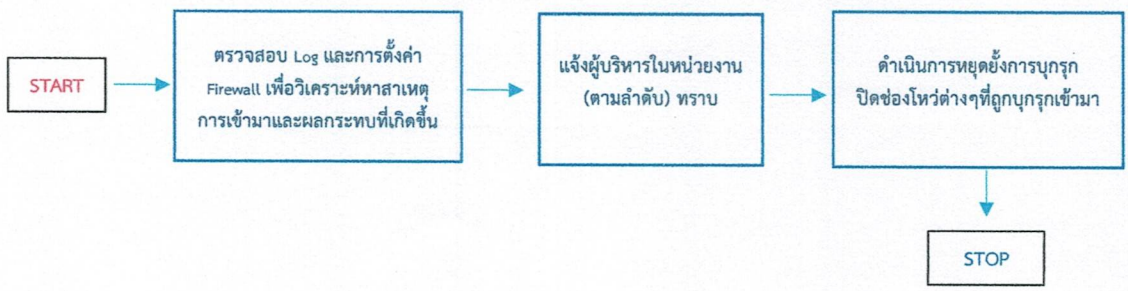
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีระบบการป้องกันไวรัสล้มเหลว



5.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
- ผู้ดูแลระบบแจ้งผู้บริหารในหน่วยงาน (ตามลำดับ) ให้ทราบโดยด่วน
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



/5.1.3 กรณีการเชื่อมโยง...

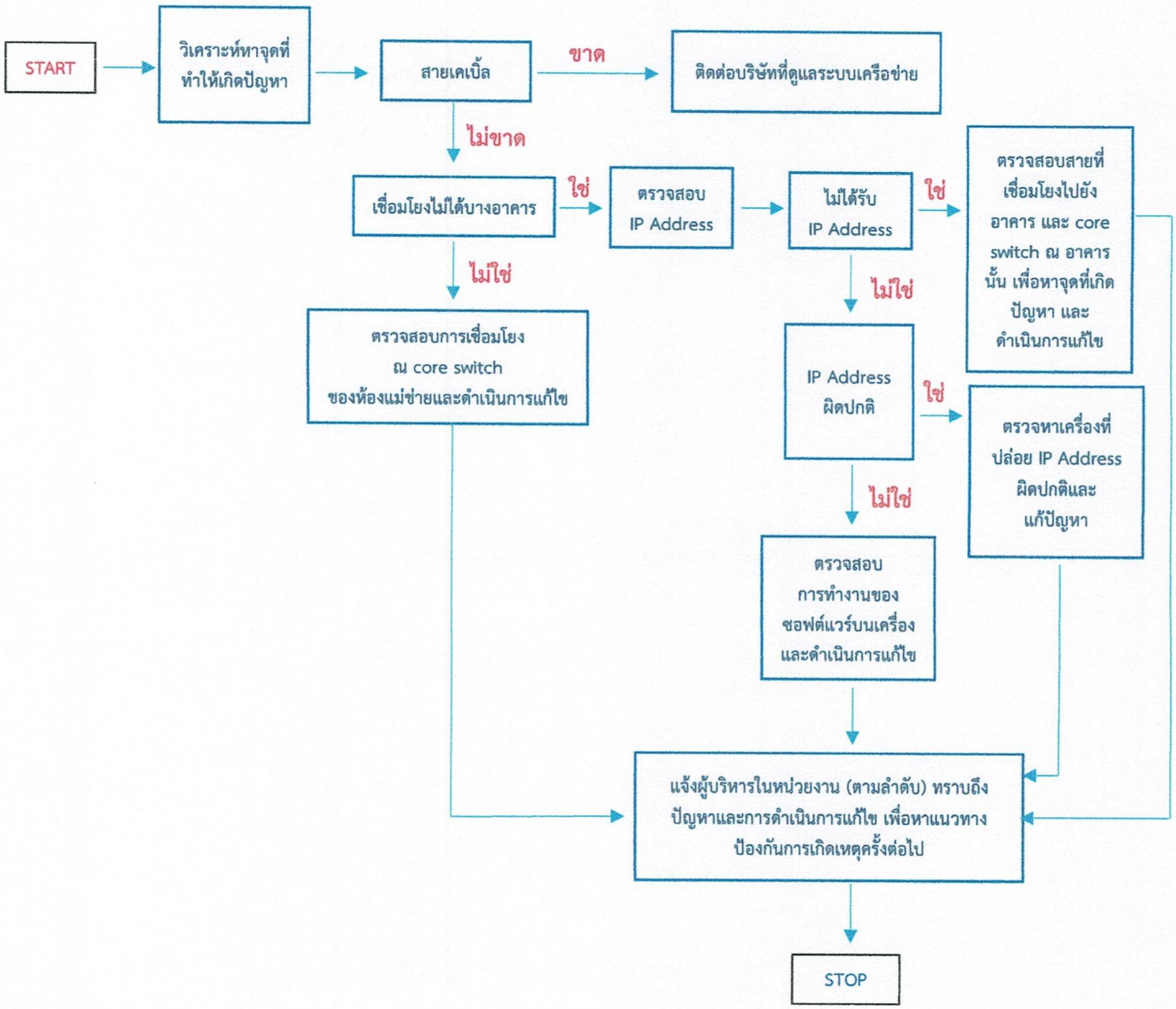
5.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

- หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

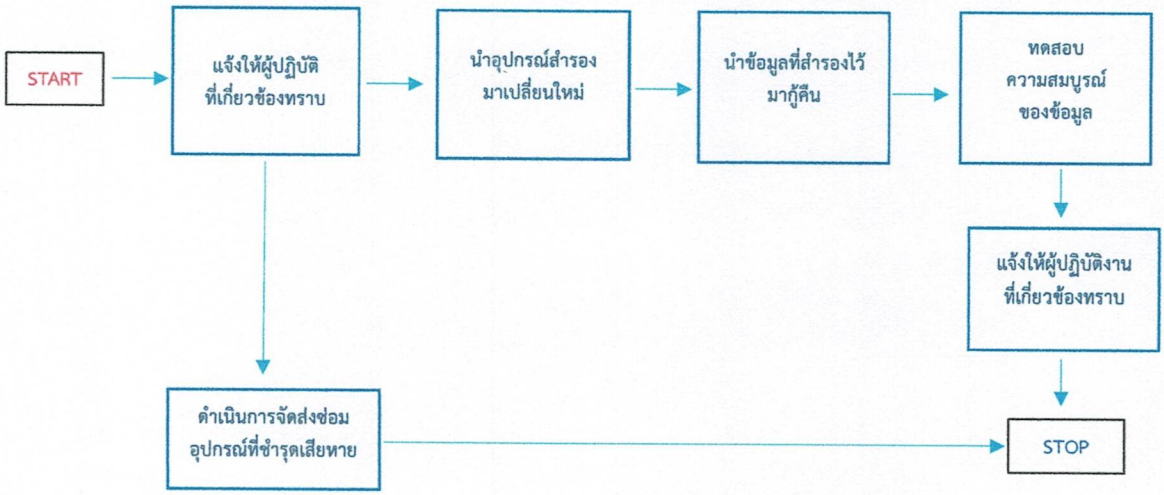


/5.1.4 กรณีอุปกรณ์...

5.1.4 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ
- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว
- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

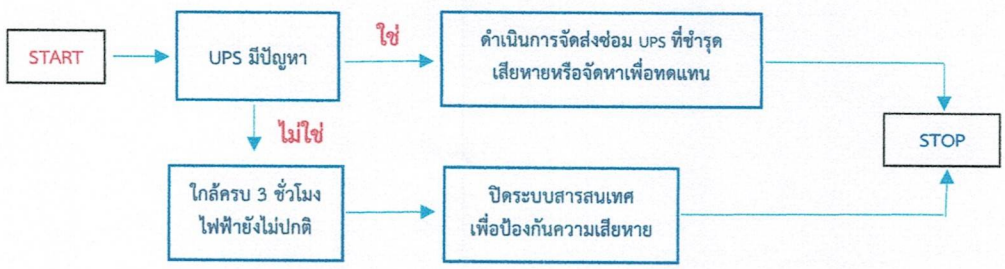
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



5.1.5 กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 3 ชั่วโมง
- หากใกล้ครบ 3 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังผู้ดูแลระบบ
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา ดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง



/5.2 สถานการณ์ฉุกเฉิน...

5.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

5.2.1 กรณีไฟไหม้

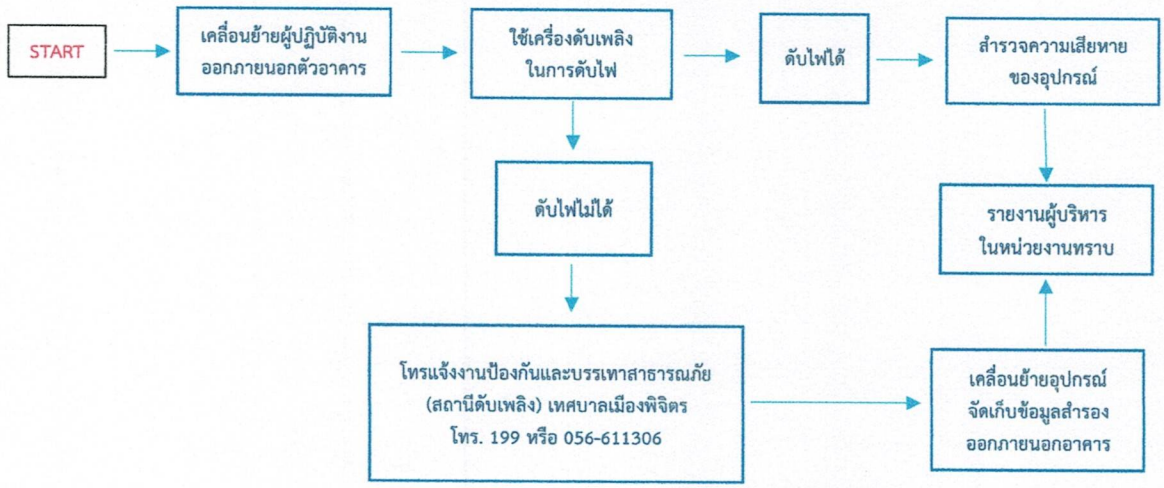
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานป้องกันและบรรเทาสาธารณภัย (สถานีดับเพลิง) เทศบาลเมืองพิจิตร โทร. 199 หรือ 056-611306

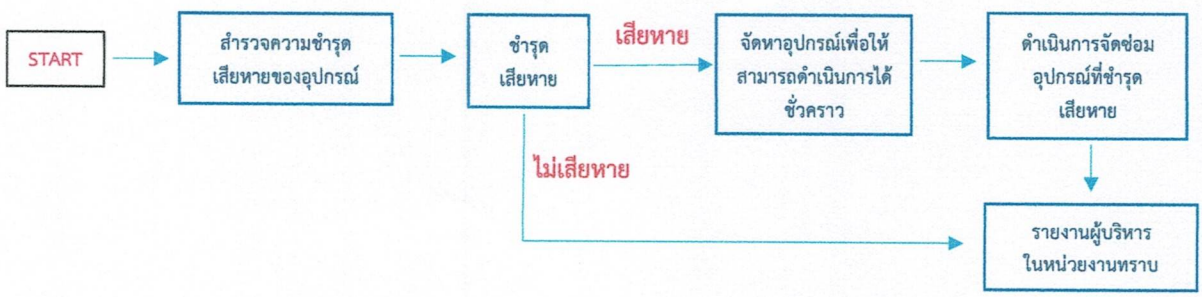
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 2 ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)

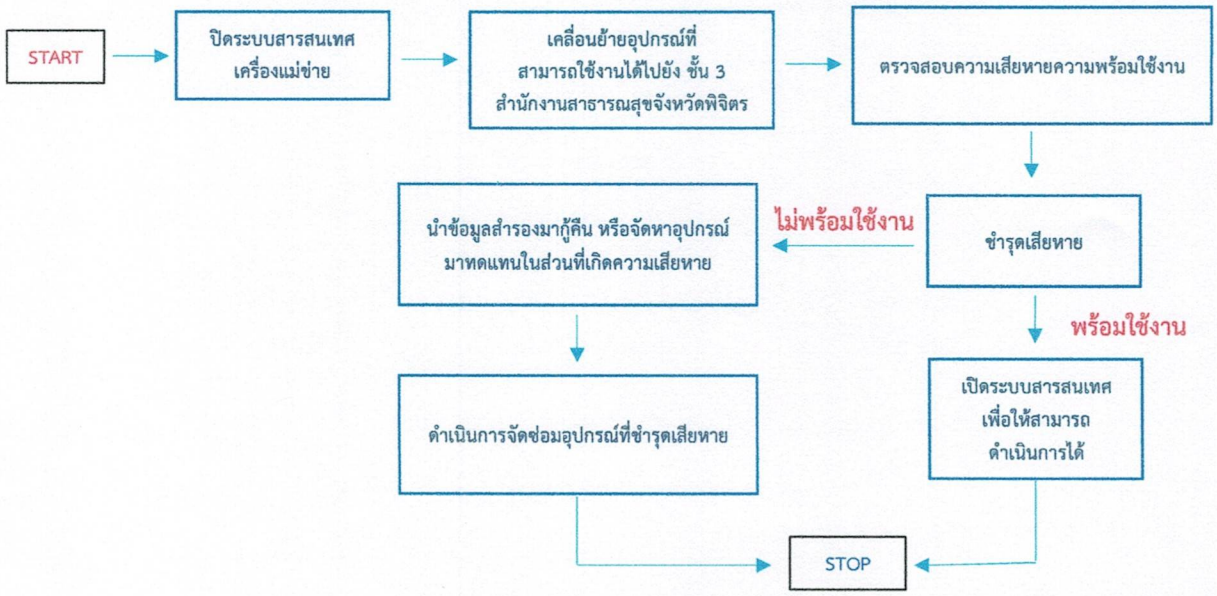


/5.2.2 กรณีน้ำท่วม...

5.2.2 กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ห้องแม่ข่ายคอมพิวเตอร์ ชั้น 3 สำนักงานสาธารณสุขจังหวัดพิจิตร
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม

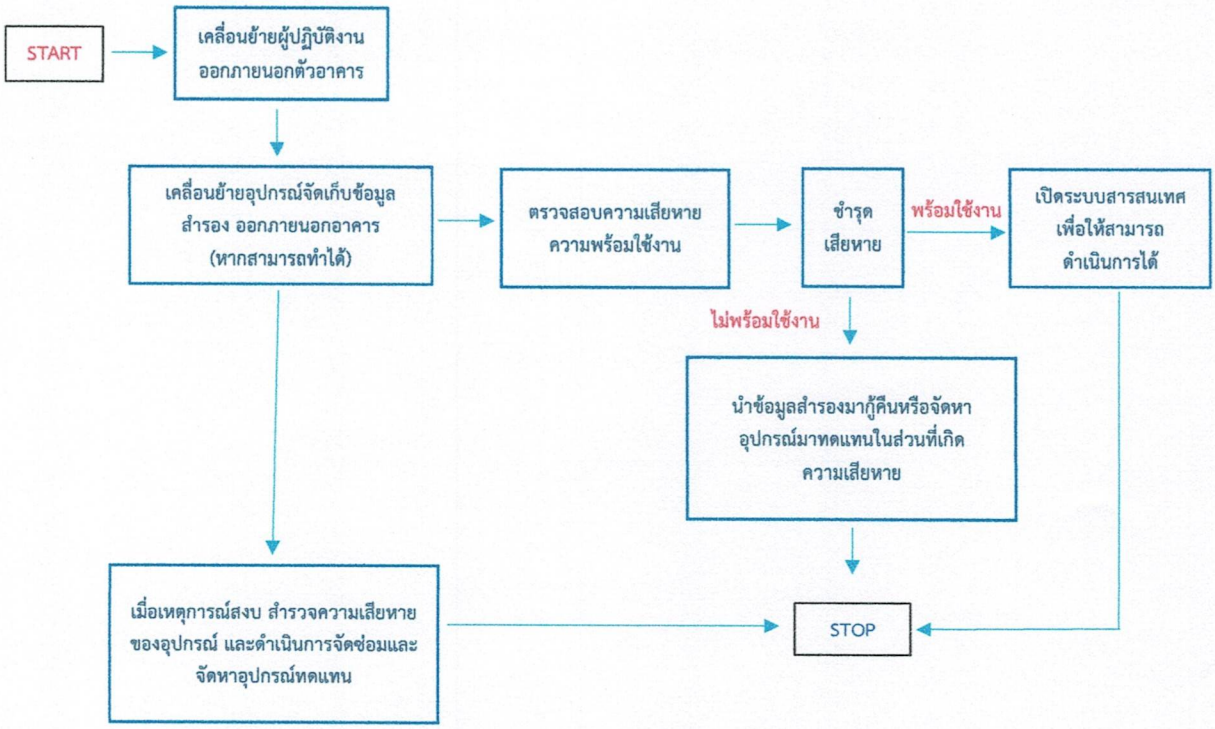


5.2.3 กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

/แผนผังแสดงขั้นตอน...

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



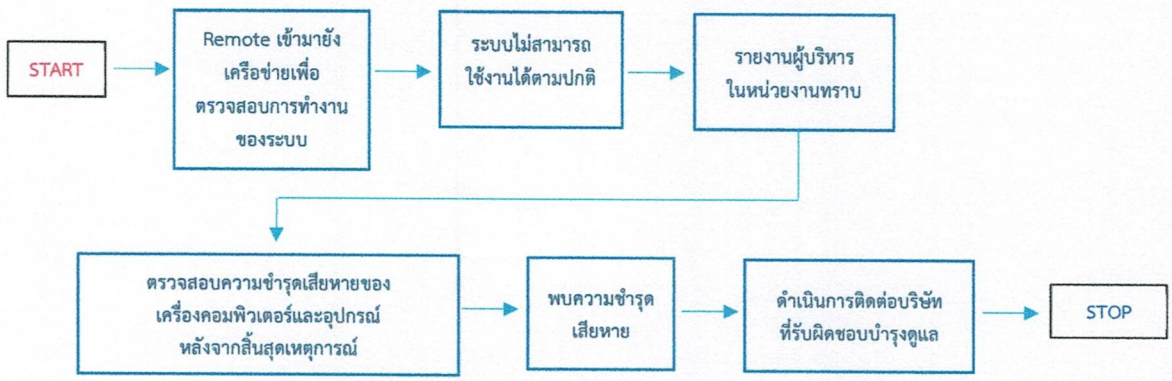
5.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติแจ้งผู้บริหารในหน่วยงานทราบ

- หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง



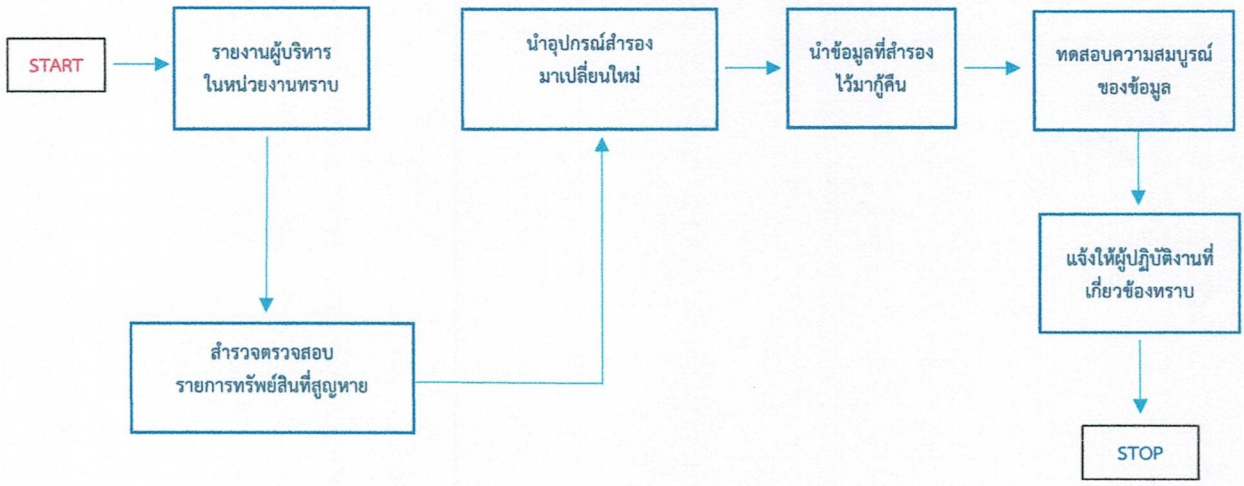
/5.4 สถานการณ์ฉุกเฉิน...

5.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

5.4.1 กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบ งานต่างๆ ได้โดยเร็วแผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

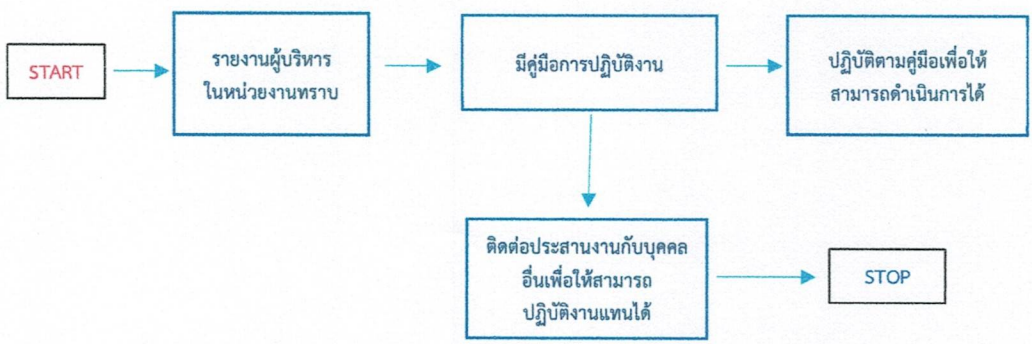
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม



5.4.2 กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้

- แจ้งผู้บริหารในหน่วยงานทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถปฏิบัติงานได้



/6. การกำหนดผู้รับผิดชอบ...

6. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ สำนักงานสาธารณสุขจังหวัดพิจิตร มีดังนี้

1. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

1.1. นายแพทย์เชี่ยวชาญ (ด้านเวชกรรมป้องกัน)

1.2. หัวหน้ากลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข

2. รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย ได้แก่

2.1 นายพินิจ พรมจาด	นักวิชาการสาธารณสุขชำนาญการ	โทร. 087-3184719
2.2 นายปรีชา บุญมี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร. 084-6887671
2.3 น.ส.อมรรัตน์ กัลป์เจริญศรี	นักวิชาการคอมพิวเตอร์	โทร. 086-9299619
2.4 นายอภินัทธ์ วัฒนไพบูลย์	นักวิชาการสาธารณสุขปฏิบัติการ	โทร. 091-0288959

3. รับผิดชอบการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

3.1 นายพินิจ พรมจาด	นักวิชาการสาธารณสุขชำนาญการ	โทร. 087-3184719
3.2 นายปรีชา บุญมี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร. 084-6887671
3.3 น.ส.อมรรัตน์ กัลป์เจริญศรี	นักวิชาการคอมพิวเตอร์	โทร. 086-9299619
3.4 นายอภินัทธ์ วัฒนไพบูลย์	นักวิชาการสาธารณสุขปฏิบัติการ	โทร. 091-0288959

4.รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน ได้แก่

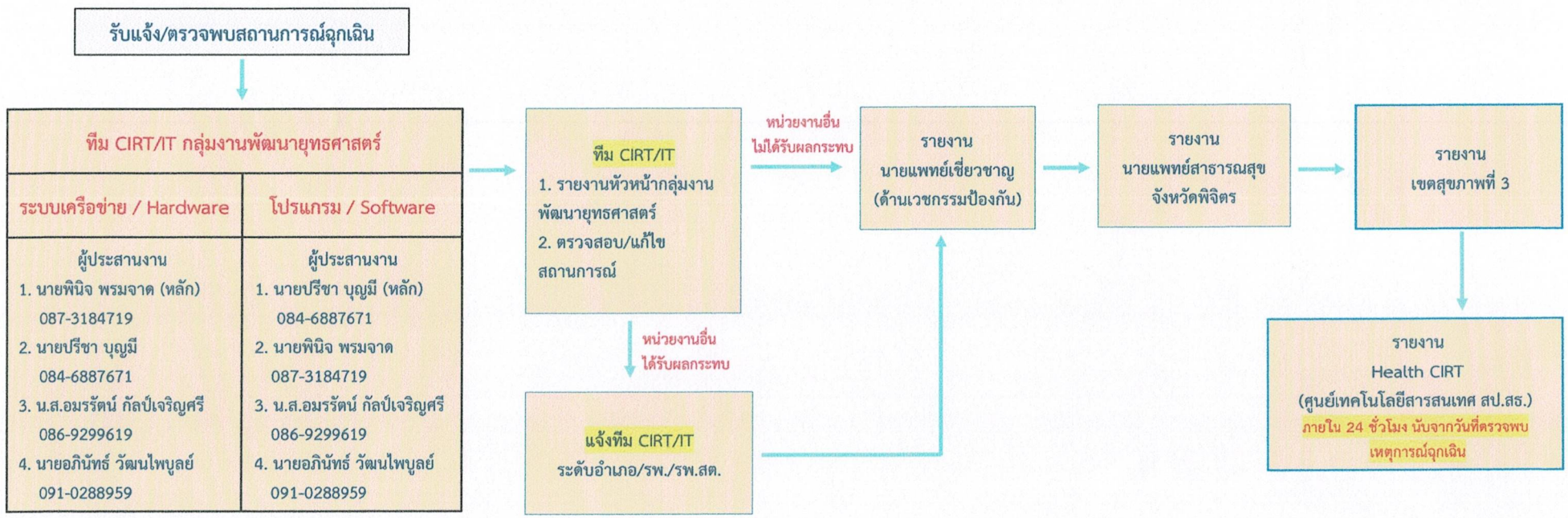
4.1 นายพินิจ พรมจาด	นักวิชาการสาธารณสุขชำนาญการ	โทร. 087-3184719
4.2 นายปรีชา บุญมี	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร. 084-6887671
4.3 น.ส.อมรรัตน์ กัลป์เจริญศรี	นักวิชาการคอมพิวเตอร์	โทร. 086-9299619
4.4 นายอภินัทธ์ วัฒนไพบูลย์	นักวิชาการสาธารณสุขปฏิบัติการ	โทร. 091-0288959

แผนรองรับสถาการณ์ฉุกเฉินฉบับนี้ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

(นายวิศิษฎ์ อภิสิทธิ์วิทยา)
นายแพทย์สาธารณสุขจังหวัดพิจิตร
มิถุนายน 2566

Flow การแจ้งสถานการณ์ฉุกเฉิน
สำนักงานสาธารณสุขจังหวัดพิจิตร

กรณี “ภัยคุกคามทางไซเบอร์”



Flow การแจ้งสถานการณ์ฉุกเฉิน
สำนักงานสาธารณสุขจังหวัดพิจิตร

กรณี “ภัยธรรมชาติ/ภัยจากบุคคล/ภัยอื่นๆ ที่ส่งผลกระทบ”