สำนักงานสาธารณสุขจังหวัดอ่างทอง

แผนรองรับสถานการณ์ฉุกเฉิน ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

งานเทคโนโลยีสารสนเทศ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข

สำนักงานสาธารณสุขจังหวัดอ่างทอง

สารบัญ

หน้า

แผนรองรับสถานการณ์ฉุกเฉิน
ระบบเทคโนโลยีสารสนเทศ (IT Contingency plan)

๑. บทนำ

ปัจจุบันสำนักงานสาธารณสุขจังหวัดอ่างทอง ได้นำระบบเทคโนโลยีสารสนเทศมาใช้ในการกำกับติดตามผลการดำเนินงานด้านสาธารณสุข และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาระบบเทคโนโลยีสารสนเทศ เพื่อความสะดวกในการทำงาน ที่เป็นประโยชน์ต่อการการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นจำเป็นต้องมีการจัดการฐานข้อมูล การเฝ้าระวังการจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย มีความพร้อมในการที่จะนำข้อมูลสารสนเทศไปใช้งานได้อย่างมีประสิทธิภาพตลอดเวลา

งานเทคโนโลยีสารสนเทศ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข ได้นำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานด้านสาธารณสุข ให้บริการผู้ป่วยในโรงพยาบาล และในโรงพยาบาลส่งเสริมสุขภาพตำบล และมีการติดตาม กำกับการดำเนินงานทั้งในระดับอำเภอ และจังหวัด ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตีจากภายนอก จากไวรัสคอมพิวเตอร์ จากปัญหาระบบไฟฟ้า และจากอัคคีภัย ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศและส่งผลกระทบต่อการดำเนินงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๒.๑ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและระบบเทคโนโลยีสารสนเทศให้เสถียรภาพและพร้อมสำหรับการใช้งาน

๒.๒ เพื่อลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

๓. การวิเคราะห์ความเสี่ยง

สำนักงานสาธารณสุขจังหวัดอ่างทอง มีการใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศ มีประสิทธิภาพ มีความมั่นคงปลอดภัย เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการการปฏิบัติงานด้านสาธารณสุข การควบคุม กำกับ ให้เกิดประโยชน์สูงสุด จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของสำนักงานสาธารณสุขจังหวัดอ่างทอง พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๓.๑ ความเสี่ยงด้านเทคนิค

เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง จากการถูกโจมตีจากไวรัสหรือโปแกรมไม่ประสงค์ดี ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ไฟฟ้าดับ เป็นต้น

๓.๒ ความเสี่ยงด้านผู้ปฏิบัติงาน

เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓.๓ ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน

เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๓.๔ ความเสี่ยงด้านการบริหารจัดการ

เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

๔. แนวทางการป้องกันและเตรียมการเบื้องต้น

๔.๑ การประกาศแผน (Activation)

สำนักงานสาธารณสุขจังหวัดอ่างทองมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการให้ความรู้ เพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้รับผิดชอบจะแจ้งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO ประจำสำนักงานสาธารณสุขจังหวัดอ่างทองทราบ เพื่อตัดสินใจต่อไป

๔.๒ กระบวนการดำเนินงาน (Procedure)

งานเทคโนโลยีสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในสำนักงานสาธารณสุขจังหวัดอ่างทอง โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ เพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง

๔.๓ การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า, สถานีดับเพลิง เป็นต้น

๔.๔ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ของงานเทคโนโลยีสารสนเทศ กลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณี คอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/โปรแกรมระบบงานที่สำคัญ
- สำรองอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือข่าย
- Flash Drive/External Hard Disk สำรองข้อมูลและระบบงานที่สำคัญ
- โปรแกรม antivirus/spyware
- แผ่น driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน

๔.๕ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยสำนักงานสาธารณสุขจังหวัดอ่างทองมีแนวทางการสำรองข้อมูลระบบคอมพิวเตอร์ ดังนี้

- ข้อมูลในระบบ Server สำรองโดยการ Backup โปรแกรมและฐานข้อมูล
- ข้อมูลของผู้ใช้งาน สำรองโดยใช้ Flash Drive/External Hard Disk/Drive Online

๔.๖ การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้

๔.๗ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔.๘ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศมีแนวทาง ดังนี้

๑) มาตรการควบคุมการเข้าออกห้อง Server โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้อง Server หากจำเป็น ให้มีเจ้าหน้าที่ของงานเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของสำนักงานสาธารณสุขจังหวัดอ่างทอง เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๔) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

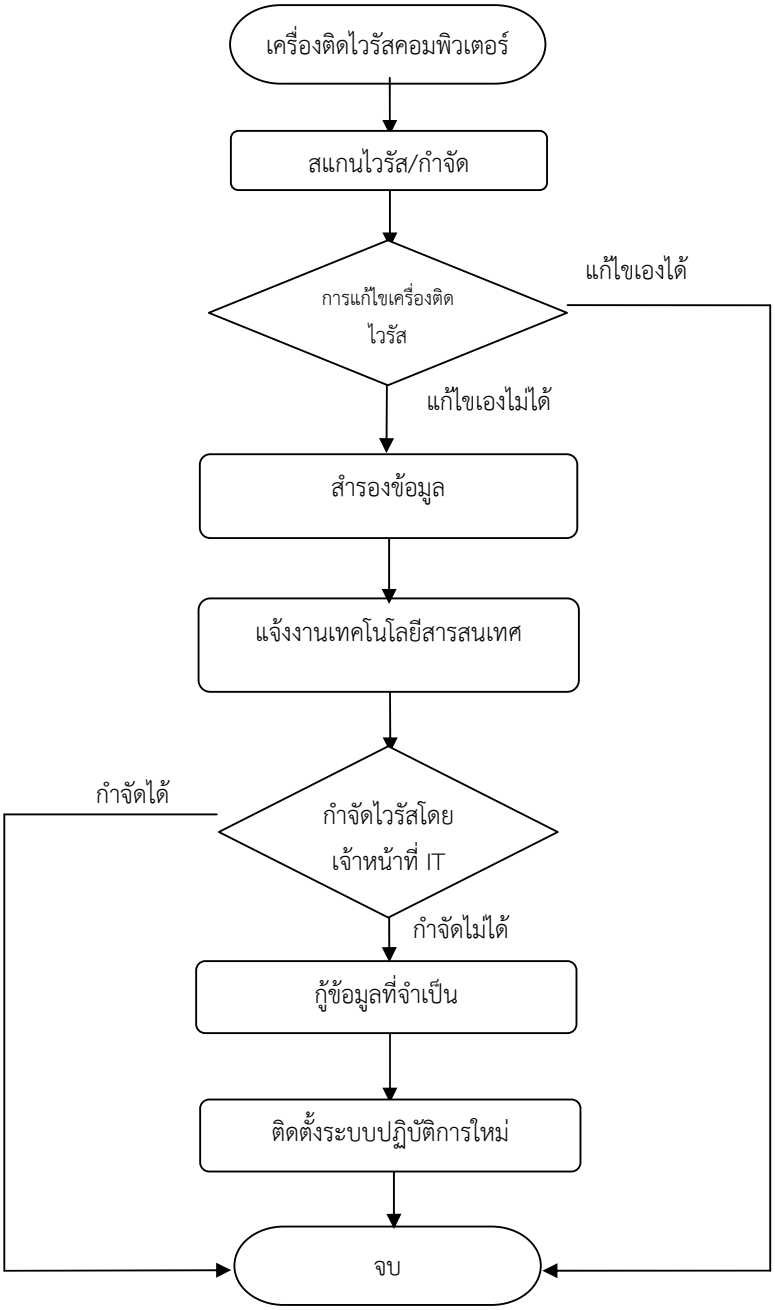
๕. แผนรองรับสถานการณ์ฉุกเฉิน

๕.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๕.๑.๑ กรณีเครื่องติดไวรัสคอมพิวเตอร์

- กรณีถูกไวรัสหรือผู้บุกรุก ให้ผู้ใช้งานสแกนไวรัส เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- ในกรณีแก้ไขเองไม่ได้ ให้สำรองข้อมูลที่จำเป็น และแจ้งเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ เพื่อดำเนินการแก้ไข
- กำจัดไวรัสและกู้ข้อมูลที่จำเป็น
- ติดตั้งระบบปฏิบัติการใหม่
- วิเคราะห์สาเหตุและผลกระทบที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ในระบบเครือข่าย
- ดำเนินการป้องกันเพื่อหยุดยั้งการแพร่กระจายของไวรัสคอมพิวเตอร์

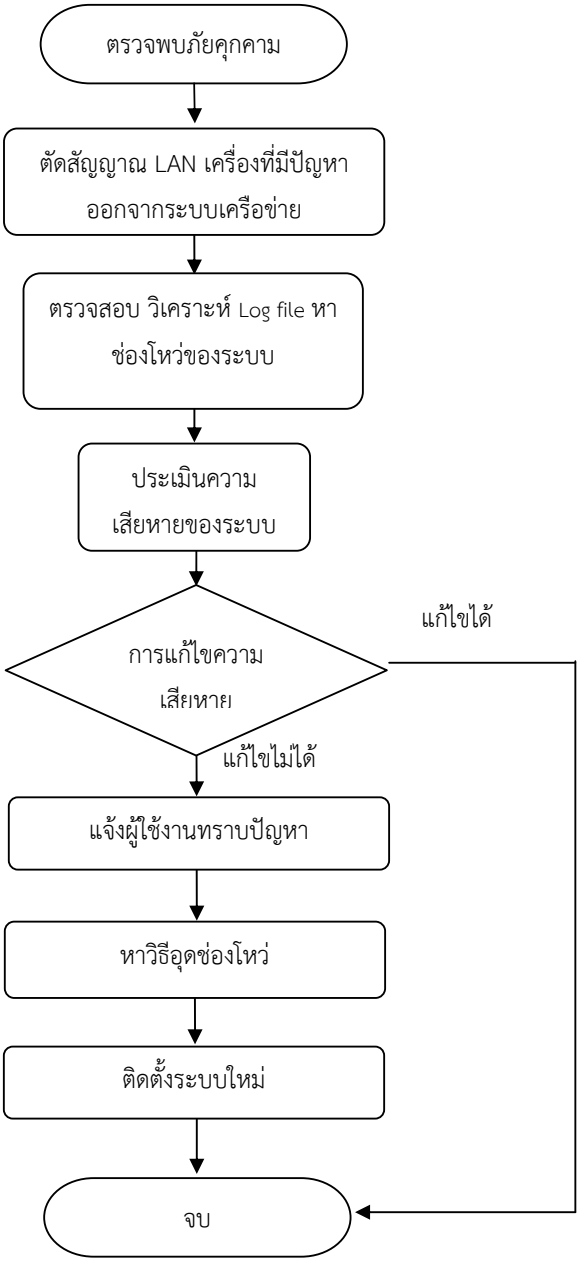
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีเครื่องติดไวรัสคอมพิวเตอร์



๕.๑.๒ กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม

- กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องตัดสัญญาณเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกบุกรุก และวิเคราะห์หาสาเหตุของการเข้ามาในระบบ โดยการตรวจสอบจาก log file และประเมินความเสียหายที่เกิดขึ้น
- ผู้ดูแลระบบดำเนินการแก้ไข
- แจ้งผู้ใช้งานรับทราบปัญหาระบบขัดข้อง
- ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้
- ในกรณีที่ไม่สามารถกู้คืนระบบได้ ต้องติดตั้งระบบใหม่ และนำข้อมูลที่สำรองไว้ นำกลับมาใช้

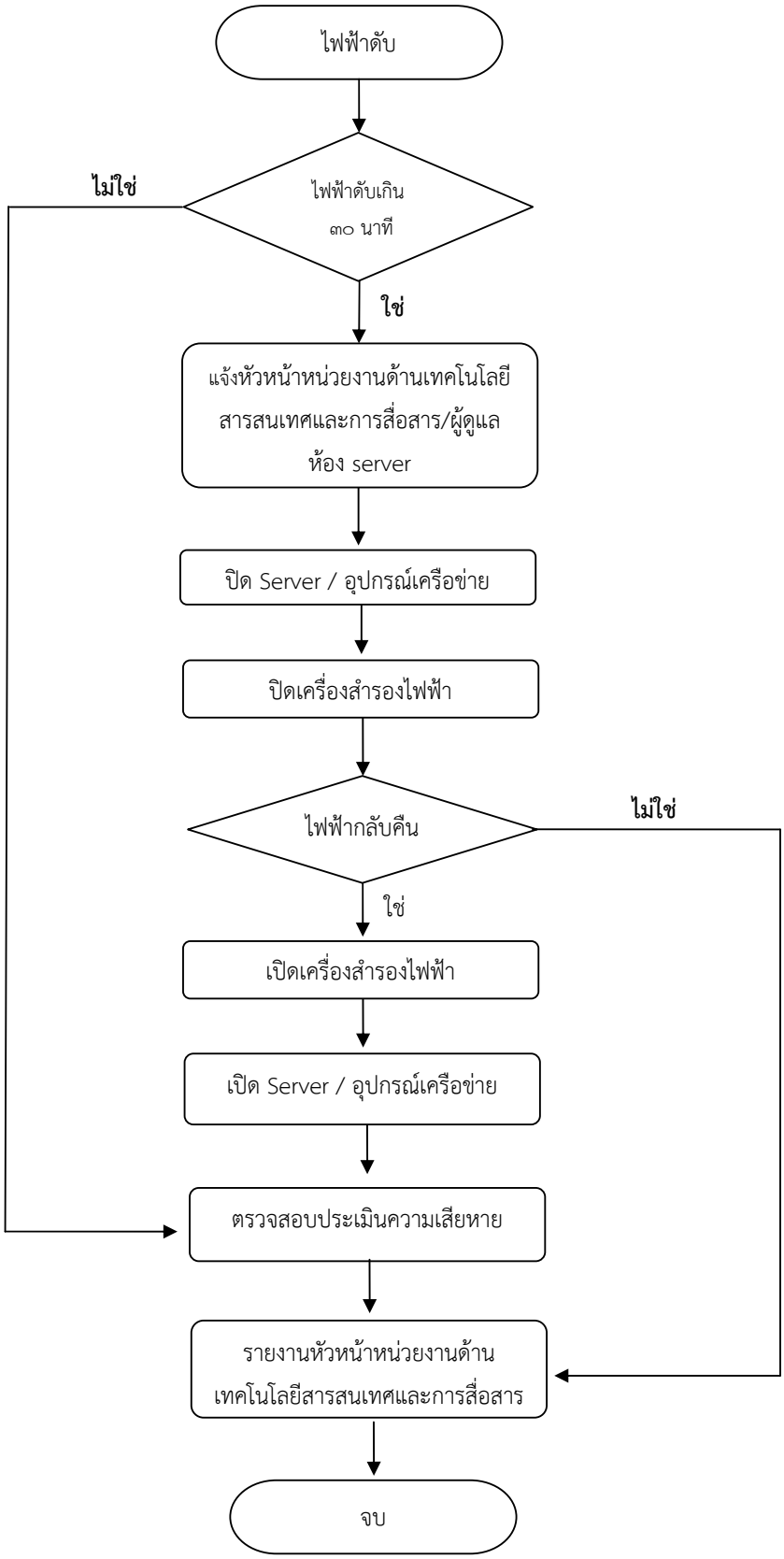
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม



๕.๑.๓ กรณีไฟฟ้าดับ

- ระบบสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ ๑ ชั่วโมง
- หากไฟฟ้าดับเกิน ๓๐ นาที ให้มีการแจ้งเตือนไปยังหัวหน้างานเทคโนโลยีสารสนเทศและผู้ดูแลห้อง Server เพื่อดำเนินการปิดระบบ ป้องกันความเสียหาย
- ในกรณีไฟฟ้ากลับคืน ทำการเปิดระบบ และประเมินความเสียหาย และรายงานหัวหน้างานเทคโนโลยีสารสนเทศ
- ในกรณีไฟฟ้าดับเกิน ๓ ชั่วโมง แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องผลิตกระแสไฟฟ้าทดแทน

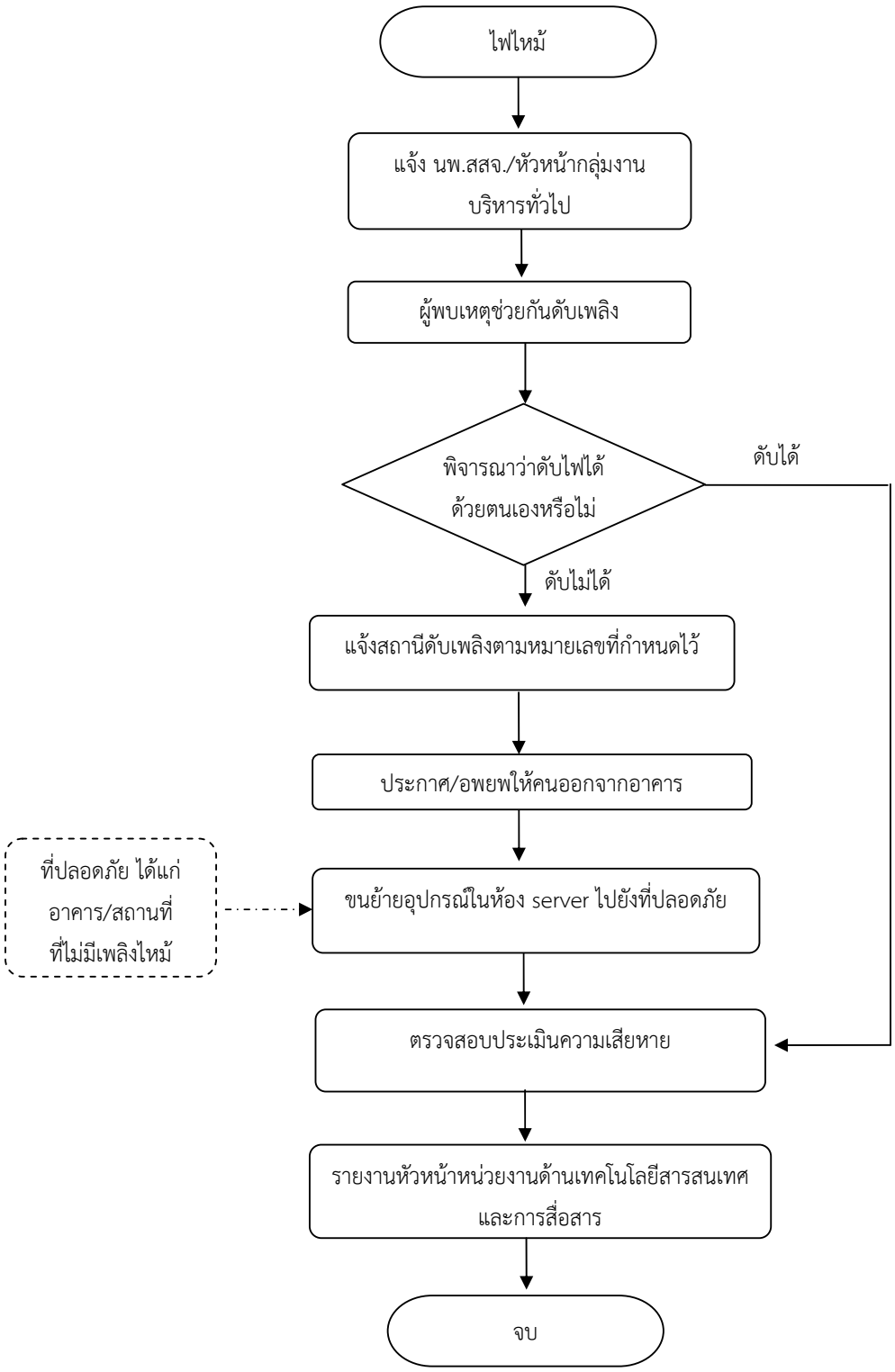
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีไฟฟ้าดับ



๕.๑.๔ กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร โทรศัพท์แจ้งนายแพทย์สาธารณสุขจังหวัดอ่างทองและหัวหน้ากลุ่มงานบริหารทั่วไปทันที และโทรศัพท์แจ้งสถานีดับเพลิงอ่างทอง โทร. ๐-๓๕๖๑-๒๗๑๑ หรือ โทร. ๑๙๙
- ขนย้ายอุปกรณ์ไปยังสถานปลอดภัย และตรวจสอบประเมินความเสียหาย
- รายงานรายงานหัวหน้าหน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้

Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีไฟไหม้



๖. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

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

๖.๑.๑ นายแพทย์สาธารณสุขจังหวัดอ่างทอง

๖.๑.๒ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO ประจำ สสจ.อ่างทอง

๖.๑.๓ คณะกรรมการบริการจัดหาระบบคอมพิวเตอร์ ประจำ สสจ.อ่างทอง

๖.๑.๔ หัวหน้ากลุ่มงานพัฒนายุทธศาสตร์สาธารณสุข สสจ.อ่างทอง

๖.๒ ผู้รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ได้แก่

๖.๒.๑ นายบัญชา แก้วสุวรรณ

๖.๒.๒ นายคงกฤช ภู่บำเพ็ญ

๖.๒.๓ นายเอกอมร มีสมศักดิ์

๖.๓ ทีมระบบสารสนเทศและฐานข้อมูล รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

๖.๓.๑ นายทวีป ทองเนื้อแปด

๖.๓.๒ นายบัญชา แก้วสุวรรณ

๖.๓.๓ นายคงกฤช ภู่บำเพ็ญ

๖.๓.๔ นายเอกอมร มีสมศักดิ์

๖.๔ ทีมบริการเทคนิคและการประสานงาน รับผิดชอบการปฏิบัติงานทางเทคนิค และประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๖.๔.๑ นายบัญชา แก้วสุวรรณ

๖.๔.๒ นายคงกฤช ภู่บำเพ็ญ

๖.๔.๓ นายเอกอมร มีสมศักดิ์

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง CIO ประจำ สสจ.อ่างทอง เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
มิถุนายน ๒๕๖๒