แนวปฏิบัติระบบสำรองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

ศูนย์สนับสนุนบริการสุขภาพที่ ๕

เพื่อให้ระบบสารสนเทศสามารถให้บริการได้อย่างต่อเนื่อง จึงกำหนดแนวปฏิบัติระบบสำรองของระบบสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน โดยมอบหมายให้ผู้ดูแลระบบที่ได้รับมอบหมาย เป็นผู้รับผิดชอบ ดังนี้

๑. ผู้ดูแลระบบต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมด พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถ แสดงถึงระบบซอฟต์แวร์ วันที่/เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิด ภัยพิบัติ เช่น ไฟไหม้ เป็นต้น
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลที่สำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. ให้จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุง แผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วย วิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

(๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถ ปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๒.๓ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณี ที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๒.๔ ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๕ ผู้ดูแลระบบมีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ อย่างน้อยปีละ ๑ ครั้ง

๒.๖ ผู้ดูแลระบบต้องกำหนดชนิดของข้อมูลและระยะเวลาที่ต้องการจะสำรองข้อมูลว่า ข้อมูลที่ต้องการสำรองเป็นข้อมูลชนิดใด และต้องใช้พื้นที่สำหรับการสำรองข้อมูลเท่าใด

๒.๗ ผู้ดูแลระบบจัดทำการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่มีความสำคัญโดยมีการสำรอง แบบเต็มรูปแบบ (Full Backup) อย่างน้อยเดือนละ ๑ ครั้ง โดยกำหนดให้เป็นวันศุกร์แรกของเดือนหรือ วันอื่นตามความเหมาะสม

๒.๘ ผู้ดูแลระบบต้องจัดทำการสำรองข้อมูลแบบบางส่วน (Incremental Backup) อย่างน้อย สัปดาห์ละ ๑ ครั้ง

๒.๙ ผู้ดูแลระบบต้องจัดทำการทดสอบการกู้กลับคืนของข้อมูล (Restore) ทุก ๖ เดือน

๒.๑๐ ผู้ดูแลระบบต้องจัดให้มีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

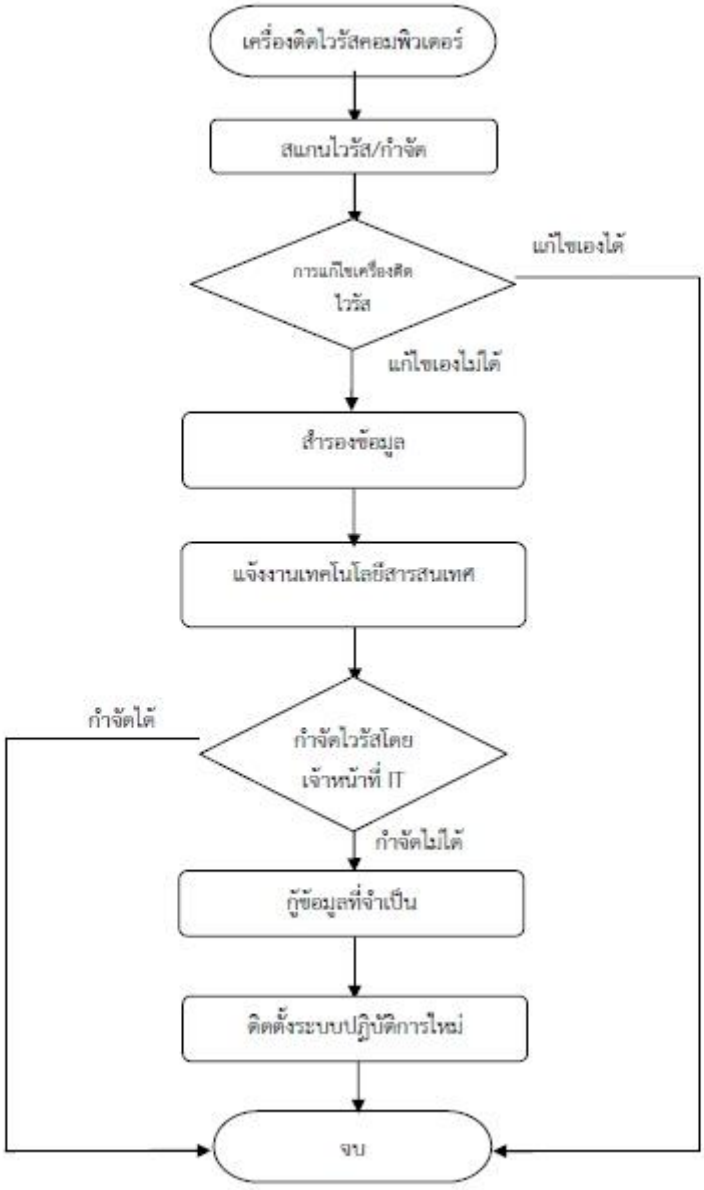
๒.๑๑ ข้อมูลที่สำรองและถูกจัดลำดับความสำคัญมากที่สุด ต้องมีการสำรองข้อมูลมากกว่า ๑ ชุด และต้องทำการสำรองข้อมูลไปยังสถานที่อื่นเพื่อความปลอดภัย

๓. แผนรองรับสถานการณ์ฉุกเฉิน สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๓.๑ กรณีเครื่องติดไวรัสคอมพิวเตอร์

- กรณีถูกไวรัสหรือผู้บุกรุก ให้ผู้ใช้งานสแกนไวรัส เพื่อจำ กัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย
- ในกรณีแก้ไขเองไม่ได้ ให้สำรองข้อมูลที่จำเป็น และแจ้งเจ้าหน้าที่งานเทคโนโลยีสารสนเทศ เพื่อดำเนินการแก้ไข
- กำจัดไวรัสและกู้ข้อมูลที่จำเป็น
- ติดตั้งระบบปฏิบัติการใหม่
- วิเคราะห์สาเหตุและผลกระทบที่เกิดขึ้นกับเครื่องคอมพิวเตอร์ในระบบเครือข่าย
- ดำเนินการป้องกันเพื่อหยุดยั้งการแพร่กระจายของไวรัสคอมพิวเตอร์

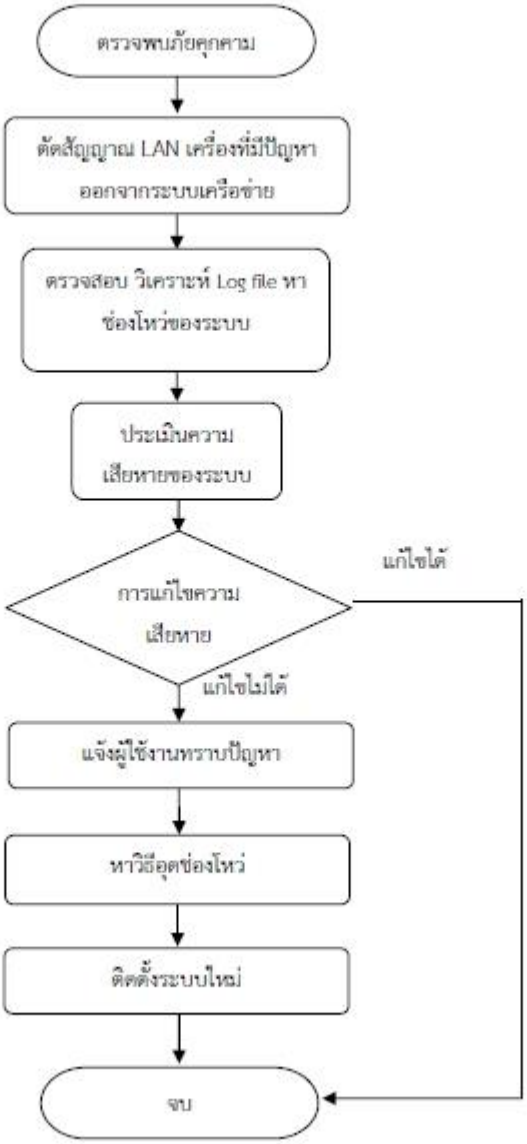
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีเครื่องติดไวรัสคอมพิวเตอร์



๓.๒ กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม

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

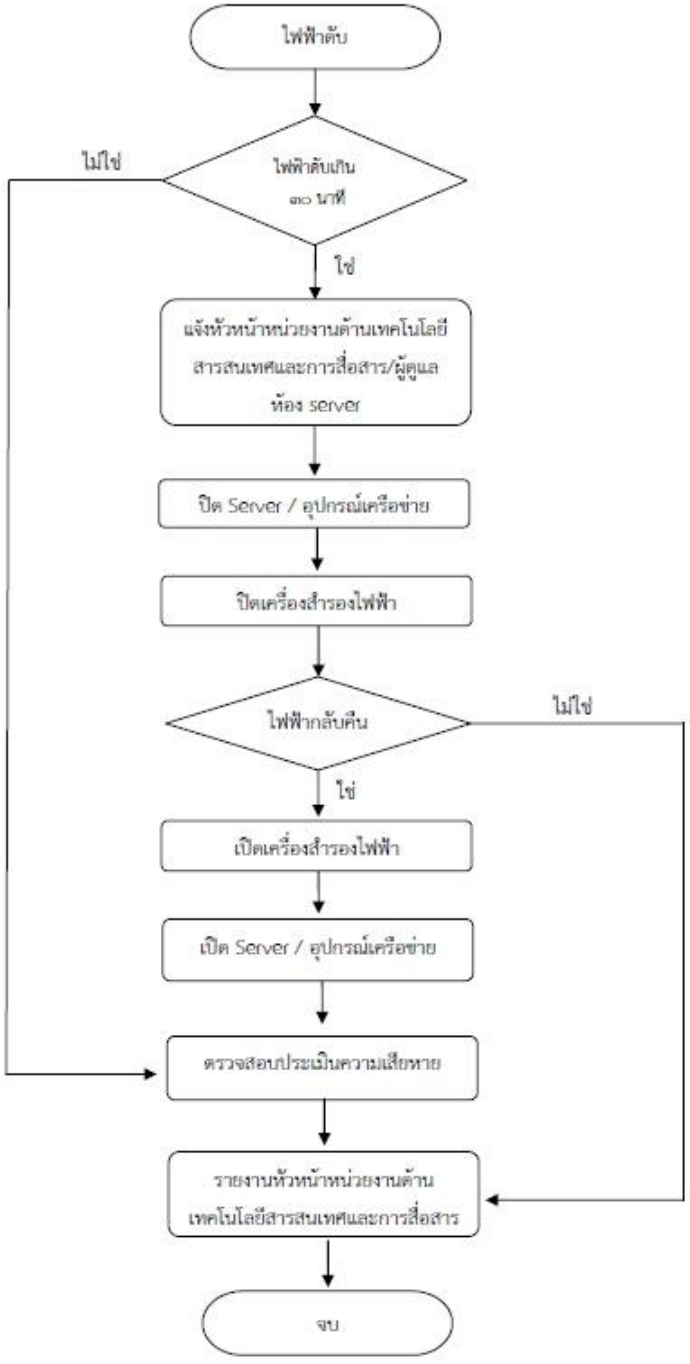
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือตรวจพบภัยคุกคาม



๓.๓ 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



๓.๔ กรณีไฟไหม้

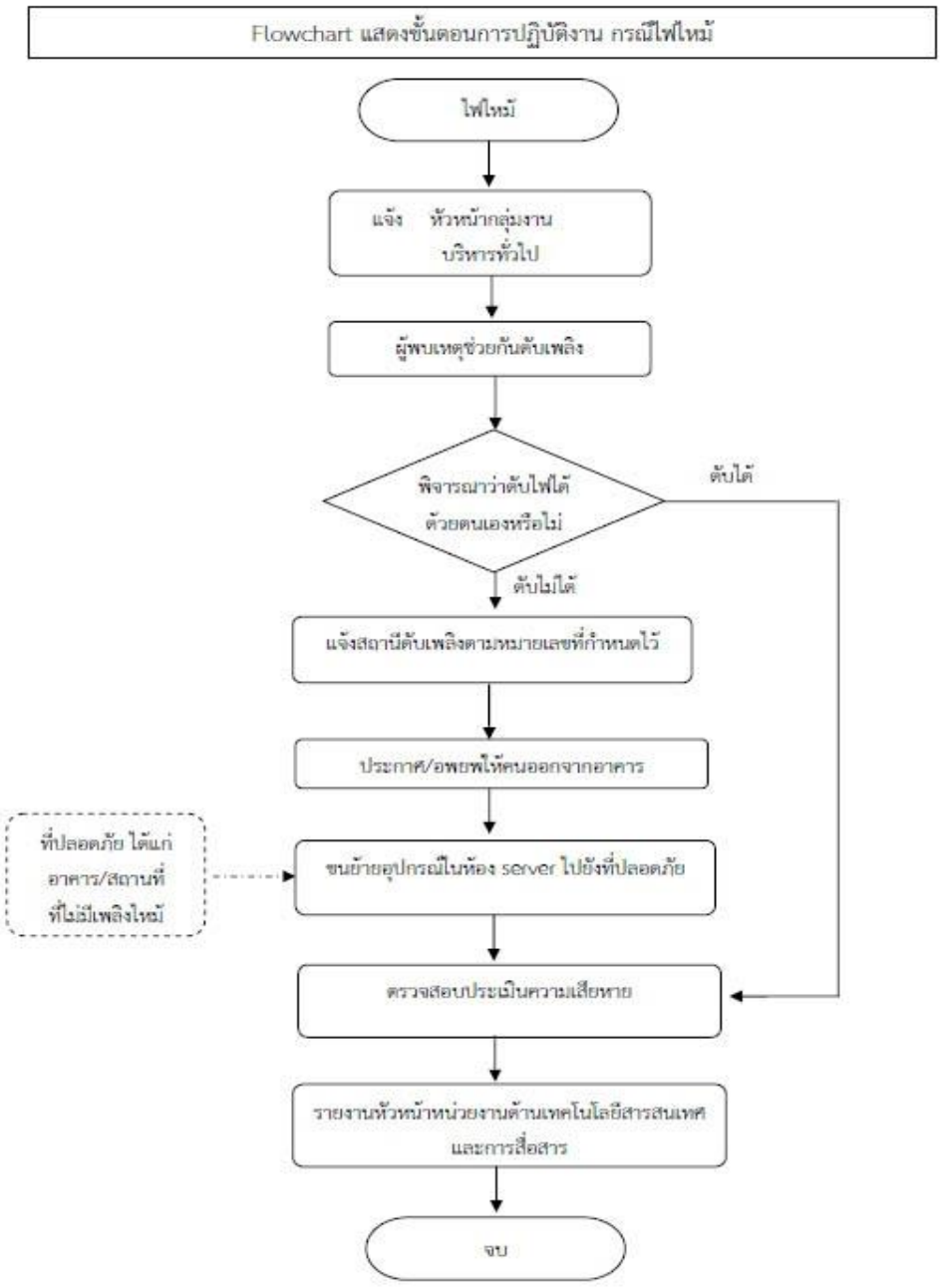
- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้

- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร โทรศัพท์แจ้งนายแพทย์สาธารณสุขจังหวัดอ่างทองและหัวหน้ากลุ่มงานบริหารทั่วไปทันที และโทรศัพท์แจ้งสถานีดับเพลิงอ่างทอง โทร. ๐-๓๕๖๑-๒๗๑๑ หรือ โทร. ๑๙๙

- ขนย้ายอุปกรณ์ไปยังสถานปลอดภัย และตรวจสอบประเมินความเสียหาย

- รายงานรายงานหัวหน้าหน่วยงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้



๔. การกำหนดผู้รับผิดชอบหน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

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

- ผู้อำนวยการศูนย์สนับสนุนบริการสุขภาพที่ ๕
- คณะกรรมการผู้รับผิดชอบตามนโยบายการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (CSO)
- หัวหน้ากลุ่มงานวิชาการและมาตรฐานระบบบริการสุขภาพ

๔.๒ ผู้รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ได้แก่

- นายสมยศ หลวงผาด นายช่างเทคนิคชำนาญงาน
- นางสาวภัฏธิดา พุทธชาด วิศวกรปฏิบัติการ ด้านชีวการแพทย์
- นางสาวพัชราวรี แจ่มศรี ปฏิบัติงานด้านคอมพิวเตอร์

๔.๓ ทีมระบบสารสนเทศและฐานข้อมูล รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

- นายสมยศ หลวงผาด นายช่างเทคนิคชำนาญงาน
- นางสาวภัฏธิดา พุทธชาด วิศวกรปฏิบัติการ ด้านชีวการแพทย์
- นางสาวพัชราวรี แจ่มศรี ปฏิบัติงานด้านคอมพิวเตอร์

๔.๔ ทีมบริการเทคนิคและการประสานงาน รับผิดชอบการปฏิบัติงานทางเทคนิค และประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

- นางสาวสิริกัญญา ดูชาติรัมย์ นักวิเคราะห์นโยบายและแผน
- นางสาวกมลรัตน์ สมัยสมภพ ปฏิบัติงานด้านพัสดุ
- นางสาวพัชราวรี แจ่มศรี ปฏิบัติงานด้านคอมพิวเตอร์

แนวปฏิบัติระบบสำรองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉินเพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ