แผนการสำรองข้อมูลพร้อมกู้คืนระบบ
IT Disaster Recovery Plan - (IT-DRP)

โรงพิมพ์ตำรวจ สำนักงานตำรวจแห่งชาติ

คำนำ

การเกิดเหตุการณ์ความไม่สงบและวิกฤตการณ์น้ำท่วมครั้งใหญ่ในประเทศไทย ซึ่งมีขนาดความเสียหายที่รุนแรง เนื่องจากเกิดขึ้นในเขตเมืองหลวงแหล่งเศรษฐกิจที่สำคัญของประเทศ ซึ่งเป็นเรื่องที่เหนือความคาดหมาย เพราะเป็นเหตุการณ์ที่ไม่เคยได้เกิดขึ้นมานานแล้ว โรงพิมพ์ตำรวจจึงได้มีการจัดทำแผนสำรองในการกู้คืนระบบคอมพิวเตอร์ เพื่อให้สามารถให้บริการและกลับมาดำเนินงานในระยะเวลาอันรวดเร็วได้ โดยที่ระบบต่าง ๆ จะต้องมีขั้นตอนกระบวนการที่ทำให้สามารถใช้งานได้อยู่ตลอดเวลา ถึงแม้จะเกิดเหตุฉุกเฉินต่าง ๆ ที่จะส่งผลกระทบทั้งทางตรงและทางอ้อมต่อระบบสารสนเทศ โรงพิมพ์ตำรวจจึงได้จัดทำแผนการสำรองข้อมูลพร้อมกู้คืนระบบ (Disaster Recovery Plan) เพื่อให้ระบบสารสนเทศสามารถใช้งานได้อย่างต่อเนื่องภายใต้สถานการณ์ของเหตุฉุกเฉิน

สารบัญ

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ
IT Disaster Recovery Plan - (IT-DRP)

บทนำ

แผนกู้คืนระบบเทคโนโลยีสารสนเทศ IT Disaster Recovery Plan -(IT-DRP) ฉบับนี้จัดทำขึ้นเพื่อให้หมวดนโยบายแผนและสารสนเทศ สามารถนำไปใช้ในการปฏิบัติงานในสภาวะวิกฤติ เช่น การเกิดอัคคีภัย การเกิดอุทกภัย การก่อการร้าย ประท้วง จลาจล ที่จะส่งผลให้ระบบสารสนเทศที่ใช้ปฏิบัติงานหลักไม่สามารถให้บริการได้ โดยแผนกู้คืนระบบสาระสนเทศ ได้แนวทางการวิเคราะห์ความสำคัญของกระบวนการในภารกิจที่มีระบบสารสนเทศที่ใช้งานเป็นหลัก ซึ่งเมื่อมีการหยุดชะงักจะก่อให้เกิดผลกระทบต่อภาระหน้าที่และฐานข้อมูลหลักของสถาบัน เช่น ระบบฐานข้อมูลเพื่อรองรับอนาคต ระบบสารสนเทศเพื่อการตัดสินใจและระบบต่าง ๆ ขอโรงพิมพ์ตำรวจมาจัดทำแผนกู้คืนระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบสามารถกลับมาดำเนินการได้ตามปกติหรือให้บริการได้ในสภาวะฉุกเฉินในระยะเวลาที่เหมาะสม ลดความความรุนแรงของเหตุการที่เกิดขึ้นได้

1. แผนการสำรองข้อมูลพร้อมกู้คืนระบบ (Disaster Recovery Plan)

1.1 หลักการและเหตุผล

ระบบข้อมูลและสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบข้อมูลและสารสนเทศสำคัญๆ จะไม่สูญหาย สามารถนำไปใช้ประโยชน์ได้อย่างมีประสิทธิภาพ โรงพิมพ์ตำรวจได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในที่ส่งผลกระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายคอมพิวเตอร์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลและสารสนเทศที่ใช้ในการบริหารจัดการและใช้สนับสนุนการดำเนินงานขององค์กรให้บรรลุตามวิสัยทัศน์

ดังนั้น การจัดทำแผนสำรองในการกู้คืนระบบคอมพิวเตอร์ เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนสู่ความเป็นปกติ ตลอดจนการดูแลรักษาฐานข้อมูลและสารสนเทศให้มีเสถียรภาพพร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

1.2 แนวทางการแก้ปัญหา

ปัญหาจากวิกฤตการณ์ที่เกิดขึ้น ทำให้องค์กรไม่สามารถ ดำเนินธุรกิจได้อย่าต่อเนื่อง เกิดผลกระทบมากมาย ทั้งในด้านความน่าเชื่อถือขององค์กร และความสามารถในการให้บริการลูกค้า จากการที่องค์กรไม่สามารถดำเนินธุรกิจได้อย่างต่อเนื่องนั้น ทำให้เกิดผลเสียต่อองค์กรอย่างมาก จึงมีความจำเป็นต้องจัดทำแผนกู้คืนระบบคอมพิวเตอร์ไว้รองรับสถานการณ์ต่างๆ

1.3 วัตถุประสงค์

1. เพื่อให้สามารถกู้คืนระบบ Computer ที่สำคัญให้สามารถกลับมาทำงานได้อย่างรวดเร็วในกรณีที่เกิดภัยพิบัติ

2. เพื่อให้พนักงานสามารถใช้งานระบบสำรองได้เมื่อเกิดภัยพิบัติ

3. เพื่อให้บริการลูกค้าได้อย่างมีประสิทธิภาพ ในขอบเขตที่ยอมรับได้

4. เพื่อวางแผนในการกู้คืนระบบที่สำคัญ และจัดเตรียมความพร้อมทางด้าน Hardware, Software และบุคลากร รวมถึงอุปกรณ์ที่จำเป็นในการกู้คืนระบบคอมพิวเตอร์

5. เพื่อให้การปฏิบัติงานดำเนินไปได้อย่างมีเสถียรภาพ

1.4 การนำระบบกลับคืนสู่สภาพปกติ

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการ ก็จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดหรือเท่าที่จะทำได้ แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน โดยดำเนินการ ดังนี้

1.4.1 จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

1.4.2 เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

1.4.3 ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 24 ชั่วโมง

1.4.4 ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

1.4.5 นำ External Harddisk ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยกู้คืนระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

1.4.6 ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

1.5 แนวทางการปฏิบัติ

1.5.1 ทุกหน่วยงาน ถือปฏิบัติตามแผนสำรองในการกู้คืนระบบคอมพิวเตอร์ ที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ ฉบับนี้

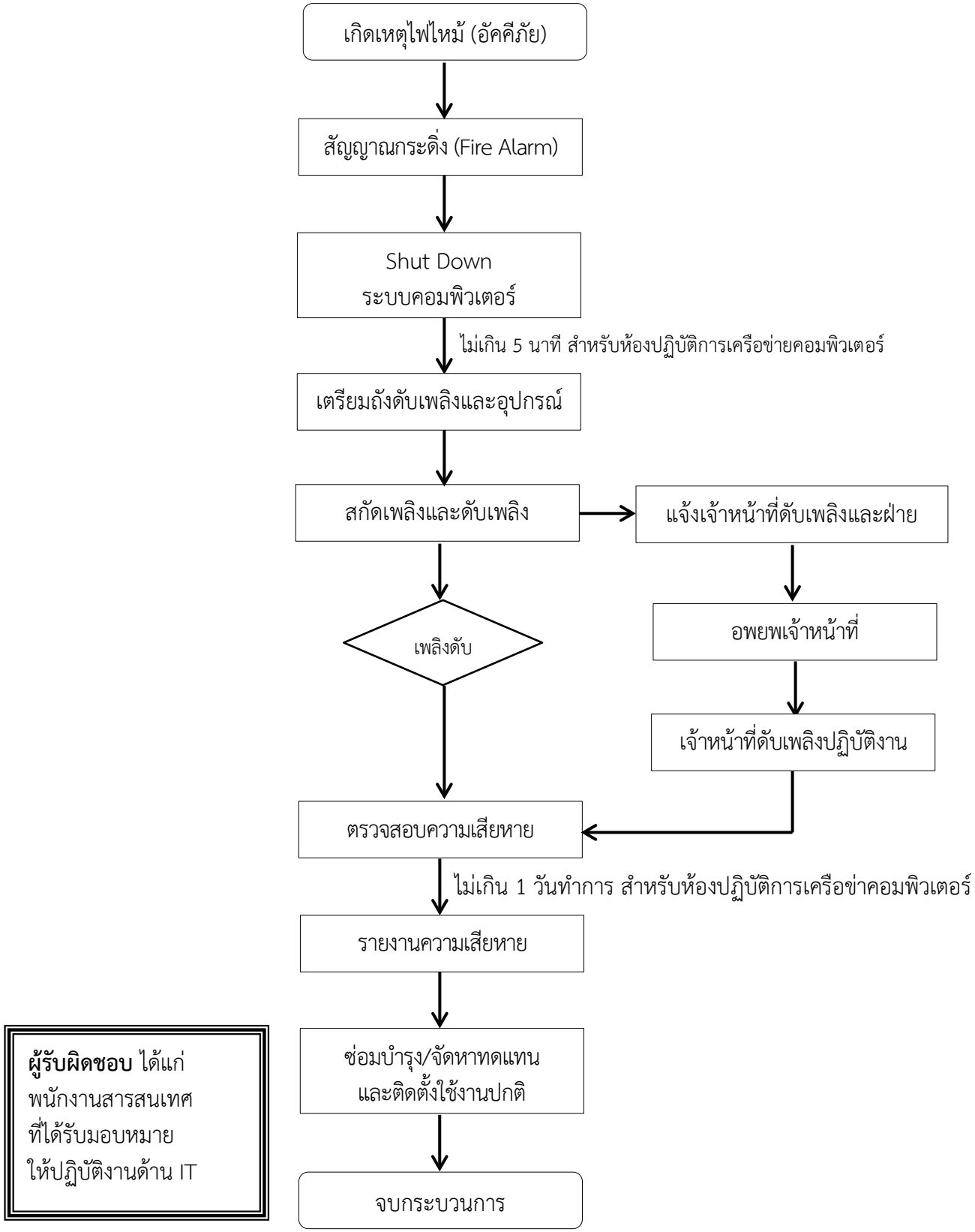
1.5.2 ทุกหน่วยงาน จัดทำ/ทบทวนและปรับปรุง คู่มือการสำรองข้อมูล

1.5.3 เมื่อมีอุปสรรคขัดข้องในการปฏิบัติตามแผนฯ ให้หน่วยงาน หาทางแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่ หากไม่สามารถแก้ไขได้ให้รายงานและขอความช่วยเหลือจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ของโรงพิมพ์ตำรวจ ทันที

2. แผนการปฏิบัติงานสำรองข้อมูลและกู้คืนข้อมูล

แสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ ดังนี้ต่อไปนี้ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติขั้นตอนในแต่กรณี โดยกรณีที่วิเคราะห์และกำหนดผังกระบวนการ ได้ประเมินจากปัจจัยด้านอาคารสถานที่ สภาพแวดล้อม บุคลากร และงบประมาณ ของโรงพิมพ์ตำรวจ

2.1 กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีกระบวนการปฏิบัติ ดังนี้



ดำเนินขั้นตอนตามแผนกู้คืน เมื่อเกิดความเสียหายจากเหตุการณ์ไฟไหม้
โดยสามารถนำข้อมูลที่สำรองไว้กลับคืนมาได้ในระยะเวลา 2.5 ชม.

2.2 กรณีโดนเจาะระบบคอมพิวเตอร์ (Hack) มีกระบวนการปฏิบัติ ดังนี้

1. ตัด Internet Connection ของเครื่องนั้นๆ เสียก่อน เพื่อหยุดการทำลายหรือขโมยข้อมูลไปมากกว่านี้

2. ตรวจดู Log ของ Server ไม่ว่าจะเป็น Log ของ OS หรือ Log ของ Web Server เพื่อค้นหาว่ามีพฤติกรรมผิดปกติใดๆ ที่เกิดขึ้นกับเครือข่าย เมื่อเวลาใด โดย IP ใด

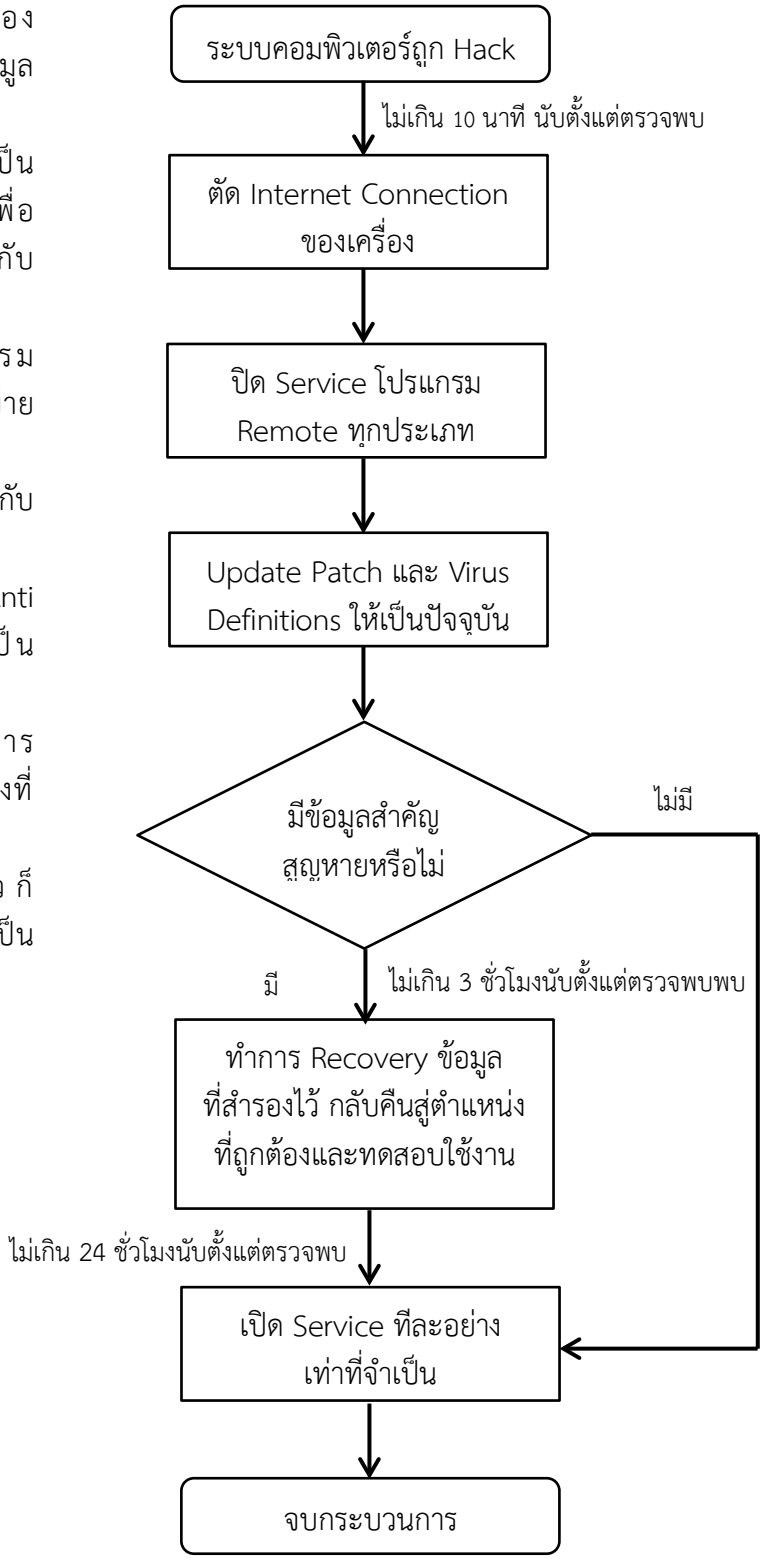
3. จัดการปิด Service ของโปรแกรม Remote ทุกประเภท ที่ติดตั้งไว้ในเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย

4. Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

5. ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบันกับทุก Server

6. กรณีข้อมูลสำคัญสูญหายให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

7. เมื่อทำขั้นตอนดังกล่าวเรียบร้อยแล้ว ก็ค่อยๆ เปิด Service ไปทีละอย่างเปิดเท่าที่จำเป็นต่อ Server เท่านั้น

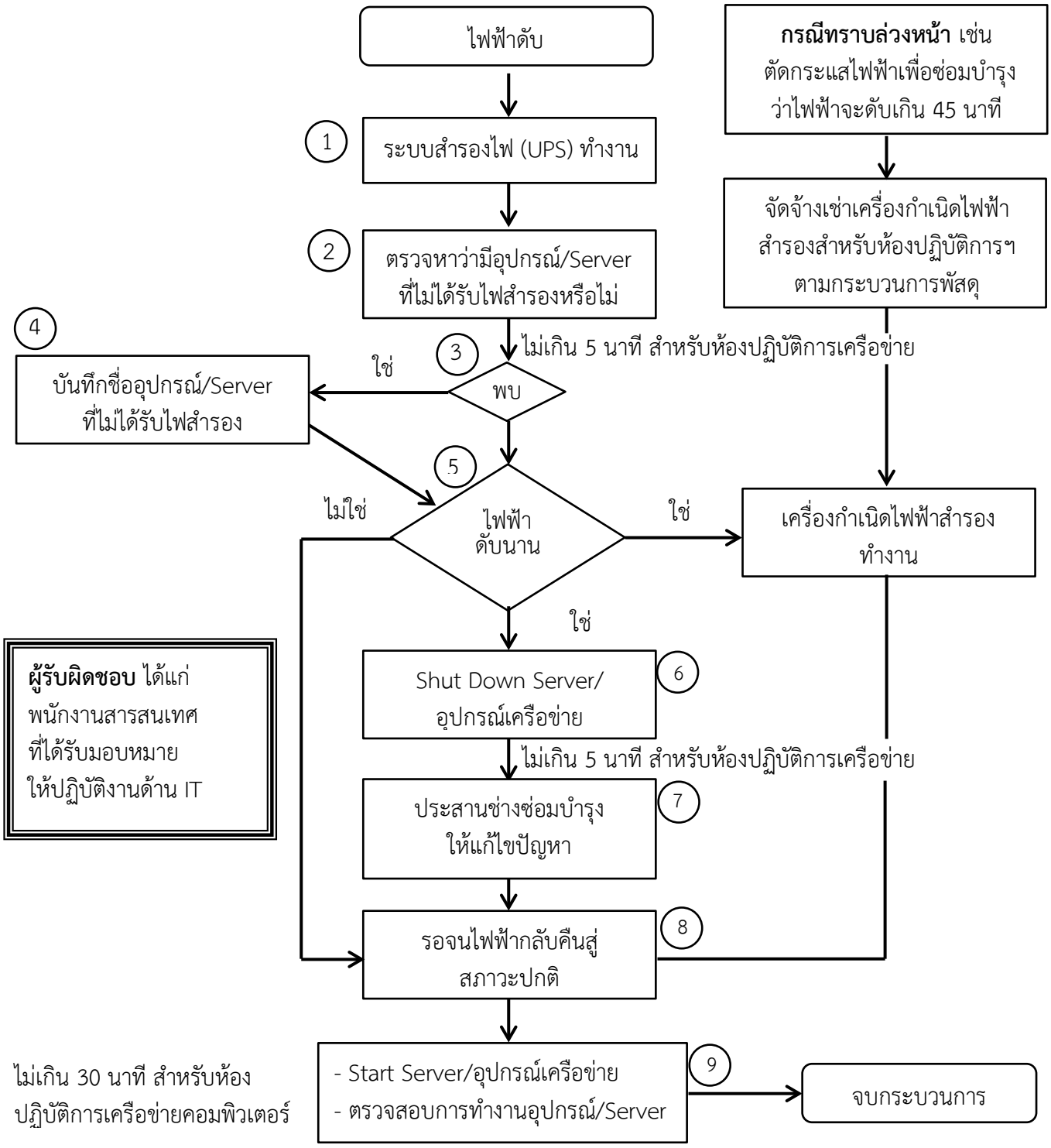


ผู้รับผิดชอบ ได้แก่ พนักงานสารสนเทศที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT

ดำเนินขั้นตอนตามแผนกู้คืน เมื่อเกิดความเสียหายจากกรณีโดนเจาะระบบคอมพิวเตอร์ (Hack) โดยสามารถนำข้อมูลที่สำรองไว้กลับคืนมาได้ในระยะเวลา 2.5 ชม.

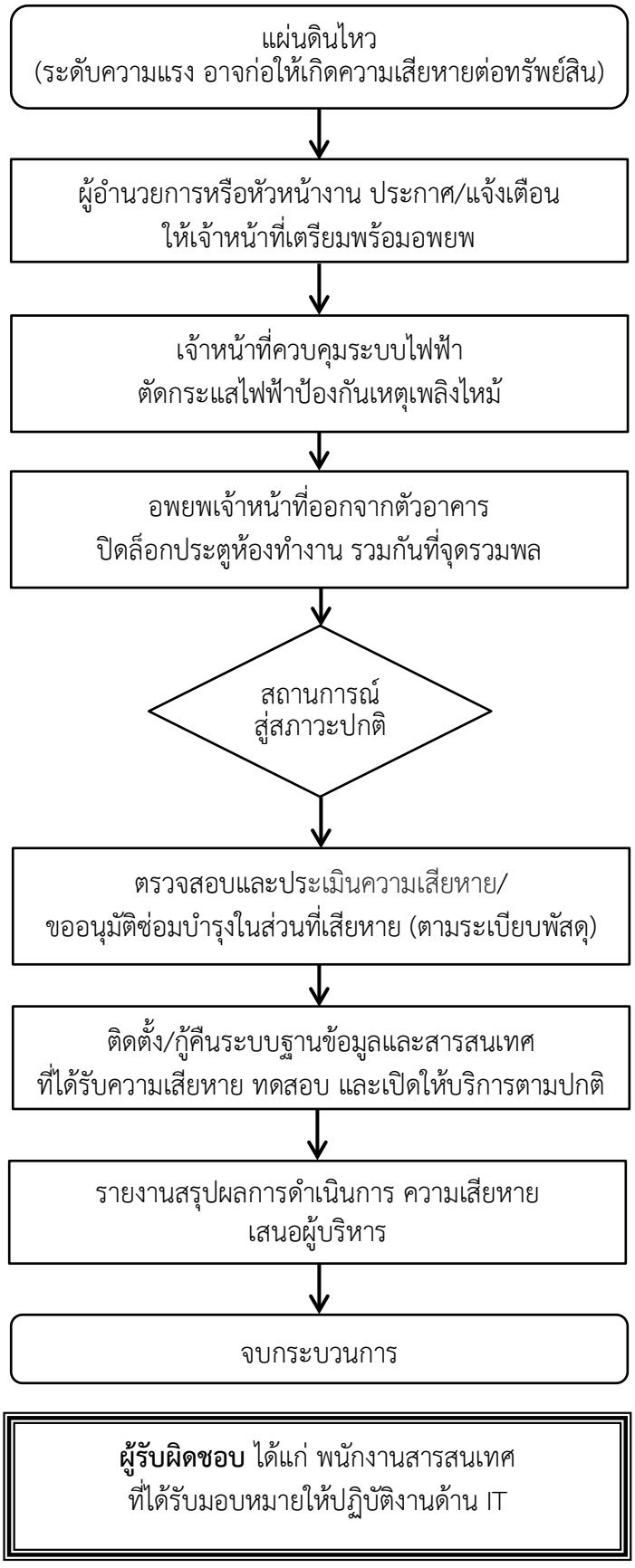
2.3 กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติ ดังนี้

กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติดังนี้ ได้เตรียมการรองรับเหตุการณ์ไฟฟ้าดับสำหรับห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ด้วยการติดตั้งเครื่องสำรองไฟฟ้า (UPS) 2 เครื่อง สำหรับห้องปฏิบัติการเครือข่ายคอมพิวเตอร์



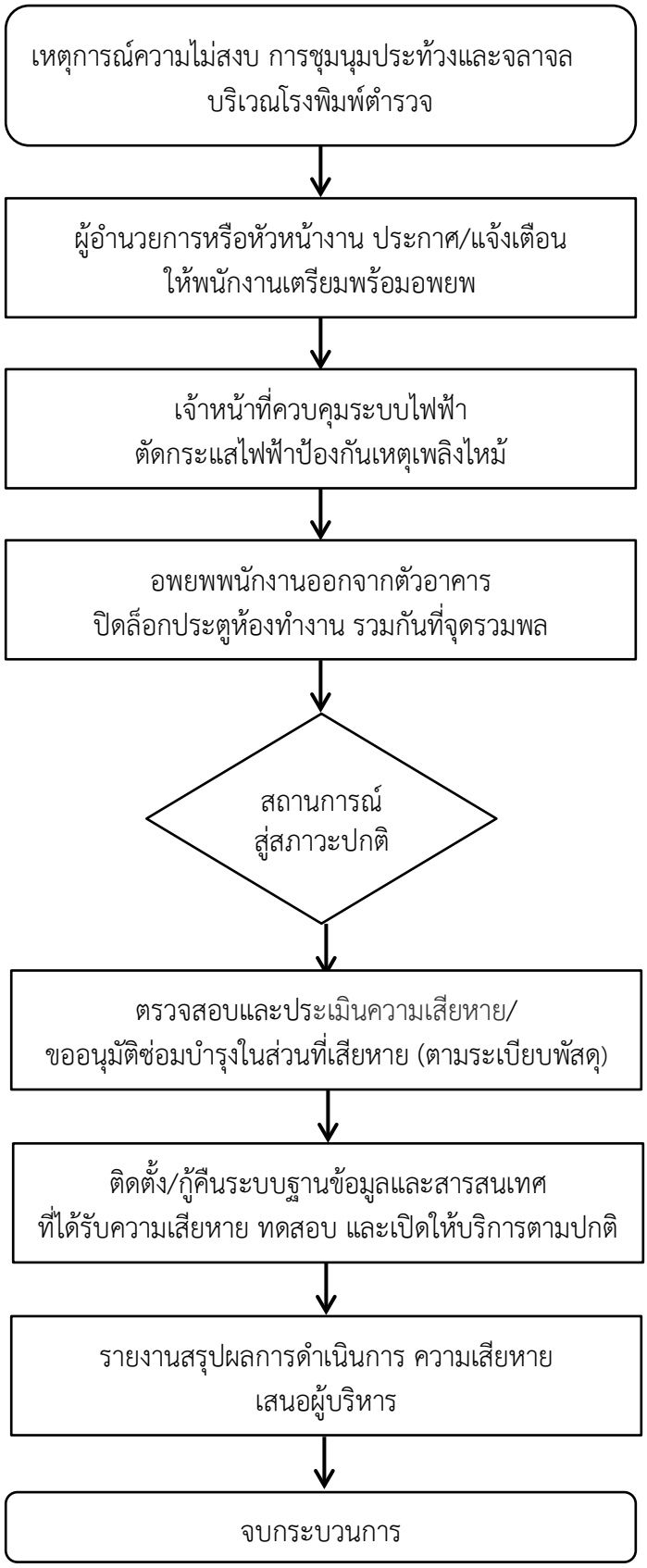
ดำเนินขั้นตอนตามแผนกู้คืน เมื่อเกิดความเสียหายจากกรณีไฟฟ้าดับ โดยสามารถนำข้อมูลที่สำรองไว้กลับคืนมาได้ในระยะเวลา 2.5 ชม.

2.4 กรณีแผ่นดินไหว มีกระบวนการปฏิบัติ ดังนี้



ดำเนินขั้นตอนตามแผนกู้คืน เมื่อเกิดความเสียหายจากกรณีแผ่นดินไหว
โดยสามารถนำข้อมูลที่สำรองไว้กลับคืนมาได้ในระยะเวลา 2.5 ชม.

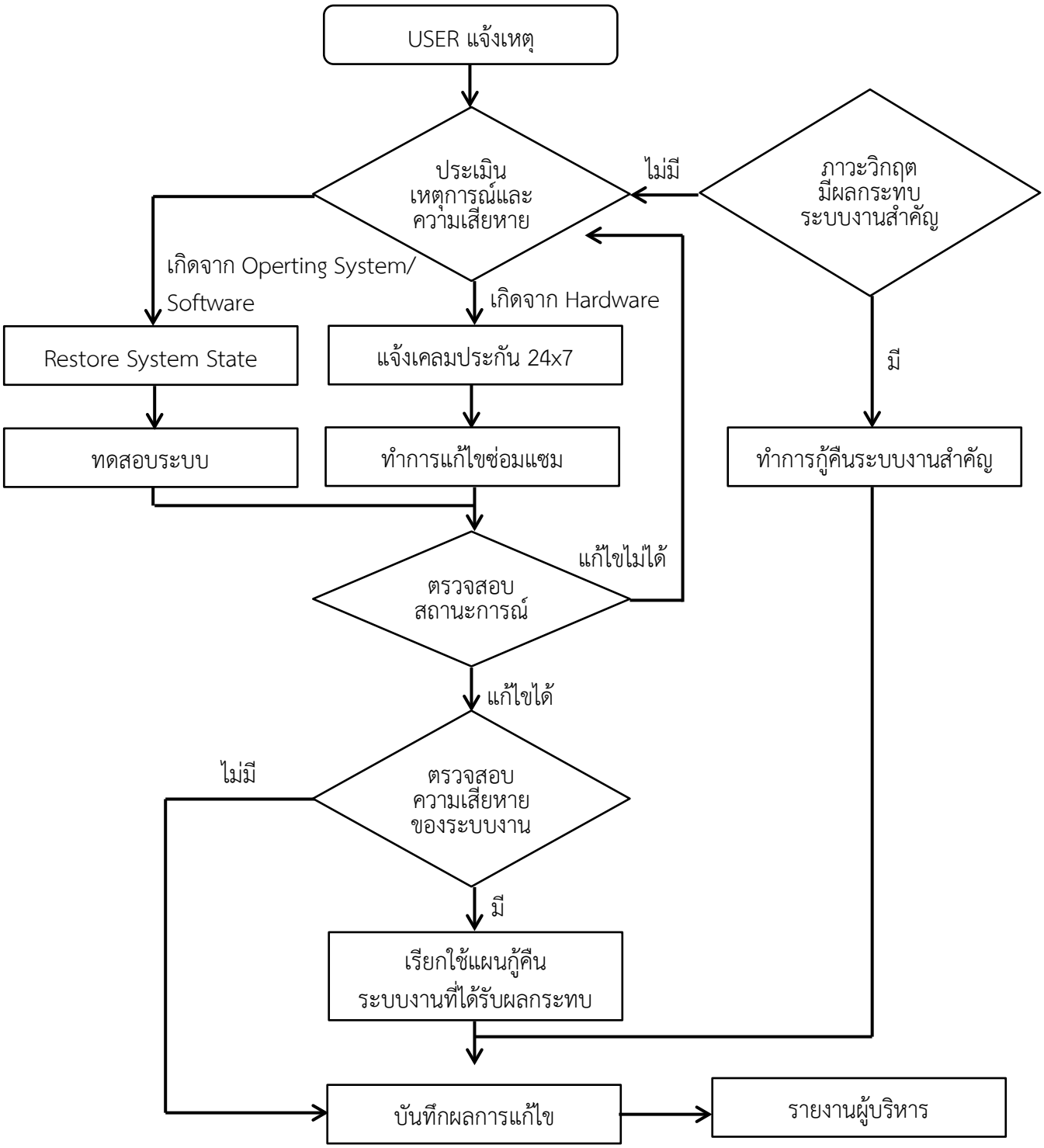
2.5 กรณีเหตุการณ์ความไม่สงบ การชุมนุมประท้วงและจลาจล มีกระบวนการปฏิบัติ ดังนี้



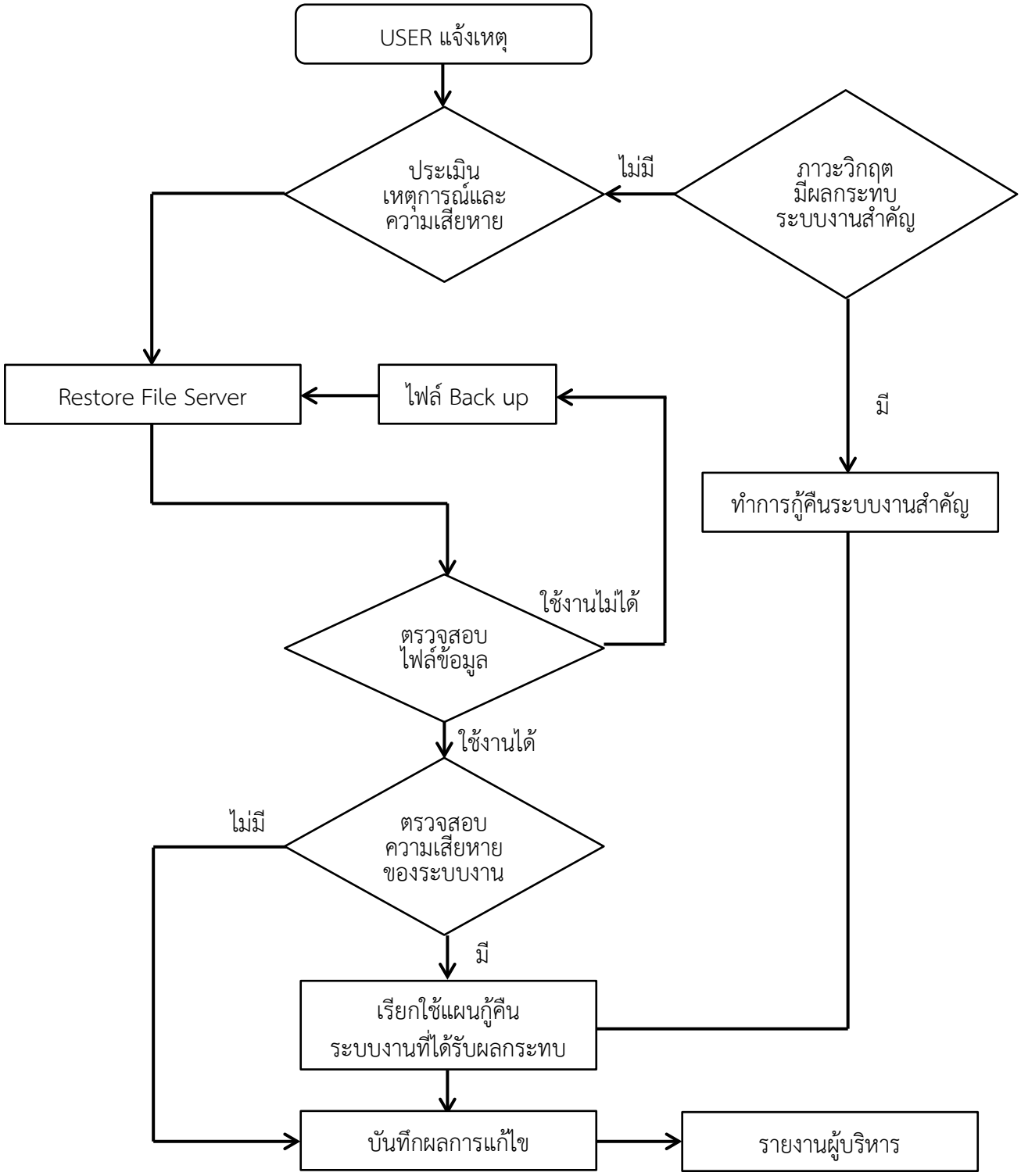
ผู้รับผิดชอบ ได้แก่ พนักงานสารสนเทศที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT

ดำเนินขั้นตอนตามแผนกู้คืน เมื่อเกิดความเสียหายจากกรณีเหตุการณ์ความไม่สงบ การชุมนุมประท้วงและจลาจล โดยสามารถนำข้อมูลที่สำรองไว้กลับคืนมาได้ในระยะเวลา 2.5 ชม.

2.6 กรณีระบบ Server ไม่สามารถใช้งานได้ มีกระบวนการปฏิบัติ ดังนี้



2.7 กรณี File ข้อมูลเสียหาย มีกระบวนการปฏิบัติ ดังนี้



3. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

7.1 ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบ การปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

7.1.1 รองผู้อำนวยการโรงพิมพ์ตำรวจ หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

7.1.2 หัวหน้าฝ่าย/หัวหน้างาน โรงพิมพ์ตำรวจ สำนักงานตำรวจแห่งชาติ

7.2 ระดับปฏิบัติ

7.2.1 คณะอนุกรรมการกำกับดูแลบริหารด้านจัดการสารสนเทศและพัฒนาระบบงาน

7.2.2 พนักงานสารสนเทศ โรงพิมพ์ตำรวจ สำนักงานตำรวจแห่งชาติ

โดยมีหน้าที่

1. ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่ายคอมพิวเตอร์ และระบบรักษาความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

2. รักษาความปลอดภัยของระบบฐานข้อมูล รวมทั้งการสำรองฐานข้อมูลสำคัญ

3. ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ ตามแต่ละกรณีเหตุการณ์ที่เกิดขึ้น

4. การติดตามประเมินผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบ รายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้