กรมสุขภาพจิต
DEPARTMENT OF MENTAL HEALTH

แผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) กรมสุขภาพจิต กระทรวงสาธารณสุข

IT Contingency Plan

สำนักเทคโนโลยีสารสนเทศ
กรมสุขภาพจิต

ปรับปรุงครั้งที่ 2
วันที่มีผลบังคับใช้ 3 เมษายน 2567

กรมสุขภาพจิต
DEPARTMENT OF MENTAL HEALTH

แผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) กรมสุขภาพจิต กระทรวงสาธารณสุข

สำนักเทคโนโลยีสารสนเทศ
กรมสุขภาพจิต

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

1. หลักการและเหตุผล

ระบบเทคโนโลยีสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการและให้บริการประชาชนในสภาวะวิกฤต เช่น เกิดเหตุไฟไหม้ (อัคคีภัย), แผ่นดินไหว, น้ำท่วม, การเกิดโรคระบาดของโรคติดเชื้อไวรัสโคโรนา 2019 (COVID-19) และเป็นมาตรการเตรียมความพร้อมรองรับสถานการณ์ของหน่วยงาน ส่งผลให้เกิดประสิทธิภาพและส่งผลต่อทางราชการอย่างสูงสุด

กรมสุขภาพจิตได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศ จึงได้ทบทวนและปรับปรุงแผนการบริหารความพร้อมต่อสภาวะวิกฤตและสามารถรองรับกรณีเกิดโรคระบาดต่อเนื่อง ซึ่งมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ (Software) รวมทั้งระบบอุปกรณ์ (Hardware) เกิดความเสียหายได้ โดยเฉพาะอย่างยิ่งระบบเทคโนโลยีสารสนเทศที่นำมาใช้ในการบริหารจัดการ

ดังนั้น กรมสุขภาพจิต จึงได้จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) กรมสุขภาพจิต กระทรวงสาธารณสุข เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมสุขภาพจิต

2. วัตถุประสงค์

2.1 เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.2 เพื่อลดความเสียหายที่จะอาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อให้การปฏิบัติงาน ดำเนินไปได้อย่างมีเสถียรภาพ และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ และสามารถรองรับการเกิดโรคระบาดต่อเนื่อง

3. เป้าหมาย

3.1 ระบบเทคโนโลยีสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ระบบข้อมูลผู้ป่วยด้านจิตเวช (Data center), เว็บไซต์กรมสุขภาพจิต (Web Application Program), ระบบข้อมูล DPIS ,ระบบข้อมูล B&P, ระบบข้อมูลการเงินการคลัง ระบบเพื่อการบริหารงานภายใน (Back Office) ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์, ระบบการจองห้องประชุม เป็นต้น

3.2 อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์แม่ข่ายระบบเน็ตเวิร์ค (Network Server), เครื่องคอมพิวเตอร์แม่ข่ายระบบฐานข้อมูล (Database Server), เครื่องคอมพิวเตอร์แม่ข่ายที่ใช้จัดเก็บและสำรองข้อมูล (Storage Server), เครื่องแม่ข่ายสำหรับให้บริการเว็บไซต์องค์กร (Web server), เครื่องคอมพิวเตอร์ป้องกันการจู่โจมข้อมูลจากบุคคลภายนอก (Firewall), เครื่องไมโครคอมพิวเตอร์, เครื่องคอมพิวเตอร์ชนิดพกพา (Note Book), เครื่องสแกนเนอร์ (Scanner), เครื่องพิมพ์เลเซอร์ (Laser Printer), เครื่องพิมพ์แบบพ่นหมึก (Inkjet Printer), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB), อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point)

4. แนวทางปฏิบัติเพื่อป้องกันและการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมด้านระบบเทคโนโลยีสารสนเทศ

4.1 อาคาร สถานที่

อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ ติดตั้งประจำโต๊ะทำงาน

4.2 ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะ ดังนี้

1. กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี
2. ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออก ของบุคคลเป็นจำนวนมาก
3. จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว
4. จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่
5. หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยก ออกมาจาก บริเวณดังกล่าว
6. ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด
7. จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

4.3 การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

1. มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสมเพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการ กำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

4.4 การควบคุมการเข้าออก อาคารสถานที่

1. กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ "พื้นที่ใช้งานระบบ" อย่างชัดเจน

2. การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

3. ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitors)

4. ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

5. บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

6. จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

7. ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและ จากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

8. มีการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

9. สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

10. มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

11. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

12. มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้าออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

13. จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานใน พื้นที่หรือบริเวณที่มีความสำคัญ

14. จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ 1 ครั้ง

4.5 ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

1. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอ ต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)
- ระบบระบายอากาศ
- ระบบปรับอากาศ และควบคุมความชื้น

2. ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

3. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

4.6 การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

1. หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

2. ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

3. ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

4. ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

5. จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

6. ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

7. พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable) สำหรับระบบสารสนเทศที่สำคัญ

8. ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

4.7 การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

1. ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาตามคำแนะนำของผู้ผลิต

2. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามคำแนะนำของผู้ผลิต

3. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

4. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์

5. ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

6. จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจาก ภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

4.8 การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

1. มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

2. กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

3. กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

4. เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและ ตรวจสอบการชำรุดเสียหายของอุปกรณ์

5. บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็น หลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

4.9 การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

1. กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

2. ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

3. เจ้าหน้าที่ที่รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของหน่วยงานให้เสมือนเป็นทรัพย์สินของตนเอง

4.10 การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment)

1. ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

2. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกัน ไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

4.11 การสำรองข้อมูล (Back Up)

1. การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในฮาร์ดดิสก์ 1 ชุดในเวลาเที่ยงคืนของทุกวัน

2. การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรอง (Backup) ข้อมูลตามระยะเวลาที่กำหนด รวมทั้งจัดให้มีระบบการบำรุงรักษา (Restructure/Reformat) ระบบฐานข้อมูล ประกอบด้วย

2.1 การสำรองข้อมูลประจำวัน จะทำการสำรองข้อมูลและโครงสร้างข้อมูล

2.2 การสำรองข้อมูลประจำสัปดาห์ จะทำการสำรองข้อมูล โครงสร้างข้อมูล และ Source Code โดยบันทึกข้อมูลลงใน External Hard disk

2.3 การสำรองข้อมูล Source Code โปรแกรมประจำเดือน

2.4 การสำรองข้อมูลประจำปี

4.12 การกู้ข้อมูล (Recovery)

1. ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้ทำการสำรองไว้ใน External Hard disk ทุกวันศุกร์ของสัปดาห์

2. ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

3. ข้อมูลที่ต้องทำการ Recovery ทันที ได้แก่ เช่น ระบบข้อมูลผู้ป่วยด้านจิตเวช (Datacenter), ระบบข้อมูล DPIS ,ระบบข้อมูล B&P,ระบบข้อมูลการเงินการคลัง ระบบเพื่อการบริหารงานภายใน (Back Office) ได้แก่ ระบบสารบรรณอิเล็กทรอนิกส์, ระบบการจองห้องประชุม โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Antivirus), โปรแกรมระบบปฏิบัติการการจัดการเครือข่าย (Network Software) และเว็บไซต์กรมสุขภาพจิต (Web Application Program)

4.13 การป้องกันไวรัส

1. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ
2. มีการตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูล
3. ใช้ความระมัดระวังในการเปิด e-mail ที่ไม่ทราบแหล่งที่มา เช่น spam mail
4. ระมัดระวังในการดาวน์โหลดไฟล์ต่าง ๆ จากอินเตอร์เน็ต เช่น เว็บไซต์ดาวน์โหลดหนังต่าง ๆ

4.14 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ มีแนวทางการควบคุมดังนี้

1. มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก มีการติดตั้งรหัส / Key card ในการเข้าออก

2. มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

3. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

4. การเรียกใช้ระบบเทคโนโลยีสารสนเทศ จากหน่วยงานต่าง ๆ ทั้งในส่วนกลาง และส่วนภูมิภาค ผู้ใช้ระบบจะต้องมีการบันทึกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ ตามอำนาจหน้าที่และความรับผิดชอบ

4.15 การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศ ของสำนักเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการ จัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

(1) USB Boot Disk

(2) เครื่องมือสำหรับการติดตั้ง ระบบปฏิบัติการ/ระบบเครือข่าย/ระบบงานที่สำคัญ

(3) ดิสก์สำรองข้อมูลและระบบงานที่สำคัญ

(4) โปรแกรม Antivirus/Antispyware

(5) driver อุปกรณ์ต่าง ๆ

(6) ระบบสำรองไฟฉุกเฉิน

(7) อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

4.16 อุปกรณ์อื่น ๆ ที่เกี่ยวข้อง ได้แก่

(1) อุปกรณ์ควบคุมการเข้าสู่เครือข่ายที่เรียกว่า Firewall ติดตั้งอยู่ที่เครื่อง Server หลัก ที่ทำหน้าที่เป็น Web Server สำหรับป้องกันการบุกรุกจากบุคคลภายนอกที่ต้องการเจาะเข้าสู่ระบบประมวลผลของกรมสุขภาพจิต คือ ระบบ Internet จำนวน 2 เครื่อง

(2) อุปกรณ์ดับเพลิงอัตโนมัติด้วยสารเคมี สำหรับอุปกรณ์ IT ติดตั้งอยู่ที่ห้อง Server สำนักเทคโนโลยีสารสนเทศ สำหรับกรณีเกิดไฟไหม้ในห้อง Server

(3) จัดให้มีระบบทำความเย็นเปิดสลับภายในห้อง Server เพื่อรักษาสมรรถนะเครื่อง Server ให้สามารถทำงานได้ตลอด 24 ชั่วโมง

(4) จัดให้มีโปรแกรมสำหรับตรวจสอบ และป้องกันการบุกรุกเข้าสู่ระบบประมวลผลฐานข้อมูลเครื่องแม่ข่ายหลัก จำนวน 1 โปรแกรม

(5) จัดให้มีโปรแกรมสำหรับป้องกันการถูกโปรแกรมไวรัสเข้าทำลายโปรแกรมระบบปฏิบัติการและระบบฐานข้อมูล (Antivirus) ได้แก่ โปรแกรม eset หรือโปรแกรมป้องกันไวรัส ตามนโยบายที่ทุกสำนัก/กองกำหนดไว้ โดยกำหนดให้ Server ตรวจสอบและ update โปรแกรมอัตโนมัติ

4.17 มาตรการความปลอดภัยด้วยรหัสผ่าน

การสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ มีวัตถุประสงค์เพื่อป้องกันมิให้บุคคลที่ไม่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ไม่สามารถเข้าถึง แก้ไข เปลี่ยนแปลง ข้อมูล หรือไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศในส่วนที่ มิได้มีอำนาจหน้าที่เกี่ยวข้อง โดย

4.17.1 กำหนดสิทธิการเข้าถึงข้อมูลและระบบเทคโนโลยีสารสนเทศ ให้แก่ผู้ใช้งานอย่างเหมาะสมกับหน้าที่และความรับผิดชอบ โดยมีระบบรักษาความปลอดภัยที่อนุญาตให้ผู้ที่เกี่ยวข้อง ผู้ที่รับผิดชอบสามารถเข้า

ในระบบได้ตาม ความรับผิดชอบ (Access) โดยมีลำดับขั้นของระบบฐานข้อมูลและการกำหนดสิทธิให้บุคคลสามารถเข้าถึงแต่ละ ระดับฐานข้อมูล ดังนี้

(1) บุคคลที่สามารถเรียกดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถแก้ไข ปรับปรุงข้อมูลได้

(2) บุคคลที่สามารถเรียกดูข้อมูลและแก้ไข ปรับปรุงข้อมูลในส่วนที่ผู้ใช้รับผิดชอบต่อความถูกต้องของข้อมูลในฐานข้อมูลนั้น

(3) บุคคลที่สามารถเรียกดู แก้ไข ปรับปรุงข้อมูล ระดับฐานข้อมูล ในกรณีที่ผู้ใช้มีข้อผิดพลาดในการปรับปรุงข้อมูล โดยให้เจ้าหน้าที่ของสำนักเทคโนโลยีสารสนเทศ หรือผู้รับผิดชอบของหน่วยงานเจ้าของระบบงาน เป็นผู้ดูแล แก้ไข ข้อมูลในส่วนนี้ ซึ่งการเข้าใช้ฐานข้อมูล ในแต่ละระบบ จะมีการกำหนดสิทธิการเข้าถึงฐานข้อมูล ตามหน้าที่ ความรับผิดชอบ ของผู้ใช้ฐานข้อมูล เพื่อรักษาความปลอดภัยของฐานข้อมูล โดยมีการกำหนด Login และ Password ในการเข้าถึงข้อมูลและผู้มีสิทธิเท่านั้นที่สามารถเข้าถึงและเปลี่ยนแปลงแก้ไขข้อมูลได้ ผู้ใช้ระบบทั่วไปที่ ผู้บังคับบัญชาที่เป็นหน่วยงานเจ้าของระบบ เป็นผู้อนุมัติให้ดำเนินการได้ โดยจะแบ่งเป็นการดูข้อมูลได้เพียงอย่างเดียว ไม่สามารถเปลี่ยนแปลงแก้ไขข้อมูลได้ และการที่สามารถปรับปรุงข้อมูลได้ ทั้งนี้เพื่อเป็นการรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ

4.17.2 กำหนดระยะเวลาการใช้งานระบบเทคโนโลยีสารสนเทศ ของผู้ใช้ระบบ (User) โดยผู้ใช้ระบบจะไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้ เมื่อพ้นระยะเวลาที่กำหนดไว้

4.17.3 การกำหนดรหัสผ่านควรมีความยาวไม่ต่ำกว่า 8 ตัวอักษร และควรใช้ ตัวเลข อักขระพิเศษประกอบและสำหรับผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ควรมีการเปลี่ยนรหัสผ่านอย่างน้อยทุก ๆ 3 เดือน ผู้ใช้งานจะต้องเก็บรหัสผ่านไว้เป็นความลับ ทั้งนี้ถ้ามีผู้อื่นรู้ รหัสผ่านจะต้องเปลี่ยนรหัสผ่านใหม่โดยทันที เพื่อป้องกันความปลอดภัยของการใช้ระบบเทคโนโลยีสารสนเทศ

5. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

5.1 กรณีเกิดเหตุไฟไหม้ (อัคคีภัย)

5.2 กรณีไฟฟ้าดับ

5.3 กรณีแผ่นดินไหว

5.4 กรณีโจรกรรมอุปกรณ์ในห้อง Data Center

5.5 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

5.6 กรณีสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

5.7 กรณีระบบเครือข่ายล่ม

5.8 กรณีระบบบริการด้านเครือข่ายล่ม

5.9 กรณีระบบสารสนเทศถูกโจมตี

5.10 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากภัยพิบัติทางธรรมชาติ

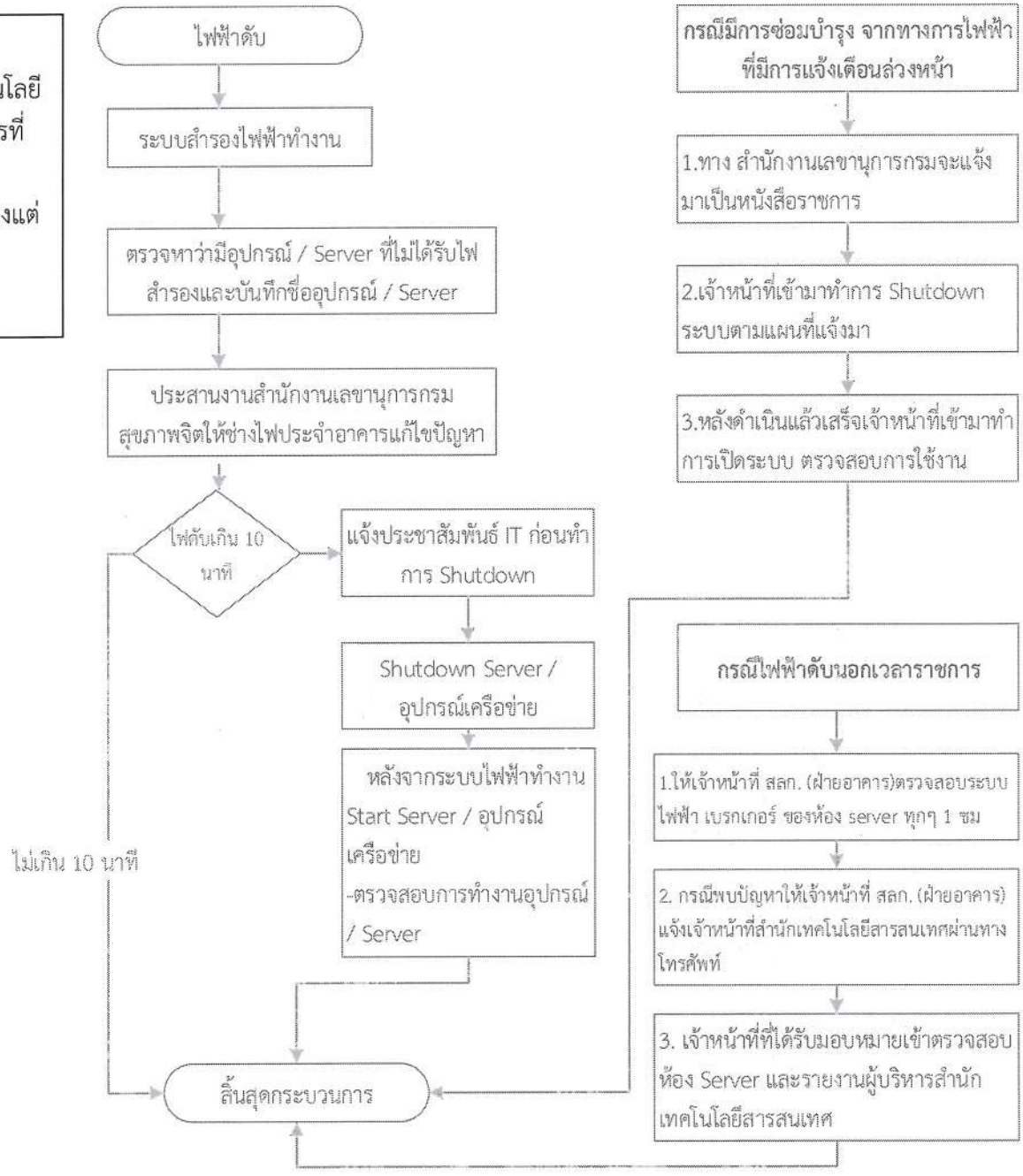
5.11 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดโรคระบาด

5.1 กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีขั้นตอนการปฏิบัติดังนี้

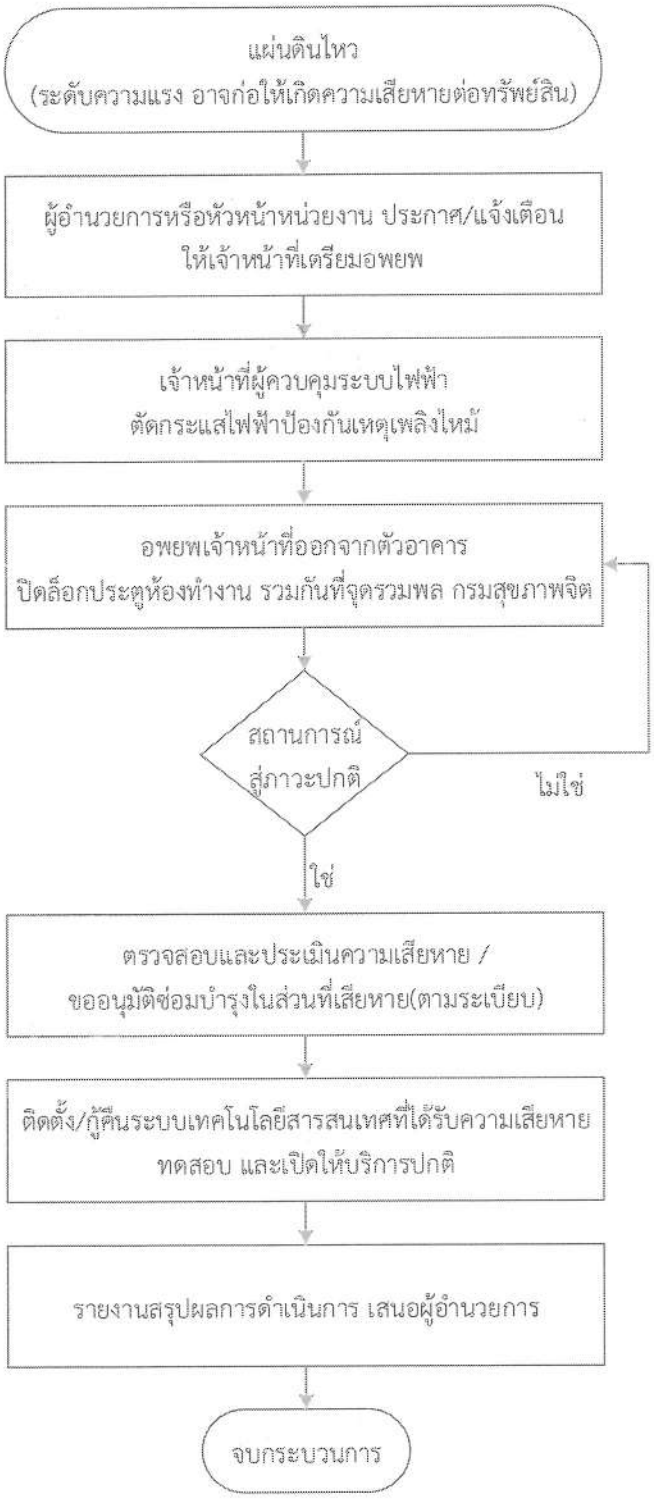
ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

5.2 กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติดังนี้

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

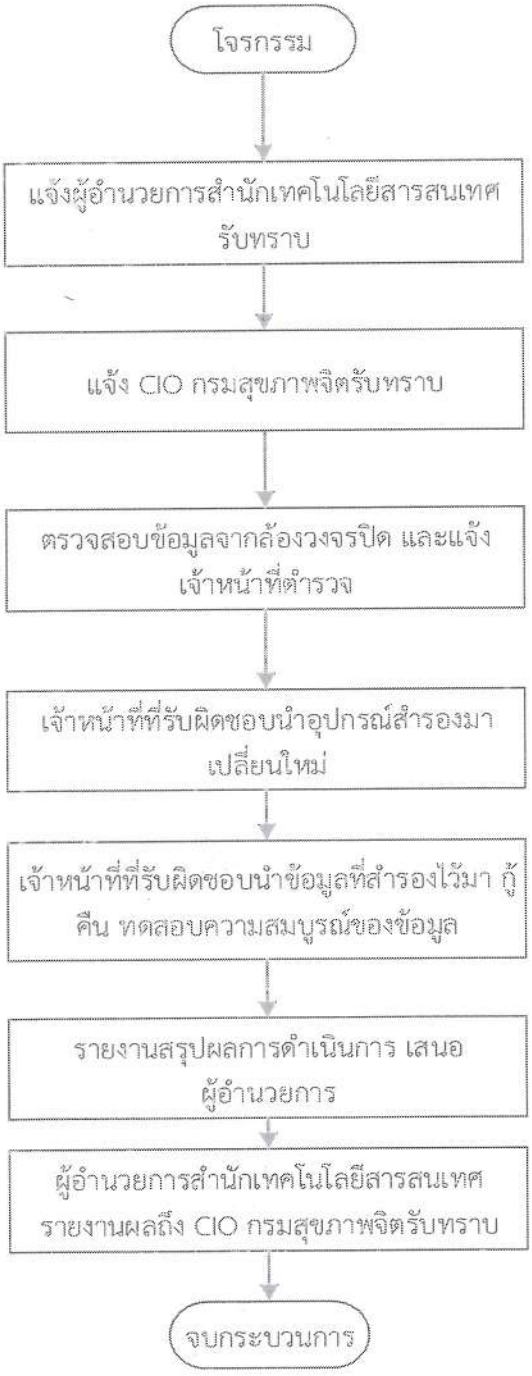


5.3 กรณีแผ่นดินไหว มีกระบวนการปฏิบัติดังนี้



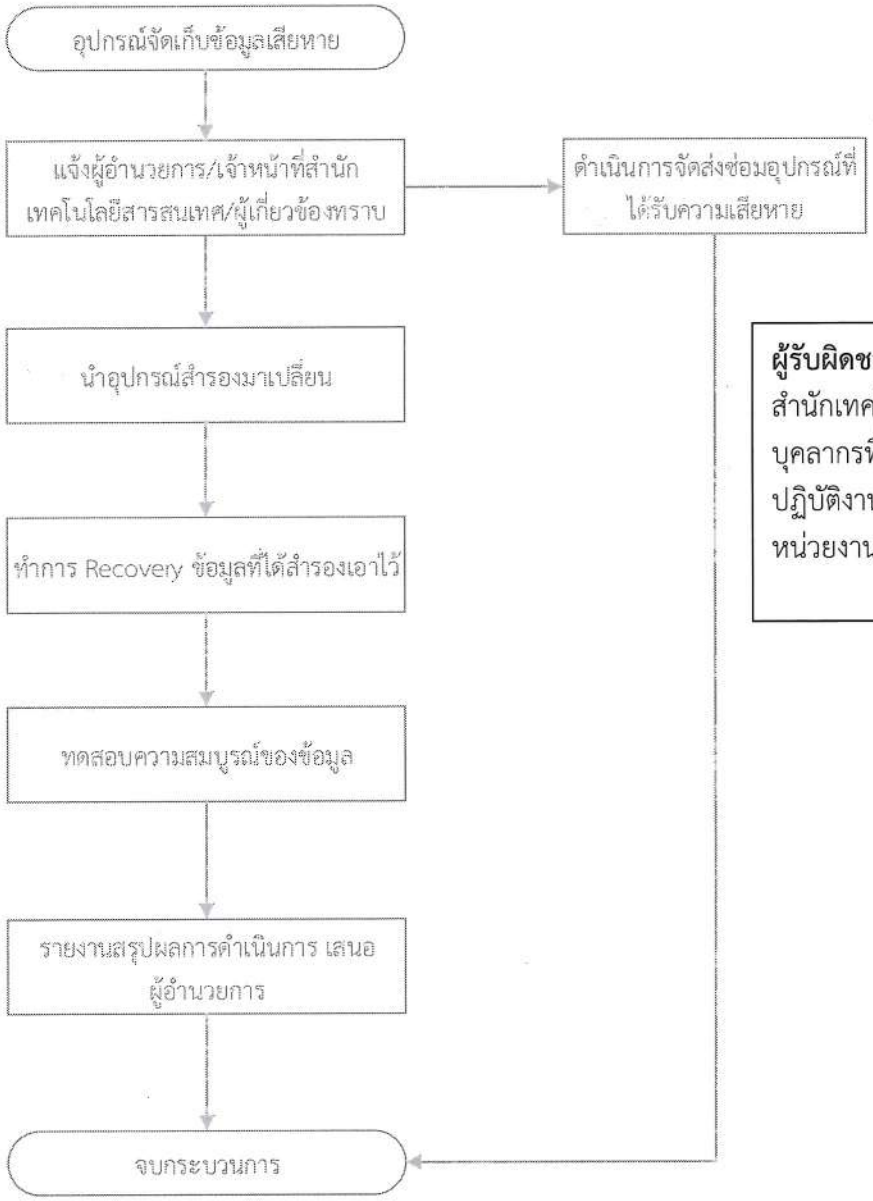
ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

5.4 กรณีโจรกรรมอุปกรณ์ในห้อง Data Center มีกระบวนการปฏิบัติดังนี้



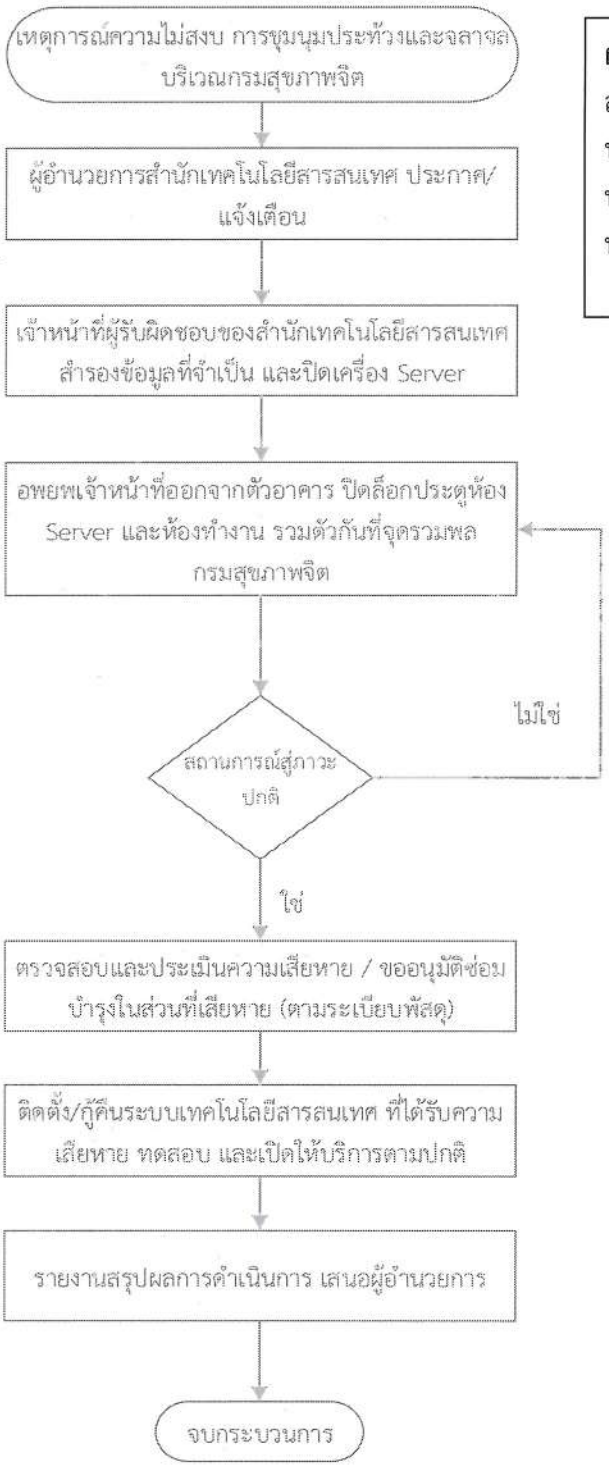
ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

5.5 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย มีกระบวนการปฏิบัติดังนี้



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

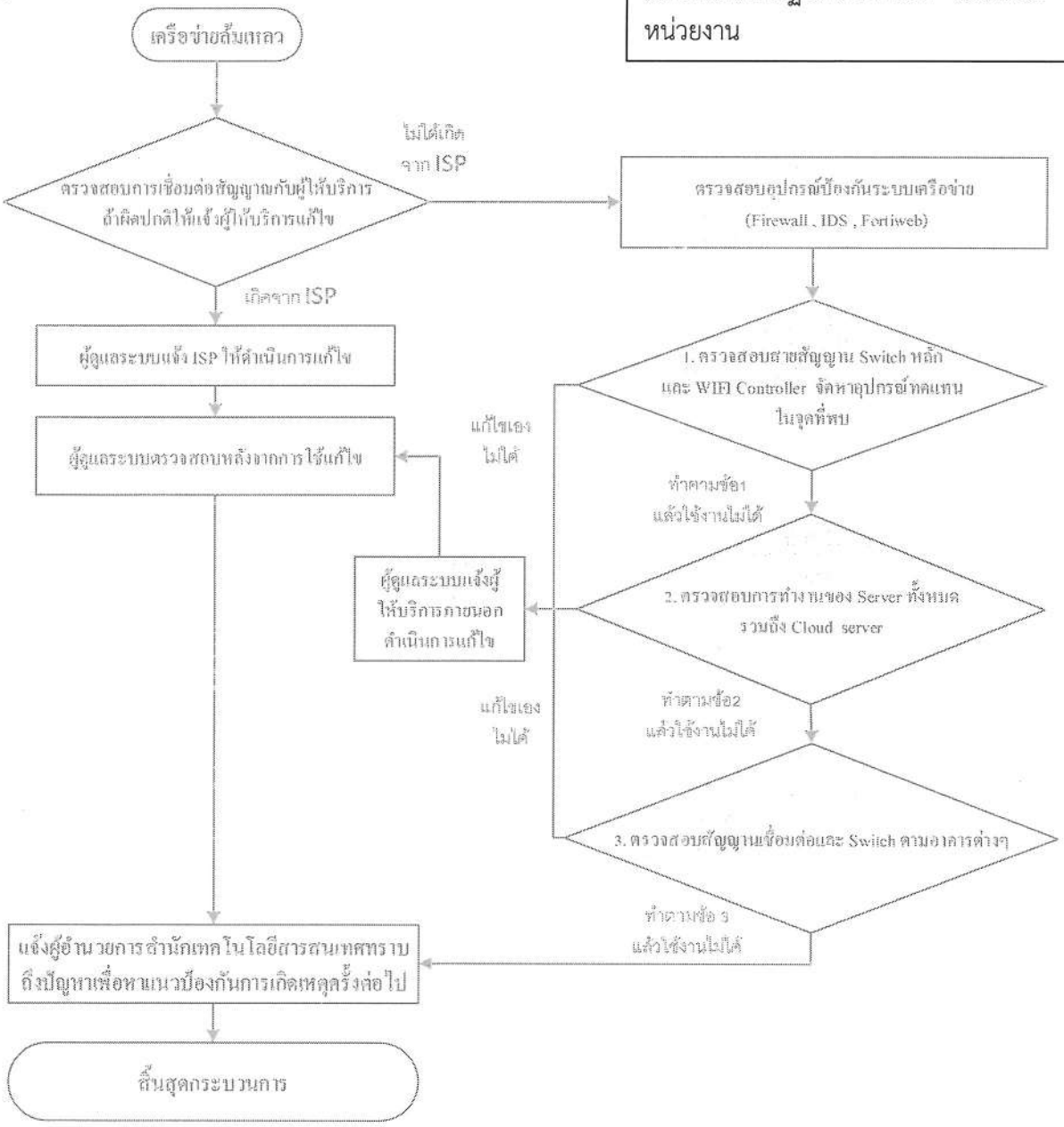
5.6 กรณีสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง มีกระบวนการปฏิบัติดังนี้



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

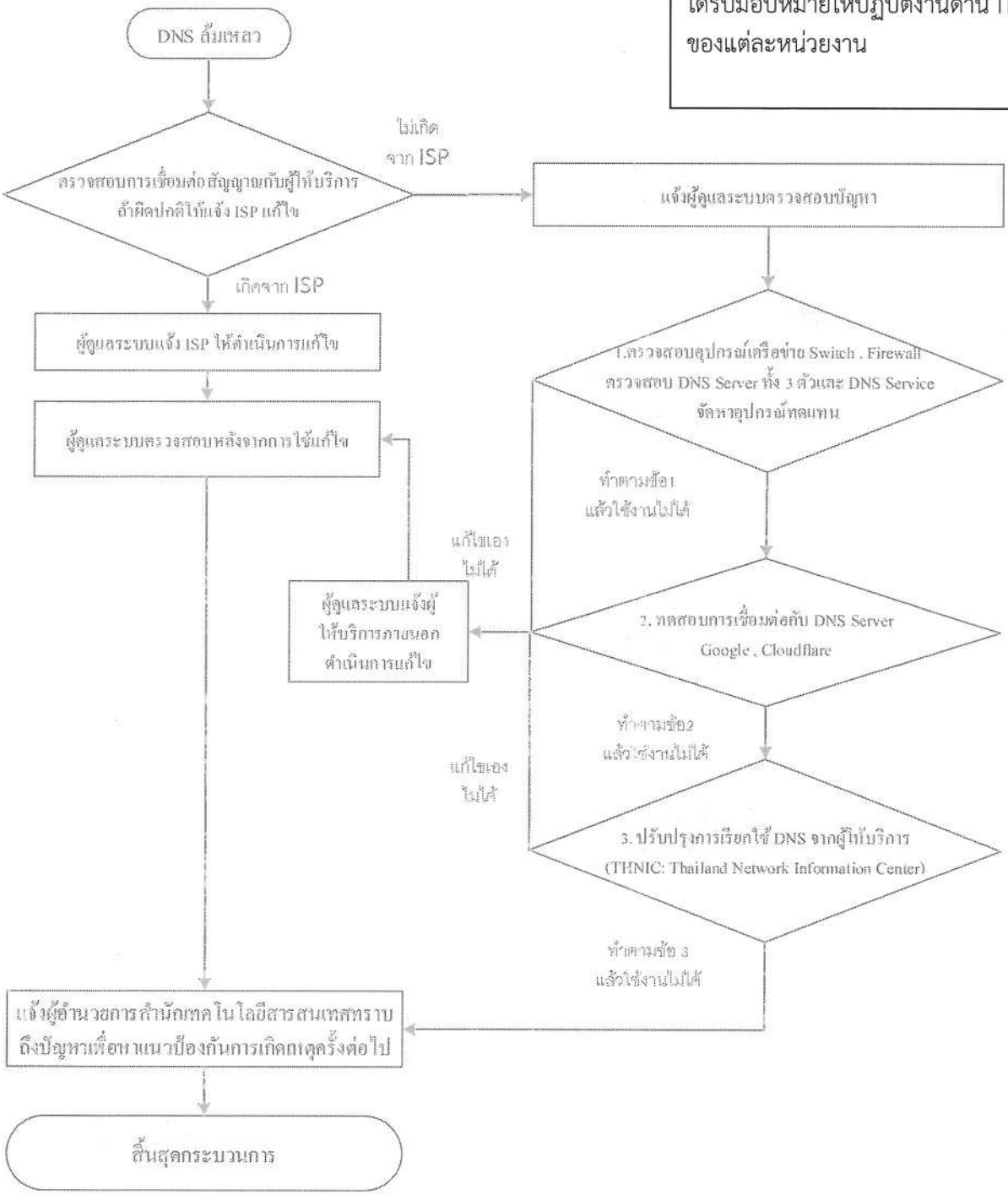
ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

5.7 กรณีระบบเครือข่ายล่ม มีกระบวนการปฏิบัติดังนี้



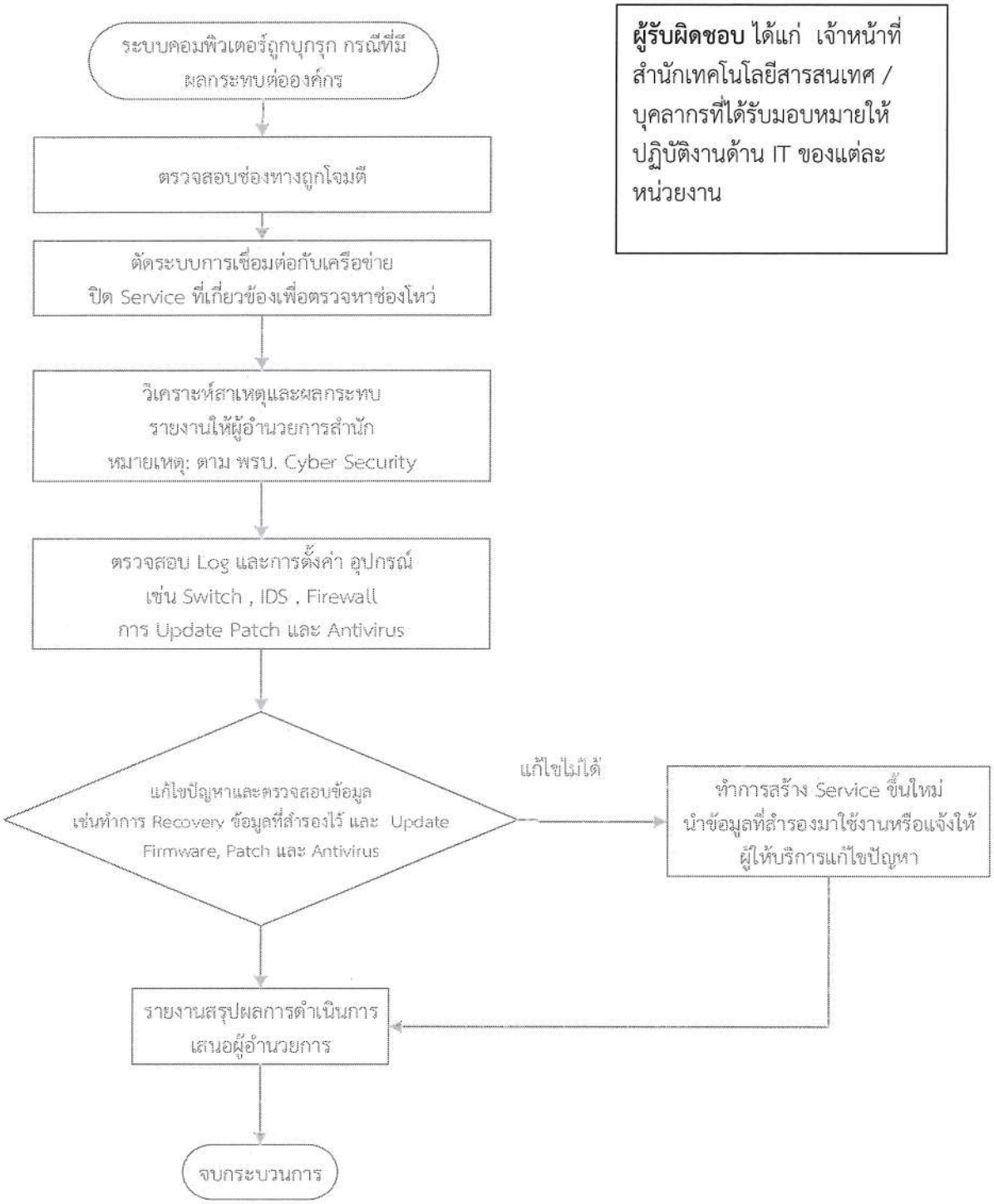
5.8 กรณีระบบบริการด้านเครือข่ายล่ม

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

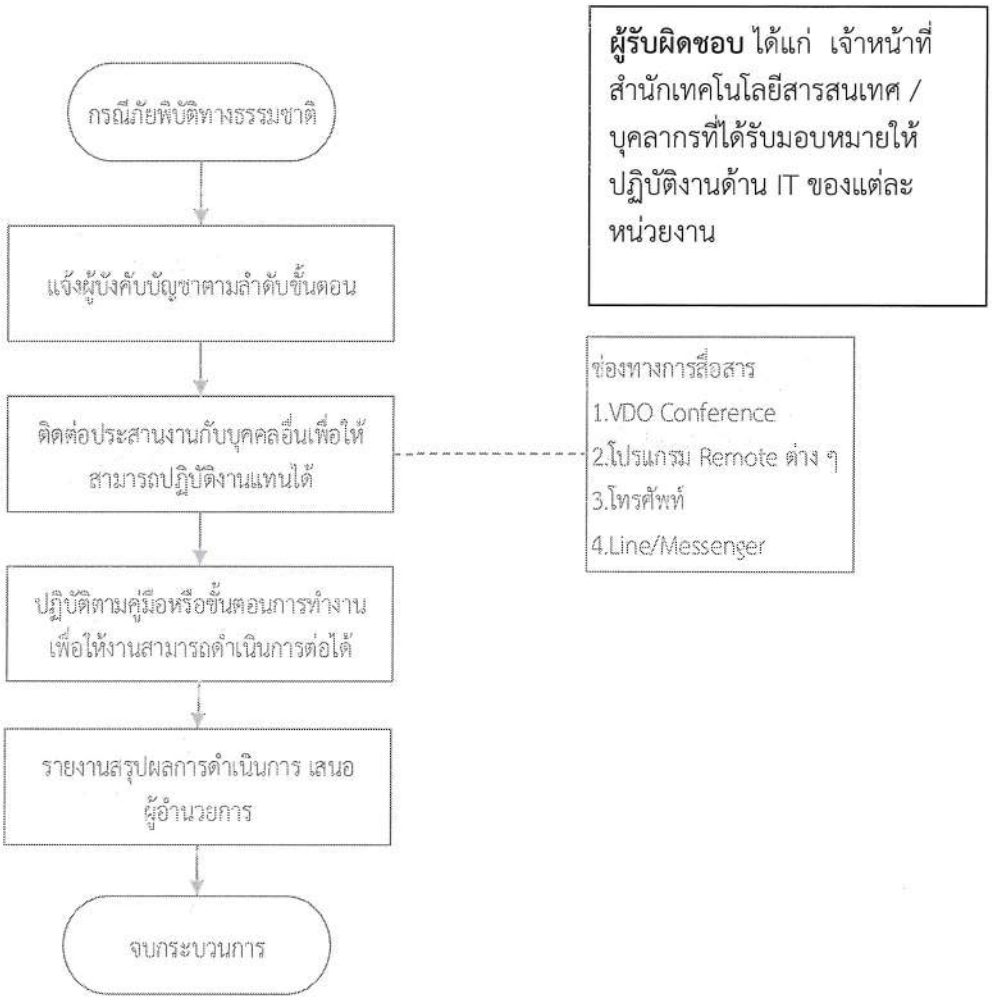


5.9 กรณีระบบสารสนเทศถูกโจมตี มีกระบวนการปฏิบัติดังนี้

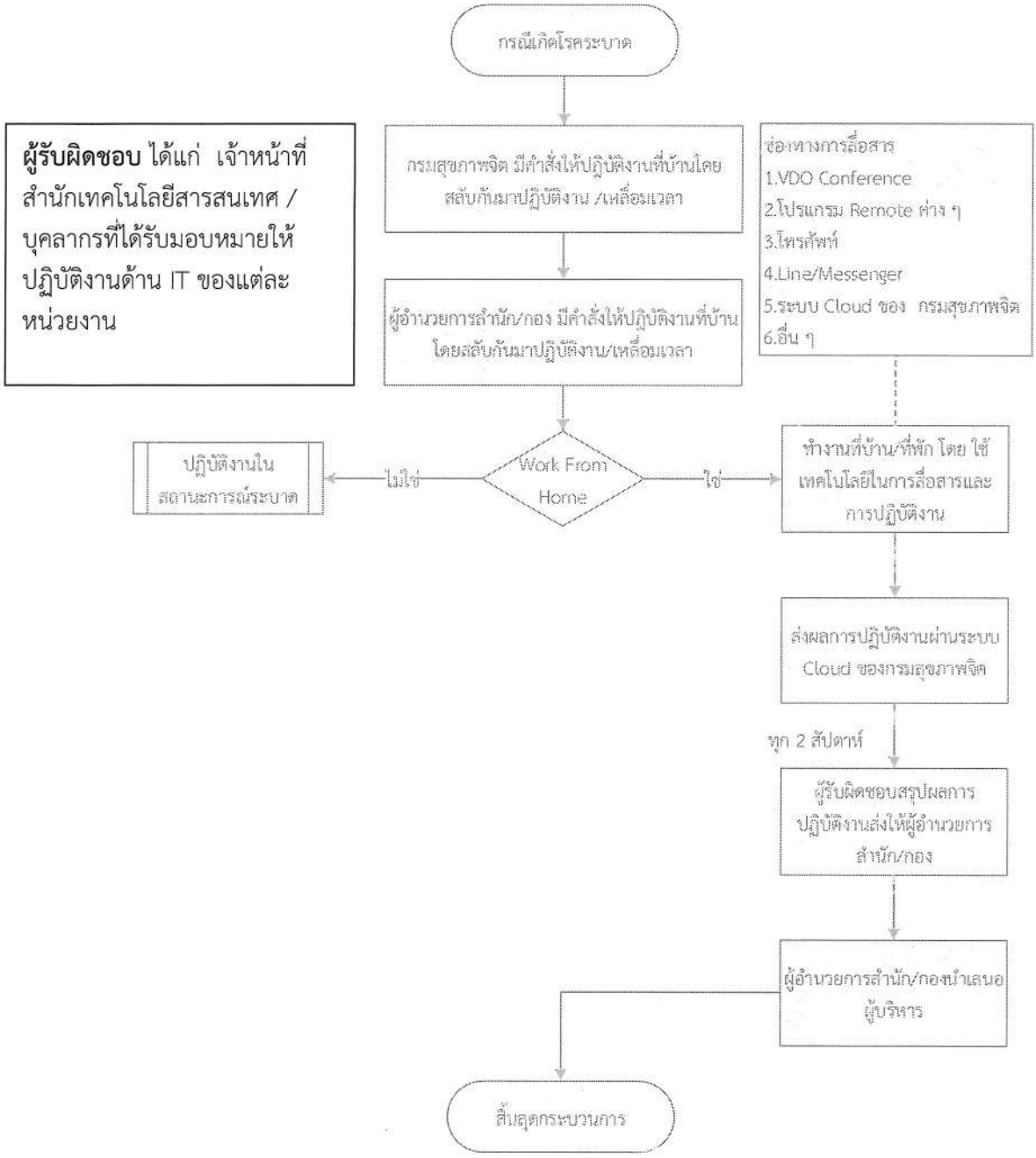
ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศ / บุคลากรที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

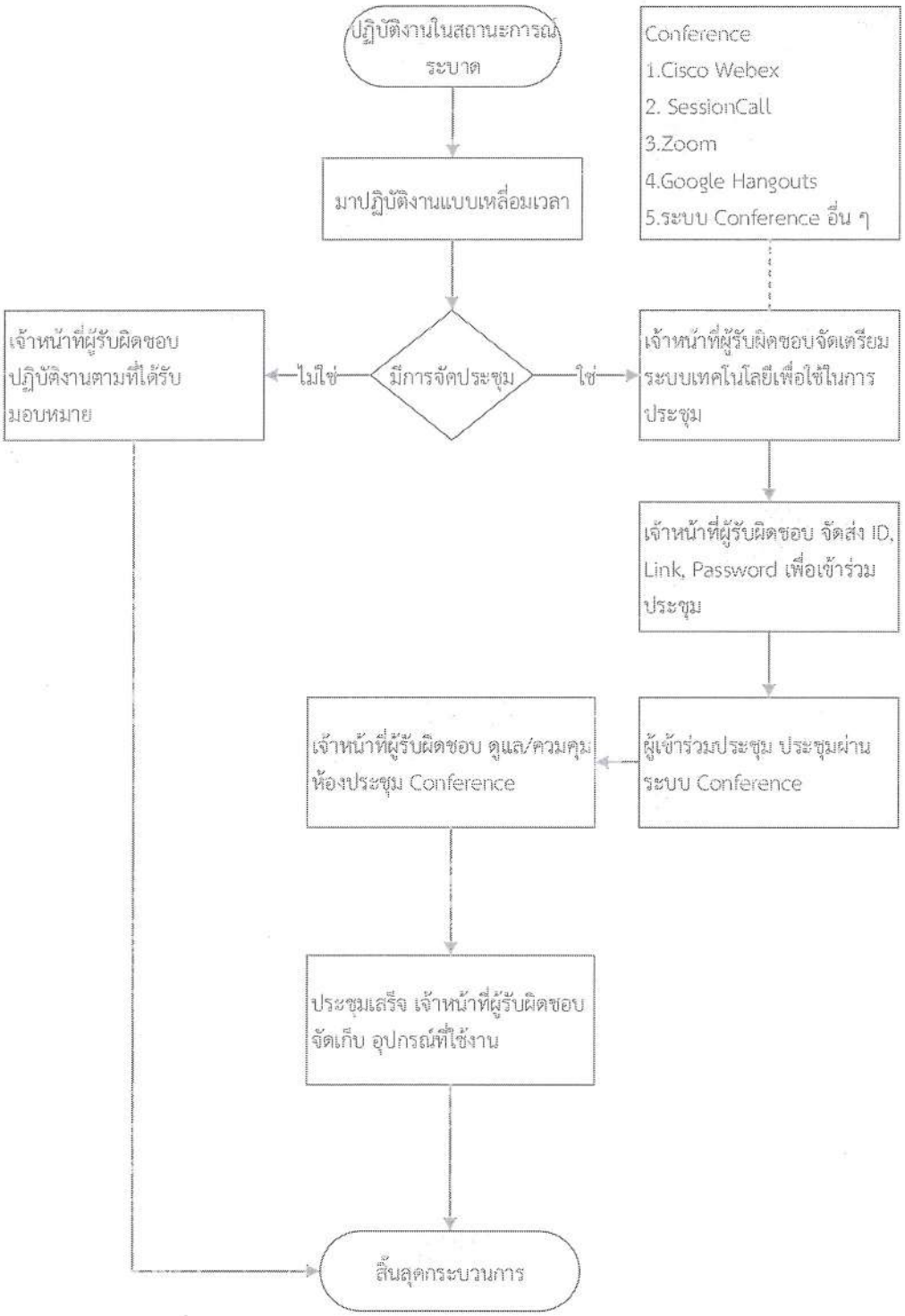


5.10 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดเหตุภัยพิบัติทางธรรมชาติ มีกระบวนการปฏิบัติดังนี้



5.11 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดโรคระบาด มีกระบวนการปฏิบัติดังนี้




ปฏิบัติงานในสถานะการณ์ระบาด
มาปฏิบัติงานแบบเหลื่อมเวลา
มีการจัดประชุม
ไม่ใช่
ใช่
เจ้าหน้าที่ผู้รับผิดชอบปฏิบัติงานตามที่ได้รับมอบหมาย
Conference
1.Cisco Webex
2. SessionCall
3.Zoom
4.Google Hangouts
5.ระบบ Conference อื่น ๆ
เจ้าหน้าที่ผู้รับผิดชอบจัดเตรียมระบบเทคโนโลยีเพื่อใช้ในการประชุม
เจ้าหน้าที่ผู้รับผิดชอบ จัดส่ง ID, Link, Password เพื่อเข้าร่วมประชุม
ผู้เข้าร่วมประชุม ประชุมผ่านระบบ Conference
เจ้าหน้าที่ผู้รับผิดชอบ ดูแล/ควบคุมห้องประชุม Conference
ประชุมเสร็จ เจ้าหน้าที่ผู้รับผิดชอบจัดเก็บ อุปกรณ์ที่ใช้งาน
สิ้นสุดกระบวนการ

6. รายชื่อผู้ติดต่อสำหรับเกิดสถานการณ์ฉุกเฉิน

กรณีอยู่ในเวลาทำการ

1. นางสาวศิริลักษณ์ และชัน	เจ้าพนักงานธุรการ	เบอร์ติดต่อ: 02-5908024
2. นางสาววันวิษา ยอดอ่วม	นักจัดการงานทั่วไป	เบอร์ติดต่อ: 02-5908132
3. นางประภาพร บุญฤกษ์	นักจัดการงานทั่วไป	เบอร์ติดต่อ: 02-5908132
4. นางเสาวนีย์ ภิญโญ	หัวหน้ากลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 1	เบอร์ติดต่อ: 02-5908035

กรณีอยู่นอกเวลาทำการ

1. นายอมรวิทย์ อมาตยคง	ผู้เชี่ยวชาญการพัฒนาระบบเครือข่ายคอมพิวเตอร์และสารสนเทศ	เบอร์ติดต่อ: 084-0099908
2. นายมณฑล บัวแก้ว	หัวหน้ากลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 3	เบอร์ติดต่อ: 089-7060538
3. นายเอกวิทย์ หยั่งบุญ	หัวหน้ากลุ่มงานพัฒนาเทคโนโลยีสารสนเทศ ชุดที่ 2	เบอร์ติดต่อ: 089-9304183

7. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่สำนักเทคโนโลยีสารสนเทศที่รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้กำกับดูแลทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

8. การกำหนดผู้รับผิดชอบ ประกอบด้วย

(1) <u>ระดับนโยบาย</u>

รองอธิบดีกรมสุขภาพจิต ที่ทำหน้าที่ CIO เป็นผู้รับผิดชอบในการสั่งการตามนโยบายของกรมสุขภาพจิต ติดตามและกำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ในระดับปฏิบัติ

(2) <u>ระดับปฏิบัติ</u> ได้แก่

ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ กรมสุขภาพจิต รับผิดชอบประสานงาน กับผู้ปฏิบัติและทีมงานด้านเทคโนโลยีสารสนเทศ ของแต่ละสำนัก/กอง ให้ความคิดเห็น เสนอแนะวิธีการ แนวทางแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการป้องกันและแก้ไขปัญหา และตรวจสอบระบบความมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ พร้อมรายงานผลการดำเนินการ โดยมอบหมายผู้ปฏิบัติตามที่สำนัก/กอง มอบหมายรับผิดชอบ

ผู้เสนอแผน

(นายทวีศักดิ์ สิริรัตน์เรขา)
ผู้อำนวยการโรงพยาบาลยุวประสาทไวทโยปถัมภ์
ปฏิบัติหน้าที่ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

ลงวันที่ ..๐๓/เมษ./๒๕๖๗..

ผู้อนุมัติ

(นายธิติ แสวงธรรม)
รองอธิบดีกรมสุขภาพจิต
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ประจำกรมสุขภาพจิต
ปฏิบัติราชการแทนอธิบดีกรมสุขภาพจิต

ลงวันที่ ..๐๑/พ.ค./๒๕๖๗..