แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ

(IT Contingency Plan)

สำนักงานปลัดกระทรวงสาธารณสุข

[ปีงบประมาณ พ.ศ.2554]

==========

จัดทำโดย : ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

สารบัญ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับ ระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) สำนักงานปลัดกระทรวงสาธารณสุข

1. หลักการและเหตุผล

ระบบข้อมูลและสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อองค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย และมั่นใจได้ว่าระบบข้อมูลและสารสนเทศสำคัญๆตามภารกิจของสำนักงานปลัดกระทรวงสาธารณสุขจะไม่สูญหาย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ

สำนักงานปลัดกระทรวงสาธารณสุข ได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในที่ส่งผลกระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายคอมพิวเตอร์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลและสารสนเทศที่ใช้ในการบริหารจัดการและใช้สนับสนุนการดำเนินงานขององค์กรให้บรรลุตามวิสัยทัศน์

ดังนั้น สำนักงานปลัดกระทรวงสาธารณสุข จึงจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนสู่ความเป็นปกติ ตลอดจนการดูแลรักษาฐานข้อมูลและสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข ให้มีเสถียรภาพพร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

2. วัตถุประสงค์

2.1 เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ

2.2 เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อให้การปฏิบัติราชการ ดำเนินไปได้อย่างมีเสถียรภาพ

2.4 เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ

2.5 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของสำนักงานปลัดกระทรวงสาธารณสุข

3. เป้าหมาย หมายถึง ระบบฐานข้อมูลและสารสนเทศกลุ่มเป้าหมายที่ต้องเฝ้าระวังและป้องกันความเสี่ยง

3.1 ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลศูนย์ปฏิบัติการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข (MOC) , ฐานข้อมูลระบบภูมิศาสตร์สารสนเทศ (GIS) , ฐานข้อมูลระบบรายงานผลการดำเนินงานตามแผนยุทธศาสตร์และแผนปฏิบัติราชการขององค์กร (MMS) , ฐานข้อมูลเพื่อการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลระบบสารบรรณอิเล็คทรอนิกส์ และฐานข้อมูลระบบ e-Paperless , โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti Virus) ,โปรแกรมระบบปฏิบัติการการจัดการเครือข่าย (Network Software) และโปรแกรมปฏิบัติการบนหน้าจอเว็บไซต์องค์กร (Web Application Program) เป็นต้น

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

4. การนำระบบสารสนเทศไปไว้ศูนย์สำรองข้อมูลฉุกเฉิน(Disaster recovery center)

การนำระบบสารสนเทศไปไว้ศูนย์สำรองข้อมูลฉุกเฉิน จะดำเนินการเมื่อผลการประเมินและวิเคราะห์สถานการณ์ความเสี่ยงอันอาจเกิดขึ้นจากเหตุภัยพิบัติ เช่น อุทกภัย พบว่ามีแนวโน้มจะเกิดเหตุการณ์ดังกล่าวในระยะเวลาอันใกล้ และหากปล่อยให้ระบบสารสนเทศดังกล่าวได้รับผลกระทบจากเหตุภัยพิบัติ จะส่งผลเสียหายต่อการดำเนินงานหลักของสำนักงานปลัดกระทรวงสาธารณสุข

โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ประสานกับสำนักงานรัฐบาลอิเล็กทรอนิกส์(องค์การมหาชน) (สรอ. หรือ EGA) เพื่อเตรียมการรับฝากระบบสารสนเทศไว้ที่ศูนย์สำรองข้อมูลฉุกเฉินของ สรอ. เมื่อถึงเวลาฉุกเฉินดังกล่าว สำหรับระบบสารสนเทศสำคัญที่จะดำเนินการทันที ได้แก่

4.1 ระบบ e-mail @health.moph.go.th และ @moph.go.th

4.2 ระบบ Web Server ได้แก่ เว็บไซต์กระทรวงสาธารณสุข เว็บไซต์ศูนย์ปฏิบัติการป้องกันและบรรเทาสาธารณภัยด้านการแพทย์และสาธารณสุข เป็นต้น

4.3 ระบบ Domain Name ภายใต้ moph.go.th

4.4 ระบบงานสำคัญตามภารกิจของสำนักงานปลัดกระทรวงสาธารณสุข เช่น MMS MOC ระบบสารบรรณอิเล็กทรอนิกส์ ระบบติดตามประเมินผล(e-Inspection) ระบบภูมิสารสนเทศด้านสาธารณสุข ระบบข้อมูลสุขภาพระดับจังหวัด เป็นต้น

5. การนำระบบกลับคืนสู่สภาพปกติ

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

1) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง

4) ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว

5) นำ BACKUP TAPE / CD-ROM / HARDDISK ที่ได้สำรองข้อมูลไว้นำกลับมา restore โดยใช้ทีมกู้ระบบ (ผู้ดูแลระบบ และทีมงานจากบริษัทฯ ที่จัดจ้างบำรุงรักษาระบบสารสนเทศ) ร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง

6) ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

6. แนวทางการปฏิบัติ

1) จัดทำ/ทบทวนและปรับปรุง คู่มือการสำรองข้อมูลและการกู้คืนข้อมูล

2) ประสานกลุ่มบริหารทั่วไป สำนักบริหารกลาง สำนักงานปลัดกระทรวงสาธารณสุข เพื่อขอเข้าร่วมการซักซ้อมกรณีเกิดเหตุไฟไหม้

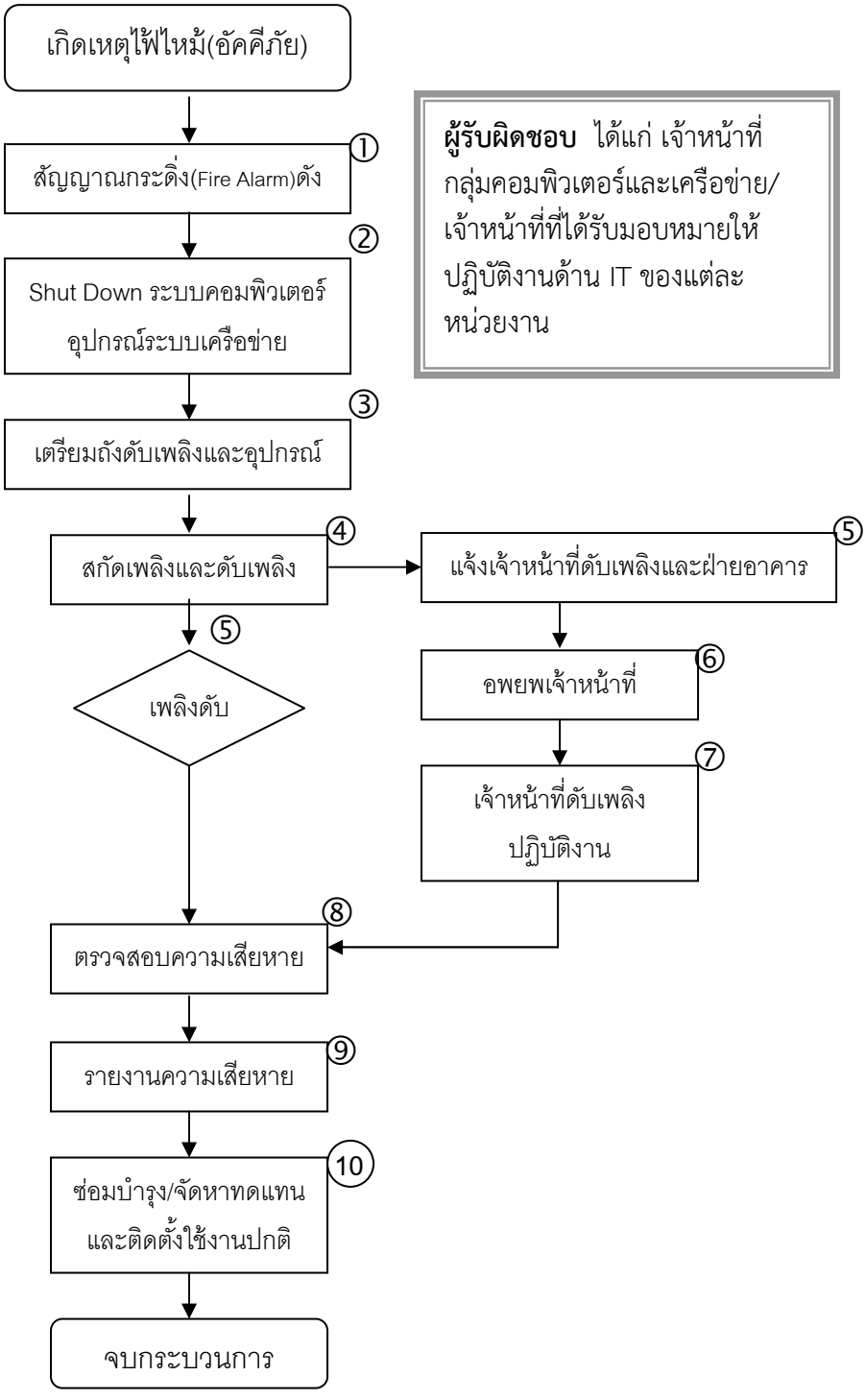
3) แจ้งเวียนหน่วยงานส่วนกลางสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ให้ถือปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ฉบับนี้

4) เมื่อมีอุปสรรคขัดข้องในการปฏิบัติตามแผนฯ ให้หน่วยงาน หาทางแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่ หากไม่สามารถแก้ไขได้ให้รายงานและขอความช่วยเหลือจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทันที

7. ผังกระบวนการ

ผังกระบวนการแสดงขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ 4 กรณีดังนี้ต่อไปนี้ พร้อมทั้งระบุผู้รับผิดชอบในการปฏิบัติขั้นตอนในแต่กรณี โดยกรณีที่วิเคราะห์และกำหนดผังกระบวนการ ได้ประเมินจากปัจจัยด้านอาคารสถานที่ สภาพแวดล้อม บุคลากร และงบประมาณ ของสำนักงานปลัดกระทรวงสาธารณสุข

7.1 กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีกระบวนการปฏิบัติดังนี้



7.2 กรณีโดนเจาะระบบคอมพิวเตอร์(Hack) มีกระบวนการปฏิบัติดังนี้

5.1 ตัด Internet Connection ของเครื่องนั้นๆ เสียก่อน เพื่อหยุดการทำลายหรือขโมยข้อมูลไปมากกว่านี้

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

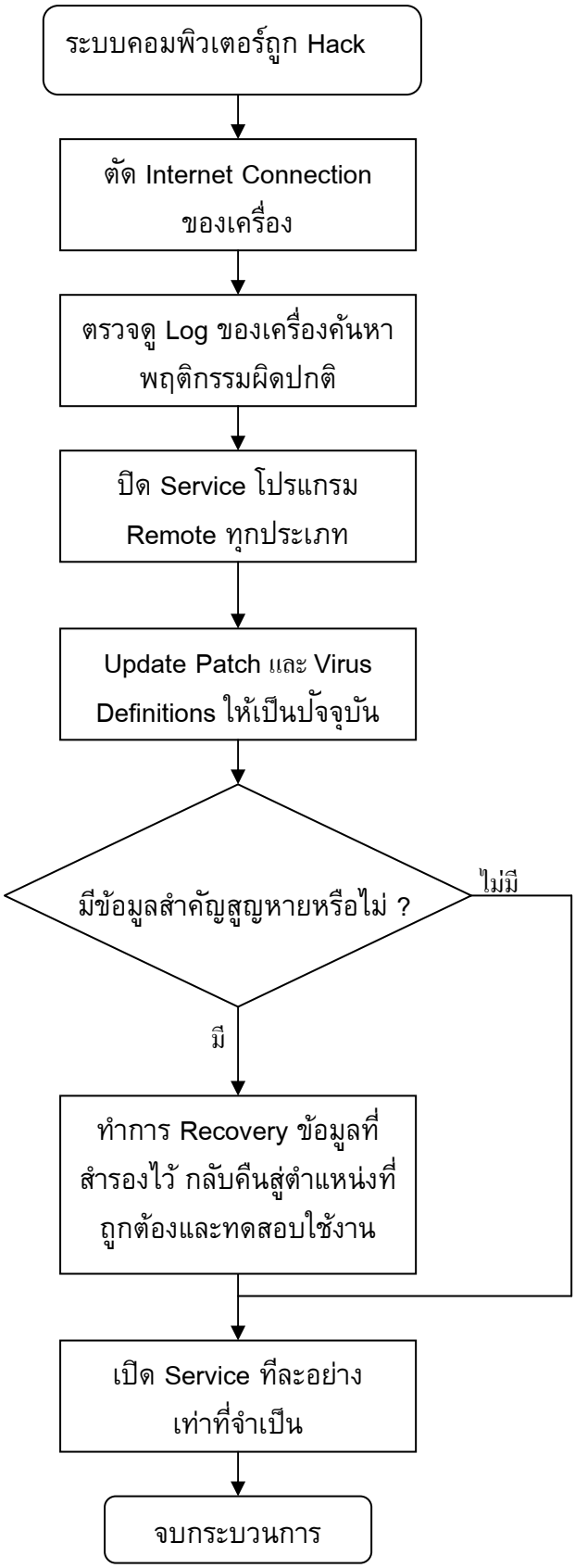
5.3 จัดการปิด Service ของโปรแกรม Remote ทุกประเภท ที่ติดตั้งไว้ในเครื่องแม่ข่ายหรืออุปกรณ์เครือข่าย

5.4 Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

5.5 ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบันกับทุก Server

5.6 กรณีข้อมูลสำคัญสูญหาย ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

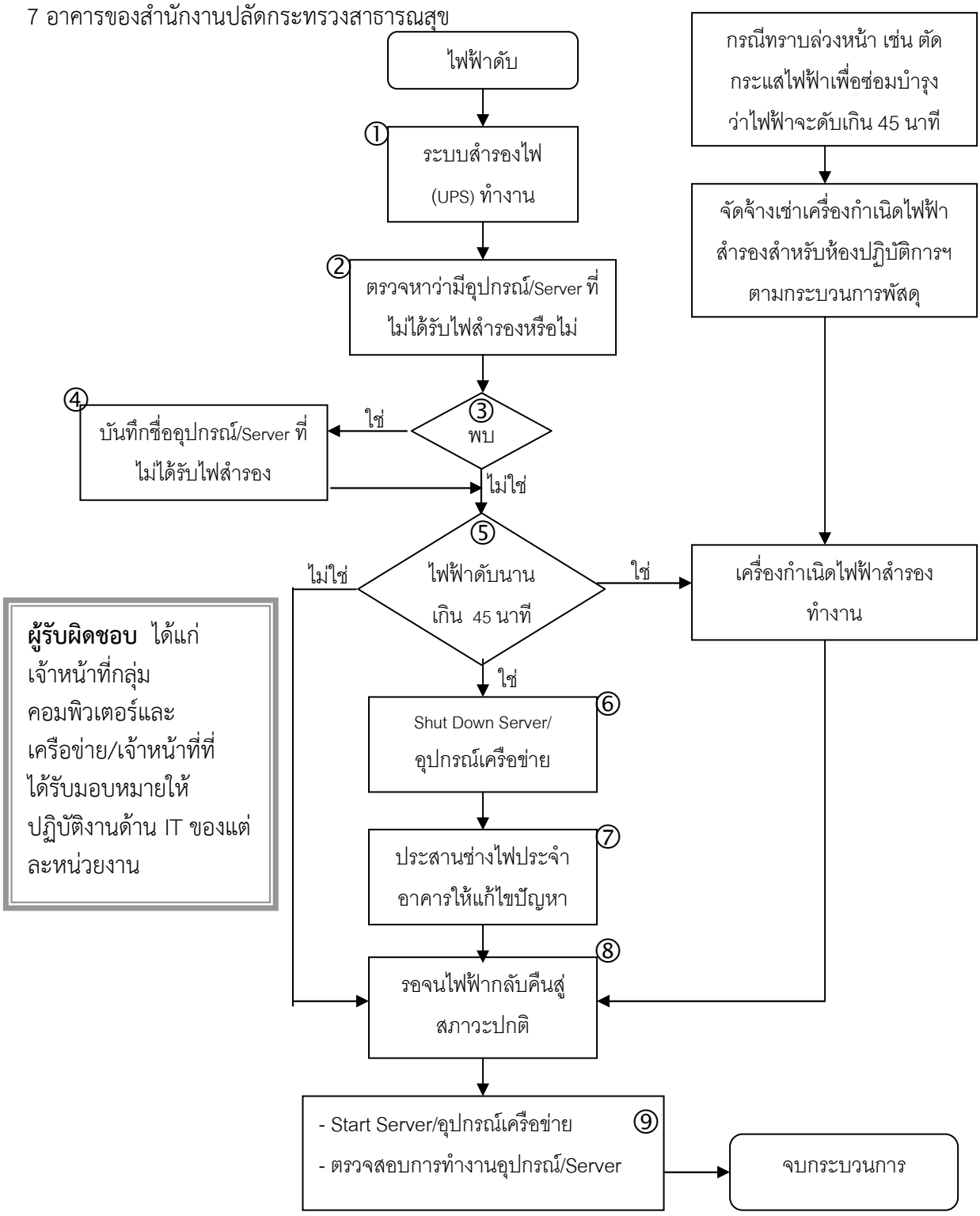
5.7 เมื่อทำขั้นตอนดังกล่าวเรียบร้อยแล้ว ก็ค่อยๆ เปิด Service ไปทีละอย่าง เปิดเท่าที่จำเป็นต่อ Server เท่านั้น



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย/เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

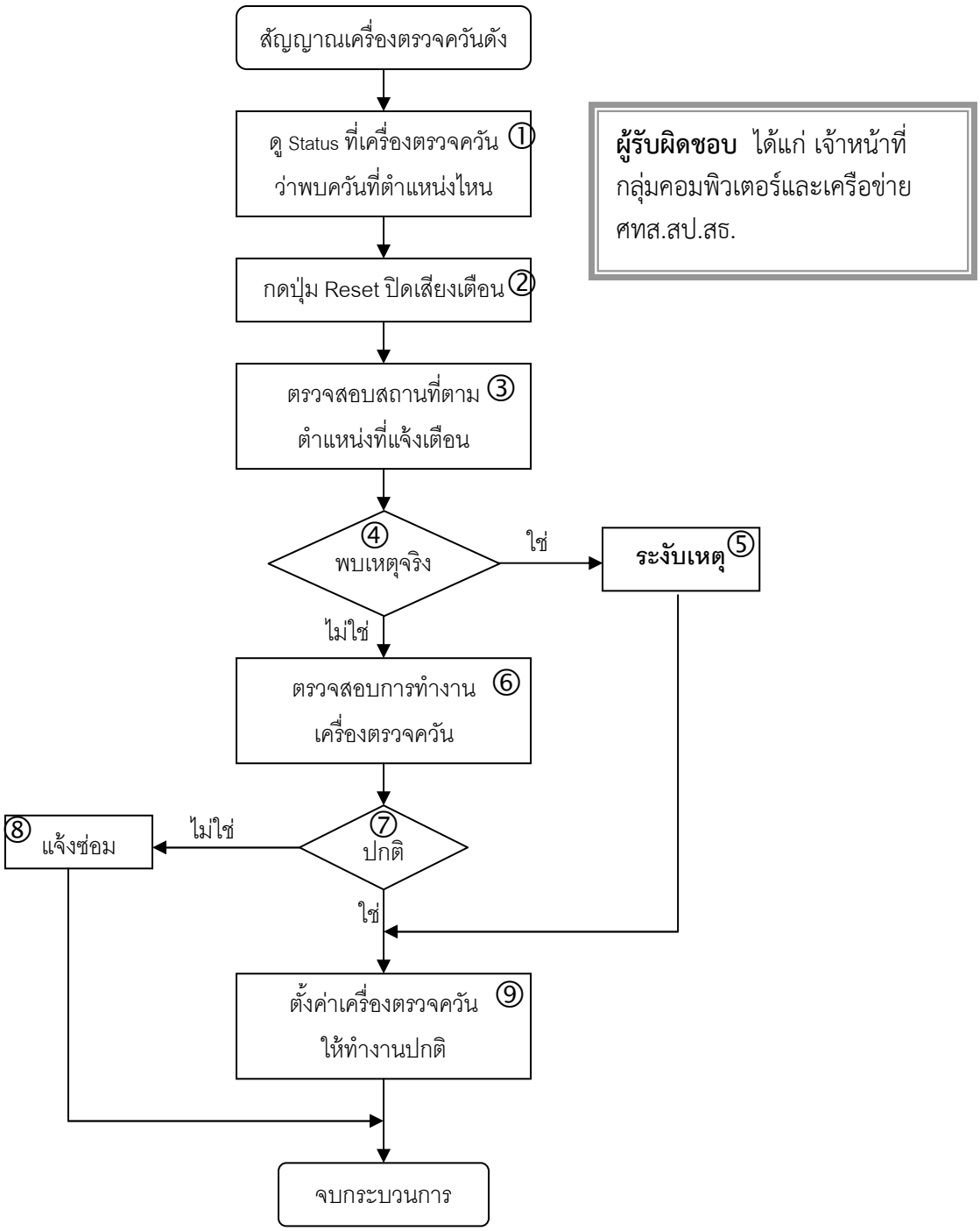
7.3 กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติดังนี้

สำนักงานปลัดกระทรวงสาธารณสุข โดยศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้เตรียมการรองรับเหตุการณ์ไฟฟ้าดับสำหรับระบบคอมพิวเตอร์ ทั้งฐานข้อมูลสำคัญ อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ และอุปกรณ์ป้องกันรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ด้วยการติดตั้งเครื่องสำรองไฟฟ้า(UPS) ขนาด 40K 1 เครื่อง และ 60K 1 เครื่อง สำหรับห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ และติดตั้งเครื่องสำรองไฟฟ้า(UPS) ขนาด 5K 1 เครื่อง สำหรับตู้อุปกรณ์กระจายสัญญาณเครือข่ายคอมพิวเตอร์ทั้ง 7 อาคารของสำนักงานปลัดกระทรวงสาธารณสุข



7.4 กรณีสัญญาณเครื่องตรวจควันดัง มีกระบวนการปฏิบัติดังนี้

ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร มีเครื่องตรวจควันติดตั้งอยู่จำนวน 1 เครื่อง ณ ห้อง 2 ซึ่งจะตรวจจับสัญญาณควันที่เกิดขึ้นภายในห้องทั้ง 2 ห้องและแจ้งตำแหน่งที่กำเนิดควัน เพื่อให้เจ้าหน้าที่ไปถึงจุดเกิดเหตุและระงับเหตุได้ทันที



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ.

8. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ดังนี้

8.1 ระดับนโยบาย รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ การปฏิบัติงานของเจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

8.1.1 รองปลัดกระทรวงสาธารณสุข ที่รับผิดชอบงานด้านเทคโนโลยีสารสนเทศ(CIO)

8.1.2 ผู้อำนวยการสำนัก/กอง/กลุ่ม สังกัดสำนักงานปลัดกระทรวงสาธารณสุข

8.2 ระดับปฏิบัติ

8.2.1 คณะทำงานบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ ตามคำสั่งสำนักงานปลัดกระทรวงสาธารณสุข

8.2.2 เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข

โดยมีหน้าที่

1. ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบเครือข่ายคอมพิวเตอร์ และระบบรักษาความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ

2. รักษาความปลอดภัยของระบบฐานข้อมูล รวมทั้งการทำสำเนาฐานข้อมูลสำคัญ

3. ปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ(IT Contingency Plan) ฉบับนี้ตามแต่ละกรณีเหตุการณ์ที่เกิดขึ้น

ผู้เสนอแผน .....

(นายสินชัย ต่อวัฒนกิจกุล)

ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

17 / พฤศจิกายน / 2553

ผู้อนุมัติ .....

(นายพรเทพ ศิริวนารังสรรค์)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

สำนักงานปลัดกระทรวงสาธารณสุข

17 / พฤศจิกายน / 2553

เมื่อเกิดปัญหาข้อขัดข้องและเกิดข้อสงสัยในทางปฏิบัติงาน ให้ติดต่อประสานงานได้ที่
กลุ่มคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
อาคาร 2 ชั้น 1 สำนักงานปลัดกระทรวงสาธารณสุข
โทรศัพท์ 025901201,025901167,025901169 หรือส่งข้อความทางจดหมายอิเล็กทรอนิกส์มาได้ที่
e-mail address : ict-moph@health.moph.go.th