แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ

(IT Contingency Plan)

สำนักงานปลัดกระทรวงสาธารณสุข

สารบัญ

เรื่อง	หน้า
1. หลักการและเหตุผล	3
2. วัตถุประสงค์	3
3. เป้าหมาย	3
4. กรณีเกิดเหตุไฟไหม้	4
5. กรณีโดนเจาะระบบคอมพิวเตอร์	5
6. กรณีไฟฟ้าดับ	6
7. กรณีสัญญาณเครื่องตรวจควันดัง	7
8. แนวทางปฏิบัติ	8

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (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

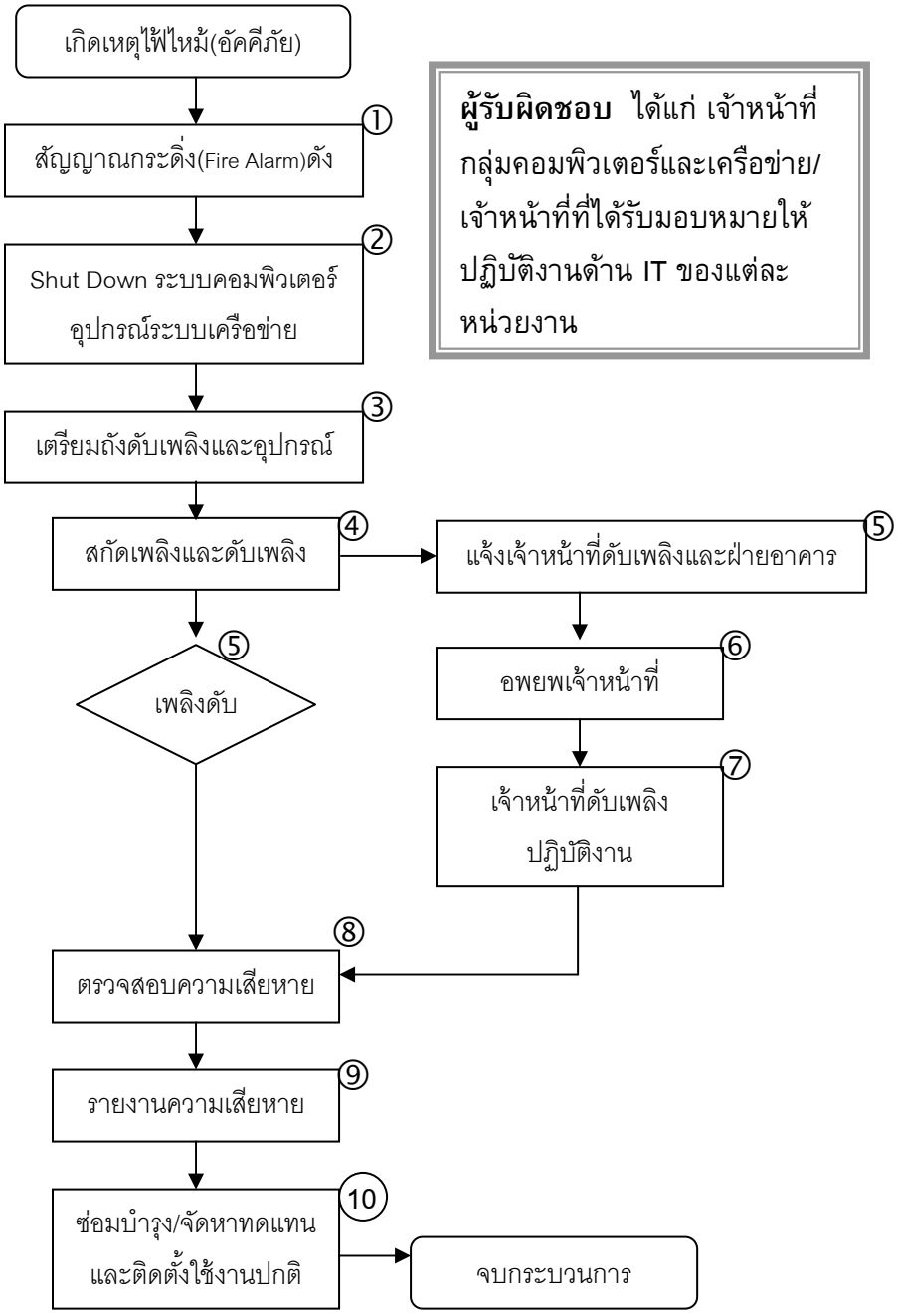
2.3 เพื่อให้การปฏิบัติราชการ ดำเนินไปได้อย่างมีเสถียรภาพ

3. เป้าหมาย

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) และโปรแกรมปฏิบัติการบนหน้าจอเว็ปไซต์องค์กร (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. กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีกระบวนการปฏิบัติดังนี้



5. 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 ที่ติดตั้งไว้ในเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย

5.4 Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

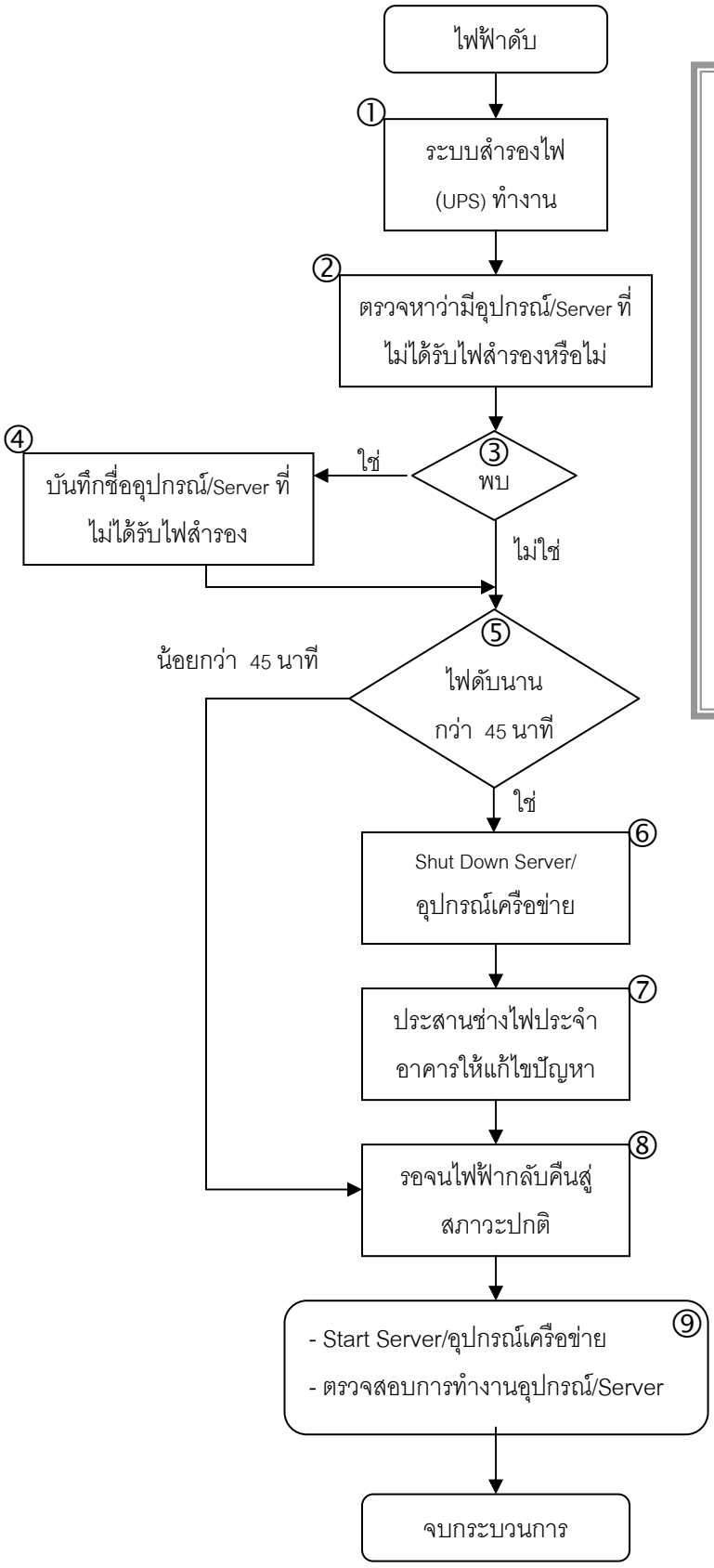
5.5 ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบันกับทุก Server

5.6 เมื่อทำขั้นตอนดังกล่าวเรียบร้อยแล้ว ก็ค่อยๆ เปิด Service ไปทีละอย่าง เปิดเท่าที่จำเป็นต่อ Server เท่านั้น

5.7 กรณีข้อมูลสำคัญสูญหาย ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย/เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

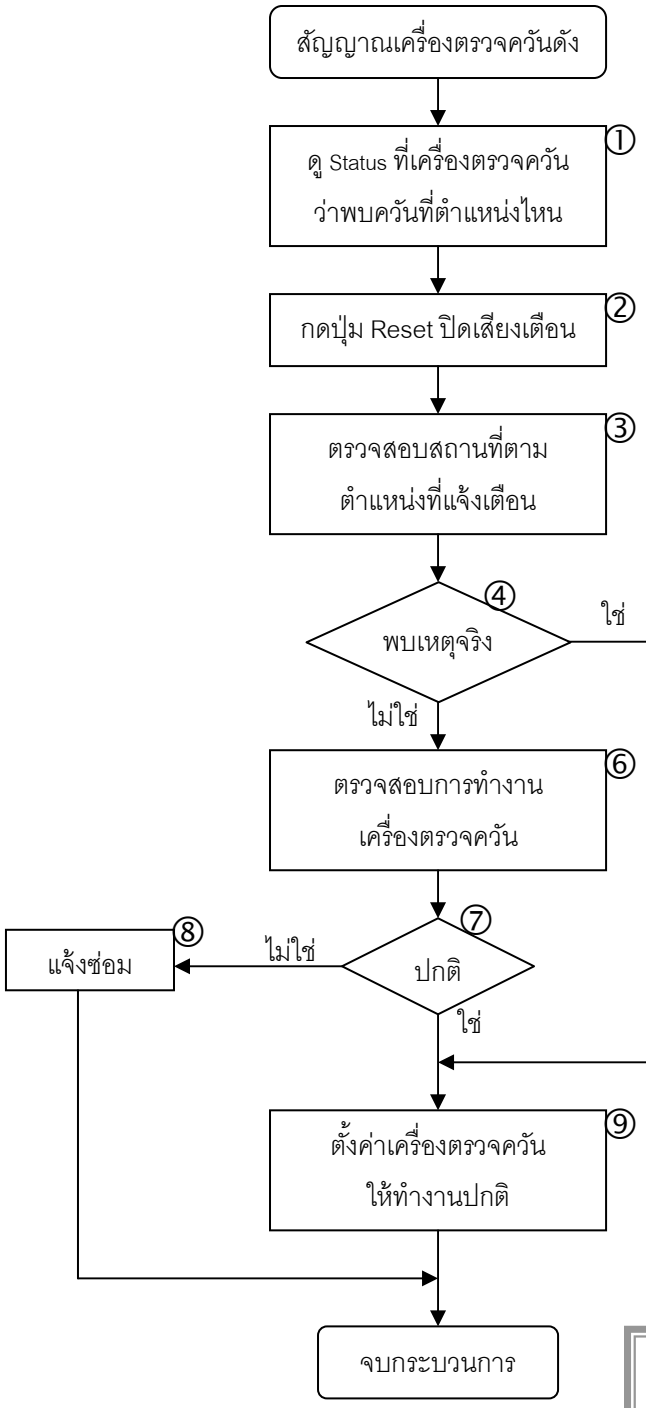
6. กรณีไฟฟ้าดับ มีกระบวนการปฏิบัติดังนี้



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย/เจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของแต่ละหน่วยงาน

หมายเหตุ ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ศทส.สป.สธ. มีระบบสำรองไฟฟ้า(UPS) ขนาดใหญ่ 60KVA จำนวน 2 ตัว รองรับอุปกรณ์เครือข่ายและเครื่องแม่ข่ายทั้งหมดภายในห้อง ได้นาน ประมาณ 45 นาที

7. กรณีสัญญาณเครื่องตรวจควันดัง มีกระบวนการปฏิบัติดังนี้



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่กลุ่มคอมพิวเตอร์และเครือข่าย ศทส.สป.สธ.

หมายเหตุ ภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ศทส.สป.สธ. มีเครื่องตรวจควันติดตั้งอยู่จำนวน 1 เครื่อง ณ ห้อง 2 ซึ่งตรวจจับสัญญาณควันที่เกิดขึ้นภายในห้องทั้ง 2 ห้องและแจ้งตำแหน่งที่เกิดควัน

8. <u>แนวทางการปฏิบัติ</u>

1) จัดทำ/ทบทวนและปรับปรุง คู่มือการสำรองข้อมูลและการกู้คืนข้อมูล
2) ประสานกลุ่มบริหารทั่วไป สำนักบริหารกลาง สำนักงานปลัดกระทรวงสาธารณสุข เพื่อขอเข้าร่วมการซักซ้อมกรณีเกิดเหตุไฟไหม้
3) แจ้งเวียนหน่วยงานส่วนกลางสังกัดสำนักงานปลัดกระทรวงสาธารณสุข ให้ถือปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ฉบับนี้
4) เมื่อมีอุปสรรคขัดข้องในการปฏิบัติตามแผนฯ ให้หน่วยงาน หาทางแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่ หากไม่สามารถแก้ไขได้ให้รายงานและขอความช่วยเหลือจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทันที

ผู้เสนอแผน .....

(นายสินชัย ต่อวัฒนกิจกุล)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
4 / ก.ย. / 2552

ผู้อนุมัติ .....

(นายศิริวัฒน์ ทิพย์ธราดล)
4 / ก.ย. / 2552

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