แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) สำนักโรคติดต่อทั่วไป

๑. หลักการและเหตุผล

ระบบฐานข้อมูลและสารสนเทศมีความสำคัญยิ่งต่อการดำเนินงานตามภารกิจและการสื่อสารของส่วนราชการ ดังนั้น สำนักโรคติดต่อทั่วไปจึงจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) เช่น กรณีไฟฟ้าขัดข้อง การเกิดอัคคีภัย ระบบถูกบุกรุก การก่อวินาศกรรม เป็นต้น ทั้งนี้ เพื่อเป็นกรอบแนวทางในการแก้ไขปัญหาให้ระบบฐานข้อมูลและสารสนเทศกลับคืนเป็นปกติ เพื่อให้ข้อมูลและระบบเทคโนโลยีสารสนเทศของสำนักฯ มีความมั่นคง ปลอดภัย พร้อมใช้งานได้อย่างมีประสิทธิภาพ สามารถนำไปใช้สนับสนุนการปฏิบัติงานให้บรรลุเป้าหมายตามวิสัยทัศน์ได้อย่างต่อเนื่อง ตลอดจนสามารถนำไปใช้ในการบริหารราชการได้อย่างมีประสิทธิภาพและประสิทธิผล

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดขั้นตอนในการปฏิบัติงาน เพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของสำนักโรคติดต่อทั่วไป

๒.๒ เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูลต่างๆ

๒.๓ เพื่อให้บุคลากรของสำนักโรคติดต่อทั่วไปสามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง

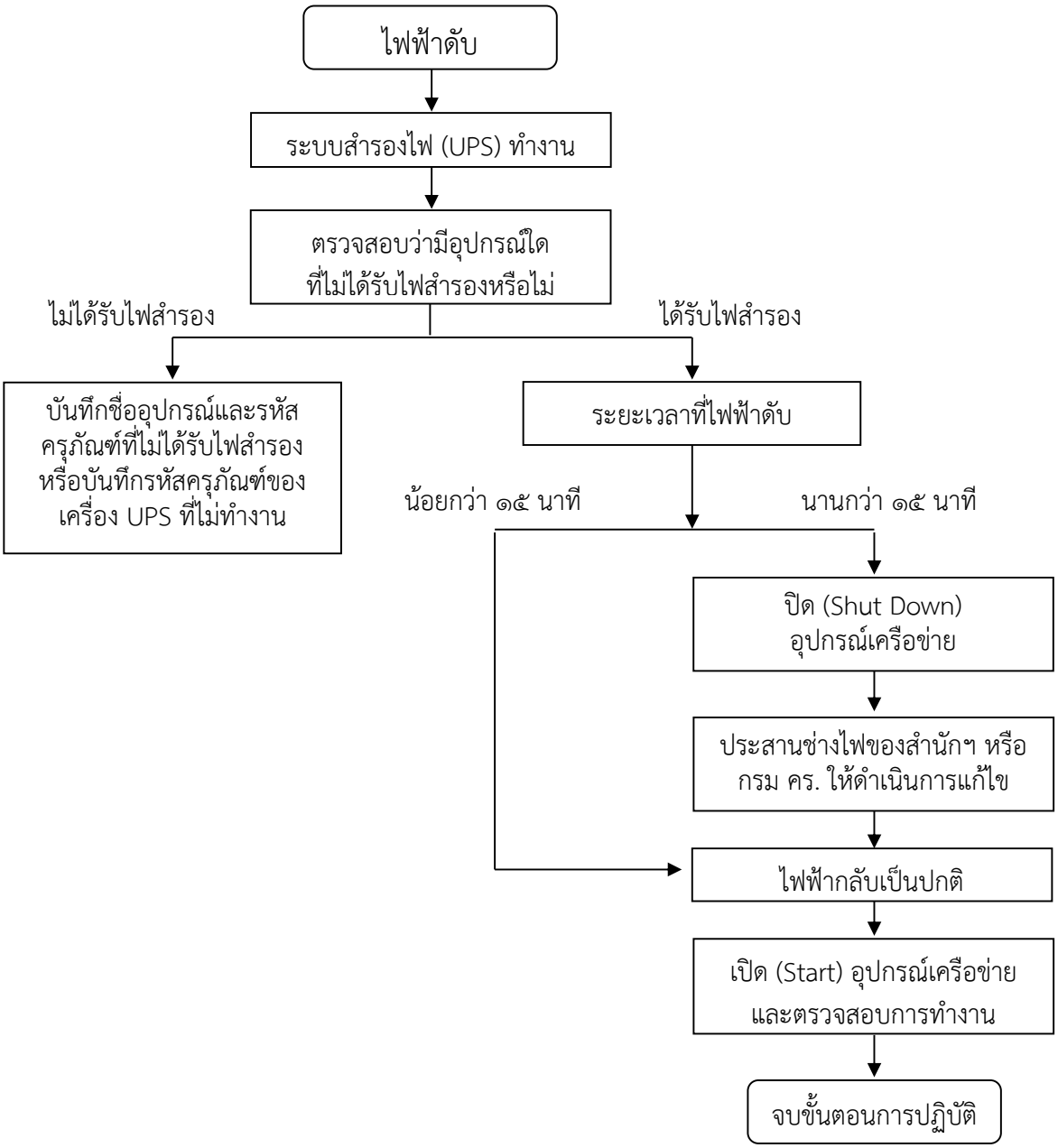
๓. เป้าหมาย

๓.๑ ระบบฐานข้อมูลสารสนเทศและโปรแกรมปฏิบัติการ (Database & Software) เช่น ฐานข้อมูลระบบรายงานผลการดำเนินงานตามแผนยุทธศาสตร์และแผนปฏิบัติราชการของสำนักฯ ฐานข้อมูลโครงการศึกษาวิจัยต่างๆ ฐานข้อมูลเพื่อการบริหารงานภายใน (Back Office) ได้แก่ ฐานข้อมูลด้านการเงิน ฐานข้อมูลทรัพยากรบุคคล ฯลฯ ระบบรับรองแหล่งผลิตอาหารปลอดโรคอหิวาตกโรค โปรแกรมผู้สัมผัสโรคพิษสุนัขบ้า โปรแกรมป้องกันไวรัสและการถูกโจมตีจากบุคคลภายนอก (Anti Virus) โปรแกรมปฏิบัติการบนเว็บไซต์ของสำนักฯ (Web Application Program) เป็นต้น

๓.๒ อุปกรณ์คอมพิวเตอร์ (Hardware) เช่น เครื่องคอมพิวเตอร์ส่วนบุคคล (Personal Computer หรือ PC), เครื่องคอมพิวเตอร์แบบพกพา (Notebook), เครื่องสแกนเนอร์ (Scanner), เครื่องพิมพ์เลเซอร์ (Laser Printer), เครื่องพิมพ์แบบพ่นหมึก (InkJet Printer), อุปกรณ์สำรองไฟฟ้าสำหรับคอมพิวเตอร์ (UPS), อุปกรณ์กระจายสัญญาณเครือข่าย (Switching HUB), อุปกรณ์กระจายสัญญาณเครือข่ายชนิดไร้สาย (Wireless Access Point) เป็นต้น

๔. กรณีไฟฟ้าขัดข้อง

กรณีที่เกิดระบบไฟฟ้าขัดข้อง มีขั้นตอนการปฏิบัติ ดังนี้



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่งานพัฒนาระบบสารสนเทศและการจัดการความรู้ และเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของกลุ่ม/ด่าน/ศูนย์/ที่ทำการแพทย์

๕. กรณีระบบเทคโนโลยีสารสนเทศถูกบุกรุก (Hack)

เมื่อทราบว่า หรือเมื่อสงสัยว่าระบบเทคโนโลยีสารสนเทศถูกบุกรุก ให้ปฏิบัติดังนี้

๕.๑ ตัด Internet Connection ของเครื่องนั้นๆ ก่อน เพื่อหยุดการทำลายหรือขโมยข้อมูลไปมากกว่านี้

๕.๒ แจ้งศูนย์สารสนเทศ กรมควบคุมโรค เพื่อตรวจสอบ Log ของ Server ไม่ว่าจะเป็น Log ของ OS หรือ Log ของ Web Server เพื่อค้นหาว่ามีสิ่งผิดปกติใดๆ เกิดขึ้นกับเครือข่าย เมื่อเวลาใด โดย IP ใด

๕.๓ ปิด Service ของโปรแกรม Remote ทุกประเภท ที่ติดตั้งไว้ในเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย

๕.๔ Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

๕.๕ ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Virus Definitions ให้เป็นปัจจุบันกับทุก Server

๕.๖ เมื่อปฏิบัติตามขั้นตอนดังกล่าวเรียบร้อยแล้ว จึงเปิด Service ไปทีละอย่าง แต่เปิดเท่าที่จำเป็นต่อ Server เท่านั้น

๕.๗ กรณีข้อมูลสำคัญสูญหาย ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่งานพัฒนาระบบสารสนเทศและการจัดการความรู้ และเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของกลุ่ม/ด่าน/ที่ทำการแพทย์

๖. กรณีเครื่องตรวจควัน (Smoke Detecter) ส่งสัญญาณเตือน

หากเครื่องตรวจควันส่งสัญญาณเตือน ให้ปฏิบัติดังนี้

๖.๑ ตรวจสอบตำแหน่งของเครื่องตรวจควันที่ส่งสัญญาณเตือน กดปุ่ม Reset เพื่อปิดเสียงเตือน

๖.๒ ค้นหาสาเหตุที่ทำให้เกิดควัน หากเป็นการส่งสัญญาณผิดพลาด (False Alarm) ให้ตรวจสอบการทำงานของเครื่อง แล้วแจ้งซ่อมในกรณีที่เครื่องขัดข้องจริง หากพบสาเหตุของควัน ให้ดำเนินการระงับเหตุตามความเหมาะสม

๖.๓ ตั้งค่าเครื่องตรวจควันให้ทำงานปกติ

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่งานพัฒนาระบบสารสนเทศและการจัดการความรู้ และเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของกลุ่ม/ด่าน/ที่ทำการแพทย์

๗. กรณีเกิดเหตุฉุกเฉิน

เมื่อเกิดเหตุฉุกเฉินที่มีอันตรายหรือคาดว่าจะเป็นอันตรายต่อบุคลากรและระบบเทคโนโลยีสารสนเทศของสำนักฯ เช่น การเกิดแผ่นดินไหว การก่อวินาศกรรม หรือได้รับการแจ้งว่ามีการใช้อาวุธชีวภาพ ฯลฯ และจำเป็นต้องอพยพเจ้าหน้าที่ออกจากอาคารโดยทันที ให้ปฏิบัติดังนี้

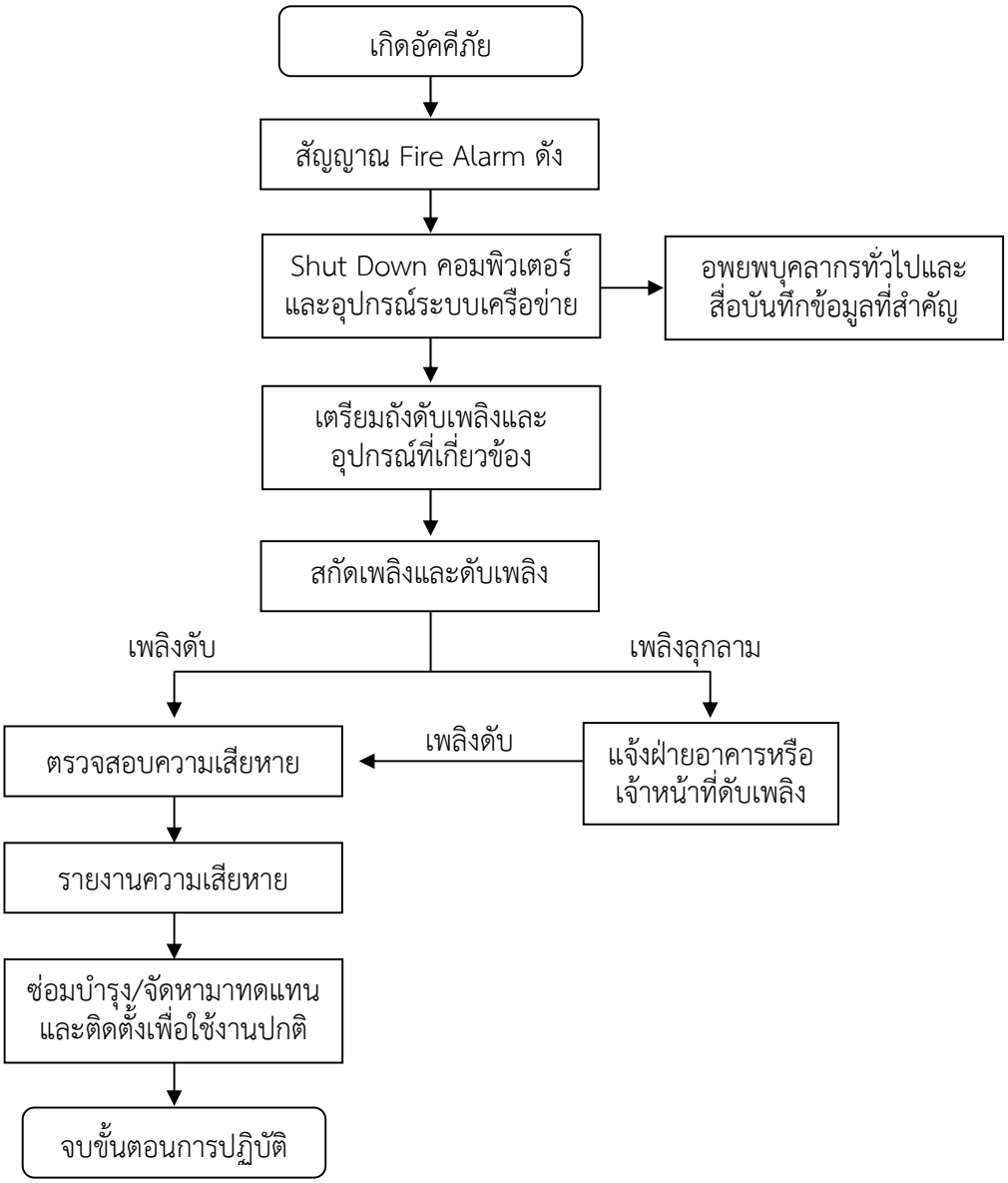
๗.๑ นำสื่อบันทึกข้อมูลที่สำคัญออกจากอาคารและนำไปเก็บรักษาไว้ในที่ปลอดภัยจนกว่าจะได้รับคำสั่งให้กลับเข้าไปในอาคารได้

๗.๒ เมื่อสถานการณ์กลับคืนสู่ภาวะปกติ ให้ดำเนินการตรวจสอบและรายงานความเสียหาย

๗.๓ กรณีที่ข้อมูลสำคัญสูญหายจาก Server / PC / Notebook ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่งานพัฒนาระบบสารสนเทศและการจัดการความรู้ และเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของกลุ่ม/ด่าน/ที่ทำการแพทย์

๘. กรณีเกิดอัคคีภัย



ผู้รับผิดชอบ ได้แก่ เจ้าหน้าที่งานพัฒนาระบบสารสนเทศและการจัดการความรู้ และเจ้าหน้าที่ที่ได้รับมอบหมายให้ปฏิบัติงานด้าน IT ของกลุ่ม/ด่าน/ที่ทำการแพทย์

๙. แนวทางปฏิบัติเพื่อเตรียมพร้อมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

๙.๑ จัดทำ/ทบทวนและปรับปรุง คู่มือการสำรองข้อมูลและการกู้คืนข้อมูล

๙.๒ จัดทำทำเนียบรายชื่อและข้อมูลสำหรับการติดต่อของเจ้าหน้าที่และหน่วยงานทั้งหมดที่เกี่ยวข้อง

๙.๓ ประเมินความเสี่ยงของการเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ และดำเนินการซ้อมแผนเป็นระยะอย่างสม่ำเสมอ โดยกำหนด scenario ตามลำดับความสำคัญและตามความเสี่ยง/โอกาสที่จะเกิด

๙.๔ แจ้งเวียนกลุ่ม/ด่าน/ที่ทำการแพทย์ ให้ถือปฏิบัติตามแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) ฉบับนี้ โดยปรับขั้นตอนการปฏิบัติให้เหมาะสมกับบริบทและสถานที่ตั้งของหน่วยงาน

๙.๕ เมื่อพบอุปสรรคหรือข้อขัดข้องในการปฏิบัติตามแผนฯ ให้หน่วยงานแก้ไขตามขีดความสามารถและอำนาจที่มีอยู่ หากไม่สามารถแก้ไขได้ ให้รายงานและขอความช่วยเหลือจากผู้บริหารทันที

ผู้เสนอแผน

(นางโศภาพรรณ วิมลรัตน์)

หัวหน้ากลุ่มยุทธศาสตร์และพัฒนาองค์กร

ผู้อนุมัติ ร.ต.อ.

(รุ่งเรือง กิจผาติ)

ผู้อำนวยการสำนักโรคติดต่อทั่วไป

วันที่ เดือนพฤศจิกายน พ.ศ. ๒๕๕๙