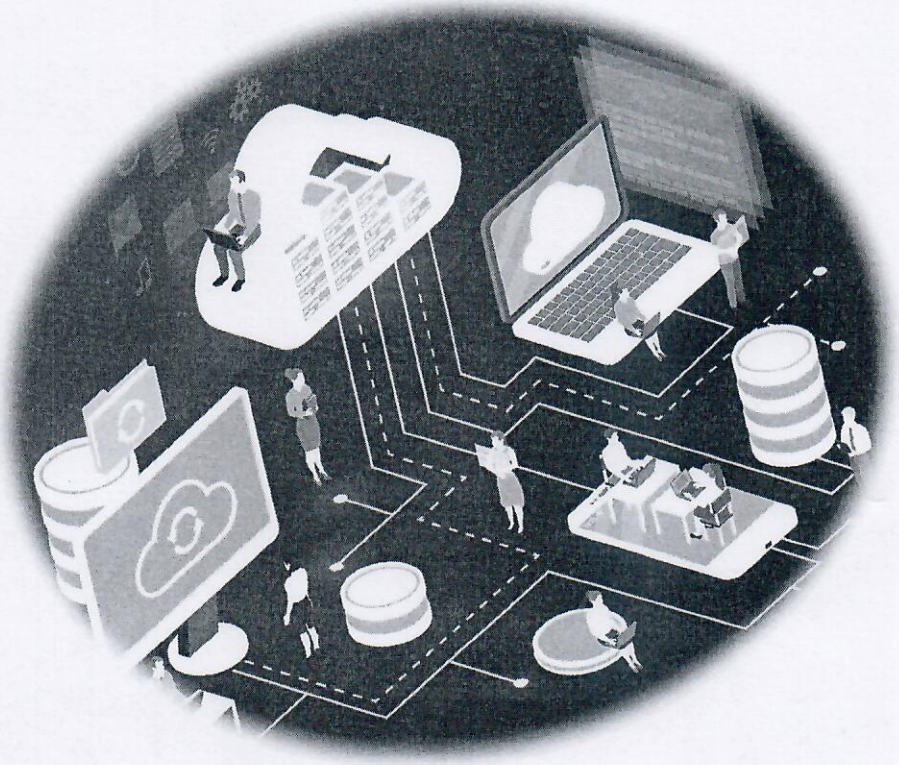
IT Contingency Plan

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

กองโรคติดต่อทั่วไป



กลุ่มยุทธศาสตร์และพัฒนาองค์กร

กองโรคติดต่อทั่วไป กรมควบคุมโรค

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

กองโรคติดต่อทั่วไป

IT Contingency Plan

สารบัญ

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ
กองโรคติดต่อทั่วไป
IT Contingency Plan

ระบบฐานข้อมูลและเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของกองโรคติดต่อทั่วไป จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ ได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบ ทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้น จึงได้จัดทำแผน รับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (**IT Contingency Plan**) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกองโรคติดต่อทั่วไป

วัตถุประสงค์

๒.๑ เพื่อกำหนดขั้นตอนในการปฏิบัติงาน เพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศของสำนักโรคติดต่อทั่วไป

๒.๒ เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและฐานข้อมูลต่างๆ

๒.๓ เพื่อให้บุคลากรของกองโรคติดต่อทั่วไปสามารถปฏิบัติงานตามภารกิจได้อย่างต่อเนื่อง

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (**IT Contingency Plan**) กองโรคติดต่อทั่วไป จัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของหน่วยงาน ประกอบด้วย

๑. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

๒. การประเมินสถานการณ์และกำหนดระดับความรุนแรง

๓. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

๔. การเตรียมความพร้อม

๕. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

๖. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ

๗. การติดตามและรายงานผล

๑. การวิเคราะห์ความเสี่ยงและประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน จำแนกเป็น ๒ กลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติอัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว เป็นต้น

๒) ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

๓) การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล

๔) ระบบกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟกระชาก

๕) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

๑) ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในกอง

๓) เจ้าหน้าที่หรือบุคลากรของกองโรคติดต่อทั่วไป ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ทั้งด้าน ฮาร์ดแวร์และซอฟต์แวร์อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

๑.๒ ประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ เมื่อหน่วยงาน มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติเพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยเจ้าหน้าที่งานสารสนเทศ นำมาสรุปเป็นข้อมูล ดังนี้

สถานการณ์ หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน ๕ คะแนน)			จัดเรียงลำดับ	
	ระบบงาน	พันธกิจ	ประชาชน	รวม	จัดลำดับ
กรณีการบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหาย หรือ ทำลายระบบข้อมูล	๕	๔	๓	๑๒	๑
กรณีไฟฟ้าดับ	๕	๓	๒	๑๐	๒
กรณีไวรัสคอมพิวเตอร์	๕	๒	๓	๘	๓

๒. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

๒.๑ การประกาศใช้แผนของหน่วยงาน มีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการกองโรคติดต่อทั่วไปอนุมัติ และทำการแจ้งหัวหน้ากลุ่มงาน /สำนักงาน ทราบ เพื่อพิจารณาประกาศใช้แผนต่อไป

๒.๒ กำหนดขั้นตอนการดำเนินงาน งานพัฒนาเทคโนโลยีสารสนเทศ กลุ่มยุทธศาสตร์และพัฒนาองค์กร จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติในหน่วยงาน โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์ สำรองเพื่อใช้ในการกู้คืนระบบ

๒.๓ การติดต่อประสานงาน มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า ,สถานีดับเพลิง ,สถานีตำรวจ เป็นต้น

๒.๔ การจัดเตรียมอุปกรณ์ งานพัฒนาเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ดังนี้

- เครื่องคอมพิวเตอร์ PC/Notebook
- Flash drive ติดตั้งระบบปฏิบัติการ
- แผนผังของเครือข่ายคอมพิวเตอร์
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- โปรแกรม antivirus
- ระบบสำรองไฟฟ้าอัตโนมัติ

๒.๕ การสำรองข้อมูล เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุก แทรกแซง เปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ มีการสำรองข้อมูลเว็บไซต์และระบบงานต่าง ๆ โดยการกำหนดความถี่ในการสำรอง และตรวจสอบการตั้งค่า (Configuration) ต่าง ๆ ของระบบการสำรองข้อมูล พร้อมทั้งทดสอบบันทึกการสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๒.๖ การป้องกันและกำจัดไวรัส มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดไวรัสสำหรับเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

๒.๗ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตของหน่วยงาน เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติเพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

๒) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ โดยได้จัดหาระบบบริหาร จัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของหน่วยงานให้ดียิ่งขึ้น

๒.๘ การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

๑) ติดตั้งเครื่องสำรองไฟฟ้าเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๑๐-๑๕ นาที

๒) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง

๓) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๓.การเตรียมความพร้อม

๓.๑ การเตรียมความพร้อมกรณีเกิดการแทรกแซงเมื่อเกิดเหตุโจมตีทางไซเบอร์ และการบุกรุก ผ่านช่องทาง Network ให้ดำเนินการ แก้ไขดังนี้

๑) ตัดสัญญาณ Internet Connection ของเครื่องนั้นๆ ก่อน เพื่อหยุดการทำลายหรือขโมยข้อมูล

๒) แจ้งกองดิจิทัลเพื่อการควบคุมโรค เพื่อตรวจสอบ Log ของ Server ไม่ว่าจะเป็น Log ของ OS หรือ Log ของ Web Server เพื่อค้นหาว่ามีสิ่งผิดปกติใดๆ เกิดขึ้นกับเครือข่าย เมื่อเวลาใด โดย IP Address ใด

๓) ปิด Service ของโปรแกรม Remote ทุกประเภท ที่ติดตั้งไว้ในเครื่องแม่ข่าย หรืออุปกรณ์เครือข่าย

๔) Update Patch ต่างๆ ให้เป็นปัจจุบันกับทุก Server และอุปกรณ์

๕) ตรวจสอบการทำงานของโปรแกรม Anti Virus และ Update Anti Virus ให้เป็นปัจจุบันกับทุก Server

๖) เมื่อปฏิบัติตามขั้นตอนดังกล่าวเรียบร้อยแล้ว จึงเปิด Service ไปทีละอย่าง แต่เปิดเท่าที่จำเป็นต่อ Server เท่านั้น

๗) กรณีข้อมูลสำคัญสูญหาย ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากกรณีไฟฟ้าดับ ไฟกระชาก กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) เปิดเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์ ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๑๐-๑๕ นาที

๒) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง

๓) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และ บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกขอมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๕) กำหนดให้มีการสำรองฐานข้อมูล และระบบงานต่าง ๆ ทุก ๑ เดือนเป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว เตรียมความพร้อมโดยติดตามสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น ดังนี้

๑.ติดตามข้อมูลข่าวสารเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้องและข้อมูลการพยากรณ์อากาศจากหน่วยงานที่เกี่ยวข้อง

๒.เมื่อเกิดเหตุฉุกเฉินที่มีอันตรายหรือคาดว่าจะเป็นอันตรายต่อบุคลากรและระบบเทคโนโลยีสารสนเทศของหน่วยงาน จำเป็นต้องอพยพเจ้าหน้าที่ออกจากอาคารโดยทันที ให้ปฏิบัติดังนี้

๒.๑) นำสื่อบันทึกข้อมูลที่สำคัญออกจากอาคารและนำไปเก็บรักษาไว้ในที่ปลอดภัยจนกว่าจะได้รับคำสั่งให้กลับเข้าไปในอาคารได้

๒.๒) เมื่อสถานการณ์กลับคืนสู่ภาวะปกติ ให้ดำเนินการตรวจสอบและรายงานความเสียหาย

๒.๓) กรณีที่ข้อมูลสำคัญสูญหายจาก Server /PC /Notebook ให้ทำการ Recovery ข้อมูลที่สำรองไว้กลับคืนสู่ตำแหน่งที่ถูกต้องและทดสอบใช้งาน

๔.การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

จัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบ ดังนี้

๔.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้คำเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบเจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่ ผู้อำนวยการกองโรคติดต่อทั่วไป ,หัวหน้ากลุ่มงาน / สำนักงาน

๔.๒ ระดับปฏิบัติเทคโนโลยีสารสนเทศและเครือข่าย

คณะทำงานด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กองโรคติดต่อทั่วไป (คำสั่งกองโรคติดต่อทั่วไป ที่ ๑๙๗/๒๕๖๕ เรื่อง แต่งตั้งคณะทำงานการจัดการข้อมูลสารสนเทศและเทคโนโลยีดิจิทัล กองโรคติดต่อทั่วไป)

๑. ศึกษาและทำความเข้าใจรูปแบบภัยคุกคาม ความรู้พื้นฐาน ของหลักการปฏิบัติด้านความมั่นคงปลอดภัยทางไซเบอร์ (Cyber Security) และสารสนเทศ

๒. ดำเนินการสื่อสารให้บุคลากรภายในหน่วยงาน ได้รับความรู้ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security) และสารสนเทศ

๓. สนับสนุนการจัดทำหรือทบทวนแผนการดำเนินงานให้สอดคล้องกับแผนระดับชาติด้านความมั่นคงปลอดภัยไซเบอร์ (Cyber Security) และสารสนเทศ

๔. รายงานเหตุการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security) และสารสนเทศให้ผู้บริหารทราบ และให้รายงายทันทีที่พบเหตุกระทบความมั่นคงปลอดภัยด้านไซเบอร์ (Cyber Security) และสารสนเทศเพื่อให้ผู้เกี่ยวข้องตรวจสอบความเสียหาย และหาทางแก้ไขได้อย่างถูกต้องโดยแบ่งทีมงาน ดังนี้

ทีมกู้คืนระบบ ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนระบบต่างๆ ให้สามารถกลับมาใช้งานได้ตามปกติ

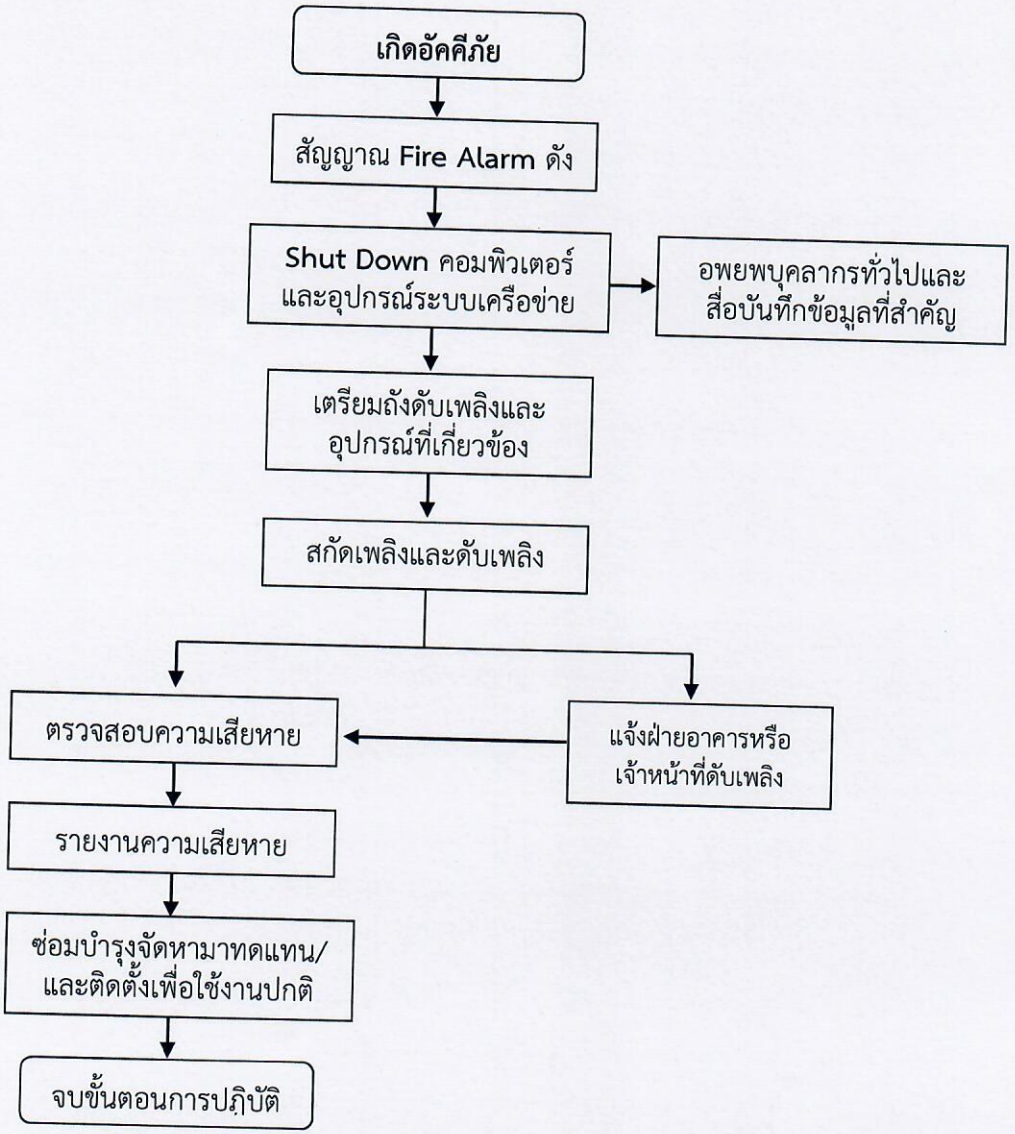
นางสาวนวพรรษ	อุทัย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร.๐๙๙-๘๖๔๘๗๔๔
นางสาวภิญญาดา	ดอนนนท์	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร.๐๙๘-๕๔๕๖๕๖๓
นางอำภาพร	รอดรัตน์	นักวิชาการคอมพิวเตอร์	โทร.๐๙๑-๙๘๖๑๒๘๒

ทีมกู้คืนเครือข่าย ทำหน้าที่บริหารจัดการแก้ไข **Network** ให้ทันท่วงที และสามารถกลับมาใช้งานได้ตามปกติ

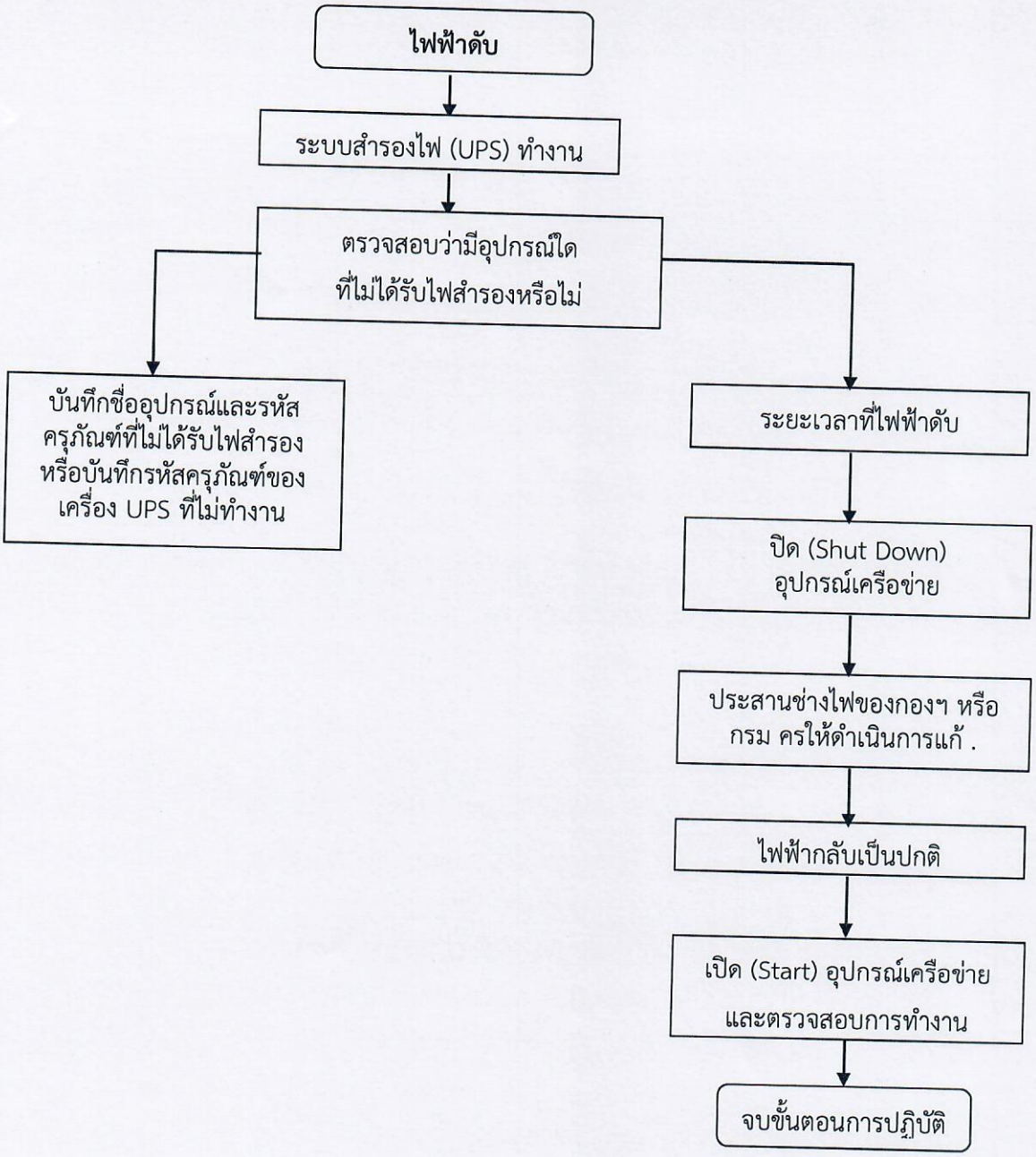
นางสาวนวพรรษ	อุทัย	นักวิชาการคอมพิวเตอร์ปฏิบัติการ	โทร.๐๙๙-๘๖๔๘๗๔๔
นางอำภาพร	รอดรัตน์	นักวิชาการคอมพิวเตอร์	โทร.๐๙๑-๙๘๖๑๒๘๒
นางสาวกัลยาณี	ดวงตา	เจ้าพนักงานคอมพิวเตอร์	โทร.๐๘๑-๗๗๑๖๐๖๑

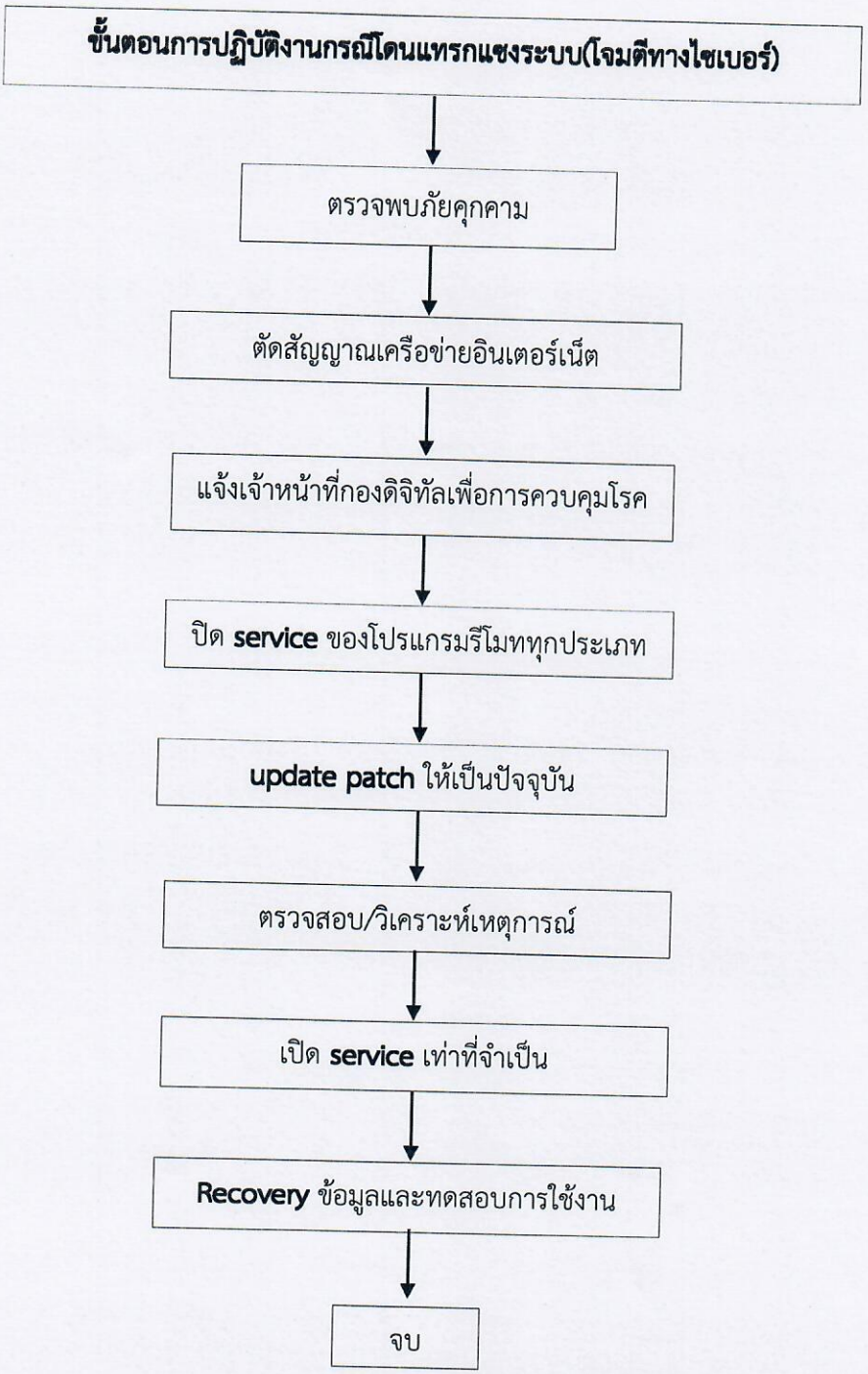
๕.ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ

๑.กรณีไฟฟ้าขัดข้อง



๒. กรณีไฟฟ้าขัดข้อง กรณีที่เกิดระบบไฟฟ้าขัดข้อง มีขั้นตอนการปฏิบัติ ดังนี้




ขั้นตอนการปฏิบัติงานกรณีโดนแทรกแซงระบบ(โจมตีทางไซเบอร์)
ตรวจพบภัยคุกคาม
ตัดสัญญาณเครือข่ายอินเตอร์เน็ต
แจ้งเจ้าหน้าที่กองดิจิทัลเพื่อการควบคุมโรค
ปิด service ของโปรแกรมรีโมททุกประเภท
update patch ให้เป็นปัจจุบัน
ตรวจสอบ/วิเคราะห์เหตุการณ์
เปิด service เท่าที่จำเป็น
Recovery ข้อมูลและทดสอบการใช้งาน
จบ

๖.การติดตามและรายงานผล กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือ ภัยพิบัติฉุกเฉิน ให้หัวหน้ากลุ่มงาน / สำนักงาน ทราบ เพื่อนำเสนอรายงานสรุปให้ผู้อำนวยการกองโรคติดต่อทั่วไป เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพสามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency) ของหน่วยงาน เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบ เทคโนโลยีสารสนเทศต่อไป

ผู้เสนอแผน

(นางวิรงรอง แก้วสมบูรณ์)
นักวิชาการสาธารณสุขชำนาญการพิเศษ
หัวหน้ากลุ่มยุทธศาสตร์และพัฒนาองค์กร
วันที่ ๒๓ มีนาคม พ.ศ. ๒๕๖๖

ผู้อนุมัติ

(นายวิชาญ บุญกิติกร)
ผู้อำนวยการกองโรคติดต่อทั่วไป
วันที่ ๒๔ มีนาคม พ.ศ. ๒๕๖๖