บันทึกข้อความ

ส่วนราชการ แผนงานเทคโนโลยี กรมสนับสนุนบริการสุขภาพ โทร.๐ ๒๕๙๐๑๖๘๑
ที่ สธ ๐๗๑๖.๐๒/ ๘๕ **วันที่** ๒๕ กันยายน ๒๕๕๕
เรื่อง ขอให้ขออนุมัติแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ(IT Contingency Plan)

เรียน ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

ตามกรอบการประเมินผลการปฏิบัติราชการ มิติภายใน ด้านการพัฒนาองค์การ ประจำปีงบประมาณ พ.ศ. ๒๕๕๕ ของส่วนราชการ ได้กำหนดตัวชี้วัดการประเมินผลการปฏิบัติราชการ ประจำปีงบประมาณ พ.ศ. ๒๕๕๕ **ตัวชี้วัดที่ ๑๑ ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศ** ในรายละเอียดการประเมิน กำหนดให้หน่วยงานมีแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ(IT Contingency Plan) และมีการซ้อมรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ

เพื่อให้สอดคล้องกับแนวทางการตรวจประเมินตัวชี้วัดที่ ๑๑ ระดับความสำเร็จของการพัฒนาปรับปรุงสารสนเทศ ศูนย์สารสนเทศได้ยกร่างแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ(IT Contingency Plan) ตามรายละเอียดที่แนบมาพร้อมนี้ และจะมีการซ้อมแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ ในวันที่ศุกร์ที่ ๒๘ กันยายน ๒๕๕๕ เวลา ๑๐.๑๕ น เป็นต้นไป โดยจะทำการทดสอบเทปสำรองข้อมูล(backup tape) และทดสอบระบบสัญญาณดับเพลิงห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งในการซ้อมครั้งนี้จะไม่กระทบต่อการดำเนินงานด้านสารสนเทศของกรมสนับสนุนบริการสุขภาพ

จึงเรียนมาโปรดพิจารณา หากเห็นชอบขอได้โปรดขออนุมัติ
๑.แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ
๒.การซ้อมแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ
ในวันที่ศุกร์ที่ ๒๘ กันยายน พ.ศ.๒๕๕๕ เวลา ๑๐.๑๕ น ณ ห้องควบคุมเครื่องแม่ข่ายศูนย์สารสนเทศ กรมสนับสนุนบริการสุขภาพ

สมสิทธิ์ พลนาคู

นายสมสิทธิ์ พลนาคู
แทนหัวหน้ากลุ่มแผนงานเทคโนโลยี

- อนุมัติแผนรับสถานการณ์ฉุกเฉินฯ และ
อนุมัติการซ้อมแผนรับสถานการณ์ฉุกเฉิน
ตามวันเวลาดังกล่าว

นายวิชัย จิตติกรยุทธนา
ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
ปฏิบัติหน้าที่แทน CIO

สารบัญ

หน้า

	แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระทบต่อระบบสารสนเทศ IT Contingency Plan	แก้ไขครั้งที่ : ๐๐ มีผลบังคับใช้ : กันยายน พ.ศ.๒๕๕๕ จำนวนแผ่น : ๑๔

๑. วัตถุประสงค์

๑.๑ เพื่อใช้เป็นแนวทางในการรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ กรมสนับสนุนบริการสุขภาพ

๑.๒ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศของกรมสนับสนุนบริการสุขภาพ

๑.๓ เพื่อเป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๑.๔ เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ

๒. ขอบเขต

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศนี้ ครอบคลุมถึงการเกิดภาวะฉุกเฉินที่อาจเกิดขึ้นภายในศูนย์สารสนเทศหรือเกิดผลกระทบจากภายนอกศูนย์สารสนเทศ กรมสนับสนุนบริการสุขภาพ ดังนี้

ภาวะฉุกเฉิน ที่เกิดจาก เพลิงไหม้ ไฟฟ้าดับ ภายในศูนย์สารสนเทศหรือผลกระทบจากภายนอกศูนย์สารสนเทศ เช่น การถูกโจมตีระบบด้วยไวรัสคอมพิวเตอร์ น้ำท่วม เป็นต้น

๓. คำจำกัดความ

๓.๑ แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ หมายถึง กระบวนการที่สำนักเทคโนโลยีสารสนเทศและการสื่อสาร และหน่วยงานภายใน กรมสนับสนุนบริการสุขภาพ ร่วมกันเตรียมการ ตรวจหา โต้ตอบ และฟื้นฟูระบบจากเหตุการณ์ที่เป็นภัยคุกคามทั้งจากมนุษย์และภัยธรรมชาติ ที่มีผลต่อระบบสารสนเทศและทรัพย์สินที่เกี่ยวข้อง

๓.๒ ภัยพิบัติ หมายถึง เหตุการณ์ที่เกิดขึ้นจากธรรมชาติ หรือเกิดจากการกระทำของมนุษย์ที่อาจเกิดขึ้นปัจจุบันทันด่วนหรือค่อยๆเกิด มีผลกระทบต่อภารกิจการดำเนินการของกรมสนับสนุนบริการสุขภาพทำให้ไม่สามารถดำเนินการได้ ภัยพิบัติอาจเป็นได้ทั้งเหตุการณ์ที่เกิดขึ้นตามธรรมชาติ เช่น อุทกภัย หรือเป็นเหตุการณ์ที่มนุษย์กระทำขึ้น เช่น การโจมตีระบบสารสนเทศของกรมสนับสนุนบริการสุขภาพ เป็นต้น

๓.๓ สถานการณ์ฉุกเฉิน หมายถึง สถานการณ์ที่เกิดขึ้นโดยบังเอิญและโดยธรรมชาติ ซึ่งก่อให้เกิดความเสียหายกับระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ สถานการณ์ฉุกเฉินมีตั้งแต่ระดับที่ไม่ร้ายแรง เช่น ไฟตก ฮาร์ดดิสก์ชำรุด ไปจนถึงระดับร้ายแรงสุด เช่น ก่อการร้าย หรือไฟไหม้ ถึงแม้ว่ากรมสนับสนุนบริการสุขภาพ จะสามารถลดความเสี่ยงและภัยคุกคามต่างๆที่อาจเกิดขึ้นได้ผ่านกระบวนการจัดการความเสี่ยงก็ตาม แต่บริการบางอย่างอยู่เหนือความควบคุมของหน่วยงานภายในกรมสนับสนุนบริการสุขภาพ และ

หน่วยงานภายในกรมสนับสนุนบริการสุขภาพก็ไม่แน่ใจด้วยว่าบริการเหล่านั้นพร้อมใช้ตลอดเวลาหรือไม่ ดังนั้น กรมสนับสนุนบริการสุขภาพจึงจำเป็นต้องมีการวางแผนรองรับสถานการณ์ฉุกเฉินและเหตุการณ์ที่ไม่คาดคิด เพื่อลดความเสี่ยงที่มีผลต่อความเสียหายของระบบสารสนเทศ

๔. เป้าหมายของการจัดทำแผนฯ

เพื่อฟื้นฟูการทำงานของระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ ให้กลับคืนสู่สภาพเดิมโดยใช้ต้นทุนน้อยที่สุด และรบกวนการดำเนินงานตามปกติของหน่วยงานให้น้อยที่สุด ดังนั้นการมีแผนฯรองรับ จะช่วยให้ระบบพร้อมใช้ตลอดเวลา แม้จะเผชิญกับเหตุการณ์ที่ไม่คาดคิด

๕. กำหนดโครงสร้างทีมงานรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ

ประกอบด้วยทีมงาน ดังนี้

๕.๑ ทีมงานคณะทำงานในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Management Team) กรมสนับสนุนบริการสุขภาพ

๕.๒ ทีมงานกอบกู้ส่วนวิศวกรรมระบบ (IT System Team)

๕.๓ ทีมงานกอบกู้ส่วนโปรแกรมประยุกต์ (Application Team)

๕.๔ ทีมงานกอบกู้ส่วนฐานข้อมูล (Database Team)

๕.๕ ทีมงานกอบกู้ส่วนระบบเครือข่าย (Network Team)

๖. บทบาทหน้าที่และความรับผิดชอบของทีมงาน (Team Role & Responsibilities)

๖.๑ ทีมงานคณะทำงานในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Management Team) กรมสนับสนุนบริการสุขภาพ ประกอบด้วย

นายวิชัย	จิตติกรยุทธนา	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร
นางอมรรัตน์	ทวีกุล	หัวหน้ากลุ่มพัฒนาระบบฐานข้อมูล
นายอภินันท์	นิลฉาย	หัวหน้ากลุ่มพัฒนาโปรแกรมประยุกต์
นายสมสิทธิ์	พลนาคู	หัวหน้ากลุ่มแผนงานเทคโนโลยี

มีหน้าที่หลักดังนี้

-ประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ

-ประเมินสถานการณ์ ควบคุม สั่งการและติดตามสถานการณ์ฉุกเฉินจากภัยพิบัติ

-อนุมัติค่าใช้จ่ายและอื่นๆ ที่เกิดขึ้นระหว่างสถานการณ์ฉุกเฉินจากภัยพิบัติ

-ประกาศยกเลิกแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ

-แถลงข่าว ประชาสัมพันธ์ ให้สัมภาษณ์และเผยแพร่ข้อมูลแก่เจ้าหน้าที่ของกรมสนับสนุนบริการสุขภาพและสาธารณชน เป็นต้น (ถ้ามี)

๖.๒ ทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team)

ประกอบด้วยหลายทีมงานย่อย ซึ่งมีหน้าที่หลักในการดำเนินกระบวนงานต่างๆ ตามหน้าที่รับผิดชอบในการกอบกู้ระบบสารสนเทศ ตามแผนการกอบกู้ระบบสารสนเทศให้กลับคืนมาได้ในระยะเวลาอันสั้นที่สุด โดยจะแบ่งหน้าที่รับผิดชอบของแต่ละทีมงานดังนี้

๖.๒.๑ ทีมกอบกู้ส่วนวิศวกรระบบ (IT System Team) ประกอบด้วย

ชื่อ – ชื่อสกุล	ตำแหน่ง	โทรศัพท์เคลื่อนที
นายวิชัย จิตติกรยุทธนา	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	๐๘๑-๒๐๖๖๕๗๘
นายจักรพงษ์ กันจันวงค์	ผู้บริหารโครงการบริษัทเทคโนเลจ คอนซัลดิงจำกัด	๐๘๖-๔๕๕๑๓๔๙
นายอภินันท์ นิลฉาย	หัวหน้ากลุ่มพัฒนาโปรแกรมประยุกต์	๐๘๑-๘๔๙๘๕๐๔
นายนภัทร ภู่คำมี	ผู้ดูแลระบบ	๐๘๖-๗๓๘๓๗๕๕

มีหน้าที่หลักดังนี้

- จัดเตรียมการย้ายส่วนประมวลผลให้สามารถดำเนินงานต่อได้
- รับผิดชอบในการกอบกู้ระบบงานหลักที่สำคัญของระบบสารสนเทศและการเชื่อมต่อกับ
- ระบบภายนอกมายังห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย (ถ้าเกิดความ เสียหาย)
- ติดต่อประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุน เช่น บริษัทคู่สัญญา หรือหน่วยของรัฐที่ให้บริการฝากคอมพิวเตอร์แม่ข่าย(co-location)
- ให้การสนับสนุนและให้คำปรึกษาทางด้านการติดตั้งและใช้งานระบบเทคโนโลยีสารสนเทศที่ห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย
- รับผิดชอบในการกอบกู้ระบบงานให้พร้อมใช้งานในเวลาที่กำหนด
- รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะ ให้ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ ทราบ

๖.๒.๒ ทีมกอบกู้ส่วนโปรแกรมประยุกต์ (Application Team) ประกอบด้วย

ชื่อ – ชื่อสกุล	ตำแหน่ง	โทรศัพท์เคลื่อนที
นายอภินันท์ นิลฉาย	หัวหน้ากลุ่มพัฒนาโปรแกรมประยุกต์	๐๘๑-๘๔๙๘๕๐๔
นายจักรพงษ์ กันจันวงค์	ผู้บริหารโครงการบริษัทเทคโนเลจ คอนซัลดิงจำกัด	๐๘๖-๔๕๕๑๓๔๙
นางสาวณิชาภัทร ชมช่อเงิน	นักวิชาการคอมพิวเตอร์	๐๘๑-๙๐๙๘๐๔๖
นายนภัทร ภู่คำมี	ผู้ดูแลระบบ	๐๘๖-๗๓๘๓๗๕๕

มีหน้าที่หลักดังนี้

-จัดเตรียมการย้ายส่วนประมวลผลของระบบงานหลัก (โปรแกรมประยุกต์ที่จำเป็นทั้งหมด) ให้สามารถดำเนินงานต่อได้
-จัดเตรียมระบบงานหลักที่สำคัญ และเทป Backup ให้พร้อมสำหรับการกอบกู้
-รับผิดชอบในการกอบกู้ระบบงานหลักที่สำคัญ (โปรแกรมประยุกต์ที่จำเป็นทั้งหมด)
-ติดต่อและประสานงานไปยังหน่วยงานที่เกี่ยวข้องเพื่อขอการสนับสนุนอุปกรณ์ต่างๆ
-ประสานงานในการกอบกู้ระบบคอมพิวเตอร์กับทีมกอบกู้ส่วนวิศวกรระบบ
-รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะ ให้ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ ทราบ

๖.๒.๓ ทีมกอบกู้ส่วนฐานข้อมูล (Database Team) ประกอบด้วย

ชื่อ – ชื่อสกุล	ตำแหน่ง	โทรศัพท์เคลื่อนที
นางอมรรัตน์ ทวีกุล	หัวหน้ากลุ่มพัฒนาระบบฐานข้อมูล	๐๘๑-๔๒๑๘๖๐๙
นายจักรพงษ์ กันจันวงค์	ผู้บริหารโครงการบริษัทเทคโนเลจ คอนซัลดิงจำกัด	๐๘๖-๔๕๕๑๓๔๙
นายนภัทร ภู่คำมี	ผู้ดูแลระบบ	๐๘๖-๗๓๘๓๗๕๕

มีหน้าที่หลักดังนี้

- จัดเตรียมระบบฐานข้อมูลและเทป Backup ให้พร้อมสำหรับการกอบกู้
- รับผิดชอบในการกอบกู้ระบบฐานข้อมูลของระบบงานที่สำคัญ
- รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะ ให้ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ ทราบ

๖.๒.๔ ทีมกอบกู้ส่วนระบบเครือข่าย (Network Team) ประกอบด้วย

ชื่อ – ชื่อสกุล	ตำแหน่ง	โทรศัพท์เคลื่อนที
นายสมสิทธิ์ พลนาคู	หัวหน้ากลุ่มแผนงานเทคโนโลยี	๐๘๖-๕๓๓๗๕๖๕
นายจักรพงษ์ กันจันวงค์	ผู้บริหารโครงการบริษัทเทคโนเลจ คอนซัลดิงจำกัด	๐๘๖-๔๕๕๑๓๔๙
นายนภัทร ภู่คำมี	ผู้ดูแลระบบ	๐๘๖-๗๓๘๓๗๕๕

มีหน้าที่หลักดังนี้

-รับผิดชอบในการดูแลแลตรวจสอบการทำงานของระบบเครือข่าย (ถ้าเกิดความเสียหาย)
-รับผิดชอบในการกอบกู้ระบบเครือข่าย
-จัดเตรียมระบบเครือข่ายสื่อสารให้พร้อมสำหรับการเปิดใช้งาน
-รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะ ให้ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ ทราบ

๖.๒.๕ ทีมสนับสนุนการดำเนินการกอบกู้ระบบสารสนเทศ ประกอบด้วย

ชื่อ – ชื่อสกุล	ตำแหน่ง	โทรศัพท์เคลื่อนที
นายวิชัย จิตติกรยุทธนา	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	๐๘๑-๒๐๖๖๕๗๘
นายจักรพงษ์ กันจันวงค์	ผู้บริหารโครงการบริษัทเทคโนเลจ คอนซัลติง จำกัด	๐๘๖-๔๕๕๑๓๔๙
นางอมรรัตน์ ทวีกุล	หัวหน้ากลุ่มพัฒนาระบบฐานข้อมูล	๐๘๑-๔๒๑๘๖๐๙
นายอภินันท์ นิลฉาย	หัวหน้ากลุ่มพัฒนาโปรแกรมประยุกต์	๐๘๑-๘๔๙๘๕๐๔
นายสมสิทธิ์ พลนาคู	หัวหน้ากลุ่มแผนงานเทคโนโลยี	๐๘๖-๕๓๓๗๕๖๕
นางกัญธิยารัตน์ รอดแสวง	นักวิชาการสถิติชำนาญการ	๐๘๙-๖๘๓๖๒๗๒
นางนงลักษณ์ นันทวนิช	หัวหน้าพัสดุ	๐๘๖-๑๔๙๑๗๒๔
นางสาวธิดารัตน์ แวงวรรณ	เจ้าหน้าที่การเงิน	๐๘๗-๙๓๒๘๖๑๑

มีหน้าที่หลักดังนี้

-จัดหาอุปกรณ์ที่สำคัญสำหรับการดำเนินการกอบกู้ระบบสารสนเทศ
-จัดหาและสนับสนุนงบประมาณในการดำเนินงาน
-ขออนุมัติงบประมาณในการดำเนินงาน
-ประสานงานกับทุกทีมในการกอบกู้ระบบสารสนเทศ
-รายงานผลการดำเนินงาน ปัญหา อุปสรรค และข้อเสนอแนะ ให้ทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ ทราบ

๗.การติดต่อสื่อสารในภาวะฉุกเฉิน

ในเวลาทำงานปกติ	ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร	ทำหน้าที่เป็นหัวหน้าทีมติดผู้ติดต่อสื่อสารหลัก โทร ๐๒-๕๙๐๑๖๘๑ มือถือ ๐๘๑-๒๐๖๖๕๗๘
และนอกเวลาทำงาน	นายอภินันท์ นิลฉาย	ทำหน้าที่เป็นหัวหน้าทีมติดผู้ติดต่อสื่อสารสำรอง โทร ๐๒-๕๙๐๑๖๘๑ มือถือ ๐๘๑-๘๔๙๘๕๐๔
	นายนภัทร ภู่คำมี	ทำหน้าที่เป็นหัวหน้าทีมติดผู้ติดต่อสื่อสารสำรอง มือถือ ๐๘๖-๗๓๘๓๗๕๕

๘.การประเมินความเสี่ยง (Risk Assessment) ของภัยพิบัติและสถานการณ์ฉุกเฉิน

ศูนย์สารสนเทศได้ประเมินความเสี่ยง(Risk Assessment)ของภัยพิบัติและสถานการณ์ฉุกเฉินที่สำคัญที่มีผลกระทบต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ โดยพิจารณาจาก ปัจจัยสภาพแวดล้อมต่างๆ มาตรการ เครื่องมือ การดำเนินงานในปัจจุบัน ดังนี้

ภัยพิบัติและสถานการณ์ฉุกเฉิน	เหตุผล
อัคคีภัย	ทำลายระบบเทคโนโลยีสารสนเทศ /ฐานข้อมูล / เอกสาร อาคาร /สถานที่ ทรัพย์สินของทางราชการ และความปลอดภัยของบุคลากร
อุทกภัย	ระบบสารสนเทศหยุดชะงัก ทำให้ไม่สามารถบรรลุเป้าหมายตามห้วงเวลาที่กำหนดได้ และอาจเกิดความเสียหายต่อสภาพแวดล้อม /ข้อมูล เอกสารและวิธีการปฏิบัติงาน
ไฟฟ้าดับ/ขัดข้อง	ทำให้ไม่สามารถเข้าถึงข้อมูล เกิดความเสียหายต่อฐานข้อมูล และระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นบ่อยครั้ง
Virus คอมพิวเตอร์	ทำให้ไม่สามารถเข้าถึงข้อมูล เกิดความเสียหายต่อฐานข้อมูล และระบบเทคโนโลยีสารสนเทศ ซึ่งเป็นเหตุการณ์ที่มีโอกาสเกิดขึ้นบ่อยครั้ง

๘.๑ การประเมินความเสี่ยง (Risk Assessment)

ศูนย์สารสนเทศได้ทำการวิเคราะห์ปัญหาความเสี่ยงในแง่ของโอกาสที่จะเกิดเหตุ (Likelihood) หรือเหตุการณ์ (event) ของภัยพิบัติที่สำคัญ ว่ามีมากน้อยเพียงไร และผลกระทบ (Impact) ที่ติดตามมาว่ามีความรุนแรงเสียหายมากน้อยเพียงใด โดยใช้เกณฑ์ในการประเมินระดับโอกาส(Likelihood) การเกิดแบ่งเป็น ๕ ระดับ ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์ต่างๆ (Likelihood)		
ระดับ	โอกาสที่จะเกิด(ความเป็นไปได้)	คำอธิบาย
๕	สูงมาก	มีโอกาสในการเกิดเกือบทุกครั้ง
๔	สูง	มีโอกาสในการเกิดค่อนข้างสูงหรือบ่อยๆ
๓	ปานกลาง	มีโอกาสเกิดบางครั้ง
๒	ต่ำ	อาจมีโอกาสเกิดแต่นานๆ ครั้ง
๑	ต่ำมาก	มีโอกาสเกิดในกรณียกเว้น

เกณฑ์ที่ใช้ในการประเมินผลกระทบ (Impact) ที่จะเกิดความเสี่ยง แบ่งออกเป็น ๕ ระดับ ดังนี้

ระดับความรุนแรงของผลกระทบ(Impact)		
ระดับ	ระดับผลกระทบ	คำอธิบาย
๕	สูงมาก	ระบบ IT ที่สำคัญทั้งหมดเกิดความเสียหายและทำให้การดำเนินงานหยุดชะงักนานเกินกว่า ๕ วัน
๔	สูง	ระบบ IT ที่สำคัญเกิดความเสียหายและทำให้การดำเนินงานหยุดชะงัก ๒ - ๕ วัน
๓	ปานกลาง	ระบบ IT มีปัญหาและมีความสูญเสียบางส่วนทำให้การดำเนินงานหยุดชะงักมากกว่า ๔ ชั่วโมงแต่ไม่เกิน ๒๔ ชั่วโมง
๒	ต่ำ	ระบบ IT มีปัญหาและมีความสูญเสียไม่มากทำให้การดำเนินงานหยุดชะงัก ๑ – ๔ ชั่วโมง
๑	ต่ำมาก	ระบบ IT มีปัญหาและเกิดความสูญเสียเพียงเล็กน้อย

๘.๒ การวิเคราะห์ผลกระทบและความรุนแรงภัยพิบัติและสถานการณ์ฉุกเฉินที่สำคัญ

ภัยพิบัติและสถานการณ์ฉุกเฉิน	โอกาสที่จะเกิด	ระดับผลกระทบ	คะแนนรวม	ลำดับที่
อัคคีภัย	๒	๕	๑๐	๒
อุทกภัย	๑	๕	๕	๔
ไฟฟ้าดับ/ขัดข้อง	๓	๕	๑๕	๑
Virus คอมพิวเตอร์	๔	๒	๘	๓

๙.แนวทางในการจัดการภัยพิบัติและสถานการณ์ฉุกเฉิน

จากการวิเคราะห์ระดับความรุนแรงที่มีผลต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ ได้กำหนดให้มีการจัดทำแผนปฏิบัติการเตรียมความพร้อมรองรับภัยพิบัติและสถานการณ์ฉุกเฉิน จำนวน ๔ แผน ซึ่งเป็นภัยพิบัติหรือสถานการณ์ฉุกเฉินที่ส่งผลกระทบรุนแรงต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ หรือส่งผลกระทบในวงกว้างต่อการปฏิบัติงาน ประกอบด้วย แผนรองรับไฟฟ้าดับ/ขัดข้อง แผนรองรับอัคคีภัย แผนรองรับไวรัสคอมพิวเตอร์ แผนรองรับอุทกภัย มีขั้นตอนดำเนินการดำเนินดังนี้

ขั้นตอนที่ ๑ การเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินก่อนเกิดภัย

ขั้นตอนที่ ๒ การปฏิบัติการขณะเกิดภัยพิบัติหรือสถานการณ์ฉุกเฉิน

ขั้นตอนที่ ๓ การปฏิบัติการฟื้นฟูบูรณะหลังเกิดภัย

ขั้นตอนที่ ๔ การติดตามและประเมินผล

ขั้นตอนที่ ๑ การเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินก่อนเกิดภัย

ในสถานการณ์ปกติให้สำนักเทคโนโลยีสารสนเทศและการสื่อสาร จัดเตรียมและจัดหาทรัพยากรที่จำเป็นเพื่อการป้องกันภัยพิบัติที่ส่งผลกระทบต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ เพื่อให้สามารถระงับภัยและแก้ไขสถานการณ์ได้ในภาวะฉุกเฉิน ได้มีประสิทธิภาพ มีขั้นการเตรียมความพร้อม ดังนี้

ด้านการจัดระบบปฏิบัติการรองรับภาวะฉุกเฉิน

๑.ทำการสำรวจจัดทำทะเบียนคอมพิวเตอร์และอุปกรณ์ที่สำคัญในห้องควบคุม เครื่องคอมพิวเตอร์แม่ข่าย(Data Center) เก็บไว้อย่างเป็นระบบสามารถเข้าถึงได้ง่าย

๒.จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ

๓.กำหนดโครงสร้าง บทบาทและหน้าที่ของทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team) ไว้เป็นลายลักษณ์อักษร

๔.จัดให้มีคู่มือการสำรองข้อมูล(backup) เก็บไว้ในที่เข้าถึงได้ง่าย

๕.ทำการตรวจสอบและบำรุงรักษา(maintenance) อุปกรณ์ที่สำคัญในห้องควบคุม คอมพิวเตอร์แม่ข่าย อาทิ ระบบคอมพิวเตอร์แม่ข่าย(server) ระบบฐานข้อมูล(database) ระบบเครือข่าย(network) ระบบไฟฟ้า ระบบสำรองไฟ ระบบป้องกันไฟไหม้ในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย ระบบป้องกันการควบคุมการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์แม่ข่าย ระบบป้องกันไวรัส คอมพิวเตอร์ ระบบไฟส่องสว่างสำรอง ระบบเครื่องปรับอากาศ ระบบกล้องวงจรปิด อย่างน้อยเดือนละ ๑ ครั้ง

๖.จัดให้มีระบบสำรองข้อมูล (Backup) ๒ รูปแบบ ได้แก่ การสำรองข้อมูลประจำวัน จะทำการสำรองข้อมูลและโครงสร้างข้อมูลที่มีการเปลี่ยนแปลง ให้ดำเนินการหลัง ๑๘.๐๐ น. โดยใช้ เทปBackup การสำรองข้อมูลประจำสัปดาห์ ดำเนินการทุกวันศุกร์ โดยทำการสำรองข้อมูลทั้งระบบ(full backup) บันทึกข้อมูลลงในเทป Backup โดยแยกเก็บเทปbackupไว้ภายนอกศูนย์สารสนเทศและสามารถนำกลับมาใช้ได้โดยง่าย

๗.จัดให้มีการทดสอบการ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการ ฐานข้อมูล ที่ทำการ Backup ไว้ในเทป Backup อย่างน้อยปีละ ๑ ครั้ง

๘.ทำการ update service patch ระบบปฏิบัติการ windows และ ระบบป้องกันไวรัสคอมพิวเตอร์ เป็นประจำ

๙.จัดเตรียมอุปกรณ์ที่สำคัญ อาทิ แผ่น BOOT แผ่นติดตั้งระบบปฏิบัติการ ระบบเครือข่าย แผ่นสำรองข้อมูล/Driver ระบบสำรองไฟฟ้าฉุกเฉิน Hard disk ระบบดับเพลิง สำรองไว้ให้พร้อมใช้งานได้ทันทีเมื่อเกิดภัย

ด้านบุคลากร

๑.จัดเตรียมเจ้าหน้าที่ที่รับผิดชอบ และจัดทำบัญชีทีมงานต่างๆ พร้อมเบอร์ โทรศัพท์ที่สามารถติดต่อได้

๒.จัดและมอบหมายเจ้าหน้าที่รับผิดชอบ ติดตามและเฝ้าระวังการเข้าถึงระบบสารสนเทศ ที่สำคัญของผู้ใช้งานและเฝ้าระวังการบุกรุกการเข้าโจมตีของผู้บุกรุกผ่านทาง ระบบเครือข่าย

ด้านการฝึกอบรม

๑.ทำการฝึกอบรมเจ้าหน้าที่ และส่งเจ้าหน้าที่เข้ารับการฝึกอบรมด้านการรักษาความมั่นคงระบบสารสนเทศ เกี่ยวกับภัยประเภทต่าง ๆ ให้สามารถป้องกันและช่วยเหลือ ตนเองได้เพื่อให้การจัดการในสถานการณ์ฉุกเฉินดำเนินไปอย่างมีประสิทธิภาพ

ด้านการจัดเตรียมสถานที่

๑.ศูนย์สารสนเทศต้องจัดเตรียมสถานที่และหาศูนย์คอมพิวเตอร์สำรองที่เหมาะสม ไว้รองรับสำหรับกรณีฉุกเฉิน

๒.หากเกิดภัยให้เคลื่อนย้ายระบบคอมพิวเตอร์และระบบงานที่สำคัญไว้ที่ห้องประชุม ๒ ชั้นที่ ๒ ตึกกองวิศวกรรมการแพทย์ กรมสนับสนุนบริการสุขภาพ

ด้านการฝึกซ้อมแผน

๑.ศูนย์สารสนเทศต้องจัดให้มีการเตรียมความพร้อมของเจ้าหน้าที่และซ้อมแผนฯเพื่อเป็น การเตรียมความพร้อมของเจ้าหน้าที่ ที่รับผิดชอบของหน่วยงาน และที่รับผิดชอบร่วมบูรณาการแผนฯและแนวทางการปฏิบัติให้ประสานสอดคล้องกัน

ขั้นตอนที่ ๒ การปฏิบัติการขณะเกิดภัยพิบัติหรือสถานการณ์ฉุกเฉิน

เมื่อเกิดหรือคาดว่าจะเกิดภัยพิบัติที่ส่งผลกระทบต่อระบบสารสนเทศกรมสนับสนุนบริการสุขภาพ ให้ผู้อำนวยการศูนย์สารสนเทศ เสนอรายงานต่อทีมงานคณะผู้บริหารในสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Management Teamประ) ประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ และดำเนินการตามแนวปฏิบัติดังนี้

ภัยพิบัติและสถานการณ์ฉุกเฉิน จากไฟฟ้าดับ/ขัดข้อง

เหตุฉุกเฉินกรณีกรณีไฟฟ้าดับ/ขัดข้อง หมายถึงไฟฟ้าดับทุกอาคาร ไม่สามารถแก้ไขด้วยเจ้าหน้าที่ของหน่วยงาน ต้องแก้ไขด้วยเจ้าหน้าที่ของการไฟฟ้านครหลวงเขตนนทบุรี

แนวปฏิบัติ

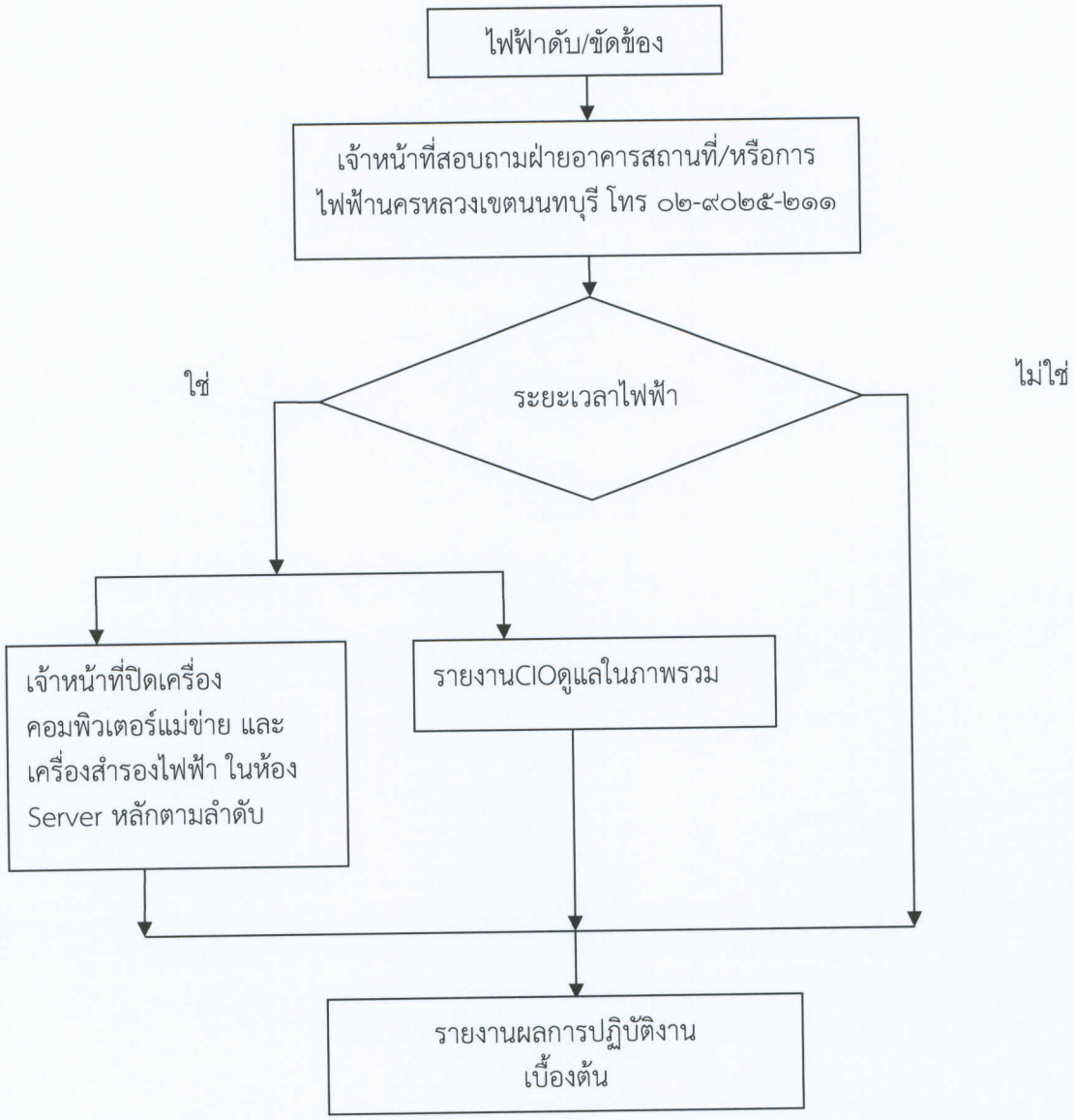
๑. ผู้พบเหตุการณ์แจ้งผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร

๒. สำนักเทคโนโลยีสารสนเทศและการสื่อสาร แจ้งการไฟฟ้านครหลวงเขตนนทบุรี เลขที่ ๒๘๕ ถนนติวานนท์ ตำบลบางกระสอ อำเภอเมือง จังหวัดนนทบุรี โทร ๐๒-๙๐๒๕-๒๑๑ , ๐๒-๙๐๒๕-๒๒๒ , ๐๒-๙๐๒๕-๓๑๑ , ๐๒-๙๐๒๕-๓๓๓

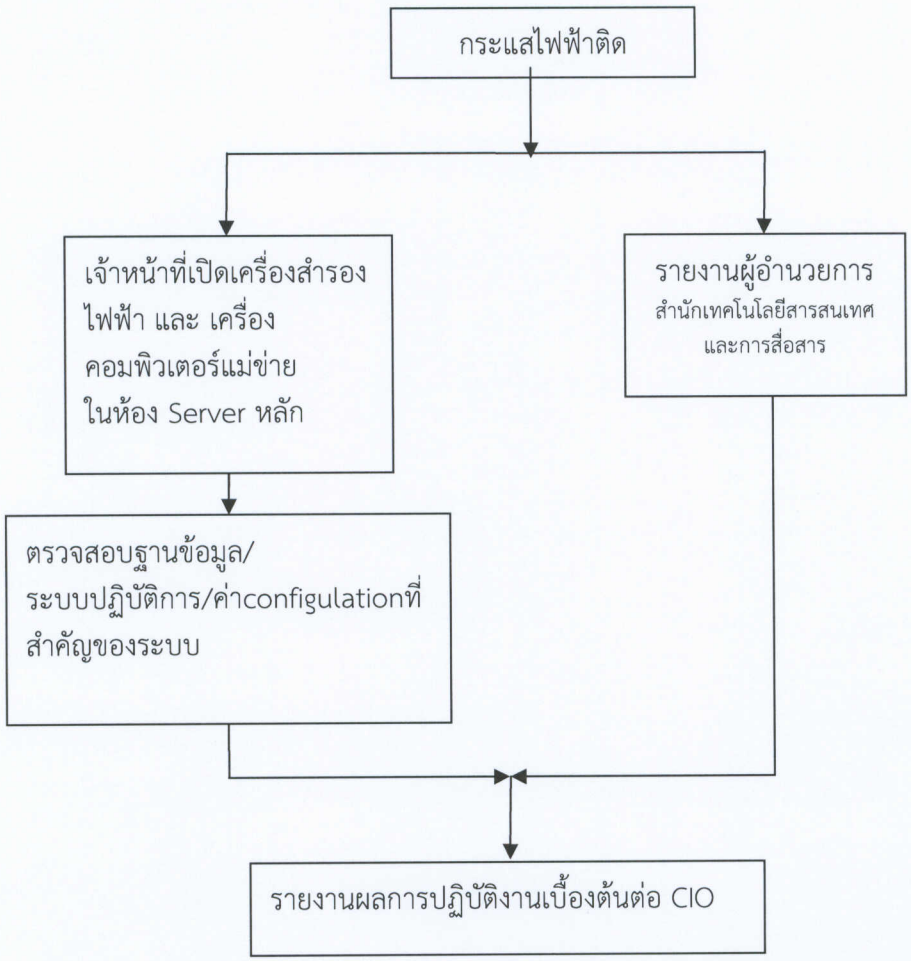
๓. ปิดระบบทั้งหมดเพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่าย

๔. เรียกประชุมทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team)

๕. เมื่อเกิดเหตุกระแสไฟฟ้าสามารถใช้งานได้ ทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team) เข้าควบคุม แก้ไข และตรวจสอบความเสียหายของระบบสารสนเทศในภาพรวม


ไฟฟ้าดับ/ขัดข้อง
เจ้าหน้าที่สอบถามฝ่ายอาคารสถานที่/หรือการไฟฟ้านครหลวงเขตนนทบุรี โทร ๐๒-๙๐๒๕-๒๑๑
ระยะเวลาไฟฟ้า
ใช่
ไม่ใช่
เจ้าหน้าที่ปิดเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องสำรองไฟฟ้า ในห้อง Server หลักตามลำดับ
รายงานCIOดูแลในภาพรวม
รายงานผลการปฏิบัติงานเบื้องต้น

ขั้นตอนปฏิบัติการเมื่อเกิดเหตุกระแสไฟฟ้าสามารถใช้งานได้



ภัยพิบัติและสถานการณ์ฉุกเฉิน กรณีเกิดอัคคีภัย

แนวปฏิบัติ

เจ้าหน้าที่ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

๑. ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ ทำการดับไฟ

๒. หากไม่สามารถดับไฟได้ ให้โทรแจ้ง สถานีดับเพลิงเทศบาลนครนนทบุรี (รัตนาธิเบศร์) ๐๒-๕๘๙-๐๔๘๙

๓. การขนย้ายอุปกรณ์ที่สำคัญตามลำดับ ในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

๔. เมื่อสามารถควบคุมอัคคีภัยได้แล้ว ให้เรียกประชุมทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team) ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบไฟฟ้า และติดตั้งอุปกรณ์ให้พร้อมใช้งาน

๕.ตรวจสอบความพร้อมใช้ของเครื่องแม่ข่ายและเครื่องลูกข่าย

เจ้าหน้าที่อื่นๆ

หากเจ้าหน้าที่ศูนย์คอมพิวเตอร์ไม่อยู่ เจ้าหน้าที่อื่นสามารถดำเนินการได้ดังนี้

๑.ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ ทำการดับไฟ

๒.หากไม่สามารถดับไฟได้ ให้โทรแจ้ง สถานีดับเพลิงเทศบาลนครนนทบุรี (รัตนาธิเบศร์) ๐๒-๕๘๙-๐๔๘๙

๓.ให้เปิดประตู้ห้อง Server หรือพังประตูเพื่อเข้าไปในห้อง server

๔.ทำการตัดสาย LAN โดยใช้คีมตัดสาย LAN ออกให้หมด

๕.ทำการถอดสายไฟที่อยู่ภายนอกตู้ Server ออกให้หมด

๖.ทำการเคลื่อนย้ายตามแผนป้องกันอัคคีภัย

ภัยพิบัติและสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว

เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย เจ้าหน้าที่ปฏิบัติดังนี้

แนวปฏิบัติ

เจ้าหน้าที่ผู้แลระบบคอมพิวเตอร์

๑. วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

๒. ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

๓. ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

๔. กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้ขอความช่วยเหลือ ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย(thaicert) ทางหมายเลขโทรศัพท์ ๐-๒๑๔๒-๒๔๘๓

๕. ให้เรียกประชุมทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team) ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่าย ระบบเครื่องคอมพิวเตอร์แม่ข่าย ระบบป้องกันไวรัส ระบบฐานข้อมูลและระบบปฏิบัติการฯลฯทำการกู้ระบบกลับมาโดยเร็ว

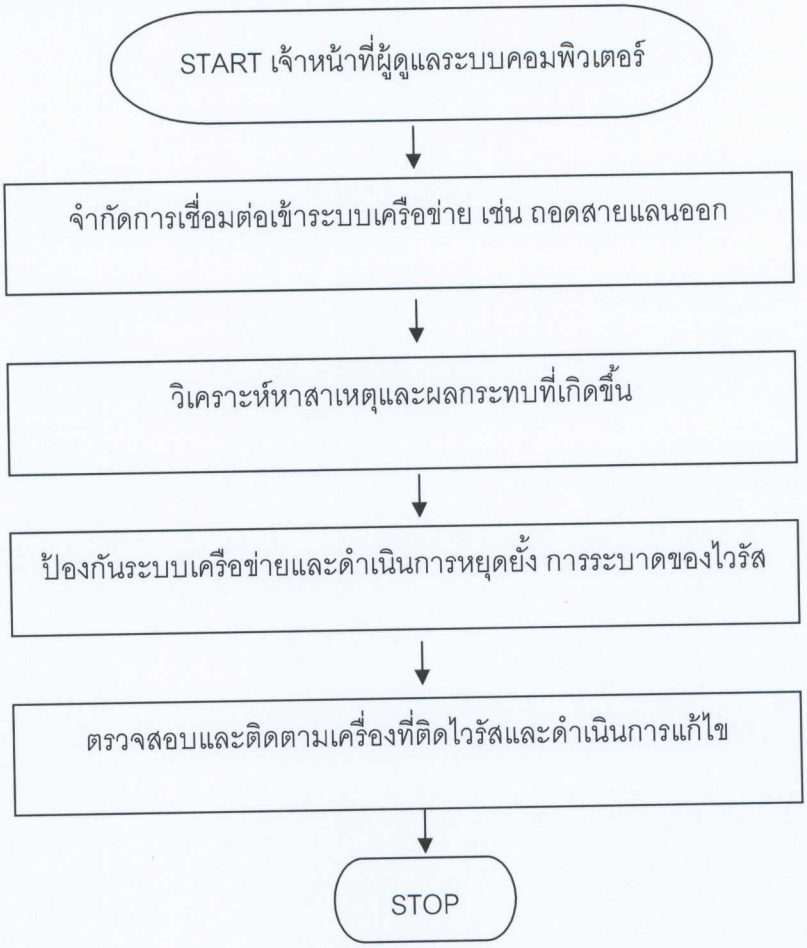
เจ้าหน้าที่ดูแลเครื่องลูกข่าย

๑. แจ้งปัญหาไวรัสคอมพิวเตอร์ ให้ผู้ดูแลระบบศูนย์สารสนเทศ ทราบ

๒. ตัดการเชื่อมต่อในระบบเครือข่าย โดยชักสายแลนออกจากเครื่องคอมพิวเตอร์/ตัดการเชื่อมต่อระบบเครื่องข่ายไร้สาย

๓. ตรวจสอบหาไวรัสที่เครื่องคอมพิวเตอร์ลูกข่าย

ผังแสดงขั้นตอนการรับมือภัยพิบัติและสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



ภัยพิบัติและสถานการณ์ฉุกเฉิน กรณีน้ำท่วม

แนวปฏิบัติ

ผู้อำนวยการศูนย์สารสนเทศ

๑. ติดตามสอบถามสถานการณ์น้ำท่วม จากศูนย์ตอบโต้ภาวะฉุกเฉินจากสถานการณ์น้ำท่วม กรมสนับสนุนบริการสุขภาพ เพื่อรับรู้สถานการณ์ของน้ำท่วม

๒. จัดหากระสอบทรายมาปิดล้อมบริเวณรอบศูนย์สารสนเทศ (อาคาร ๗ ชั้น ๕) ให้สูงอย่างน้อย ๓๐ เซนติเมตร

๓. เรียกประชุม ทีมงานปฏิบัติการกอบกู้สถานการณ์ฉุกเฉินจากภัยพิบัติที่มีผลกระบบต่อระบบสารสนเทศ (Crisis Operation Team) หาแนวทางกรอบกู้ระบบสารสนเทศ

๔. หากพิจารณาสถานการณ์แล้วเห็นว่าไม่ปลอดภัย ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศและการสื่อสาร ขออนุญาตCIO เคลื่อนย้ายระบบสารสนเทศที่สำคัญไปไว้ที่ ห้องประชุม ๒ ชั้น ๒ ตึกกองวิศวกรรมการแพทย์

ผู้ดูแลระบบคอมพิวเตอร์ ดำเนินการดังนี้

๑.ปิดระบบและทำการเคลื่อนย้ายอุปกรณ์สำคัญต่างๆที่ยังสามารถใช้งานได้ ไปติดตั้ง ณ ห้องประชุม ๒ ชั้น ๒ ตึกกองวิศวกรรมการแพทย์

๒. สำรวจความเสียหาย ความพร้อมใช้งาน หากชำรุดเสียหาย ไม่พร้อมใช้งาน ให้นำระบบสำรองที่จัดเก็บไว้มากู้คืนหรือจัดหาอุปกรณ์มาทดแทน ในส่วนที่เกิดความเสียหาย หากพร้อมใช้งาน ให้ ทำการเปิดระบบสารสนเทศเพื่อสามารถดำเนินการได้

๓. ให้รายงาน ตรวจสอบรายการทรัพย์สิน ที่เสียหายและดำเนินการจัดซ่อมอุปกรณ์ที่ชำรุดเสียหาย

ขั้นตอนที่ ๓ การปฏิบัติการฟื้นฟูบูรณะหลังเกิดภัย

เมื่อสถานการณ์ฉุกเฉินได้กลับคืนสู่ภาวะปกติแล้ว ประเมินความเสียหาย ทำการฟื้นฟูพื้นที่หรือสถานที่ประสบภัยพิบัติ จะดำเนินการภายหลังที่ภัยยุติหรือผ่านพ้นไปแล้ว โดยการซ่อมแซมสภาพพื้นที่และบูรณะโครงสร้างพื้นฐานที่ชำรุดเสียหายให้กลับคืนสู่สภาพเดิมตามขั้นตอน ดังนี้

๑ สำรวจความเสียหายของระบบสารสนเทศ ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย อุปกรณ์สารสนเทศและการสื่อสารที่สำคัญ

๒. ซ่อมแซมส่วนที่เสียหายหรือที่ได้รับผลกระทบตามที่พิจารณาเห็นว่าเป็นสิ่งที่สามารถซ่อมแซมกู้คืนได้โดยเร็ว เพื่อให้สามารถดำเนินการต่อได้อย่างต่อเนื่อง ในกรณีที่ไม่สามารถซ่อมแซมได้ให้จัดการรื้อถอนออกไปเพื่อป้องกันอันตรายที่อาจจะเกิดขึ้น

๓. กรณีที่เกินขีดความสามารถของส่วนราชการ/หน่วยงาน ให้ขอรับการสนับสนุนจากหน่วยเหนือขึ้นไปตามลำดับ ได้แก่ งบประมาณของกระทรวง งบประมาณของกรม หรืองบกลาง

ขั้นตอนที่ ๔ การติดตามและประเมินผล

เมื่อภัยพิบัติและสถานการณ์ฉุกเฉินยุติแล้ว ให้หัวหน้าหน่วยงานที่รับผิดชอบ ดำเนินการติดตามและประเมินผลการป้องกันและแก้ไขปัญหาสถานการณ์ที่เกิดขึ้น ทั้งด้านสถานการณ์ภัยพิบัติ ด้านการปฏิบัติในการระงับและบรรเทาภัย ด้านการให้ความช่วยเหลือ และด้านอื่นๆ ต่ออธิบดีกรมสนับสนุนบริการสุขภาพ เพื่อให้ทราบข้อบกพร่องที่ต้องปรับปรุงแก้ไข และเป็นแนวทางในการบริหารจัดการภัยพิบัติและสถานการณ์ฉุกเฉินในอนาคต และควรปรับปรุงแผนฯทุกๆ ๑ ปี

ผู้เสนอแผนฯ สมสิทธิ์ พลนาคู

(นายสมสิทธิ์ พลนาคู)

หัวหน้ากลุ่มแผนงานเทคโนโลยี

ขั้นตอนการทดสอบแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ
ที่มีผลกระทบต่อระบบสารสนเทศ (Test IT Contingency Plan)
วันที่ ๒๘ กันยายน ๒๕๕๕ เวลา ๑๐.๐๐ น ณ ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย
สำนักเทคโนโลยีสารสนเทศและการสื่อสาร กรมสนับสนุนบริการสุขภาพ

ทดสอบระบบไฟไหม้ เริ่มทดสอบเวลา ๑๐.๑๕ น

ขั้นตอน		กิจกรรม	ผู้รับผิดชอบ	เวลาที่คาดประมาณเสร็จ	เวลาที่ใช้เสร็จจริง
ขั้นตอนที่ ๑	สัญญาณไฟไหม้ใน ห้องควบคุมแม่ข่ายดังขึ้น ระบบดับเพลิงห้องควบคุมคอมพิวเตอร์แม่ข่ายดับทำงานอัตโนมัต	เจ้าหน้าที่ศูนย์ไปหยิบเครื่องดับเพลิงเตรียมเข้าควบคุมเพลิงไหม้	นายนภัทร ภู่คำมี เจ้าหน้าที่จ้าหน้าที่บริษัทเทคโนเลจคอนซัลติง	๒๐ นาที	๒๕ นาที
ขั้นตอนที่ ๒	เจ้าหน้าที่อพยพหนีไฟ	เจ้าหน้าที่ศูนย์สารสนเทศอพยพหนีไฟไปทางประตูหน้า พบกันที่จุดนัดหมาย (ใต้อาคาร ๗)	นายสมสิทธิ์ พลนาคู	๑๕ นาที	๑๐ นาที
ขั้นตอนที่ ๓	เพลิงสงบ	เจ้าหน้าที่เข้าตรวจสอบความเสียหาย	ทีมกอบกู้ส่วนวิศวกรรม (เจ้าหน้าที่บริษัทเทคโนเลจคอนซัลติง จำกัดทีมกอบกู้ฐานข้อมูล (คุณนภัทร ภู่คำมี)	๑ ชั่วโมง	๑ ชม ๓๐ นาที

ขั้นตอน		กิจกรรม	ผู้รับผิดชอบ	เวลาที่คาดประมาณเสร็จ	เวลาที่ใช้เสร็จจริง
			ทีมกอบกู้ส่วนโปรแกรมประยุกต์ (คุณอภินันท์ นิลฉาย) ทีมกอบกู้ระบบเครือข่าย (คุณสมสิทธิ์ พลนาคู)		
ขั้นตอนที่ ๔	ทดสอบการrestore ระบบจัดเก็บเอกสาร	เจ้าหน้าที่นำเทปbackup Restore ข้อมูลกลับ	คุณนภัทร ภู่คำมี	๒ ชั่วโมง	๑ ชั่วโมง ๓๐ นาที
ขั้นตอนที่ ๕	ทดสอบระบบทั้งหมด	เจ้าหน้าที่ทีมกอบกู้ระบบทีมต่างๆ ทดสอบระบบทั้งหมดและเปิดใช้งานระบบ	ทีมกอบกู้ส่วนวิศวกรรม ทีมกอบกู้ฐานข้อมูล ทีมกอบกู้ส่วนโปรแกรมประยุกต์ ทีมกอบกู้ระบบเครือข่าย	๑ ชั่วโมง	๑ ชั่วโมง ๒๐ นาที

ปิดการทดสอบเวลา ๑๔.๕๕ นาที ใช้เวลาในการทดสอบ ๔.๕๕ นาที