คู่มือการปฏิบัติงาน (SOP) กระบวนงานรับมือภัยคุกคามสารสนเทศ
กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

๑. วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติตามขั้นตอนของการรับมือภัยคุกคามสารสนเทศ กรณีเกิดอัคคีภัยหรืออุทกภัยให้เป็นไปตามมาตรฐานที่กำหนด

๒. ขอบเขต

๒.๑ รองรับเฉพาะการรับมือภัยคุกคามสารสนเทศ กรณีเกิดอัคคีภัยหรืออุทกภัยเท่านั้น

๓. แผนภูมิการทำงาน

ตามเอกสารแนบ

๔. รายละเอียดขั้นตอนการปฏิบัติงาน

ขั้นตอนที่ ๑ : พิจารณาสถานการณ์ที่เกิดขึ้นว่าเป็นอัคคีภัยหรืออุทกภัย

ขั้นตอนที่ ๒ : ตรวจสอบว่ามีเจ้าหน้าที่ศูนย์คอมพิวเตอร์อยู่หรือไม่

- ถ้าเจ้าหน้าที่คอมพิวเตอร์อยู่ ให้ไขกุญแจเปิดประตูห้อง Server
- ถ้าเจ้าหน้าที่คอมพิวเตอร์ไม่อยู่ ให้พังประตูเข้าไปห้อง Server

ขั้นตอนที่ ๓ : ถอดสายไฟและสาย LAN ที่เชื่อมต่ออปุกรณ์ออกให้หมด

ขั้นตอนที่ ๔ : ทำการเคลื่อนย้ายตามแผนป้องกันอัคคีภัยหรืออุทกภัย

ขั้นตอนที่ ๕ : การขนย้ายคอมพิวเตอร์และอุปกรณ์ต่อพ่วง พิจารณาตามลำดับความสำคัญดังต่อไปนี้

ลำดับที่ ๑ เครื่อง Server เว็บ สสม. , Server HOSPITAL OS
ลำดับที่ ๒ Computer PC
ลำดับที่ ๓ Computer Notebook
ลำดับที่ ๔ Switch, HUB, Access Point
ลำดับที่ ๕ Printer
ลำดับที่ ๖ เครื่องสำรองไฟฟ้า (UPS)

ขั้นตอนที่ ๖ : เมื่อสถานการณ์อยู่ในภาวะปกติแล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่ายอินเตอร์เน็ต ,ระบบไฟฟ้า

ขั้นตอนที่ ๗ : ติดตั้งอุปกรณ์ต่างๆ ให้พร้อมใช้งาน

ขั้นตอนที่ ๘ : ตรวจสอบความพร้อมใช้งานของเครื่องลูกข่าย

กระบวนงานรับมือภัยคุกคามสารสนเทศ
กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

วัตถุประสงค์

เพื่อเป็นแนวทางในการปฏิบัติตามขั้นตอนของการรับมือภัยคุกคามสารสนเทศ กรณีเกิดอัคคีภัย หรืออุทกภัยให้เป็นไปตามมาตรฐานที่กำหนด

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	จุดควบคุมความเสี่ยง	ระยะเวลา
กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน	๑. พิจารณาสถานการณ์ที่เกิดขึ้น -อัคคีภัย -อุทกภัย	บุคลากรมีการเตรียมความพร้อมซ้อมแผนอัคคีภัยและอุทกภัยทุกปี	๓๐ นาที / ครั้ง
นายวิทยุทธ์ นิลรัตน์	๒. เจ้าหน้าที่อยู่หรือไม่ อยู่ ไม่อยู่	มีการเตรียมเจ้าหน้าที่ฝ่ายอื่นไว้สำรองทุกครั้ง	๓๐ นาที / ครั้ง
นายเมธีร์ ชะรัดรัมย์	๓. ไขกุญแจเปิดประตูห้อง Server หรือพังประตูเข้าไปห้อง Server	เก็บกุญแจห้อง Server ไว้อย่างเป็นระเบียบ หาง่าย และมีอุปกรณ์สำรองในการพังประตูห้อง Server	๓๐ นาที / ครั้ง
นายเทวพงศ์ วงค์เขื่อนแก้ว	๔. ถอดสายไฟและสาย LAN ที่เชื่อมต่ออุปกรณ์ออกให้หมด	มีอุปกรณ์ป้องกันไฟฟ้ารัดวงจร	๓๐ นาที / ครั้ง
นายวิทยุทธ์ นิลรัตน์	๕. เคลื่อนย้ายตามแผนป้องกันอัคคีภัยหรืออุทกภัย	จัดเตรียมบุคคลากรไว้ให้เพียงพอทุกครั้งสำหรับการเตรียมรับสถานการณ์อัคคีภัยและอุทกภัย	๓๐ นาที / ครั้ง

ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติงาน	จุดควบคุมความเสี่ยง	ระยะเวลา
นายเมธีร์ ชะรัดรัมย์ นายเทวพงศ์ วงค์เขื่อนแก้ว นายวิทยุทธ์ นิลรัตน์ นายกันตินันท์ ภู่ทอง	๖. เคลื่อนย้ายอุปกรณ์ไปยังจุดรวมพลหรือสถานที่ปลอดภัย ตามลำดับความสำคัญดังต่อไปนี้ ลำดับที่ ๑ เครื่อง Server เว็บ สสม. , Server HOSPITAL OS, NAS Storage ลำดับที่ ๒ Computer PC ลำดับที่ ๓ Computer Notebook ลำดับที่ ๔ Switch, HUB, Access Point ลำดับที่ ๕ Printer ลำดับที่ ๖ เครื่องสำรองไฟฟ้า (UPS)	คลื่อนย้ายเฉพาะอุปกรณ์ที่ยังสามรถเคลื่อนย้ายได้	๓๐ นาที / ครั้ง
นายเทวพงศ์ วงค์เขื่อนแก้ว	๗. เมื่อสถานการณ์อยู่ในภาวะปกติแล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่ายอินเตอร์เน็ต ,ระบบไฟฟ้า	มีการสำรองระบบอินเตอร์เน็ต ,ระบบไฟฟ้าไว้ใช้งานกรณีฉุกเฉิน	๓๐ นาที / ครั้ง
นายวิทยุทธ์ นิลรัตน์	๘. ติดตั้งอุปกรณ์ต่าง ๆ ให้พร้อมใช้งาน	มีการติดตั้งอุปกรณ์ต่าง ๆ ให้พร้อมใช้งานในส่วนที่จำเป็นก่อนแล้วทยอยติดตั้งในส่วนที่เหลือทั้งหมด	๓๐ นาที / ครั้ง
นายเมธีร์ ชะรัดรัมย์	๙. ตรวจสอบความพร้อมใช้งานของเครื่องลูกข่าย	ตรวจสอบความพร้อมของเครื่องแม่ข่ายที่ส่งมายังเครื่องลูกข่าย	๓๐ นาที / ครั้ง
รวมระยะเวลาทั้งหมด			**๒๗๐ นาที**

ตารางวิเคราะห์ระดับความเสี่ยง

กระบวนงานภัยคุกคามสารสนเทศ

กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

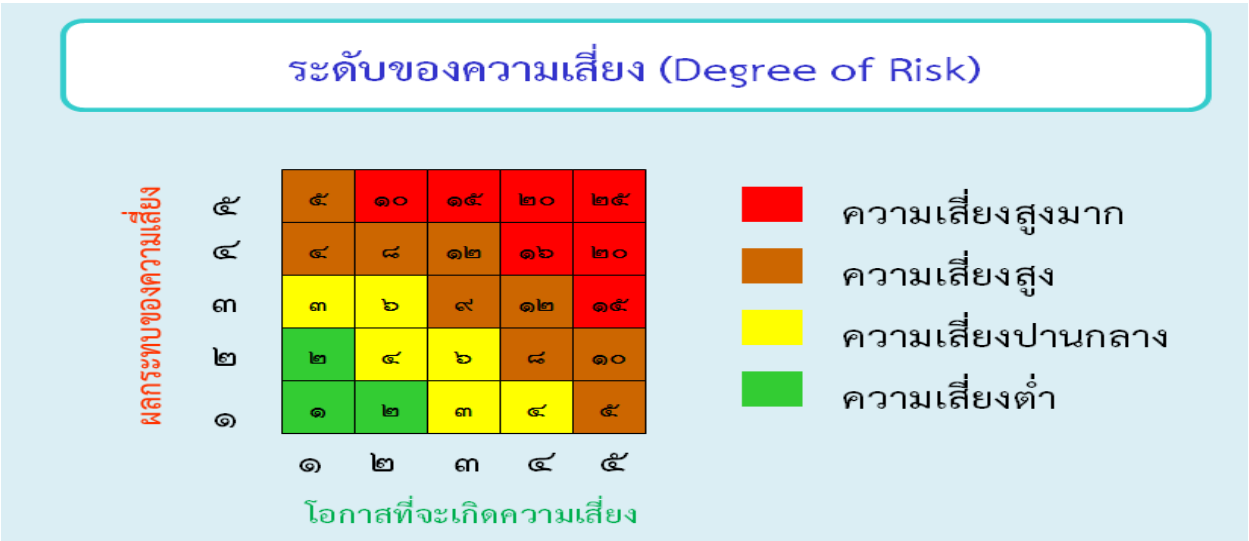
ภารกิจตามกฎหมาย/แผนงาน/ภารกิจอื่น ๆที่สำคัญ/ขั้นตอน	วัตถุประสงค์	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง				ลำดับความเสี่ยง
				โอกาส	ผลกระทบ	ระดับความเสี่ยง		
						คะแนน	ระดับ	
กระบวนงานภัยคุกคามสารสนเทศ ๑. ความเสี่ยงจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	เพื่อลดความเสี่ยงจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	จำนวนครั้งของการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม	ไฟไหม้ จากอุบัติเหตุไฟฟ้าลัดวงจร การวางเพลิง - ภัยธรรมชาติ	๒	๔	๘	สูง	๑

ตารางวิเคราะห์ความเสี่ยง

เกณฑ์การประเมินระดับโอกาสของความถี่ที่จะเกิดขึ้น

ความเสี่ยงจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม

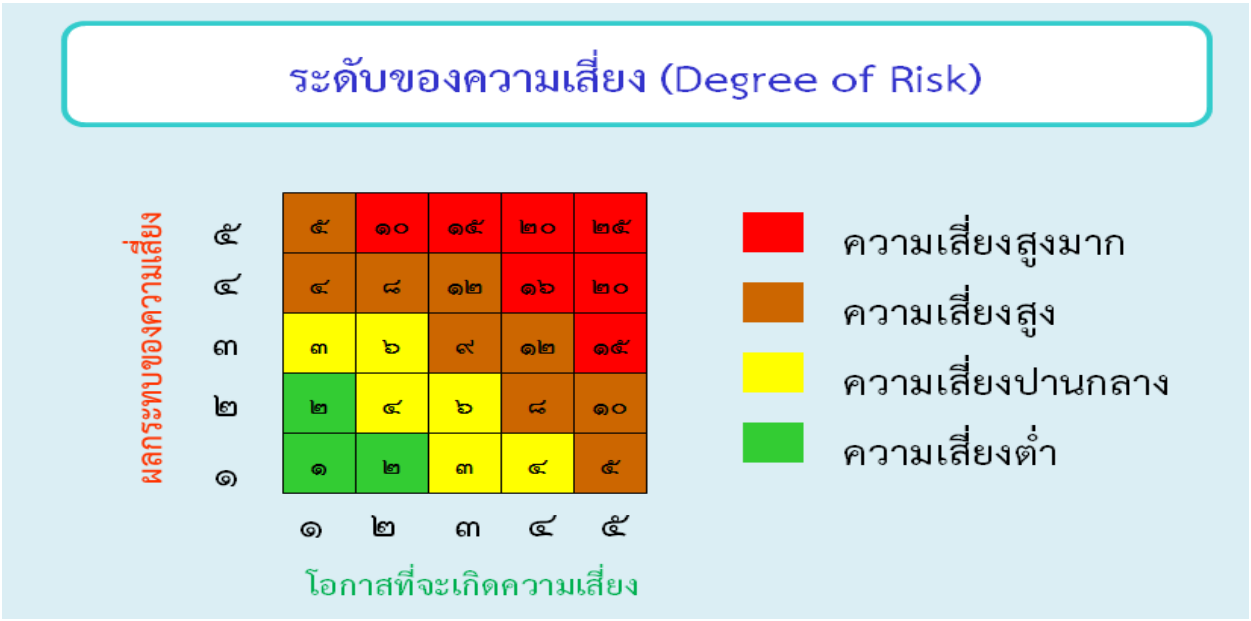
โอกาสที่จะเกิดขึ้น	**ระดับคะแนน**	**โอกาสที่จะเกิดความเสี่ยง**
เกิดความเสียหายจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม ๙๐	๕	สูงมาก
เกิดความเสียหายจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม ๗๐-๘๙	๔	สูง
เกิดความเสียหายจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม ๕๐-๖๙	๓	ปานกลาง
เกิดความเสียหายจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม ๓๐-๔๙	๒	น้อย
เกิดความเสียหายจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม ๑๐-๒๙	๑	น้อยมาก



เกณฑ์การประเมินระดับผลกระทบของความเสี่ยงที่จะเกิดขึ้น

ความเสี่ยงจากการไม่ปฏิบัติตามแผนการเกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม

ผลกระทบที่จะเกิดขึ้น	ระดับคะแนน	โอกาสที่จะเกิดความเสี่ยง
กระทบกับหน่วยงานมากที่สุด	๕	สูงมาก
กระทบกับหน่วยงานมาก	๔	สูง
กระทบกับหน่วยงานปานกลาง	๓	ปานกลาง
กระทบกับหน่วยงานน้อย	๒	น้อย
กระทบกับหน่วยงานน้อยที่สุด	๑	น้อยมาก



แบบสอบถามกระบวนงานการรับมือภัยคุกคามสารสนเทศ
กลุ่มงานพัฒนาองค์กรและขับเคลื่อนกำลังคน

แบบสอบถามนี้เหมาะสำหรับผู้ตอบแบบสอบถามผู้ที่เกี่ยวข้องหรือผู้ที่ซึ่งคุ้นเคยเกี่ยวกับด้านการรับมือภัยคุกคามสารสนเทศ ข้อสรุปคำตอบจะต้องมาจากการสังเกตการณ์และการสัมภาษณ์ผู้มีความรู้ในเรื่องนี้
แบบสอบถามด้านการรับมือภัยคุกคามสารสนเทศ ประกอบด้วย

แบบสอบถามด้านกระบวนงานการรับมือภัยคุกคามสารสนเทศ

คำถาม	**มี / ใช่**	**ไม่มี / ไม่ใช่**	**คำอธิบาย/คำตอบ**
ขั้นตอนพิจารณาสถานการณ์ที่เกิดขึ้น			
๑.ได้มีเตรียมรับแผนรับมือกับภัยคุกคามสารสนเทศ เช่น อัคคีภัย อุทกภัย			
๒.ได้มีการฝึกซ้อมแผนรับมือกับภัยคุกคามสารสนเทศ เช่น อัคคีภัย อุทกภัย			
ขั้นตอนถอดสายไฟและสาย LAN ที่เชื่อมต่ออปุกรณ์ออกให้หมด			
๑.มีบุคลากรพร้อมในการช่วยถอดสายไฟและสาย LAN ที่เชื่อมต่ออุปกรณ์ออกให้หมด			
๒.ได้มีการถอดสายไฟและสาย LAN ที่เชื่อมต่ออุปกรณ์ออกให้หมด			
ขั้นตอนเคลื่อนย้ายตามแผนป้องกันอัคคีภัยหรืออุทกภัย			
๑.มีแผนรับมือกับภัยคุกคามสารสนเทศอัคคีภัย			
๒.มีแผนรับมือกับภัยคุกคามสารสนเทศอุทกภัย			
ขั้นตอนเมื่อสถานการณ์อยู่ในภาวะปกติแล้ว ให้ดำเนินการตรวจสอบความเรียบร้อยของระบบเครือข่ายอินเตอร์เน็ต ,ระบบไฟฟ้า			
๑.ได้มีการติดตั้งอุปกรณ์ต่าง ๆ ให้พร้อมใช้งาน			
๒.มีการตรวจสอบความพร้อมใช้งานของเครื่องลูกข่าย			

สรุป : .....

ชื่อผู้รายงาน.....

ตำแหน่ง .....

วันที่...../...../.....