แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติ
ของระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ศูนย์เทคโนโลยีสารสนเทศ

กองบริการดิจิทัลอุตุนิยมวิทยา

กรมอุตุนิยมวิทยา

ปีงบประมาณ 2567

ชื่อเรื่อง	แผนป้องกันและแก้ปัญหาจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)
เอกสารหมายเลข	IT01-03
รุ่นเอกสาร	4.0
วันปรับปรุงล่าสุด	14 มีนาคม 2567
หน่วยงานผู้รับผิดชอบ	ศูนย์เทคโนโลยีสารสนเทศ กองบริการดิจิทัลอุตุนิยมวิทยา กรมอุตุนิยมวิทยา

คำนำ

กรมอุตุนิยมวิทยา ได้ตระหนักถึงความสำคัญของข้อมูลและสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ จึงจำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่างๆ อันอาจจะเกิดขึ้นกับข้อมูล และระบบสารสนเทศ จึงได้จัดทำแผนป้องกันและแก้ปัญหาจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการปฏิบัติการบำรุงรักษา ป้องกัน และแก้ไขปัญหาที่อาจเกิดขึ้นต่อระบบสารสนเทศ และอาจส่งผลกระทบต่อเสถียรภาพของข้อมูลและระบบสารสนเทศ รวมทั้งระบบคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบ ฐานข้อมูล และระบบเครือข่ายของกรมอุตุนิยมวิทยาต่อไป

ศูนย์เทคโนโลยีสารสนเทศ

มีนาคม 2567

สารบัญ

สารบัญรูป

สารบัญตาราง

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญ

กรมอุตุนิยมวิทยา มีพันธกิจหลักในการตรวจอากาศ พยากรณ์อากาศ เตือนภัยธรรมชาติ และให้บริการสารสนเทศอุตุนิยมวิทยา กรมฯ ได้ใช้เทคโนโลยีสารสนเทศเพื่อสนับสนุนการดำเนินงานตามภารกิจเป็นอย่างมาก ทั้งในด้านการรายงานผลการตรวจอากาศ การประมวลผลข้อมูลอุตุนิยมวิทยา การประมวลผลเพื่อการพยากรณ์อากาศ การให้บริการข้อมูลข่าวอากาศ ตลอดจนใช้ในกิจกรรมการบริหารงานทั่วไป เพื่อให้บริการแก่ประชาชนอย่างถูกต้อง รวดเร็ว และมีประสิทธิภาพ

จากลักษณะงานของกรมอุตุนิยมวิทยาที่ต้องให้บริการอย่างรวดเร็ว มีความถูกต้อง เชื่อถือได้ ทำให้ต้องใช้ระบบเทคโนโลยีสารสนเทศที่มีประสิทธิภาพและสามารถปฏิบัติงานได้ตลอดเวลา การชำรุด บกพร่องของอุปกรณ์ ซอฟท์แวร์ รวมทั้งข้อมูลและสารสนเทศ จะส่งผลให้ระบบเทคโนโลยีสารสนเทศมีความบกพร่อง หรือแม้แต่ระบบสารสนเทศไม่สามารถทำงานได้อย่างเต็มประสิทธิภาพ อาจก่อให้เกิดผลเสียร้ายแรงต่อการปฏิบัติงานโดยรวม ดังนั้น เสถียรภาพของระบบเทคโนโลยีสารสนเทศจึงมีความสำคัญเป็นอย่างยิ่ง การจัดทำแผนป้องกันและแก้ปัญหาจากภัยพิบัติ จะช่วยให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงมากขึ้น เพราะสามารถใช้เป็นแนวทางในการป้องกัน และแก้ปัญหาข้อขัดข้อง และลดความเสียหายที่อาจเกิดจากภัยพิบัติได้

1.2 วัตถุประสงค์

1) สร้างความพร้อมในการรองรับสถานการณ์ที่อาจเกิดขึ้นและทำให้ระบบสารสนเทศขาดเสถียรภาพหรือไม่สามารถใช้งานได้อย่างมีประสิทธิภาพ

2) เพื่อให้สามารถกู้คืนระบบสารสนเทศและข้อมูล ให้สามารถกลับมาใช้งานได้ดังเดิมในระยะเวลารวดเร็ว

3) เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ และการปฏิบัติงานที่เกี่ยวข้องกับการใช้เทคโนโลยีสารสนเทศ

4) เพื่อจัดให้มีการบริหารและจัดการความเสี่ยงที่มีต่อระบบสารสนเทศสำคัญ อันจะก่อให้เกิดการหยุดชะงักของระบบได้

5) เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับใช้งานตลอดเวลา

1.3 ขอบเขตของแผน

แผนป้องกันและแก้ไขปัญหาจากภัยพิบัติของระบบเทคโนโลยีสารสนเทศของกรมอุตุนิยมวิทยา ประกอบด้วยส่วน 2 ส่วนหลักคือ

ส่วนที่หนึ่งเป็นการวิเคราะห์ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ และการวางมาตรการป้องกันภัยพิบัติ

ส่วนที่สองเป็นแผนแก้ไขปัญหาเมื่อเกิดความเสียหายจากภัยพิบัติ (Contingency Plan) ซึ่งประกอบด้วย 2 ส่วนย่อยคือ

1) วิธีปฏิบัติเมื่อเกิดเหตุ (Emergency Action Plan) จะช่วยให้ผู้ปฏิบัติงานสามารถปฏิบัติได้อย่างถูกต้อง

2) แนวทางการฟื้นฟูระบบที่เสียหายจากภัยพิบัติ (Disaster Recovery Plan) จะกำหนดวิธีปฏิบัติและขั้นตอนในการกู้คืนระบบที่เสียหายให้สามารถกลับมาปฏิบัติงานหรือจัดหาระบบมาปฏิบัติงานทดแทนให้ได้มากที่สุดในระยะเวลาที่สั้นที่สุด

ซึ่งทั้งวิธีปฏิบัติเมื่อเกิดเหตุ และแนวทางการฟื้นฟูระบบที่เสียหายจากภัยพิบัติ จะช่วยให้การดำเนินงานด้านเทคโนโลยีสารสนเทศของหน่วยงานไม่หยุดชะงัก หรือชะงักเพียงระยะเวลาที่สั้นที่สุด และให้สามารถบรรเทาความเสียหายที่อาจจะเกิดขึ้นได้มากที่สุด

1.4 ผู้รับผิดชอบ

ทีมปฏิบัติการแก้ไขปัญหาจากสถานการณ์ ความไม่แน่นอนและภัยพิบัติของศูนย์เทคโนโลยีสารสนเทศ กรมอุตุนิยมวิทยา มีหน้าที่ความรับผิดชอบในการแก้ไขปัญหา ดังนี้

1.4.1 ระดับนโยบาย

- รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจน ติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

ผู้รับผิดชอบ ได้แก่ DCIO, ผู้อำนวยกองบริการดิจิทัลอุตุนิยมวิทยา, ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

1.4.2 ระดับปฏิบัติ

- รับผิดชอบ กำกับดูแล การปฏิบัติงานของผู้ปฏิบัติ ศึกษา ทบทวน วางแผน ติดตาม การบริหารความเสี่ยง และระบบรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศและฐานข้อมูล

ผู้รับผิดชอบ คือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

- รับผิดชอบดูแล บำรุงรักษา ระบบเครื่องคอมพิวเตอร์ ระบบเครือข่ายและความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไข ข้อบกพร่องต่างๆ ของระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งการทำสำเนาแฟ้มข้อมูลและฐานข้อมูล

ผู้รับผิดชอบ คือ นักวิชาการคอมพิวเตอร์และนายช่างไฟฟ้า ในศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายหน้าที่

- รับผิดชอบในการรักษาความปลอดภัยของแต่ละระบบฐานข้อมูล

ผู้รับผิดชอบ คือ นักวิชาการคอมพิวเตอร์และนายช่างไฟฟ้า ในศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายหน้าที่

- รับผิดชอบความปลอดภัยทั่วไป

ผู้รับผิดชอบ คือ นายช่างไฟฟ้า ในศูนย์เทคโนโลยีสารสนเทศที่ได้รับมอบหมายหน้าที่

1.5 สมมติฐานและเหตุการณ์ภัยพิบัติ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ครอบคลุมเฉพาะเหตุการณ์ ดังต่อไปนี้

1.5.1 การแก้ไขความล้มเหลวของระบบคอมพิวเตอร์ เนื่องจากระบบไฟฟ้าขัดข้อง

1.5.2 การแก้ไขปัญหาเนื่องจากระบบเครือข่ายสื่อสารไม่สามารถใช้งานได้

1.5.3 การแก้ไขปัญหาเนื่องจากเครื่องคอมพิวเตอร์ขัดข้อง หรืออุปกรณ์ประกอบอื่นๆ ชำรุด

1.5.4 การแก้ไขปัญหาเนื่องจากเพลิงไหม้

1.5.5 การแก้ไขปัญหาเนื่องจากการภัยคุกคามทางเทคโนโลยีสารสนเทศ เช่น การเจาะระบบ

1.6 ข้อจำกัดของแผน

1.6.1 แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ ให้ความสำคัญกับทีมปฏิบัติการแก้ปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ดังนั้น การแก้ไขปัญหาจากสถานการณ์ดังกล่าวจะต้องมีบุคลากรพร้อมเพรียงในการปฏิบัติงาน จึงจะมีประสิทธิภาพและประสิทธิผล

1.6.2 กรณีเกิดเหตุนอกเวลาราชการ การจัดการแก้ไขปัญหาอาจจะไม่บรรลุตามระยะเวลาที่กำหนดไว้ เพราะมีเจ้าหน้าที่เข้าเวรปฏิบัติราชการเพียง 2 คน และอาจไม่สามารถกู้คืนระบบได้ เพราะขาดความชำนาญในการปฏิบัติทางเทคนิคต่างๆ

1.6.3 บุคคลากรในทีมย่อยมีจำนวนจำกัด อาจต้องใช้บุคลากรทีมอื่นร่วมปฏิบัติงานด้วย

บทที่ 2
ความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

2.1 การบริหารความเสี่ยง

1) เพื่อเป็นเครื่องมือในการสร้างองค์ความรู้ด้านบริหารความเสี่ยง

2) ผู้ปฏิบัติงาน เข้าใจหลักการ แนวคิด วิธีการ และกระบวนการบริหาร ความเสี่ยง

3) เพื่อให้ผู้ปฏิบัติงานรับทราบขั้นตอน กระบวนการ และสามารถวางแผนบริหารความเสี่ยงขององค์กร

4) เพื่อเป็นเครื่องมือในการสื่อสารและสร้างความเข้าใจ ความสัมพันธ์ ตลอดจนเชื่อมโยงการบริหารความเสี่ยงกับกลยุทธ์ขององค์กร

5) เพื่อเป็นเครื่องมือช่วยในการปลูกฝังวัฒนธรรมองค์กรที่มุ่งเน้นการสร้างองค์ความรู้ ด้านการบริหารความเสี่ยงไปยังผู้บริหารและบุคลากรทุกระดับ

2.2 การพิจารณาความเสี่ยง

การพิจารณาความเสี่ยง หลังจากประเมินความเป็นไปได้ขอโอกาสที่จะเกิด Likelihood Score และผลกระทบ (ความรุนแรง) (Impact Score) ของปัจจัยเสี่ยงต่าง ๆ โดยนำความเสี่ยงที่ระบุไว้แล้วทั้งหมดมาพิจารณาประเมินระดับความรุนแรงของผลกระทบ (Impact) จากความเสี่ยงนั้น โดยแบ่งออกเป็น 3 ระดับ และมีเกณฑ์ในการประเมินความรุนแรงของผลกระทบดังนี้

ตารางที่ 1 ประเมินระดับความรุนแรงของผลกระทบ

ระดับของผลกระทบ	รายละเอียด
มาก (3)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ ขาดความต่อเนื่องในการให้บริการมากกว่า 1 ชั่วโมง ส่งผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการทั้งภายในและภายนอกองค์กร
ปานกลาง (2)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการหยุดชะงักชั่วคราวเป็นระยะเวลาไม่เกิน 30 นาที – 1 ชั่วโมง ไม่มีผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการ
น้อย (1)	มีผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ การให้บริการหยุดชะงักชั่วคราวเป็นระยะเวลา 15 - 30 นาที ไม่มีผลกระทบต่อภาพลักษณ์ ความเชื่อมั่นของผู้ใช้บริการ

ประเมินโอกาสในการเกิดภัยคุกคาม หรือ ความเสี่ยง (Likelihood) โดยแบ่งโอกาสมากน้อยตามจำนวนครั้งของการเกิดภัยคุกคาม หรือความเสี่ยงนั้น โดยระดับความเสี่ยงแบ่งออกเป็น 3 ระดับ ดังนี้

ตารางที่ 2 ระดับโอกาสในเกิดภัยคุกคาม

ระดับโอกาสเกิดเหตุการณ์	ความหมาย
มาก (3)	มีโอกาสเกิดเหตุการณ์ > 6 ครั้ง ภายในระยะเวลา 1 ปี
ปานกลาง (2)	มีโอกาสเกิดเหตุการณ์ระหว่าง 1 – 6 ครั้ง ภายในระยะเวลา 1 ปี
น้อย (1)	มีโอกาสเกิดเหตุการณ์ไม่เกิน 1 ครั้ง ภายในระยะเวลา 1 ปี

คำนวณหาระดับความเสี่ยง โดยใช้ข้อมูลของระดับผลกระทบ (Impact) คูณกับระดับโอกาสของการเกิดเหตุการณ์ที่จะเกิด ดังนี้

ระดับความเสี่ยง = ระดับผลกระทบ x ระดับโอกาสการเกิด

Risk Level (impact) (Likelihood)

ระดับความเสี่ยง (Risk Level) สามารถแบ่งได้ตามผลการคูณผลกระทบ และ โอกาสเกิดได้ตามแผนภาพดังนี้

ตารางที่ 3 คำนวณระดับความเสี่ยงจากโอกาสที่จะเกิดและผลกระทบ

ระดับค่าความเสี่ยง (Risk Level)		โอกาสที่จะเกิด (Likelihood Rating)		
		1	2	3
ผลกระทบ (Impact Rating)	3	3x1=3	3x2=6	3x3=9
	2	2x1=2	2x2=4	2x3=6
	1	1x1=1	1x2=2	1x3=3

ตารางที่ 4 แนวทางการจัดการความเสี่ยง

คะแนนความเสี่ยง	ระดับความเสี่ยง	แนวทางการจัดการความเสี่ยง
1-2	ความเสี่ยงต่ำ **Low**	1) ยอมรับความเสี่ยง Risk Accept 2) เฝ้าระวังความเสี่ยง Risk Monitor
3-4	ความเสี่ยงปานกลาง **Medium**	1) กำหนดมาตรการเพื่อควบคุมความเสี่ยง Risk Controlling 2) ถ่ายโอนความเสี่ยง Risk Transferring
6-9	ความเสี่ยงสูง **High**	1) วางแผนเพื่อกำจัด Risk Avoid หรือลดความเสี่ยง Risk Reduce โดยจัดทำในแผนการจัดการความเสี่ยง (Risk Treatment Plan) 2) จัดทำแผนต่อเนื่องทางธุรกิจ BCP

ความเสี่ยงจากสาเหตุต่าง ๆ ที่อาจก่อให้เกิดความเสียหายแก่ระบบเทคโนโลยีสารสนเทศ มีมากมาย แต่ความเสี่ยงที่ได้กำหนดไว้สำหรับศูนย์เทคโนโลยีสารสนเทศ ความเสี่ยงที่ครอบคลุมด้านต่าง ๆ มีดังนี้

2.3.1 ความเสี่ยงด้านสิ่งแวดล้อม หมายถึง ความเสี่ยงหรือความเสียหายอันเนื่องมาจากการเปลี่ยนแปลงต่อสภาพแวดล้อมทั้งภายในและภายนอกองค์กร ได้แก่

- อัคคีภัย
- น้ำท่วม
- แผ่นดินไหว สึนามิ
- อากาศร้าย เช่น พายุ ลมแรง ฟ้าผ่า ฯลฯ
- ฝุ่น ควัน
- สัตว์ เช่น หนู แมลง ฯลฯ
- น้ำจากการรั่วซึม เช่น ท่อน้ำ หลังคารั่ว ระบบทำความเย็นรั่วซึม ฯลฯ
- การสั่นสะเทือน เช่น รถบรรทุก เครื่องบิน ฯลฯ
- การรบกวนจากคลื่นแม่เหล็กไฟฟ้า
- โรคระบาด

2.3.2 ความเสี่ยงระบบสนับสนุน หมายถึง ความเสี่ยงหรือความเสียหายอันเนื่องมาจากการระบบที่เกี่ยวข้องต่างๆ โดยรอบทั้งทางตรง และ ทางอ้อม ได้แก่

- ระบบไฟฟ้าขัดข้อง ไฟฟ้าดับ

- ระบบปรับอากาศขัดข้อง
- ระบบสื่อสารขัดข้อง
- ระบบเครือข่ายสาธารณ(อินเตอร์เน็ต) ใช้การไม่ได้
- การกระทำของบุคคล ได้แก่ การติดตั้งอุปกรณ์หรือโปรแกรม ไม่เหมาะสม ไม่ได้มาตรฐาน
- การบำรุงรักษาระบบไม่ถูกต้องตามหลักการ
- การขาดอัตรากำลังบุคลากรเพื่อปฏิบัติงานดูแลระบบ

2.3.3 ความเสี่ยงด้านการปฏิบัติงาน หมายถึง ความเสี่ยงที่เกิดจากการการดำเนินการในการปฏิบัติงานของบุคลากร ซึ่งส่งผลต่อการปฏิบัติงานต่าง ๆ ทำให้ไม่บรรลุวัตถุประสงค์เป้าหมายที่กำหนด และเกิดความเสียหายขึ้น ได้แก่

- การขนส่ง เคลื่อนย้าย อุปกรณ์ที่ไม่เหมาะสม เช่น ตกหล่น กระแทก ฯลฯ
- จากอุบัติเหตุ หรือความประมาท
- การเข้าใช้ระบบโดยไม่ได้รับอนุญาต
- การโจรกรรมอุปกรณ์ หรือจารกรรมข้อมูล
- การขู่เข็ญบังคับเอาข้อมูลความลับ
- การก่อวินาศกรรมกับฮาร์ดแวร์และซอฟท์แวร์
- การก่อวินาศกรรม จลาจล สงคราม การปิดล้อมของผู้ชุมนุมหรือผู้ไม่ประสงค์ดี

2.3.4 ความเสี่ยงจากภัยทางไซเบอร์ หมายถึง ความเสี่ยงที่เกิดจากผลกระทบจากการหยุดชะงักต่อการให้บริการ จากการละเมิดข้อมูล การขโมยข้อมูล หรือการทำลายข้อมูล เพื่อให้ไม่สามารถให้บริการได้ ตัวอย่างของความเสี่ยงทางไซเบอร์ ได้แก่

- Ransomware (แรนซัมแวร์) โจมตีข้อมูล ไฟล์ และเอกสารภายในระบบสารสนเทศของเป้าหมายโดยวิธีการเข้ารหัสข้อมูลด้วยวิธีการต่าง ๆ เช่น การเข้ารหัสด้วย Advanced Encryption Standard (AES) ซึ่งเป็นหนึ่งในมาตรฐานการเข้ารหัสที่ได้รับความเชื่อถือในอุตสาหกรรมและองค์กรต่าง ๆ ที่ต้องการสร้างความมั่นใจและความปลอดภัยของข้อมูลเพื่อไม่ให้ผู้อื่นสามารถล่วงรู้ความลับของข้อมูลได้ ด้วยเหตุนี้จึงทำให้ผู้ไม่หวังดีได้มีการพัฒนามัลแวร์ได้มีการเอาประโยชน์ของการเข้ารหัสนี้มาใช้ประโยชน์ด้วยการเข้ารหัสข้อมูลของเป้าหมายทำให้ไม่สามารถเข้าใช้ข้อมูลได้จนกว่าจะจ่ายค่าไถ่ข้อมูลให้กับผู้พัฒนา Ransomware
- Malware (มัลแวร์) หรือ Malicious Software (ซอฟต์แวร์อันตราย) คือซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี เพื่อขโมยข้อมูลและสร้างความเสียหายให้กับระบบคอมพิวเตอร์ โดยมัลแวร์นั้นได้แบ่งออกเป็นหลายประเภท เช่น Virus (ไวรัส) worms (เวิร์ม) Trojan (โทรจัน) Spyware (สปายแวร์) Adware (แอดแวร์)

ระบุความเสี่ยงทั้งหมด ดังนี้

ตารางที่ 5 การประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>1. อัคคีภัย</td><td>อัคคีภัยจากอุบัติเหตุไฟฟ้า ไฟฟ้าลัดวงจร</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>2. น้ำท่วม</td><td>กรณีน้ำท่วมจะส่งผลกระทบต่อระบบไฟฟ้า และ ระบบไฟฟ้าสำรองซึ่งติดตั้งอยู่ที่ชั้น 1</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>3. แผ่นดินไหว</td><td>กรณีเกิดภัยพิบัติ ทำให้อาคารเสียหาย อาคารแตกร้าว ฝนตกทำให้น้ำฝนรั่วเข้าภายในอาคาร</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (□)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>4. โรคระบาด</td><td>การปฏิบัติงาน ของบุคลากรไม่ได้ประสิทธิภาพ มีผลกระทบทางด้านสุขภาพ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>5. อากาศร้าย เช่น ฟ้าผ่า ฯ</td><td>กรณีฟ้าฝ่า ทำให้อุปกรณ์เสียหาย</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>6. ฝุ่น ควัน</td><td>ฝุ่น ควัน มีผลต่อการตรวจจับของอุปกรณ์ตรวจจับควัน</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง(3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>7. สัตว์ เช่น หนู แมลง ฯลฯ</td><td>หนูกัดสายไฟฟ้า สายสัญญาต่างๆ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
<tr><td>8. น้ำจากการรั่วซึม</td><td>ท่อน้ำ หลังคารั่ว
ระบบทำความเย็นรั่วซึม ฯ
น้ำหยด</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table>
<tr><th></th><th colspan="3">ผลกระทบ</th></tr>
<tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr>
<tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr>
<tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr>
<tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr>
</table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>9. การสั่นสะเทือน เช่น รถบรรทุก เครื่องบิน ฯลฯ</td><td>การสั่นสะเทือนมีผลต่อกระจกและรอยร้าวของอาคาร</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>10. การรบกวนจากคลื่นแม่เหล็กไฟฟ้า</td><td>การส่งผลกระทบต่อระบบอิเล็กทรอนิกส์ อุปกรณ์การควบคุมบางอย่างทำงานผิดพลาด</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td></td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>11. ระบบไฟฟ้าขัดข้อง ไฟฟ้าดับ</td><td>การจ่ายไฟฟ้า ของการไฟฟ้านครหลวงเกิดปัญหา ไฟฟ้าดับ หม้อแปลงระเบิด
กรณีกระรอก ถูกไฟฟ้าช็อตทำให้ไฟฟ้าลัดวงจร
ความผิดพลาดของอุปกรณ์สำรองไฟฟ้า หรือ ระบบ Power Supply</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>12. ระบบปรับอากาศขัดข้อง</td><td>ระบบปรับอากาศ บำรุงรักษาอย่างต่อเนื่อง บางครั้งเกิดกรณีพัดลมคอมเพสเซอร์เกิดการร้อนแล้วช็อต ทำให้เกิดปัญหาอุปกรณ์ต่าง ๆ เสื่อมสภาพทำให้ต้องตรวจสอบอยู่เสมอ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>13. ระบบสื่อสารขัดข้อง</td><td>การขัดข้องของ อุปกรณ์ เดินสายระหว่างตึก</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>14. ระบบเครือข่ายสาธารณะ (อินเตอร์เน็ต) ใช้การไม่ได้</td><td>ระบบเครือข่ายสาธารณะ (อินเตอร์เน็ต) ซึ่งใช้บริการจากหน่วยงานภายนอก กรณีสายไฟเบอร์สื่อสารข้อมูล ขัดข้อง</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>15. การติดตั้งอุปกรณ์หรือโปรแกรม ไม่เหมาะสม ไม่ได้มาตรฐาน</td><td>การกระทำของบุคคล เช่น การติดตั้งอุปกรณ์หรือโปรแกรมไม่เหมาะสม ไม่ได้มาตรฐาน</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (1)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>16. การบำรุงรักษาระบบไม่ถูกต้องตามหลักการ</td><td>ขาดงบประมาณในการบำรุงรักษา ฯ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>17. การขาดอัตรากำลังบุคลากรเพื่อปฏิบัติงานดูแลระบบ</td><td>ขาดบุคลากรที่ปฏิบัติงานเพื่อตรวจสอบสภาพแวดล้อมต่าง ๆ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>18. การขนส่ง เคลื่อนย้าย อุปกรณ์ที่ไม่เหมาะสม</td><td>การขนส่ง เคลื่อนย้าย ตกหล่น กระแทก ฯลฯ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>19. อุบัติเหตุ หรือความประมาท</td><td>ความประมาทในการปฏิบัติงาน เช่น ทางด้านไฟฟ้า ทางด้านการติดตั้ง</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>20. การเข้าใช้ระบบโดยไม่ได้รับอนุญาต</td><td>การลักลอบเข้าระบบโดยไม่ได้รับอนุญาต</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>21. การโจรกรรมอุปกรณ์ หรือจารกรรมข้อมูล</td><td>การขโมยของ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>22. การขู่เข็ญบังคับเอาข้อมูลความลับ</td><td>หลอกให้เหยื่อ ปลอมตัวเป็นผู้อื่นที่มีความสำคัญมาก ๆ เช่น ผู้บริหาร
เสนอผลตอบแทนเพื่อสร้างแรงจูงใจ</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>23. การก่อวินาศกรรมกับฮาร์ดแวร์และซอฟท์แวร์</td><td>แฮ็กเกอร์
การโจมตีการให้บริการ
การดักจับข้อมูล
คำสั่งเจตนาร้าย
ความผิดพลาดของ Software
ไวรัส/เวิร์ม</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>24. การก่อวินาศกรรม จลาจล การปิดล้อม</td><td>การก่อวินาศกรรม การปิดล้อมของผู้ชุมนุมหรือผู้ไม่ประสงค์ดี</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
</table>

<table>
<tr><th>ความเสี่ยงด้านเทคโนโลยีสารสนเทศกิจกรรม/ความเสี่ยง</th><th>ลักษณะความเสี่ยง</th><th>ผลกระทบ/
ผู้ได้รับลกระทบ</th></tr>
<tr><td>25. Ransomware (แรนซัมแวร์)</td><td>เครื่องคอมพิวเตอร์ติดมัลแวร์ เรียกค่าไถ่ ไม่สามารถเข้าถึงไฟล์ได้</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
<tr><td>26. Malware มัลแวร์ อื่น ๆ</td><td>เครื่องคอมพิวเตอร์ติด มัลแวร์ Malicious Software ซอฟต์แวร์ ซอฟต์แวร์ที่พัฒนาโดยผู้ไม่หวังดี</td><td>โอกาสเกิด ปานกลาง x ผลกระทบ สูง
<table><tr><th></th><th colspan="3">ผลกระทบ</th></tr><tr><th>โอกาสเกิด</th><th>ต่ำ (1)</th><th>กลาง (2)</th><th>สูง (3)</th></tr><tr><td>สูง (3)</td><td>3</td><td>6</td><td>9</td></tr><tr><td>กลาง (2)</td><td>2</td><td>4</td><td>6</td></tr><tr><td>ต่ำ (1)</td><td>1</td><td>2</td><td>3</td></tr></table></td></tr>
</table>

2.4 สรุปผลการประเมินความเสี่ยง

ภัยจากสาเหตุต่างๆ มีโอกาสเกิดขึ้นไม่เท่ากัน และผลกระทบเมื่อเกิดขึ้นก่อให้เกิดความเสียหาย ที่รุนแรงแตกต่างกัน จากการประเมินที่ตั้ง สิ่งแวดล้อม อาคาร การติดตั้งอุปกรณ์ และการปฏิบัติงานของศูนย์เทคโนโลยีสารสนเทศ และระบบสารสนเทศในความรับผิดชอบ ผลการประเมินความเสี่ยงสรุปได้ ดังนี้

ตารางที่ 6 สรุปผลความเสี่ยงของระบบเทคโนโลยีสารสนเทศ

ชนิดของความเสี่ยง	โอกาสเกิด	ผลกระทบ	ระดับความสำคัญ
สิ่งแวดล้อม			
1. อัคคีภัย	ปานกลาง	สูง	สูง
2. น้ำท่วม	ต่ำ	สูง	ปานกลาง
3. แผ่นดินไหว	ต่ำ	สูง	ปานกลาง
4. โรคระบาด	ปานกลาง	ปานกลาง	ปานกลาง
5. อากาศร้าย	ปานกลาง	ต่ำ	ปานกลาง
6. ฝุ่น ควัน	ต่ำ	ต่ำ	ต่ำ
7. สัตว์ เช่น หนู แมลง	ต่ำ	ต่ำ	ต่ำ
8. น้ำจากการรั่วซึม	ต่ำ	ปานกลาง	ต่ำ
9. การสั่นสะเทือน เช่น รถบรรทุก เครื่องบิน	ต่ำ	ต่ำ	ต่ำ
10. การรบกวนจากคลื่นแม่เหล็กไฟฟ้า	ต่ำ	ปานกลาง	ต่ำ
ระบบสนับสนุน			
11. ระบบไฟฟ้าขัดข้อง ไฟฟ้าดับ	ปานกลาง	สูง	สูง
12. ระบบปรับอากาศขัดข้อง	ปานกลาง	สูง	สูง
13. ระบบสื่อสารขัดข้อง	ต่ำ	สูง	ปานกลาง
14. ระบบอินเตอร์เน็ตใช้การไม่ได้	ปานกลาง	สูง	สูง
การกระทำของบุคคล			
15. การติดตั้งอุปกรณ์หรือโปรแกรม ไม่เหมาะสม ไม่ได้มาตรฐาน	ต่ำ	สูง	ปานกลาง
16. การบำรุงรักษาระบบไม่ถูกต้องตามหลักการ	ต่ำ	ปานกลาง	ต่ำ
17. การขาดอัตรากำลังบุคลากรที่ดูแลระบบ	ปานกลาง	ปานกลาง	ปานกลาง
18. การขนส่ง เคลื่อนย้าย อุปกรณ์ที่ไม่เหมาะสม	ต่ำ	ปานกลาง	ต่ำ

ชนิดของความเสี่ยง	โอกาสเกิด	ผลกระทบ	ระดับความสำคัญ
19. อุบัติเหตุ หรือความประมาท	ต่ำ	ปานกลาง	ต่ำ
20. การเข้าใช้ระบบโดยไม่ได้รับอนุญาต	ต่ำ	ปานกลาง	ต่ำ
21. การโจรกรรมอุปกรณ์หรือจารกรรมข้อมูล	ต่ำ	สูง	ปานกลาง
22. การขู่เข็ญบังคับเอาข้อมูลความลับ	ต่ำ	สูง	ปานกลาง
23. การก่อวินาศกรรมกับฮาร์ดแวร์และซอฟท์แวร์	ต่ำ	สูง	ปานกลาง
24. การก่อวินาศกรรม จลาจล การปิดล้อม	ต่ำ	สูง	ปานกลาง
ความเสี่ยงจากภัยทางไซเบอร์			
25. Ransomware (แรนซัมแวร์)	ต่ำ	สูง	ปานกลาง
26. Malware มัลแวร์	ต่ำ	ปานกลาง	ต่ำ

ผลการประเมินความเสี่ยงนี้ จะถูกนำไปใช้ในการพิจารณาวางแผน กำหนดมาตรการจัดการป้องกัน และแก้ไขปัญหาจากภัยพิบัติต่าง ๆ ตามความเหมาะสม ในขั้นตอนต่อไป

บทที่ 3
มาตรการป้องกันภัยพิบัติ

3.1 ข้อปฏิบัติเพื่อหลีกเลี่ยงหรือลดความเสี่ยงในการเกิดภัยพิบัติ

3.3.1 มีการกำหนดแนวนโยบายแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศ

3.3.2 มีการมอบหมายหน้าที่ในการรักษาความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศให้ผู้รับผิดชอบทราบและถือปฏิบัติ

3.3.3 มีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) โดยแสดงขั้นตอนที่เกี่ยวข้องทั้งหมดในการแก้ไขปัญหาที่เกิดขึ้น

3.3.4 มี Site สำรอง ในกรณี Site หลักใช้งานไม่ได้ โดยติดตั้งไว้ที่ อาคาร 50 ปีอุตุนิยมวิทยา ชั้น 9

3.3.5 มีการเก็บข้อมูลสำรองไว้ต่างพื้นที่ โดยส่งข้อมูลสำรองไปเก็บที่ศูนย์อุตุนิยมวิทยาภาคเหนือ จังหวัดเชียงใหม่

3.3.6 มีการกำหนด ทบทวน แผนการรักษาความปลอดภัยเป็นประจำทุกปี

3.3.7 มีการฝึกซ้อมแผนการรักษาความปลอดภัยเป็นประจำ

3.4 ข้อปฏิบัติขณะเกิดเหตุการณ์ภัยพิบัติ

3.4.1 ประสานงานแจ้งผู้บริหารและรวมทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติทันทีที่เกิดเหตุการณ์ภัยพิบัติ

3.4.2 ทีมจัดการทั่วไปหรือผู้ที่รับทราบเหตุการณ์ จะต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ จากนั้นจะมีการรวมตัวกันของทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติเพื่อปฏิบัติตามแผนฯ ที่ได้กำหนดไว้

3.4.3 ปฏิบัติการป้องกันอุปกรณ์คอมพิวเตอร์และระบบสารสนเทศสำคัญ

3.4.4 ในระหว่างการเกิดเหตุการณ์ภัยพิบัติ ทีมแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติจะต้องขนย้ายอุปกรณ์คอมพิวเตอร์ที่สำคัญ ซึ่งรวมถึงฐานข้อมูลและแฟ้มข้อมูลที่สำรองไว้มายังสถานที่ปลอดภัยตามขั้นตอนที่ได้ระบุไว้

3.5 ข้อปฏิบัติหลังเกิดเหตุการณ์ภัยพิบัติ

3.5.1 ประเมินความเสียหายและกำหนดสถานที่สำหรับการกู้คืน

ภายหลังเหตุการณ์บรรเทาหรือสงบลงแล้ว ทีมประเมินความเสียหายระบบคอมพิวเตอร์และเครือข่าย ต้องดำเนินการสำรวจและประเมินความเสียหายของอุปกรณ์คอมพิวเตอร์และเครือข่าย รวมทั้งกำหนดระยะเวลาโดยประมาณในการแก้ไข ซ่อมแซม เพื่อให้กลับมาใช้งานได้ดังเดิม

(1) ในการประเมินความเสียหายของห้องคอมพิวเตอร์หลัก ให้ดำเนินการประเมินความเสียหายโดยทีม นักวิชาการคอมพิวเตอร์ เจ้าหน้าที่พัสดุ หรือ วิศวกรในสาขาที่เกี่ยวข้อง รวมทั้ง รปภ. เพื่อร่วมกันพิจารณาว่าห้องคอมพิวเตอร์หลักเกิดความเสียหายมากน้อยเพียงใด

(2) อุปกรณ์ที่ชำรุดแต่ยังใช้งานได้ อุปกรณ์ที่เสียหาย หรือสูญหาย จะต้องพิจารณาจัดหาตามความเหมาะสมและความจำเป็นเร่งด่วนต่อไป

(3) ให้นำผลการประเมินความเสียหาย ไปพิจารณา ประกอบการตัดสินใจว่าจะกลับมาใช้ Site หลักเมื่อใดหรือจะใช้ Site สำรองในการกู้คืนระบบทั้งหมด

3.5.2 การติดตั้งระบบที่ Site สำรอง

การติดตั้งระบบที่ Site สำรอง กรณีที่ Site หลักเสียหายจนไม่สามารถใช้งานได้ จะเริ่มต้นจากการใช้อุปกรณ์คอมพิวเตอร์ที่มีอยู่ใน Site สำรอง และอุปกรณ์ที่นำออกมาจาก Site หลักได้ ในการดำเนินการเพื่อให้ Site สำรอง สามารถใช้งานทดแทน Site หลักได้ จะต้องดำเนินการให้แล้วเสร็จภายใน 24 ชั่วโมง สำหรับระบบที่มีความสำคัญยิ่งยวด และให้แล้วเสร็จภายใน 3 วัน สำหรับระบบที่เร่งด่วน หรือ ไม่ส่งผลกระทบในวงกว้าง และต้องประสานงานกับผู้เกี่ยวข้องทั้งภายในและภายนอก ให้สามารถเข้าใช้งานจาก Site สำรอง ได้

3.6 การรักษาความปลอดภัยของอาคาร สถานที่

3.6.1 การควบคุมการเข้าออกศูนย์คอมพิวเตอร์

เนื่องจากศูนย์เทคโนโลยีสารสนเทศมีความเสี่ยงที่จะถูกบุกรุกจากบุคคลที่ไม่หวังดี และความสูญเสียที่จะเกิดจากการกระทำของผู้บุกรุกอาจมีความรุนแรงสูงจึงจำเป็นต้องมีระบบการควบคุมการเข้าออกอาคาร และห้องปฏิบัติงานต่างๆอย่างดี อาคารศูนย์เทคโนโลยีสารสนเทศ ห้องระบบคอมพิวเตอร์และเครือข่ายหลัก ห้องควบคุมระบบ ห้องปฏิบัติงานที่สำคัญต่างๆ มีการควบคุมการเข้าออกด้วยระบบบัตรอนุญาตอิเล็กทรอนิกส์ (Electronic Key Card) ซึ่งระบบสามารถให้สิทธิหรือยกเลิกสิทธิการเข้าออก ของแต่ละบุคคลว่าสามารถเข้าออกห้องใด ในช่วงเวลาใด และเก็บประวัติการเข้าออกอาคารและห้องต่าง ๆ ไว้

3.6.2 การป้องกันอัคคีภัย

อัคคีภัยแม้ว่าจะมีโอกาสเกิดไม่มาก แต่หากเกิดแล้วจะทำความเสียหายรุนแรงมากจึงต้องวางระบบป้องกันไว้เป็นอย่างดีโดยมีการติดตั้ง ระบบป้องกันเพลิงไหม้ ดังนี้

(1) ระบบเตือนไฟไหม้ (Fire Alarm System) ซึ่งมีอุปกรณ์ตรวจจับควันไฟในจุดที่สำคัญกระจายอยู่ทั่วอาคาร หากเกิดสงสัยว่าจะเกิดเพลิงไหม้ระบบจะส่งสัญญาณเสียง เตือนให้ได้ยินทั่วทั้งอาคารและบริเวณใกล้เคียง

(2) ถังดับเพลิงตามจุดติดตั้งบริเวณต่างๆ สามารถนำมาใช้ดับเพลิงได้หากเกิดเหตุ

(3) ระบบดับเพลิงอัตโนมัติ ซึ่งทำงานร่วมกับระบบเตือนไฟไหม้ หากอุปกรณ์ตรวจจับควันไฟยืนยันว่าเกิดไฟไหม้ หัวฉีดดับเพลิงที่ติดตั้งบนฝ้าเพดานก็จะฉีดสารเคมี (FM200) ลงมาดับไฟ โดยหัวฉีดนี้ติดตั้งในห้องคอมพิวเตอร์และเครือข่ายหลัก

3.6.3 การป้องกันไฟฟ้าขัดข้อง

ไฟฟ้าขัดข้องเป็นสาเหตุให้ระบบคอมพิวเตอร์หยุดทำงานก่อให้เกิดความเสียหายรุนแรงจึงจำเป็นต้องมีมาตรการป้องกันโดย

(1) มีเครื่องสำรองไฟฟ้า (UPS) ขนาดใหญ่ (125 KVA) 1 ชุด สำหรับสำรองไฟฟ้าให้กับระบบคอมพิวเตอร์ทั้งเครื่องแม่ข่ายระบบสารสนเทศต่าง ๆ และอุปกรณ์เครือข่ายหลัก รวมทั้งอุปกรณ์ประกอบอื่น ๆ ในห้องระบบคอมพิวเตอร์และเครือข่ายหลัก

(2) มีเครื่องสำรองไฟฟ้า (UPS) ขนาดเล็กสำหรับเครื่องคอมพิวเตอร์ และอุปกรณ์ที่มีความสำคัญ

(3) มีเครื่องกำเนิดไฟฟ้า (Generator) พร้อมน้ำมันสำรอง ซึ่งจะทำงานโดยอัตโนมัติเมื่อไฟฟ้าดับ เพื่อจ่ายกระแสไฟฟ้าให้กับระบบคอมพิวเตอร์ และอุปกรณ์ที่จำเป็นในศูนย์เทคโนโลยีสารสนเทศให้สามารถปฏิบัติงานได้ในกรณีไฟฟ้าดับได้ไม่น้อยกว่า 8 ชั่วโมง

3.6.4 การควบคุมอุณหภูมิและความชื้น

มีระบบปรับอากาศที่มีระบบควบคุมความชื้นสำหรับห้องระบบคอมพิวเตอร์และเครือข่ายหลัก 2 ชุด ทำงานสลับกัน ซึ่งเป็นระบบที่แยกจากระบบปรับอากาศรวมของอาคาร และมีไฟฟ้าจากเครื่องกำเนิดไฟฟ้าจ่ายให้ในกรณีไฟฟ้าดับด้วย

3.7 ระบบคอมพิวเตอร์และเครือข่าย

3.7.1 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย

(1) ให้ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย เฝ้าระวังภัยคุกคามทางเทคโนโลยีสารสนเทศที่อาจเกิดขึ้นกับเครื่องคอมพิวเตอร์แม่ข่ายอย่างต่อเนื่อง

(2) มีการกำหนดสิทธิให้เจ้าหน้าที่ในแต่ละระดับให้สามารถใช้งานเครื่องคอมพิวเตอร์แม่ข่ายได้ตามหน้าที่ความรับผิดชอบ และเจ้าหน้าที่จะต้องทำการใส่บัญชีผู้ใช้ (User name) และรหัสผ่าน (Password) ในการ Log in เข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และจะต้อง Log out ออกทันทีที่เลิกใช้งาน หากลืมระบบจะ Log out โดยอัตโนมัติหากไม่มีการใช้งานในระยะเวลาที่กำหนด

(3) มีการบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์โดยจ้างบริษัทเอกชนดำเนินการ และเจ้าหน้าที่ของกรมฯ ตรวจสอบเป็นประจำตามกำหนดเวลา

(4) มีการทำ Backup ของระบบสารสนเทศ โปรแกรมระบบ ฐานข้อมูลและแฟ้มข้อมูล บนเครื่องแม่ข่ายระบบสารสนเทศทุกเครื่อง

(5) ห้ามบุคคลผู้ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องระบบคอมพิวเตอร์และเครือข่ายหลัก รวมทั้งห้องที่มีความสำคัญอื่นๆ หากจำเป็น ให้มีเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ รับผิดชอบในการนำเข้าไปและเฝ้าติดตามตลอดเวลา

3.7.2 การรักษาความปลอดภัยระบบเครือข่าย และคอมพิวเตอร์ลูกข่าย

(1) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้าสู่ระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์ ทั้งเครื่องคอมพิวเตอร์แม่ข่าย และคอมพิวเตอร์ลูกข่ายได้

(2) มีระบบให้บริการเครือข่ายไร้สายสำหรับบุคคลภายนอก โดยอนุญาตให้ใช้งานชั่วคราวด้วยการลงทะเบียนและขอรับรหัสผ่านที่กลุ่มงานประชาสัมพันธ์

(3) ทำการตรวจสอบข้อมูลการจราจรบนเครือข่ายอินเตอร์เน็ตขององค์กรอย่างสม่ำเสมอ เพื่อค้นหาสิ่งผิดปกติที่อาจเกิดจากการโจมตี บุกรุก

(4) ติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ ที่เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายทุกเครื่อง และมีการปรับปรุง virus signatures/definitions ให้เป็นปัจจุบันอย่างสม่ำเสมอ โดยเครื่องคอมพิวเตอร์ลูกข่ายสามารถ update ได้โดยอัตโนมัติจาก Antivirus Server ของกรม

(5) มีกำหนดระเบียบวิธีปฏิบัติในการใช้คอมพิวเตอร์แม่ข่าย คอมพิวเตอร์ส่วนบุคคล และเครือข่ายให้ผู้ใช้ทราบทั่วกัน

(6) มีการบำรุงรักษาเครื่องคอมพิวเตอร์ และอุปกรณ์คอมพิวเตอร์โดยจ้างบริษัทเอกชนดำเนินการ และมีเจ้าหน้าที่ที่ดูแล และช่วยแก้ไขปัญหาต่าง ๆ

3.8 ระบบสารสนเทศและข้อมูล

(1) มีการสำรองข้อมูล (Backup) ในแฟ้มข้อมูลและฐานข้อมูลตามกำหนดเวลาลงสื่อเก็บหลายชนิด เช่น เทป ฮาร์ดดิสก์ Optical Disk รวมทั้งมีการทำ Online backup สำหรับข้อมูลสำคัญที่ใช้งานประจำ

(2) มีการทดสอบการกู้คืนข้อมูลจากข้อมูลที่ Backup ไว้

(3) มีการกำหนดสิทธิสำหรับผู้ใช้ข้อมูลให้เข้าถึงข้อมูลใดได้บ้าง และสามารถ เพิ่มเติม แก้ไข ลบ ข้อมูลได้หรือไม่

3.9 การสำรองและกู้คืนข้อมูลและระบบสารสนเทศ

3.9.1 มาตรการดำเนินงาน

การสำรองข้อมูลจะต้องดำเนินการตามมาตรการที่กำหนดต่อไปนี้

(1) ข้อมูลและซอฟต์แวร์ที่เกี่ยวข้องของระบบงานแต่ละระบบ จะต้องถูกสำเนาอย่างครบถ้วนและเป็นระบบ เพื่อให้แน่ใจว่าข้อมูลที่มีการเพิ่มเติม แก้ไข เปลี่ยนแปลง จะถูกทำสำเนาไว้ครบถ้วน

(2) มีการบันทึกรายละเอียดการสำรองข้อมูล เช่น ชนิดข้อมูล ชื่อผู้บันทึก วันเวลา ฯลฯ

(3) สื่อที่ใช้ในการบันทึกข้อมูล เช่น เทป หรือแผ่น Optical Disk จะต้องมีฉลากติดที่ระบุรายละเอียดข้อมูลในสื่อนั้น ชนิดของข้อมูล ข้อมูลเป็นของระบบงานใด วันที่ทำการบันทึกไว้ อย่างชัดเจน

(4) ข้อมูลสำรองจะต้องจัดเก็บในสถานที่ที่มีความปลอดภัย

(5) จะต้องมีการทดสอบเป็นประจำว่า ข้อมูลที่สำรองสามารถนำกลับมาใช้ได้

3.9.2 ชนิดและความถี่ในการสำรองข้อมูล

การสำรองข้อมูลของศูนย์เทคโนโลยีสารสนเทศ กรมอุตุนิยมวิทยา จะต้องทำการสำรองข้อมูลของระบบต่าง ๆ เป็นประจำอย่างเคร่งครัดตามชนิดและความถี่ที่แสดงตาม ภาคผนวก 1

3.9.3 วิธีการปฏิบัติงาน

ให้ปฏิบัติตามแผนปฏิบัติการสำรองข้อมูลของศูนย์เทคโนโลยีสารสนเทศ กรมอุตุนิยมวิทยา และให้เป็นไปตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมอุตุนิยมวิทยา

บทที่ 4
การแก้ไขปัญหาจากภัยพิบัติ

ในกรณีที่เกิดเหตุ ศูนย์เทคโนโลยีสารสนเทศได้มีแผนปฏิบัติการในการแก้ไขปัญหาแยกตามเหตุการณ์ดังนี้

4.1 การแก้ไขปัญหาเนื่องจากระบบไฟฟ้าขัดข้อง

เนื่องจากเครื่องคอมพิวเตอร์ และอุปกรณ์เครือข่ายคอมพิวเตอร์ส่วนใหญ่ต้องการกระแสไฟฟ้าที่เรียบ สม่ำเสมอ ดังนั้นสิ่งที่มักจะเกิดขึ้นและยากที่จะหลีกเลี่ยงได้ก็คือ ผลกระทบต่างๆ ที่เกิดขึ้นจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ การสูญหายของข้อมูลที่สำคัญ ระบบไม่สามารถใช้งานได้ตามปกติ จึงได้กำหนดหลักการปฏิบัติไว้ดังนี้

4.1.1 การปฏิบัติเมื่อเกิดเหตุ

(1) เมื่อเกิดกระแสไฟฟ้าดับหากสาเหตุมาจากระบบสายส่งของการไฟฟ้านครหลวงให้เจ้าหน้าที่ที่รับผิดชอบแจ้งการไฟฟ้านครหลวงทันที

(2) หากไฟฟ้าดับจากสาเหตุอื่น เช่น ขัดข้องที่ตู้จ่ายไฟ หรือเครื่องสำรองไฟฟ้า (UPS) ให้เจ้าหน้าที่ที่รับผิดชอบตรวจสอบตามขั้นตอนที่ระบุไว้ในแต่ละจุด และแจ้งบริษัทที่รับบำรุงรักษาให้แก้ไขทันที (ถ้ามี) และถ้าไม่มีการจ้างเหมาบำรุงรักษาให้แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และดำเนินการแจ้งซ่อมแซมโดยเร็ว

(3) ตรวจสอบการทำงานของเครื่องกำเนิดไฟฟ้าและระดับน้ำมันเชื้อเพลิงให้อยู่ในสภาพพร้อมใช้งานไม่น้อยกว่า 12 ชั่วโมง

(4) ในกรณีเครื่องกำเนิดไฟฟ้าไม่ทำงาน ให้ตรวจสอบและประมาณการเวลาที่เครื่องสำรองไฟฟ้าสามารถจ่ายไฟให้กับอุปกรณ์พร้อมแจ้งผู้รับผิดชอบทราบทันที

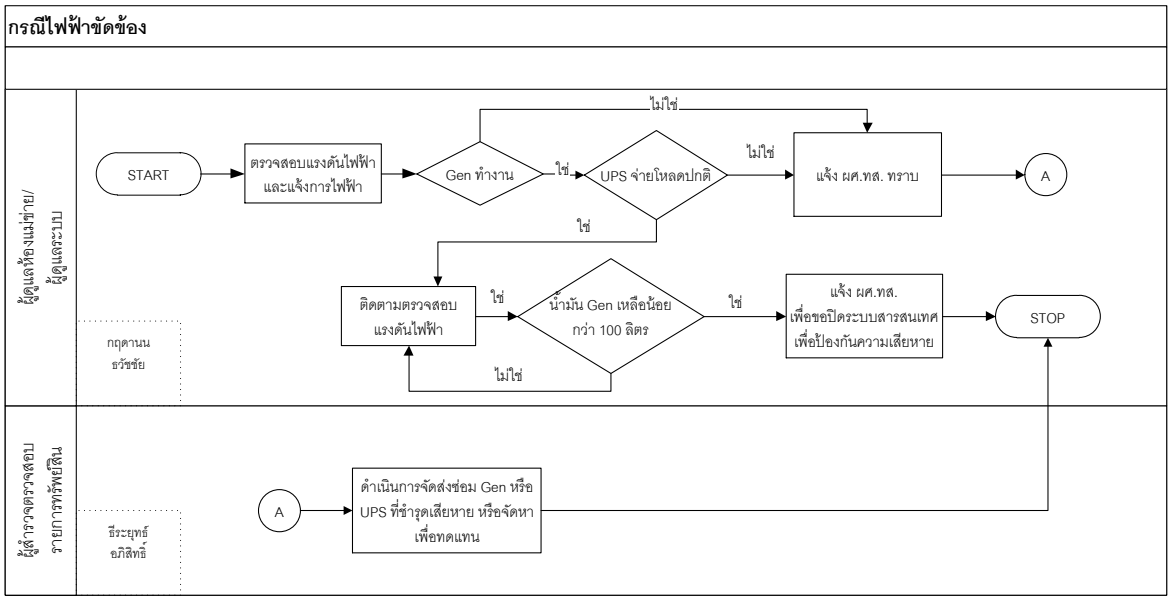
(5) ลดปริมาณการใช้ไฟฟ้าในจุดที่ไม่สำคัญ เพื่อให้เครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์เครือข่ายหลัก สามารถปฏิบัติงานได้นานที่สุด

(6) หากจำเป็นต้องปิดเครื่องแม่ข่าย หรืออุปกรณ์เครือข่ายหลัก ให้หยุด process ของระบบงานต่าง ๆ และ shutdown ระบบ โดยแจ้งผู้ใช้งาน ให้ทราบก่อน shutdown ระบบด้วย

(7) เครื่องลูกข่ายเมื่อเกิดกระแสไฟฟ้าดับให้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ และปิดเครื่องคอมพิวเตอร์อย่างปลอดภัย

(8) ปิดอุปกรณ์เครื่องใช้ไฟฟ้าที่ไม่จำเป็น

(9) กรณีไฟฟ้าตก ไฟฟ้ากระชาก หากเครื่องคอมพิวเตอร์แม่ข่ายดับ ให้ตรวจสอบการทำงานของเครื่องสำรองไฟ (UPS) เครื่องป้องกันไฟกระชาก (Voltage stabilizer) และ ตรวจสอบเครื่องคอมพิวเตอร์ว่าขัดข้อง หรือเกิดความเสียหายต่อ ข้อมูล หรือ Hard disk หรือไม่ หากพบการชำรุดแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้บริหารทราบ พร้อมดำเนินการแก้ไขในเบื้องต้น



รูปที่ 1 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

4.1.2 แนวทางการฟื้นฟูระบบ

(1) หาเครื่องแม่ข่ายมาทดแทนเครื่องที่เสียหาย แล้วกู้คืน (Restore) โปรแกรมระบบงานและข้อมูลที่สำรอง (Backup) ไว้

(2) เปลี่ยนชิ้นส่วนอุปกรณ์ที่เสียหาย

(3) พยายามกู้คืนข้อมูลใน Hard disk หากไม่สำเร็จให้ใช้ข้อมูลที่ Backup ไว้ล่าสุด

(4) ทบทวนมาตรการการรักษาความปลอดภัยให้รัดกุมยิ่งขึ้น

4.2 การแก้ไขปัญหาเนื่องจากระบบเครือข่ายสื่อสารล้มเหลว

4.2.1 การปฏิบัติเมื่อเกิดเหตุ

(1) กรณีเครือข่ายอินเตอร์เน็ตขัดข้อง ให้แจ้งส่วนสื่อสารอุตุนิยมวิทยาภายในประเทศหรือผู้ให้บริการอินเตอร์เน็ตทำการแก้ไข

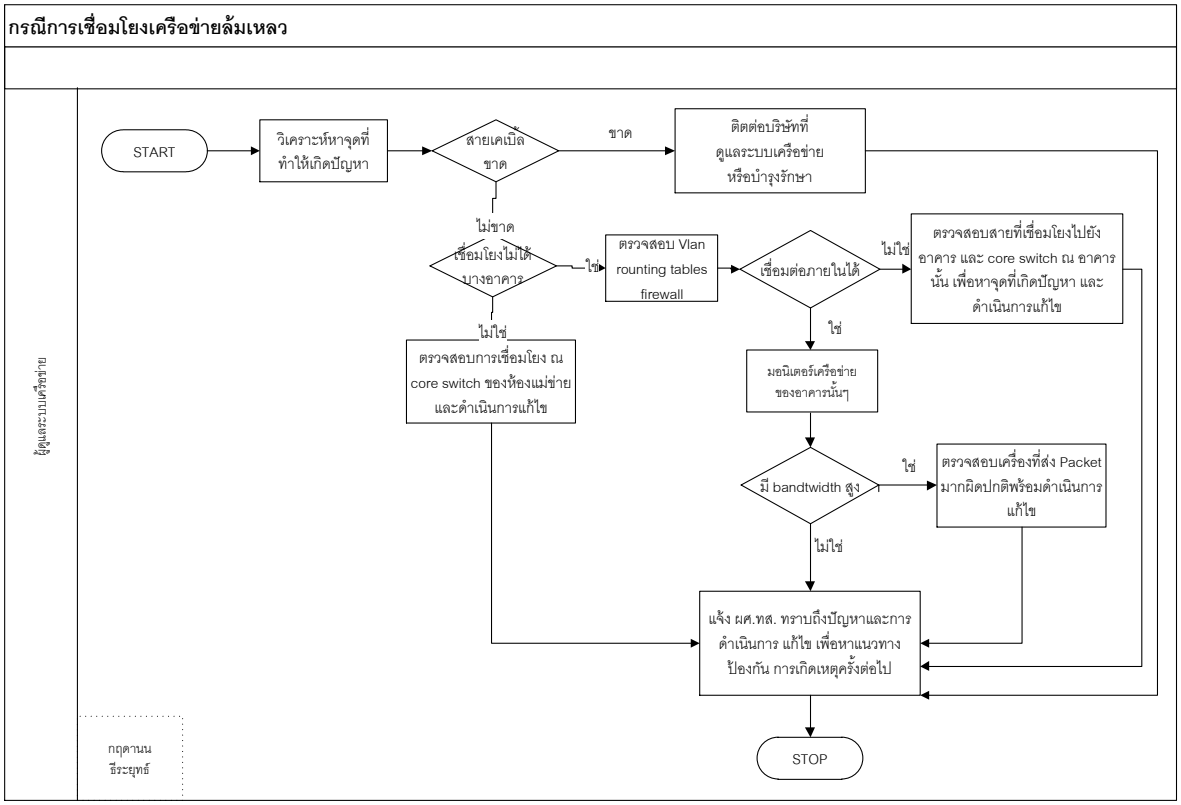
(2) กรณีวงจรเช่า (Leased line) ขัดข้องแจ้งผู้ให้บริการ (โทรคมนาคมแห่งชาติ หรือ NT หรือ GIN NOC แล้วแต่กรณี)

(3) กรณีเครือข่ายภายในขัดข้องแจ้งผู้ดูแลระบบให้เจ้าหน้าที่ทางเทคนิคตรวจสอบแก้ไข

(4) หากอุปกรณ์เครือข่ายหลัก เช่น Core Switch, Firewall ชำรุด ให้แจ้งให้บริษัทที่รับจ้างเหมาบำรุงรักษาระบบเครือข่าย ดำเนินการแก้ไขซ่อมแซมโดยเร็ว

(5) หากอุปกรณ์กระจายสัญญาณ (Switch) ที่ไม่อยู่ในสัญญาจ้างเหมาบำรุงรักษาชำรุด ให้จัดหาเพื่อใช้ทดแทน

(6) รายงานผู้ดูแลระบบเครือข่ายทราบการขัดข้อง และแจ้งให้ผู้ได้รับผลกระทบจากการขัดข้องทราบด้วย ดังแผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



รูปที่ 2 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

4.2.2 แนวทางการฟื้นฟูระบบ

(1) จ้างซ่อมอุปกรณ์ที่ชำรุด หรือจัดซื้อมาทดแทน

(2) บันทึกรายละเอียด สถิติ การชำรุดของระบบ และอุปกรณ์เพื่อเป็นแนวทางในการปรับปรุงระบบเครือข่าย และสื่อสารต่อไป

4.3 เครื่องคอมพิวเตอร์ ขัดข้อง หรืออุปกรณ์ชำรุด

เป็นปัญหาจากการติดตั้ง การบำรุงรักษา การใช้งานของบุคลากร หรือการหมดอายุการใช้งานของอุปกรณ์

4.3.1 การปฏิบัติเมื่อเกิดเหตุ

(1) เครื่องแม่ข่าย

- ผู้ปฏิบัติงานแจ้งให้เจ้าหน้าที่ที่รับผิดชอบด้านเทคนิคตรวจสอบ
- ตรวจสอบหาสาเหตุการชำรุดของ Hardware และ Software
- หากไม่สามารถแก้ไขได้ ให้แจ้งบริษัทที่รับจ้างเหมาะบำรุงรักษา ดำเนินการแก้ไขซ่อมแซม หรือจัดหาทดแทน
- รายงานสถานสภาพการชำรุดให้ผู้บริหารทราบ และแจ้งให้ผู้ใช้ระบบทราบ
- หาเครื่องแม่ข่ายมาใช้งานทดแทน

(2) เครื่องลูกข่าย

- แจ้งเจ้าหน้าที่ที่รับผิดชอบด้านเทคนิคตรวจสอบหาสาเหตุของการชำรุด
- ทำการซ่อมแซมแก้ไขเบื้องต้น
- หากไม่สามารถแก้ไขได้ในเบื้องต้น ให้ติดต่อบริษัทที่รับจ้างบำรุงรักษาดำเนินการ (หากเป็นเครื่องในสัญญา)

4.3.2 แนวทางการฟื้นฟูระบบ

(1) เครื่องแม่ข่าย

- หากการซ่อมแซมต้องใช้เวลานานให้จัดหาเครื่องแม่ข่ายมาใช้ทดแทน
- ติดตั้งซอฟท์แวร์ระบบงาน รวมทั้งกู้คืน (Restore) ข้อมูลที่ Backup
- ปรับแต่งค่าระบบ (System Configuration) ของระบบให้เหมือนเดิม ทดสอบโปรแกรมระบบงานให้เครื่องใช้งานได้สมบูรณ์
- ตั้งงบประมาณจัดหาทดแทนเครื่องแม่ข่ายมาใช้แทนเครื่องที่ประสิทธิภาพต่ำ หรือหมดอายุการใช้งาน
- ทบทวนมาตรการในการปฏิบัติการ และบำรุงรักษา

(2) เครื่องลูกข่าย

- จัดหาอุปกรณ์ใหม่ทดแทนอุปกรณ์ที่ชำรุด
- หากการซ่อมแซมต้องใช้เวลานานให้จัดหาเครื่องสำรองให้ใช้ทดแทนไปก่อน
- ติดตั้งซอฟท์แวร์ ที่จำเป็นต่อการใช้งาน

- ตั้งงบประมาณจัดหาทดแทนเครื่องและอุปกรณ์ที่ประสิทธิภาพต่ำ ไม่คุ้มกับการซ่อมแซม หรือหมดอายุการใช้งาน

4.4 อัคคีภัย

อาคารศูนย์เทคโนโลยีสารสนเทศเป็นอาคาร 3 ชั้น ตั้งแยกอิสระจากอาคารอื่นมีถนนและรั้วรอบอาคาร รถดับเพลิงสามารถเข้าถึงได้โดยง่ายหากเกิดเพลิงไหม้ ภายในตัวอาคารติดตั้งระบบตรวจจับควัน และระบบดับเพลิงอัตโนมัติ แต่หากเกิดอัคคีภัยในอาคาร จึงได้กำหนดหลักการปฏิบัติไว้ดังนี้

4.4.1 มาตรการในการป้องกันเหตุเพลิงไหม้

(1) มีสัญญาณเตือนภัยเมื่อเกิดไฟไหม้ติดตั้งกระจายอยู่ทุกชั้นของอาคารศูนย์เทคโนโลยีสารสนเทศ

(2) มีสัญญาณแจ้งเตือนไฟไหม้ (แบบกดปุ่ม) กระจายอยู่ทุกชั้น

(3) มีอุปกรณ์ดับเพลิงชนิด CO2 ติดตั้งกระจายอยู่ทุกชั้นของอาคารศูนย์เทคโนโลยีสารสนเทศ

(4) มีระบบดับเพลิงแบบ FM-200 (ชนิดก๊าซฮาร์ลอน) ในห้องคอมพิวเตอร์หลัก

(5) มีเครื่องตรวจจับควัน ติดตั้งอยู่ในทุกห้องของอาคารศูนย์เทคโนโลยีสารสนเทศ

(6) มีการตรวจสอบอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้สามารถใช้งานได้ตามปกติ ดังนี้

- สัญญาณเตือนภัย
- อุปกรณ์ดับเพลิง
- ถังดับเพลิง
- สัญญาณแจ้งเตือนไฟไหม้ (แบบกดปุ่ม)
- เครื่องตรวจจับควันไฟ
- ระบบดับเพลิงแบบ FM-200

(7) มีการซ้อมหนีไฟอย่างน้อยปีละ 1 ครั้ง

(8) ต้องจัดทำบัญชีทรัพย์สินทางเทคโนโลยีสารสนเทศที่มีความสำคัญพร้อมตั้งติดสติกเกอร์ที่ตัวทรัพย์สินนั้น แยกเป็นสี แดง เหลือง เขียว โดย

(9) สีแดง หมายถึงทรัพย์ที่มีความสำคัญมาก ต้องเคลื่อนย้ายเร่งด่วนกรณีเกิดเหตุ

(10) สีเหลือง หมายถึงทรัพย์สินที่มีความสำคัญรองจากทรัพย์สินสีแดง

(11) สีเขียว หมายถึงทรัพย์สินที่มีความสำคัญ

(12) จัดทำรายงานผลการซ้อมหนีไฟ เพื่อนำมาปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติในครั้งถัดไป

(13) มีการประชาสัมพันธ์เสียงตามสาย เพื่อให้ความรู้ แนวทางปฏิบัติขณะเกิดเหตุเพลิงไหม้เป็นประจำ

4.4.2 ขณะเกิดเหตุเพลิงไหม้

ขณะเกิดเพลิงไหม้ ให้ปฏิบัติ ดังนี้

(1) เมื่อได้ยินเสียงสัญญาณแจ้งเหตุเพลิงไหม้ให้รีบอพยพตามเส้นทางที่ได้กำหนดไว้ อย่าตื่นตระหนก ออกจากอาคารให้เร็วที่สุดตามเส้นทางหนีไฟที่กำหนดไว้

(2) ห้องที่มีการล็อกประตูด้วยบัตรอิเล็กทรอนิกส์ (Key Card) ให้ปลดสวิทช์ควบคุมประตูเพื่อปลดปล่อยการล็อกประตู

(3) ผู้นำทางหนีไฟ นำเจ้าหน้าที่ออกไปยังทางหนีไฟที่ใกล้ที่สุดตามที่ได้กำหนดไว้

(4) หากเส้นทางหนีไฟเต็มไปด้วยกลุ่มควันให้ใช้ผ้าชุบน้ำคลุมตัว และปิดจมูก ป้องกันการสำลักควัน แล้วหมอบคลานเนื่องจากอากาศบริสุทธิ์จะอยู่ด้านล่าง

(5) ห้ามใช้ลิฟต์ เพราะขณะเกิดเพลิงไหม้ไฟฟ้าจะดับทำให้ลิฟต์ค้างทำให้ด้านในของตัวลิฟต์ไม่มีอากาศ

(6) เมื่อออกจากอาคารแล้วให้ไปรวมตัวกันที่จุดรวมพลเพื่อตรวจนับ

(7) โทรศัพท์แจ้งหน่วยดับเพลิง โทร. 199 ทันที ป้อมยามหน้ากรม 6399

(8) ผู้ที่ไม่มีหน้าที่เกี่ยวข้องกับการจัดการทรัพย์สินภายในอาคาร หรือการเคลื่อนย้ายอุปกรณ์ทางเทคโนโลยีสารสนเทศ หรือการดับเพลิง ไม่ควรกลับเข้าไปในอาคารอีก

(9) ในกรณีที่ยังสามารถขนย้ายอุปกรณ์ได้ ให้ผู้มีหน้าที่ขนย้ายอุปกรณ์คอมพิวเตอร์ดำเนินการ ดังนี้

(10) เมื่อได้ยินเสียงสัญญาณแจ้งเหตุเพลิงไหม้ให้รีบเข้าไปยังห้องคอมพิวเตอร์หลัก นำอุปกรณ์คอมพิวเตอร์ที่สำคัญออกจากห้อง โดยอุปกรณ์คอมพิวเตอร์ที่สำคัญจะติดสติ๊กเกอร์สีแดงไว้

(11) รีบออกจากห้องคอมพิวเตอร์หลักและไปยังทางหนีไฟที่ใกล้ที่สุด ให้เร็วที่สุด และให้ไปยัง Site สำรอง เพื่อดำเนินการกู้คืนระบบงานทีสำคัญ

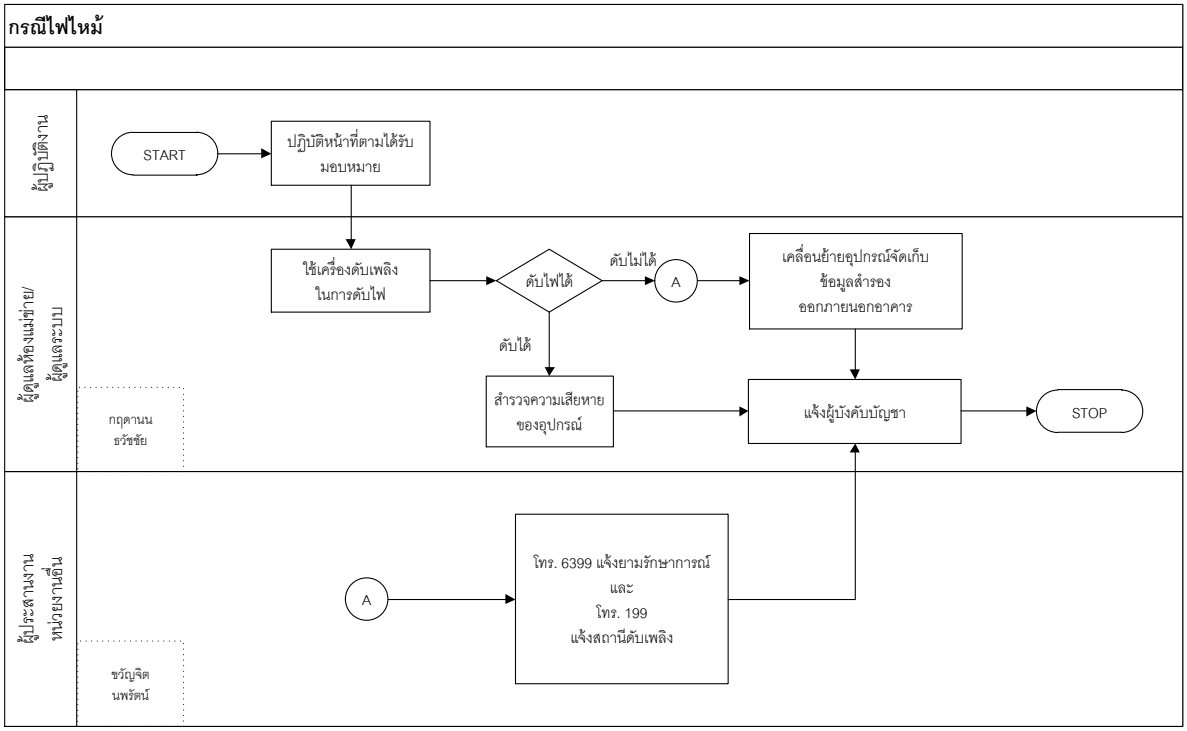
(12) ในกรณีที่จำเป็นจะต้องหน่วงเวลาการฉีดน้ำยาของระบบดับเพลิง FM-200 ให้ปฏิบัติตามคู่มืออย่างเคร่งครัด

4.4.3 เส้นทางการอพยพหนีไฟในอาคาร

(1) ทางออกที่ 1 ประตูหลักหน้าอาคาร

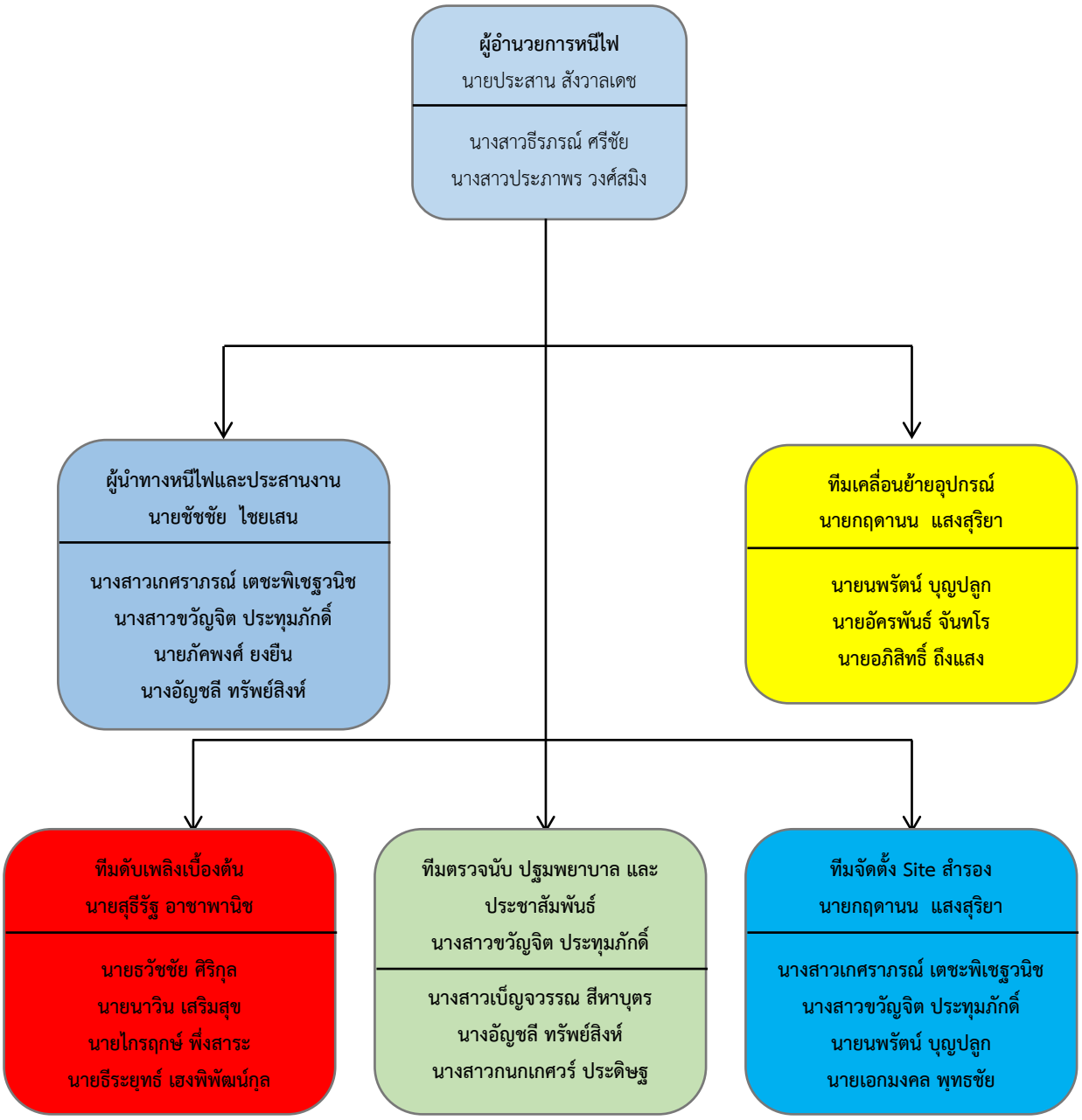
(2) ทางออกที่ 2 ประตูหลังอาคาร ผ่านห้องควบคุมระบบไฟฟ้าและระบบปรับอากาศ

(3) ทางออกที่ 3 ประตูด้านตะวันตกตรงข้ามอาคารสถานีวิทยุ(โรงอาหาร)



รูปที่ 3 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเพลิงไหม้ขณะมีผู้ปฏิบัติงาน

4.4.4 แผนผังการมอบหมายหน้าที่ในกรณีเกิดอัคคีภัย



รูปที่ 4 แผนผังการมอบหมายหน้าที่ในกรณีเกิดอัคคีภัย

ตารางที่ 7 การมอบหมายหน้าที่ความรับผิดชอบกรณีเกิดอัคคีภัย

หน้าที่ความรับผิดชอบ	ผู้ปฏิบัติ
ผู้อำนวยการหนีไฟ ทำหน้าที่ - อำนวยการ และสั่งการในการอพยพหนีไฟ และการดับเพลิง - แจ้งผู้บังคับบัญชาระดับเหนือขึ้นไป - ประเมินความเสียหาย และแจ้งผู้เกี่ยวข้อง	**หัวหน้าทีม** - นายประสาน สังวาลเดช **ผู้ช่วย** - นางสาวธีราภรณ์ ศรีชัย - นางสาวประภาพร วงศ์สมิง
ทีมอพยพหนีไฟประสานงาน ทำหน้าที่ - นำเจ้าหน้าที่หนีไฟตามเส้นทางที่กำหนด - อำนวยความสะดวกแก่ผู้หนีไฟ - แจ้งยาม 6399 และหน่วยงานดับเพลิง 199	**หัวหน้าทีม** - นายชัชชัย ไชยเสน **ผู้ช่วย** -นางสาวเกศราภรณ์ เตชะพิเชฐวนิช - นางสาวขวัญจิต ประทุมภักดิ์ - นายภัคพงศ์ ยงยืน - นางอัญชลี ทรัพย์สิงห์
ทีมเคลื่อนย้ายอุปกรณ์ ทำหน้าที่ - ขนย้าย เทป Harddisk สำรองข้อมูล ที่สำคัญออกจากห้องคอมพิวเตอร์หลัก	**หัวหน้าทีม** - นายกฤดานน แสงสุริยา **ผู้ช่วย** - นายนพรัตน์ บุญปลูก - นายอัครพันธ์ จันทโร - นายอภิสิทธิ์ ถึงแสง
ทีมดับเพลิงเบื้องต้น ทำหน้าที่ - สำรวจจุดที่เกิดเพลิงไหม้ - ทำการดับเพลิงด้วยเครื่องดับเพลิงเคมี - กำหนดให้เครื่องดับเพลิงอัตโนมัติ ไม่ทำงาน หรือ ปล่อยให้ทำงาน	**หัวหน้าทีม** - นายสุธีรัฐ อาชาพานิช **ผู้ช่วย** - นายธวัชชัย ศิริกุล - นายนาวิน เสริมสุข - นายไกรฤกษ์ พึ่งสาระ - นายธีระยุทธ์ เฮงพิพัฒน์กุล
ทีมตรวจนับ ปฐมพยาบาลและประชาสัมพันธ์ ทำหน้าที่ - แจ้งยามรักษาการณ์ของกรมฯ - แจ้งหน่วยดับเพลิงภายนอก และเจ้าหน้าที่ตำรวจตามภาคผนวก 3	**หัวหน้าทีม** - นางสาวขวัญจิต ประทุมภักดิ์ **ผู้ช่วย** - นางสาวเบ็ญจวรรณ สีหาบุตร

หน้าที่ความรับผิดชอบ	ผู้ปฏิบัติ
- ทำการตรวจนับบุคคลที่อพยพออกจากอาคาร และผู้ปฏิบัติงานในอาคารขณะเกิดเหตุ - ปฐมพยาบาลเบื้องต้นแก่ผู้ประสบอุบัติเหตุ - ประสานงานหน่วยพยาบาลภายนอกเพื่อช่วยเหลือผู้ประสบอุบัติเหตุ - ประชาสัมพันธ์ และให้ข้อมูลข่าวสารแก่บุคคลภายนอก	- นางอัญชลี ทรัพย์สิงห์ - นางสาวกนกเกศวร์ ประดิษฐ
ทีมจัดตั้ง Site สำรอง ทำหน้าที่ - จัดเตรียมระบบคอมพิวเตอร์สำหรับ Site สำรอง - ปรับแต่งระบบปฏิบัติการและ Application Server ที่จำเป็น - นำข้อมูลสำรองขึ้นใช้งาน - เชื่อมโยงระบบเครือข่ายที่เกี่ยวข้อง - แจ้งทีมประชาสัมพันธ์ แจ้งหน่วยงานที่เกี่ยวข้อง ถ้ามีการเปลี่ยนแปลงช่องทางการใช้ระบบสารสนเทศหรือการสืบค้นข้อมูล	**หัวหน้าทีม** - นายกฤดานน แสงสุริยา **ผู้ช่วย** - นางสาวเกศราภรณ์ เตชะพิเชฐวนิช - นางสาวขวัญจิต ประทุมภักดิ์ - นายนพรัตน์ บุญปลูก - นายเอกมงคล พุทธชัย

4.4.5 ขณะเกิดเหตุเพลิงไหม้

ให้บุคคลที่อยู่ภายในอาคารปฏิบัติหน้าที่ตามที่ได้รับมอบหมายกรณีเกิดอัคคีภัย ในข้อ 4.4.4

4.4.6 หลังเกิดเหตุเพลิงไหม้

ให้ดำเนินการดังนี้

ตารางที่ 8 ข้อปฏิบัติหลังเกิดเหตุเพลิงไหม้

ข้อปฏิบัติ	ระยะเวลา	ผู้รับผิดชอบ
สำรวจยอดผู้ได้รับผลกระทบหรือประสบอุบัติเหตุ พร้อมทั้งรายงานผู้บังคับบัญชา	3 ชั่วโมง	ทีมตรวจนับ ปฐมพยาบาล และประชาสัมพันธ์
เปิดระบบคอมพิวเตอร์สำรองสำหรับระบบสารสนเทศที่มีความสำคัญยิ่งยวด	24 ชั่วโมง	ทีมจัดตั้ง Site สำรอง
ประสานหน่วยงานภายนอกสืบสวนสอบสวนสาเหตุการเกิดเพลิงไหม้	1 ชั่วโมง	ทีมตรวจนับ ปฐมพยาบาล และประชาสัมพันธ์
ประเมินความเสียหายของพื้นที่เกิดเหตุและรายงานผู้บังคับบัญชา	48 ชั่วโมง	เจ้าหน้าที่ทุกคนที่เกี่ยวข้อง

4.5 การบุกรุกทางเครือข่าย

4.5.1 ปัญหาจาก Malware มัลแวร์ หรือ ไวรัสคอมพิวเตอร์และการเจาะระบบ

มาตรการในการป้องกันก่อนเกิดเหตุโดนเจาะระบบ มีมาตรการในการป้องกัน ดังนี้

(1) ติดตั้งโปรแกรมป้องกันไวรัสและปรับปรุง Virus Signature หรือภัยคุกคามอื่น ๆ ในเครื่องคอมพิวเตอร์ทุกเครื่องให้ทันสมัย

(2) ดำเนินการตรวจสอบการกำหนดค่า Rule ของอุปกรณ์ Firewall ที่เหมาะสมเครือข่ายให้เด่นชัดระหว่างเครือข่ายที่ต้องรับความเสียง และเครื่องข่ายที่ต้องการความปลอดภัยสูงสุด

(3) ตรวจสอบอุปกรณ์ตรวจจับการบุกรุก หรือ log file ของเครื่องแม่ข่ายว่ามีเหตุพยายามบุกรุกเข้ามาในระบบหรือไม่

(4) เผยแพร่ ประชาสัมพันธ์ ให้เจ้าหน้าที่ในองค์กรปฏิบัติตาม พรบ. ว่าด้วยการกระทำความผิดทางคอมพิวเตอร์ พ.ศ. 2550 และ ฉบับที่ 2 พ.ศ. 2560 และแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมอุตุนิยมวิทยา

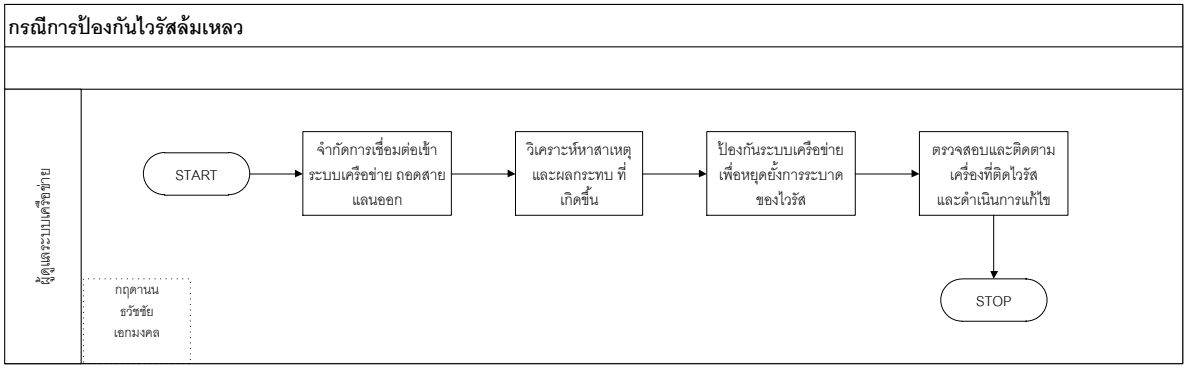
(5) มีเจ้าหน้าที่ดูแลระบบเครือข่ายคอยตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ต

(6) รายงานผลการตรวจสอบการป้องกันการโดนเจาะระบบแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

4.5.2 การปฏิบัติขณะเกิดเหตุ

(1) กรณีถูกโจมตีจาก Malware มัลแวร์ หรือ ไวรัสคอมพิวเตอร์คอมพิวเตอร์

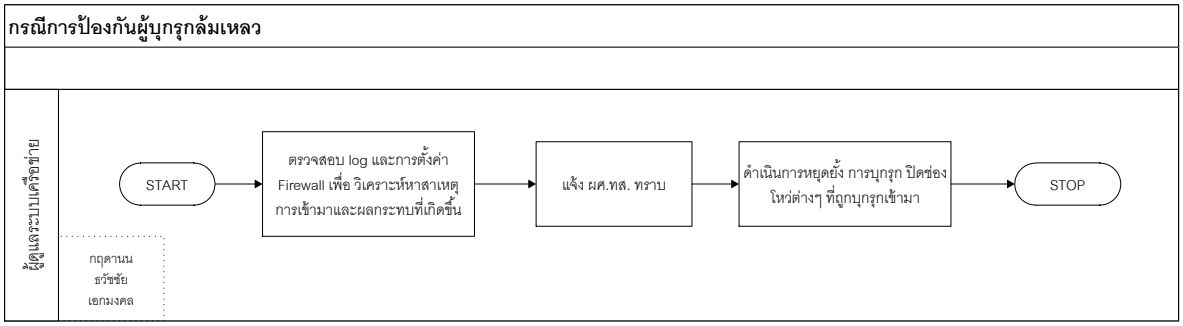
- เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึง สายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว
- ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามลำดับความสำคัญของการให้บริการ
- ทำการตรวจสอบ Malware Virus และ Malicious Software ต่าง ๆ
- กำจัดไวรัสบนเครื่องคอมพิวเตอร์ในเครือข่าย หากไม่มีโปรแกรมกำจัดไวรัส ให้ Download โปรแกรมสำหรับแก้ไขไวรัสที่ตรวจพบมาใช้ และ Update ฐานข้อมูลไวรัสของโปรแกรม Antivirus แล้วทำการตรวจหาไวรัสบนระบบอีกครั้ง
- หากยังไม่สามารถแก้ปัญหาได้ให้ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบ Server และ/หรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด



รูปที่ 5 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีป้องกันไวรัสล้มเหลว

(2) กรณีถูกเจาะระบบ

- ตัดการเชื่อมต่อของระบบที่ถูกบุกรุกจากระบบเครือข่าย
- ทำสำเนาระบบที่เสียหาย
- ทำการตรวจสอบ Transaction log files
- ดูการเปลี่ยนแปลงของระบบจาก software หรือ configuration files
- ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้ เช่น Network Sniffers, Trojan Horse Programs



รูปที่ 6 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีป้องกันผู้บุกรุกล้มเหลว

4.5.3 แนวทางการฟื้นฟูระบบ

(1) กรณีถูกโจมตีจากคอมพิวเตอร์ Malware มัลแวร์ หรือ ไวรัสคอมพิวเตอร์

- ทำการตรวจสอบระบบ Firewall และการตั้งค่า Policy
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ
- ปรับปรุงโปรแกรม Antivirus หรือหาตัวที่ดีกว่าเดิม และบังคับให้มีการใช้ทั้งระบบโดยเคร่งครัด
- หากยังมีปัญหาประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ระบบ

(2) กรณีถูกเจาะระบบ

- ในกรณีที่คอมพิวเตอร์ถูกเจาะระบบ System ต่าง ๆ รวมทั้ง Kernel ข้อมูล ไฟล์ต่าง ๆ อาจจะถูกแก้ไขโดยที่เราไม่รู้ วิธีเดียวที่ให้ความมั่นใจได้ว่าระบบมีความปลอดภัยอีกครั้ง โดยการติดตั้งระบบ OS ทั้งหมดใหม่ รวมทั้ง Patch ที่แก้ไขล่าสุดด้วย
- ติดตั้งระบบงานใหม่เฉพาะที่จำเป็นในการใช้งาน
- เปลี่ยน Password ทั้งหมด
- ทำการตรวจสอบระบบ Firewall และการตั้งค่า Policy ให้เหมาะสมยิ่งขึ้น
- ปรึกษากับหน่วยงานที่เกี่ยวข้องในการรักษาความปลอดภัยและหน่วยงานที่เกี่ยวข้องเพื่อขอความช่วยเหลือในการวางมาตรการ และการปฏิบัติ
- ปรับปรุงและปฏิบัติตามข้อปฏิบัติที่เกี่ยวกับการรักษาความปลอดภัย
- ตรวจสอบนโยบายของระบบตรวจจับการบุกรุก (Intrusion Detection System)
- การตรวจสอบ Log กรณีถูกเจาะระบบ
- การตรวจสอบ Access log, Syslog, Event log
- การตรวจสอบ IP Address
- การตรวจสอบ Service Port ที่ถูกเปิดอยู่ในปัจจุบัน
- การตรวจสอบเวลาที่โดนเจาะระบบ
- การวิเคราะห์ log

4.6 การเสียหายของอุปกรณ์จัดเก็บข้อมูล

4.6.1 ก่อนเกิดเหตุ

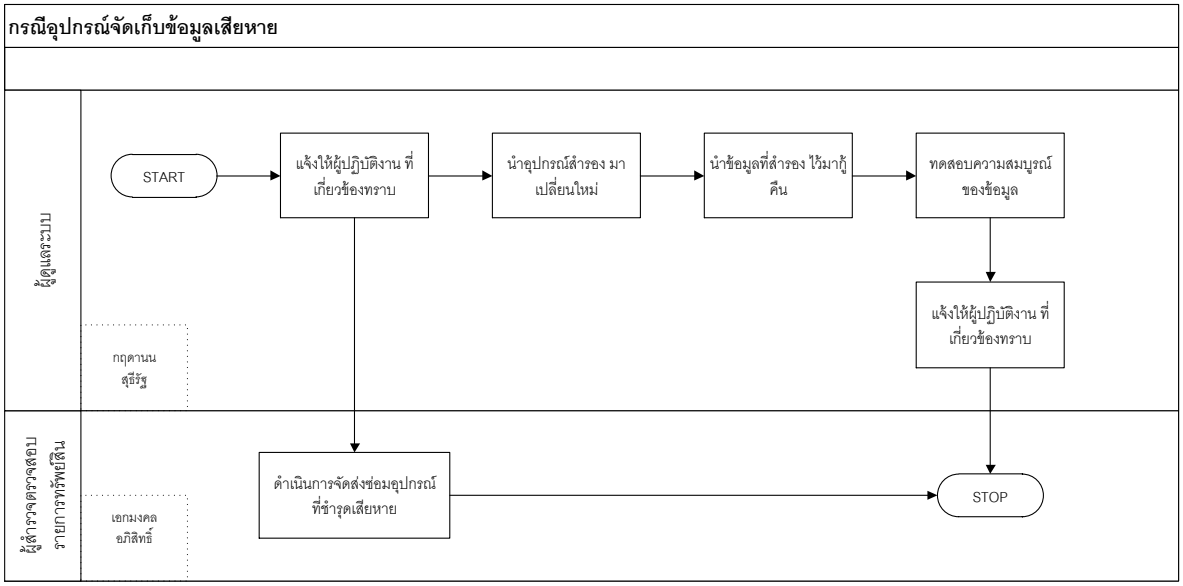
มีมาตรการป้องกันความเสียหายของอุปกรณ์จัดเก็บข้อมูล ดังนี้

(1) ติดตั้งระบบจัดเก็บข้อมูลสำรอง หรือ ติดตั้งระบบเก็บข้อมูลที่สนับสนุนการทำงานคงเสถียรภาพเช่น การทำ RAID ของ Harddisk หรือ ใช้ระบบจัดเก็บข้อมูลที่มีสมรรถนะและความน่าเชื่อถือสูง เช่น SAN

(2) ตรวจสอบความครบถ้วน สมบูรณ์ของสื่อจัดเก็บข้อมูลเป็นประจำ

(3) ประเมินความเสี่ยงของข้อมูลที่มีระดับความสำคัญ และจัดทำระบบการสำรองที่มีประสิทธิภาพ

(4) จัดหาสื่อจัดเก็บข้อมูลสำรองให้เพียงพอต่อการนำขึ้นมาใช้ทดแทนได้ทันทีเมื่อสื่อหลักชำรุดเสียหาย



รูปที่ 7 แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

4.6.2 แนวทางการฟื้นฟูระบบ

(1) นำอุปกรณ์สำรองขึ้นมาใช้

(2) นำข้อมูลที่สำรองไว้มาใช้งานและปรับปรุงให้ทันสมัยมากที่สุด

(3) ทดสอบความทันสมัยของข้อมูล

(4) จัดส่งอุปกรณ์เข้าซ่อม หรือ จัดหาใหม่ทดแทน กรณีไม่สามารถซ่อมแซมได้

ภาคผนวก ก
ข้อปฏิบัติในการสำรองข้อมูลและระบบ

1.1 มาตรการดำเนินงาน

การสำรองข้อมูลจะต้องดำเนินการตามมาตรการที่กำหนดต่อไปนี้

1) ข้อมูลและซอฟต์แวร์ที่เกี่ยวข้องของระบบงานแต่ละระบบ จะต้องถูกสำเนาอย่างครบถ้วนและเป็นระบบ เพื่อให้แน่ใจว่าข้อมูลที่มีการเพิ่มเติม แก้ไข เปลี่ยนแปลง จะถูกทำสำเนาไว้ครบถ้วน

2) มีการบันทึกว่าได้ทำการสำรองข้อมูลอะไรบ้าง เมื่อใด

3) สื่อที่ใช้ในการบันทึกข้อมูล เช่น เทป หรือแผ่น Optical Disk จะต้องมีฉลากติดที่ระบุ

4) รายละเอียดข้อมูลในสื่อนั้น ชนิดของข้อมูล ชื่อแฟ้มข้อมูล ข้อมูลเป็นของระบบงานใด วันที่ทำการบันทึกไว้ อย่างชัดเจน

5) ข้อมูลที่ทำการบันทึกเป็นข้อมูลสำรองชุดหนึ่ง จะต้องเก็บในสถานที่ที่มีความปลอดภัยจากภัยพิบัติที่อาจจะเกิดขึ้น

6) จะต้องมีการทดสอบเป็นประจำว่า ข้อมูลที่สำรองสามารถนำกลับมาใช้ได้

7) ระบบสารสนเทศในความรับผิดชอบที่จะต้องสำรอง ควบคุม ติดตาม ให้สามารถใช้งานได้มีดังนี้

ตารางที่ 9 การสำรองข้อมูลของระบบสารสนเทศ

ข้อมูล	เครื่องคอมพิวเตอร์	ปริมาณข้อมูลสำรอง
1. ระบบเมล์กรม(@tmd.go.th)	IBM system X3650 M3	900 GB.
2. ระบบเว็บไซต์ของกรมอุตุนิยมวิทยา	Virtual Machine	436 GB.
3. ระบบเว็บไซต์ภายในของกรมอุตุนิยมวิทยา (Intranet)	Virtual Machine	91 GB
4. ระบบบริการสารสนเทศภูมิอากาศ (CIS)	Virtual Machine	20 GB
5. ฐานข้อมูลภูมิอากาศ	Virtual Machine	101 GB
6. ระบบยื่นคำขอข้อมูลสถิติอุตุนิยมวิทยา	IBM system X3650 M3	17 GB
7. ระบบสลิปเงินเดือน	Virtual Machine	3 GB.
8. ระบบการจัดการความรู้ในกรมอุตุนิยมวิทยา (KM)	Virtual Machine	26 GB.
9. ระบบติดตามและประเมินผลตามคำรับรองการปฏิบัติราชการกรมอุตุนิยมวิทยา	Virtual Machine	20 GB
10. ระบบติดตาม ตรวจสอบและรายงานผลการใช้จ่ายงบประมาณ	Virtual Machine	20 GB.

11. ระบบติดตามแผนผลการปฏิบัติงาน	Virtual Machine	20 GB.
12. ระบบ Web Hosting	Virtual Machine	800 GB.
13. ข้อมูลการอัพโหลดไฟล์	Virtual Machine	40 GB.
14. การบริการข้อมูลอุตุนิยมวิทยาและแผ่นดินไหวผ่าน API	Virtual Machine	60 GB.

หมายเหตุ ปริมาณข้อมูลที่สำรองที่มากกว่าหรือน้อยกว่าข้อมูลจริงขึ้นอยู่กับนโยบายการสำรองข้อมูลแต่ละระบบ

1.2 ชนิดและความถี่ในการสำรองข้อมูล

การสำรองข้อมูลประจำวัน/สัปดาห์ ของศูนย์เทคโนโลยีสารสนเทศ กรมอุตุนิยมวิทยา ทำการสำรองข้อมูลของระบบต่าง ๆ ดังนี้

ตารางที่ 10 ชนิดและความถี่ในการสำรองข้อมูล

ลำดับ	รายการ	Media	ข้อมูลที่สำรอง	ความถี่การสำรองข้อมูล
1	ระบบเมล์กรม(@tmd.go.th)	Disk	ข้อมูลบัญชีและข้อมูลผู้ใช้งาน	ทุกวัน
2	ระบบเว็บไซต์ของกรมอุตุนิยมวิทยา	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
3	ระบบเว็บไซต์ภายในของกรมอุตุนิยมวิทยา (Intranet)	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
4	ระบบบริการสารสนเทศภูมิอากาศ (CIS)	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
5	ฐานข้อมูลภูมิอากาศ	Disk	ฐานข้อมูล	ทุกวัน
6	ระบบยื่นคำขอข้อมูลสถิติอุตุนิยมวิทยา	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
7	ระบบสลิปเงินเดือน	Disk	เว็บไซต์และฐานข้อมูล	อังคาร พฤหัสบดี
8	ระบบการจัดการความรู้ในกรมอุตุนิยมวิทยา (KM)	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
9	ระบบติดตามและประเมินผลตามคำรับรองการปฏิบัติราชการกรมอุตุนิยมวิทยา	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
10	ระบบติดตาม ตรวจสอบและรายงานผลการใช้จ่ายงบประมาณ	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
11	ระบบติดตามแผนผลการปฏิบัติงาน	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
12	ระบบ Web Hosting	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน
13	ข้อมูลการอัพโหลดไฟล์	Disk	ไฟล์	ทุกวัน
14	การบริการข้อมูลอุตุนิยมวิทยาและแผ่นดินไหวผ่าน API	Disk	เว็บไซต์และฐานข้อมูล	ทุกวัน

1.3 การสำรองข้อมูลประจำวัน

การสำรองข้อมูลประจำวันหรือในวันที่กำหนดในแต่ละสัปดาห์ให้ดำเนินการดังนี้

1) ตรวจสอบตารางการสำรองข้อมูลและติดตามผลการทำงาน

2) ตรวจเช็คสคริปต์หรือชุดคำสั่งที่ตั้งไว้ทำงานหรือไม่หรือตรวจสอบรายงาน

3) เขียนรายละเอียดของข้อมูล ชนิด ชื่อแฟ้ม และรายละเอียดอื่นๆ ที่เกี่ยวข้อง บนฉลาก ติดกำกับบนสื่อข้อมูล

4) บันทึกรายละเอียดของข้อมูลที่สำรอง พร้อมลงลายมือชื่อผู้ปฏิบัติงานสำรองข้อมูลหรือผู้ตรวจสอบ

1.4 การสำรองโปรแกรมระบบงาน

ศูนย์เทคโนโลยีสารสนเทศ ทำการสำรองโปรแกรมระบบงานต่าง ๆ และ ซอร์สโค้ดของโปรแกรมต่าง ๆ ลงบนสื่อข้อมูล เพื่อจะได้นำกลับมาใช้งานได้ หากโปรแกรมที่ติดตั้งไว้เดิมเกิดความเสียหาย

1.5 การสำรองข้อมูลเก็บไว้ที่อื่น

การจัดเก็บ Media ที่ใช้สำหรับสำรองข้อมูล ศูนย์เทคโนโลยีสารสนเทศ ได้ทำการจัดเก็บ Media แยกเป็น 2 ชุดโดยแยกเก็บคนละอาคารกัน ในที่ ๆ ปลอดภัย มิดชิด เพื่อเป็นการรักษาความปลอดภัยของข้อมูล ในกรณีที่เกิดภัยพิบัติกับอาคารใดอาคารหนึ่งแล้ว สามารถนำเทปสำรองข้อมูลอีกชุดหนึ่งมาใช้งานต่อไปได้

1) สำรองข้อมูลลงสื่อจำนวน 2 ชุด โดยชุดที่ 1 จะเก็บไว้ที่ศูนย์เทคโนโลยีสารสนเทศ ส่วนชุดที่ 2 จะเก็บไว้ที่ อาคาร 50 ปีอุตุนิยมวิทยา ชั้น 9

2) สำรองข้อมูลผ่านเครือข่ายอินเตอร์เน็ต (FTP) ไปเก็บที่เซิร์ฟเวอร์ที่ติดตั้งที่ศูนย์อุตุนิยมวิทยาภาคเหนือ จ.เชียงใหม่

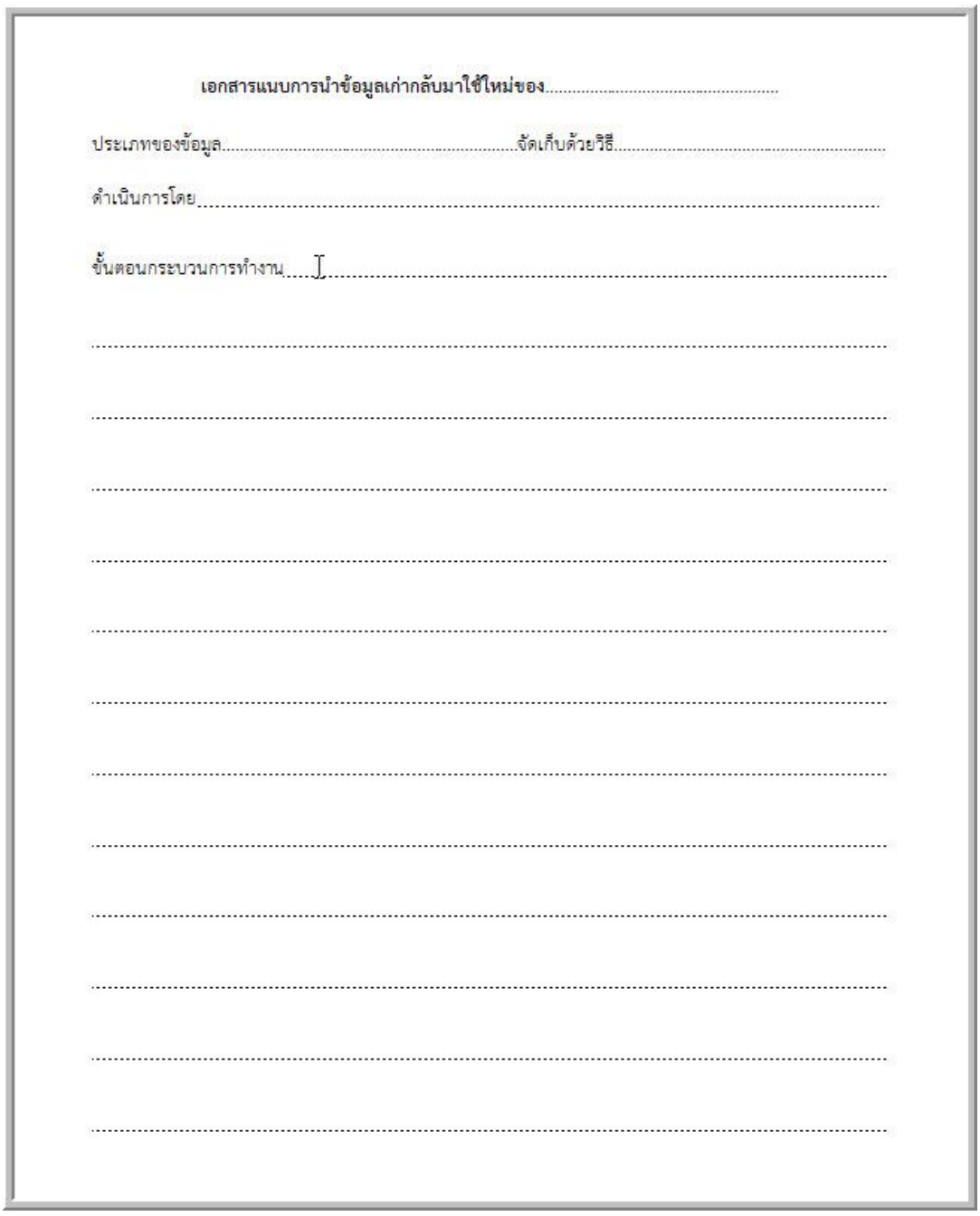
3) การสำรองข้อมูลไว้ต่างพื้นที่ชุดโปรแกรมสำเร็จรูปไม่สามารถดำเนินการได้โดยง่ายเนื่องจากปัญหาเรื่องการติดต่อสื่อสาร จึงต้องใช้ชุดคำสั่งสำรองข้อมูลให้เป็นไฟล์เดียว เช่น .zip .tar .bak และรู้การใช้คำสั่ง rsync ftp และ scp เป็นต้น

1.6 การกู้คืนข้อมูล

ศูนย์เทคโนโลยีสารสนเทศ จะดำเนินการทดสอบการกู้คืนข้อมูล กับระบบที่มีคุณสมบัติใกล้เคียงกับระบบที่ใช้งานอยู่ โดยจะทำการทดสอบอย่างน้อย 6 เดือนต่อครั้งโดยการนำข้อมูลที่ได้ทำการสำรองไว้มาทำการ Restore และทดสอบการปฏิบัติงาน รวมทั้งทำการบันทึกผลการกู้คืนข้อมูล และผู้รับผิดชอบการกู้คืนข้อมูล ดังตัวอย่างเอกสารที่ 3 บันทึกการกู้คืนข้อมูล และตัวอย่างเอกสารที่ 4 การนำข้อมูลเก่ากลับมาใช้งาน

บันทึกการกู้คืนข้อมูล			
วันเดือนปี	ข้อมูลหรือระบบที่ทำการกู้คืน	ผู้รับผิดชอบ	หมายเหตุ
11-5-2563	OS and DB cdms ,DB climate	กฤดานน	เอกสารแนบ
วันที่ไฟดับ	Configure network ชั้น 9 ขัดข้อง		

รูปที่ 8 ตัวอย่างเอกสารที่ 3 บันทึกการกู้คืนข้อมูล



รูปที่ 9 ตัวอย่างเอกสารที่ 4 เอกสารการใช้งานข้อมูล

ภาคผนวก ข
ขั้นตอนการซ้อมอพยพหนีไฟในอาคารศูนย์เทคโนโลยีสารสนเทศ

ตารางที่ 11 ขั้นตอนการซ้อมอพยพหนีไฟในอาคารศูนย์เทคโนโลยีสารสนเทศ

ขั้นตอนที่	รายละเอียด	ผู้รับผิดชอบ
1	ชี้แจงให้เจ้าหน้าที่ในอาคารทราบ - ทส. แจ้งข้อปฏิบัติให้ทุกคนในอาคารทราบ	ผศ.ทส.
2	ออกบันทึกประกาศให้ทุกคนทราบถึงกำหนดวันและเวลาซ้อมรวมทั้งแผนการซ้อม - แจ้งกำหนดการและขั้นตอนในการซ้อม	ผศ.ทส.
3	จำลองสถานการณ์ การเกิดเพลิงไหม้ในห้องคอมพิวเตอร์หลัก โดย - การเกิดควัน/เพลิง - การใช้เครื่องดับเพลิงเคมี - การใช้เครื่องดับเพลิงอัตโนมัติ	ทีมดับเพลิง
4	- ผู้พบเห็นควันไฟตะโกน “ไฟไหม้” และ - แจ้งประกาศเสียงตามสายแจ้งเหตุเพลิงไหม้และให้ทุกคนอพยพออกจากอาคาร - ทีมควบคุมเพลิงกด Fire Siren	ทีมดับเพลิง
5	- เจ้าหน้าที่อพยพออกจากอาคาร ไปรวมตัวกันที่ “จุดรวมตัวหน้าอาคาร” (ยกเว้นผู้มีหน้าที่อื่น ให้ดำเนินการตามหน้าที่โดยเร็ว ออกไปรวมตัวหน้าอาคาร)	ทุกคน (ยกเว้นผู้มีหน้าที่)
6	ทีมต่างๆ ดำเนินการดังนี้ - ทีมอพยพ : นำข้าราชการ –เจ้าหน้าที่ไปตามเส้นทางที่กำหนด - ทีมเคลื่อนย้ายอุปกรณ์ : ขนย้ายอุปกรณ์จัดเก็บข้อมูลที่จำเป็น - ทีมดับเพลิง : ดับเพลิงเบื้องต้น เปิด/ปิด ระบบดับเพลิงอัตโนมัติ - ทีมตรวจนับ/ปฐมพยาบาล : นับจำนวน เจ้าหน้าที่ และปฐมพยาบาลเบื้องต้น, ประชาสัมพันธ์	ทีมงานทุกคน
7	อำนวยความสะดวกการหนีไฟ ตรวจสอบการตกค้าง ได้รับบาดเจ็บ ของ ข้าราชการ ลูกจ้างทั้งหมด	ทุกทีม
8	ตรวจรายชื่อเจ้าหน้าที่ทั้งหมด	ทีมตรวจนับ
9	แจ้งให้ทุกคนทราบว่าเหตุการณ์ได้สงบแล้วสามารถกลับเข้าอาคารได้	ผอ.บด.
10	จัดการประชุมคณะกรรมการฯ และสรุปผลการซ้อม	ทุกทีม

ภาคผนวก ค
หน่วยงานที่เกี่ยวข้องในกรณีเกิดเหตุฉุกเฉินเพลิงไหม้

ตารางที่ 12 ข้อมูลติดต่อของหน่วยงานภายใน

ชื่อหน่วยงาน	ที่อยู่	การติดต่อ
เลขานุการกรม	ชั้น 6 อาคาร 50 ปีอุตุนิยมวิทยา	โทรศัพท์ 0 2399 4021
กลุ่มบริหารพัสดุ ลก.	อาคารกลุ่มบริหารพัสดุ ลก.	โทรศัพท์ 0 2393 5615
เจ้าหน้าที่รักษาความปลอดภัย (รปภ.)		โทรศัพท์ 0 2399 4566, 0 2399 4568-74 ต่อ 6399 ,6251

ตารางที่ 13 ข้อมูลติดต่อของหน่วยงานภายนอก

ชื่อหน่วยงาน	ที่อยู่	การติดต่อ
สถานีตำรวจนครบาลบางนา	13 ถนนศรีนครินทร์ เขตประเวศ กรุงเทพฯ 10250	โทรศัพท์. 0-2396-1656-8, 0-2393-7151
สถานีตำรวจภูธรสำโรงเหนือ	77 หมู่ 4 ถ.สุขุมวิท ต.สำโรงเหนือ อ.เมือง จ.สมุทรปราการ 10270	โทรศัพท์ 02-758-4925 Fax : 02-758-4925
สถานีตำรวจนครบาลพระโขนง	2007 ถนนสุขุมวิท แขวงพระโขนงเหนือ เขตวัฒนา กรุงเทพมหานคร	โทรศัพท์. 0-2332-2361-6
ตำรวจดับเพลิงพระโขนง	ถนนสุขุมวิท แขวงพระโขนงเหนือ เขตวัฒนา กรุงเทพมหานคร	โทรศัพท์. 0-2311-4808
โรงพยาบาลทหารเรือ	120 ถ.สรรพาวุธ แขวงบางนา เขตบางนา กทม 10260	โทรศัพท์. 0-2475-2416, 0-2475-2414,0-2173-6548
โรงพยาบาลสมุทรปราการ	71 ถ.จักกะพาก ต.ปากน้ำ อ.เมือง จ.สมุทรปราการ 10270	โทรศัพท์.0-2701-8132-9