

แผนแก้ไขปัญหจากสถานการณ์ ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)



ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร



<https://www.forest.go.th/it>

คำนำ

กรมป่าไม้ มีภารกิจเกี่ยวกับการการอนุรักษ์ สงวน คุ้มครอง ปันฟู ดูแลรักษา ส่งเสริม ทำนุบำรุงป่า และการดำเนินการเกี่ยวกับการป่าไม้ การทำไม้ การเก็บหาของป่า การใช้ประโยชน์ที่ดินป่าไม้ และการอื่นเกี่ยวกับป่าและอุตสาหกรรมไม้ ให้เป็นไปตามระเบียบและกฎหมายที่เกี่ยวข้อง ด้วยกลยุทธ์เสริมสร้างความร่วมมือของประชาชนเป็นหลัก เพื่อเพิ่มมูลค่าทางเศรษฐกิจของประเทศ และพัฒนาคุณภาพชีวิตของประชาชน และภารกิจอื่นตามที่กฎหมายกำหนด ในการดำเนินการดังกล่าว กรมป่าไม้ ได้นำเทคโนโลยีดิจิทัลมาใช้ในการกิจของกรมป่าไม้ เพื่อสนับสนุนการปฏิบัติงานตามภารกิจของกรมป่าไม้ และนโยบายของรัฐบาล โดยมีการพัฒนาอย่างต่อเนื่องตามเทคโนโลยีที่เปลี่ยนแปลงไป เพื่อให้กรมป่าไม้มีระบบเทคโนโลยีดิจิทัลที่เหมาะสมและปลอดภัย ทันสมัย มีประสิทธิภาพและประสิทธิผล ตอบสนองการบูรณาการข้อมูลที่มีประสิทธิภาพและเพิ่มประสิทธิภาพในการบริหารจัดการหน่วยงาน เพื่อให้สามารถบริการแก้ไขปัญหาแก่หน่วยงานภายในกรมป่าไม้และประชาชนได้อย่างทั่วถึง กรมป่าไม้ ใช้งานเทคโนโลยีสารสนเทศมาช่วยสนับสนุนการปฏิบัติงานตามภารกิจ ทำให้การบริหารจัดการงานด้านป่าไม้เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ตระหนักถึงความสำคัญของข้อมูลและระบบสารสนเทศ รวมทั้งระบบเครือข่ายคอมพิวเตอร์ ที่อาจเกิดความเสียหายจากสถานการณ์ฉุกเฉินและ/หรือภัยพิบัติต่างๆ จึงจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ขึ้น เพื่อใช้เป็นกรอบแนวทางในการดูแลรักษา และป้องกันปัญหาอันอาจส่งผลกระทบต่อฐานข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ต่อเชื่อม รวมทั้งระบบเครือข่ายคอมพิวเตอร์ของกรมป่าไม้

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร กรมป่าไม้

เมษายน ๒๕๖๘

สารบัญ

หน้า

๑. บทนำ.....	๑
๒. วัตถุประสงค์ (Objective).....	๑
๓. การวิเคราะห์ความเสี่ยง.....	๒
๔. ขอบเขตการดำเนินงานของแผนแก้ไขปัญหจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ.....	๓
๕. ผู้รับผิดชอบและหน้าที่ของทีมแก้ไขปัญหจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ.....	๕
๖. แผนแก้ไขปัญหจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ	
(๑) กรณีเกิดอัคคีภัย.....	๘
(๒) กรณีเกิดแผ่นดินไหว.....	๑๑
(๓) กรณีไฟฟ้าขัดข้อง.....	๑๒
(๔) กรณีโจรกรรม.....	๑๓
(๕) กรณีติดไวรัส หรือ Malware.....	๑๔
(๖) กรณีการเชื่อมโยงเครือข่ายล้มเหลว.....	๑๕
(๗) กรณีป้องกันผู้บุกรุกล้มเหลว.....	๑๖
๗. การติดตามและรายงานผล.....	๑๖
๘. การทบทวนแผนแก้ไขปัญหจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ.....	๑๖

สารบัญภาพ

หน้า

รูปที่ ๑	ทีมแก้ปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ.....	๕
รูปที่ ๒	กรณีเกิดอัคคีภัย (ขณะมีผู้ปฏิบัติงานอยู่).....	๙
รูปที่ ๓	กรณีเกิดอัคคีภัย (ขณะไม่มีผู้ปฏิบัติงาน).....	๑๐
รูปที่ ๔	กรณีเกิดแผ่นดินไหว.....	๑๑
รูปที่ ๕	กรณีไฟฟ้าขัดข้อง.....	๑๒
รูปที่ ๖	กรณีโจรกรรม.....	๑๓
รูปที่ ๗	กรณีติดไวรัสหรือ Malware.....	๑๔
รูปที่ ๘	กรณีการเชื่อมโยงเครือข่ายล้มเหลว.....	๑๕
รูปที่ ๙	กรณีป้องกันผู้บุกรุกล้มเหลว.....	๑๖

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan)

๑. บทนำ

ปัจจุบัน หน่วยงานทั้งภาครัฐและเอกชนมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการเปลี่ยนแปลงด้านเทคโนโลยีสารสนเทศที่มีการเปลี่ยนแปลงอย่างต่อเนื่อง จึงต้องมีการวางแผนสำหรับการจัดการ ฝ่าละออง และดูแลรักษาฐานข้อมูลและระบบสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการเผชิญหน้ากับสถานการณ์ที่จะเกิดขึ้นได้ทันทั่วทั้งที่ตลอดเวลา

กรมป่าไม้ ได้พัฒนาระบบเครือข่ายทั้งภายในและภายนอก เพื่อใช้ในการเชื่อมโยงข้อมูล และยังมี การพัฒนาระบบงานต่างๆ สำหรับใช้ในการบริหารจัดการ การปฏิบัติงาน และเผยแพร่ประชาสัมพันธ์ ดังนั้น เพื่อให้สามารถใช้งานเครือข่ายและระบบงานต่างๆ ได้อย่างต่อเนื่อง ทั้งนี้ อาจเกิดความเสียหายจากภัยพิบัติตามธรรมชาติ การโจมตีจากบุคคล จากปัญหาระบบไฟฟ้า หรือปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการทำงานของกรมป่าไม้ ดังนั้น เพื่อป้องกันและแก้ไขปัญหาที่อาจเกิดขึ้น จึงมีความจำเป็นที่จะต้องมีการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT contingency Plan) เพื่อรับมือกับสถานการณ์ต่างๆ ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศได้อย่างเหมาะสมและมีประสิทธิภาพ

ปัจจุบัน มีภัยพิบัติใหม่ๆ เกิดขึ้นมากมาย กรมป่าไม้ ได้ตระหนักถึงความสำคัญของความเสียหายที่อาจเกิดขึ้นได้กับระบบเทคโนโลยีสารสนเทศ จึงได้ทบทวนปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) เพื่อให้พร้อมต่อสภาวะวิกฤติและสามารถรองรับภัยพิบัติต่างๆ ที่อาจเกิดขึ้นได้

๒. วัตถุประสงค์

๒.๑ เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและระบบสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒.๒ เพื่อให้สามารถรับมือกับเหตุการณ์ที่ทำให้ระบบงานสำคัญหยุดชะงักได้อย่างมีประสิทธิภาพรวมทั้งสามารถกู้คืนระบบงานเพื่อให้กลับคืนมาภายในระยะเวลาที่กำหนดไว้

๒.๓ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันทั่วทั้งที่

๒.๔ เพื่อลดความเสียหายที่อาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๒.๕ เพื่อสร้างความมั่นใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและระบบสารสนเทศ

๒.๖ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓. การวิเคราะห์ความเสี่ยง

เนื่องจากการกิจของกรมป่าไม้มีความสำคัญ เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ มีความมั่นคงปลอดภัยสามารถสนับสนุนการปฏิบัติงานของกรมป่าไม้ให้เกิดประโยชน์สูงสุด

กรมป่าไม้จึงได้วิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ แบ่งได้ดังนี้

๑. ความเสี่ยงทางด้านกายภาพและสิ่งแวดล้อม หมายถึง ความเสี่ยงที่เกิดจากภัยคุกคามทางธรรมชาติ สิ่งที่มีมนุษย์กระทำขึ้น ลักษณะทางกายภาพสิ่งแวดล้อมทั้งโดยเจตนาและไม่เจตนา เช่น วัตถุภัย น้ำท่วม ไฟป่า เพลิงไหม้ กระแสไฟฟ้าขัดข้อง การเข้า-ออก ห้องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วงโดยไม่ได้รับอนุญาต เป็นต้น

๒. ความเสี่ยงด้านบุคลากร หมายถึง ความเสี่ยงที่เกิดจากบุคลากรทั้งภายในและภายนอกที่เกี่ยวข้องกับการดำเนินงานด้านเทคโนโลยีสารสนเทศ รวมถึงการวางแผน การมอบหมายหน้าที่ การปฏิบัติงาน การตรวจสอบ และสิทธิของบุคลากร/คณะทำงานที่มีส่วนเกี่ยวข้องกับการดำเนินการทุกฝ่ายอย่างละเอียดถี่ถ้วน เพื่อให้บุคลากรมีความรู้ ความเข้าใจในการใช้งานการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓. ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ หมายถึง ความเสี่ยงที่เกิดจากความผิดพลาดของโหนดของอุปกรณ์ ตลอดจนการเคลื่อนย้ายอุปกรณ์โดยไม่ได้รับอนุญาต การติดตั้งอุปกรณ์ในพื้นที่ไม่เหมาะสม การถูกภัยคุกคามจากภัยต่างๆ เช่น ไวรัสคอมพิวเตอร์ เป็นต้น

๔. ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์ หมายถึง ความเสี่ยงที่เกิดจากระบบงานโปรแกรมต่างๆ ที่ได้จัดทำและพัฒนาขึ้น รวมถึงโปรแกรมประยุกต์อื่นๆ ที่ใช้ประกอบการใช้งาน เช่น การใช้โปรแกรมที่ไม่มีลิขสิทธิ์ถูกต้อง ความผิดพลาดที่เกิดขึ้นจากการเขียนโปรแกรม โปรแกรมที่พัฒนาขึ้นมาแล้วมีช่องโหว่ทำให้ผู้บุกรุกเข้ามาแก้ไขเปลี่ยนแปลงคำสั่งและการถูกผู้ไม่ประสงค์ดีทำลายระบบ (Hacker) การพัฒนาระบบสารสนเทศที่ไม่มีการกำหนดสิทธิ์การเข้าถึงระบบ เป็นต้น

๕. ความเสี่ยงด้านระบบเครือข่าย หมายถึง ความเสี่ยงหรือภัยต่างๆ ที่เกิดขึ้นกับระบบเครือข่ายขององค์กร ทั้งเครือข่ายอินทราเน็ต (Intranet) และเครือข่ายอินเทอร์เน็ต (Internet) ซึ่งรวมถึงภัยที่มีสาเหตุมาจากภายในระบบเครือข่ายเอง ได้แก่ ความเสี่ยงด้านกายภาพ ความเสี่ยงด้านระบบปฏิบัติการ ความเสี่ยงระบบแม่ข่าย เป็นต้น และความเสี่ยงจากภัยภายนอก ได้แก่ การบุกรุกระบบเครือข่าย และความเสี่ยงจากภัยคุกคามต่างๆ

๖. ความเสี่ยงด้านข้อมูล หมายถึง ความเสี่ยงที่เกิดจากข้อมูล และฐานข้อมูลในระบบสารสนเทศ อันอาจจะก่อให้เกิดความเสียหาย ได้แก่ การทำลายข้อมูล การแก้ไขข้อมูลโดยไม่ได้รับอนุญาต การโจรกรรมข้อมูลที่สำคัญ เป็นต้น

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศของกรมป่าไม้ ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมป่าไม้ มีประสิทธิภาพ และมีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแล

รักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๔. ขอบเขตการดำเนินงานของแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ในการใช้งานแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ มีขอบเขตที่กำหนดไว้ดังนี้

๑. แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติครอบคลุมเฉพาะเหตุการณ์ดังต่อไปนี้

๑.๑ ความเสี่ยงด้านกายภาพและสิ่งแวดล้อม

- กรณีเกิดอัคคีภัย วาตภัย อุทกภัย ไฟฟ้า น้ำท่วม แผ่นดินไหว วินาศภัย ก่อการร้าย
- กรณีกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ แรงดันไฟฟ้าไม่คงที่
- กรณีคอมพิวเตอร์ถูกโจรกรรม
- กรณีแมลงหรือสัตว์กัดแทะสายไฟฟ้าหรือสายสัญญาณ
- กรณีการแพร่ระบาดของโรคติดต่อ เช่น COVID-๑๙
- กรณีแผ่นดินไหว

๑.๒ ความเสี่ยงด้านบุคลากร

- กรณีบุคลากรสายงานคอมพิวเตอร์ขาดความรู้และทักษะในการปฏิบัติงาน
- กรณีเจ้าหน้าที่ใช้คอมพิวเตอร์หรือเครือข่ายผิดวัตถุประสงค์

๑.๓ ความเสี่ยงด้านอุปกรณ์เทคโนโลยีสารสนเทศ

- กรณีการใช้งานระบบ Web Conference
- กรณีการติดไวรัสคอมพิวเตอร์หรือ Malware

๑.๔ ความเสี่ยงด้านโปรแกรมคอมพิวเตอร์

- กรณีการพัฒนาระบบสารสนเทศถูกเข้าถึงโดยไม่ได้รับอนุญาต
- กรณีการละเมิดลิขสิทธิ์โปรแกรม
- กรณีระบบงานสารสนเทศไม่ตอบสนองความต้องการของผู้ใช้งาน

๑.๕ ความเสี่ยงด้านระบบเครือข่าย

- กรณีการเชื่อมโยงเครือข่ายล้มเหลว
- กรณีไฟไหม้เครื่องแม่ข่ายหรือภายในห้อง Data Center
- กรณีระบบไฟฟ้าห้อง Data Center ไม่เสถียร
- กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่ายไม่สามารถให้บริการได้อย่างต่อเนื่อง
- กรณีเกิดการโจมตี (Hack) ระบบเครือข่าย
- กรณีระบบงานสารสนเทศของกรมไม่สามารถให้บริการได้

๑.๖ ความเสี่ยงด้านข้อมูล

- กรณีข้อมูลและสารสนเทศไม่ถูกต้องและเป็นปัจจุบัน
- กรณีการสำรองและกู้คืนข้อมูลล้มเหลว
- กรณีเกิดการรั่วไหลจากการเปลี่ยนมือผู้ใช้
- กรณีการประมวลผลและเปิดเผยข้อมูลส่วนบุคคลไม่เป็นไปตามพระราชบัญญัติคุ้มครอง

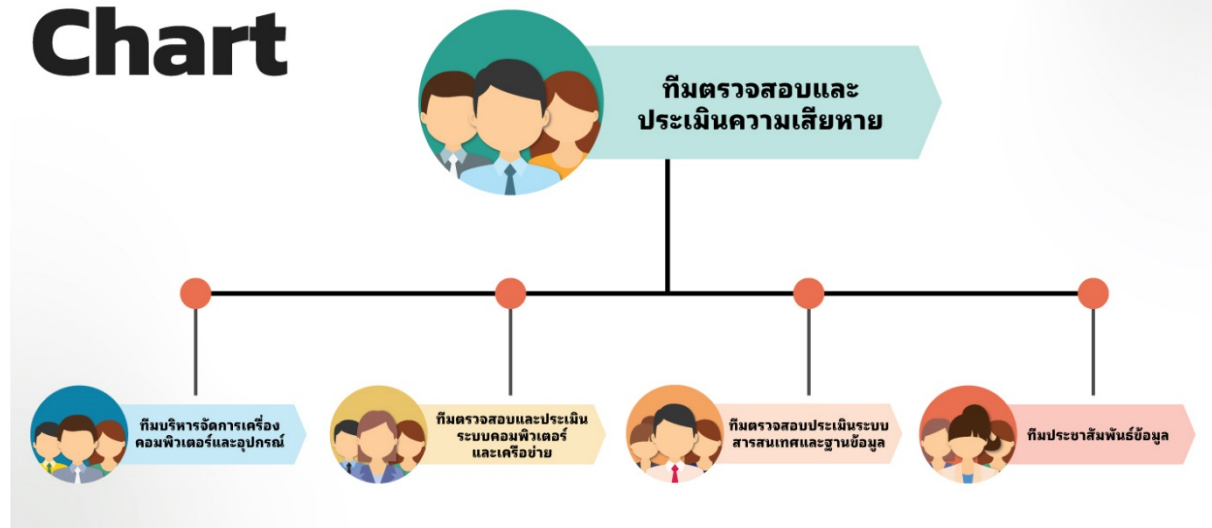
ข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒

๒. ระบบงานที่สำคัญที่จะต้องดำเนินการ จำนวน ๑๕ ระบบ ประกอบด้วย
- (๑) ระบบบริหารจัดการเรื่องร้องเรียน
 - (๒) ระบบติดตามการบุกรุกทำลายป่าและควบคุมไฟป่า
 - (๓) ระบบฐานข้อมูลเชิงแผนที่
 - (๔) ระบบการออกใบอนุญาตและควบคุมการเคลื่อนที่ไม่ใช่เพื่อประกอบการส่งออกปศุสัตว์
 - (๕) ระบบสารบรรณอิเล็กทรอนิกส์
 - (๖) ระบบเว็บไซต์กรมป่าไม้
 - (๗) ระบบภูมิศาสตร์สารสนเทศเพื่อการบริหาร (GIS)
 - (๘) ระบบปฏิบัติการค้นหาพื้นที่บุกรุกด้วยโปรแกรมคอมพิวเตอร์ (ระบบพิทักษ์ไพร)
 - (๙) ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS)
 - (๑๐) ระบบแผนงาน งบประมาณ และการติดตามประเมินผล
 - (๑๑) ระบบรับเงินกลางด้วยอิเล็กทรอนิกส์
 - (๑๒) ระบบขออนุญาตอุตสาหกรรมไม้ (e - Permit) กรมป่าไม้
 - (๑๓) ระบบการแลกเปลี่ยนข้อมูลอิเล็กทรอนิกส์ตามระบบ NSW สำหรับการนำเข้า ส่งออกสินค้าไม้ และผลิตภัณฑ์จากไม้ (e - Payment)
 - (๑๔) ระบบบริหารข้อมูลการเบิกจ่ายเงิน กรมป่าไม้
 - (๑๕) ระบบทะเบียนครุภัณฑ์ กรมป่าไม้
๓. ระยะเวลาที่ไม่เหมาะสมให้บริการระบบงานสำคัญไม่เกิน ๒๔ ชั่วโมง
๔. เจาะระบบ หมายถึง เหตุการณ์ที่ระบบถูกเปลี่ยนแปลง เครื่องคอมพิวเตอร์แม่ข่ายเสียหาย อันเกิดจากผู้ไม่ประสงค์ดีเข้ามาทำลาย
๕. เครื่องคอมพิวเตอร์แม่ข่ายและเครือข่ายสื่อสารขัดข้อง หมายถึง เหตุการณ์ที่เครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายสื่อสาร และอุปกรณ์อื่นๆ ที่เกี่ยวข้อง ไม่สามารถใช้งานได้
๖. ไฟดับ หมายถึง เหตุการณ์ที่อุปกรณ์ในห้อง Data Center ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารใช้งานไม่ได้
๗. ไฟไหม้ หมายถึง เหตุการณ์ที่ทำลายหรือก่อให้เกิดความเสียหายต่อห้อง Data Center โดยจะต้องดำเนินการปรับปรุง/แก้ไขห้อง Data Center และจัดซื้อจัดหาอุปกรณ์ใหม่
๘. น้ำท่วม หมายถึง ภัยที่เกิดขึ้นเนื่องจากมีน้ำเป็นสาเหตุ อาจจะเป็นน้ำท่วม น้ำป่า หรืออื่นๆ โดยปกติ อุทกภัยเกิดจากฝนตกหนักต่อเนื่องกันเป็นระยะเวลานาน บางครั้งทำให้เกิดแผ่นดินถล่ม อาจมีสาเหตุจากพายุหมุนเขตร้อนลมมรสุมมีกำลังแรง ร่องความกดอากาศต่ำที่มีกำลังแรง ร่องความกดอากาศต่ำที่มีกำลังแรง อากาศแปรปรวน น้ำทะเลหนุน แผ่นดินไหว เขื่อนพัง ทำให้เกิดอุทกภัยได้เสมอ
๙. แผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้ ให้ความสำคัญกับทีมแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ดังนั้น บุคลากรส่วนใหญ่หรือทั้งหมดจะต้องอยู่ครบครันหรือมอบหมายผู้เกี่ยวข้อง เพื่อให้การแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัตินี้มีประสิทธิภาพ
๑๐. หากเกิดภัยพิบัติในช่วงนอกเวลาราชการหรือในวันหยุดราชการ แผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติอาจไม่สามารถปฏิบัติได้หรืออาจไม่สัมฤทธิ์ผลเท่าที่ควร
๑๑. แต่ละทีมย่อยของทีมแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ สามารถใช้บุคลากรร่วมกันได้

๕. ผู้รับผิดชอบและหน้าที่ของทีมแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้แต่งตั้งทีมงานในการแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่างๆ ที่อาจจะเกิดขึ้นกับระบบสารสนเทศของกรมป่าไม้ ประกอบไปด้วยทีมย่อยที่เกี่ยวข้อง ดังนี้

Organization Chart



รูปที่ ๑ ทีมแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

ทีมตรวจสอบและประเมินความเสี่ยง

หัวหน้าทีม : ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร

ทีมงาน : ผู้อำนวยการส่วนอำนวยการ

ผู้อำนวยการส่วนบริหารเทคโนโลยีสารสนเทศและการสื่อสาร

ผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย

ผู้อำนวยการส่วนระบบสารสนเทศและภูมิสารสนเทศ

หน้าที่รับผิดชอบ

๑. ทำหน้าที่ควบคุม กำหนด สั่งการ คณะทำงานที่เกี่ยวข้อง ดำเนินการตามขั้นตอนที่กำหนด

๒. รายงานปัญหา และวิธีการแก้ไขปัญหที่เกิดขึ้นให้ผู้บริหารรับทราบ

ทีมบริหารจัดการเครื่องคอมพิวเตอร์และอุปกรณ์

หัวหน้าทีม : ผู้อำนวยการส่วนอำนวยการ

ทีมงาน : นายอภิสิทธิ์ ปะสาวะเท

นางสาวชนันท์เนตร์ ปุณณะนา

นางณภาพัช แจ็กแป้น

นายวิบูลย์ชัย ปาสองห้อง

นางสาวณัฐกฤตา ธัญญกิจกุล

หน้าที่รับผิดชอบ

๑. ประสานและจัดการงานทั่วไปที่เกี่ยวกับการจัดหาอุปกรณ์ที่เกี่ยวข้องกับการปฏิบัติงาน
๒. ช่วยดำเนินการด้านการงบประมาณในการจัดหาอุปกรณ์และซอฟต์แวร์ต่างๆ ที่จำเป็นต่อการกู้คืนระบบ
๓. หากมีอุปกรณ์เสียหาย จัดทำรายละเอียดเพื่อของบประมาณในการซ่อมแซมหรือจัดหาใหม่
๔. ช่วยจัดทำเอกสารต่างๆ ที่เกี่ยวข้อง
๕. ให้ความช่วยเหลือทีมอื่นๆ

ทีมตรวจสอบและประเมินผลระบบคอมพิวเตอร์และเครือข่าย

หัวหน้าทีม : ผู้อำนวยการส่วนระบบคอมพิวเตอร์และเครือข่าย

ทีมงาน : นายณภัทร ดลเสถียร

นายกิตติทัศน์ สุริยา

นางสาวปริยานุช กิตติสิทธิโชค

นางสาวธันชนก ชฎามหากุล

หน้าที่รับผิดชอบ

๑.๑ จัดการระบบคอมพิวเตอร์และความปลอดภัย

- (๑) ประสานสำนักบริหารกลาง เพื่อตรวจสอบความเสียหายของสถานที่ และร่วมประเมินความเสียหาย
- (๒) ดูแลการซ่อมแซมศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ชั้น ๓ อาคารเทียมนคมกฤต ที่ได้รับความเสียหาย
- (๓) ตรวจสอบความพร้อมและการทำงานของอุปกรณ์สำรองไฟฟ้า (UPS) และอุปกรณ์เครื่องปั่นไฟ (Generator)
- (๔) รักษาความปลอดภัยบริเวณที่ต้องมีการควบคุมต่างๆ

๑.๒ ตรวจสอบและประเมินระบบคอมพิวเตอร์

- (๑) ตรวจสอบความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ โดยมุ่งเน้นที่เครื่องคอมพิวเตอร์แม่ข่ายหลักของกรมฯ พร้อมประเมินความเสียหาย วิธีการแก้ไข และระยะเวลาที่ระบบจะสามารถใช้งานได้ปกติ
- (๒) จัดทำสรุปผลการตรวจสอบความเสียหายและเสนอแนวทางการดำเนินงานในแต่ละด้าน เสนอผู้บริหาร และผู้ที่เกี่ยวข้องดำเนินการแก้ไข

๑.๓ ตรวจสอบและประเมินระบบเครือข่ายสื่อสาร

- (๑) ประเมิน ตรวจสอบ ความเสียหายที่เกิดขึ้น
- (๒) ให้ข้อมูลที่จำเป็นเพื่อจัดหาอุปกรณ์ที่สำคัญ เพื่อให้ทีมบริหารจัดการเครื่องคอมพิวเตอร์และอุปกรณ์ ดำเนินการจัดหาอุปกรณ์
- (๓) ประเมินระยะเวลาในการซ่อมแซมหรือเปลี่ยน ทดแทนทรัพย์สินที่เกิดการเสียหาย
- (๔) ติดตั้งระบบคอมพิวเตอร์และระบบเครือข่ายให้สามารถใช้งานได้ดังเดิม
- (๕) ดูแลการกู้คืนระบบคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานให้สามารถใช้งานได้

ทีมตรวจสอบประเมินระบบสารสนเทศและฐานข้อมูล

หัวหน้าทีม : ผู้อำนวยการส่วนระบบสารสนเทศและภูมิสารสนเทศ

ทีมงาน : นายวีร์ ศรีทิพโพธิ์

นางสาวชนัญจิตต์ เหลี่ยมสุวรรณ

นายดำรงศักดิ์ ธนินบุญ

นางสาวกนกพรรณ สงเคราะห์ราษฎร์

นายภาคิน กรณ์ชนกฤติ

นายเพชร วรรณศุภ

หน้าที่รับผิดชอบ

๑.๑ ตรวจสอบและประเมินระบบงาน

- (๑) ตรวจสอบความเสียหายของระบบงานและระบบสารสนเทศอื่นๆ ที่อยู่ในความรับผิดชอบของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
- (๒) ตรวจสอบความครบถ้วนของระบบงานที่กู้คืน
- (๓) ร่วมมือกับทีมระบบคอมพิวเตอร์และเครือข่าย ในการทดสอบระบบภายหลังจากการกู้คืน
- (๔) ทดสอบระบบงานร่วมกับผู้ใช้งาน

๑.๒ ตรวจสอบและประเมินฐานข้อมูล

- (๑) ตรวจสอบความเสียหายของฐานข้อมูล
- (๒) ตรวจสอบความครบถ้วนของฐานข้อมูล
- (๓) ร่วมมือกับทีมระบบคอมพิวเตอร์และเครือข่าย ในการทดสอบระบบภายหลังจากการกู้คืน

ทีมประชาสัมพันธ์ข้อมูล

หัวหน้าทีม : ผู้อำนวยการส่วนบริหารเทคโนโลยีสารสนเทศและการสื่อสาร

ทีมงาน : นางสาวมนัญญา ลงสุวรรณ

นายถนอม เพ็ญนาลัย

นายวิบูลย์ชัย ปาสองห้อง

หน้าที่รับผิดชอบ

แจ้งรายละเอียด สาเหตุ และระยะเวลาในการแก้ไขปัญหา กรณีไม่สามารถใช้งานระบบคอมพิวเตอร์และเครือข่ายได้ ให้แก่ผู้ใช้งานทั้งส่วนกลางและส่วนภูมิภาคทราบ

๖. แผนแก้ไขปัญหามาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

แผนแก้ไขปัญหามาจากความไม่แน่นอนและภัยพิบัติฉบับนี้ แสดงถึงขั้นตอนในการป้องกันจากเหตุการณ์ภัยพิบัติที่สามารถทำลายหรือก่อให้เกิดความเสียหายอย่างสูงต่อระบบเทคโนโลยีสารสนเทศ ซึ่งอยู่ที่ห้อง Data Center ชั้น ๓ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคารเทียมนคมกฤส กรมป่าไม้ ๖๑ ถ.พหลโยธิน แขวงลาดยาว เขตจตุจักร กรุงเทพฯ ๑๐๙๐๐ โดยรายละเอียดของแผนแก้ไขปัญหามาจากความไม่แน่นอนและภัยพิบัติ (IT Contingency Plan) ที่จัดขึ้นจะกล่าวถึง การเตรียมความพร้อมในด้านต่างๆ ก่อนเกิด ขณะเกิด และหลังเกิดเหตุการณ์ภัยพิบัติต่างๆ กับระบบสารสนเทศของกรมป่าไม้ โดยมีรายละเอียดและวิธีการดังต่อไปนี้

- กรณีเกิดอัคคีภัย

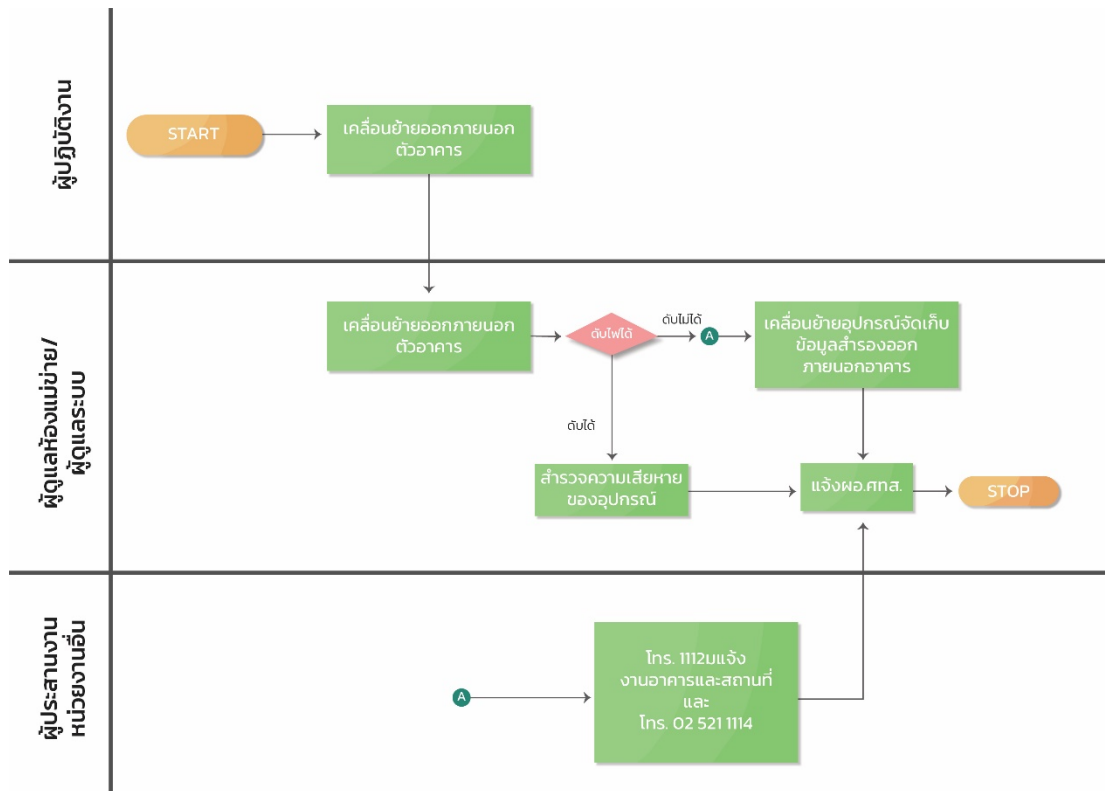
๑) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ทำการดับไฟ

๒) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานอาคารสถานที่ ที่เบอร์ ๕๐๑๑ และโทรแจ้งสถานีดับเพลิง บางเขนที่เบอร์ ๐๒ ๕๒๑ - ๐๓๙๗

๓) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน ปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจสอบไฟและดับไฟอัตโนมัติ

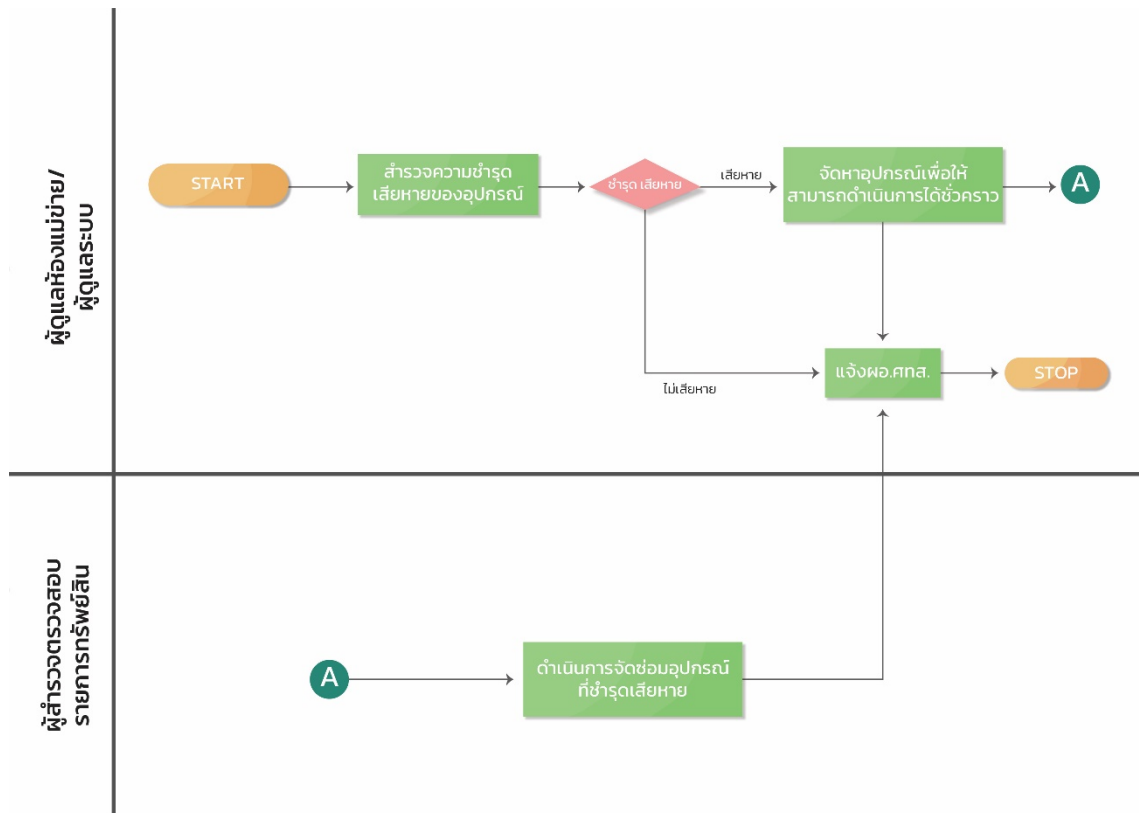
๔) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดอัคคีภัย (ขณะมีผู้ปฏิบัติงานอยู่)



รูปที่ ๒ กรณีเกิดอัคคีภัย (ขณะมีผู้ปฏิบัติงานอยู่)

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดอัคคีภัย (ขณะไม่มีผู้ปฏิบัติงาน)

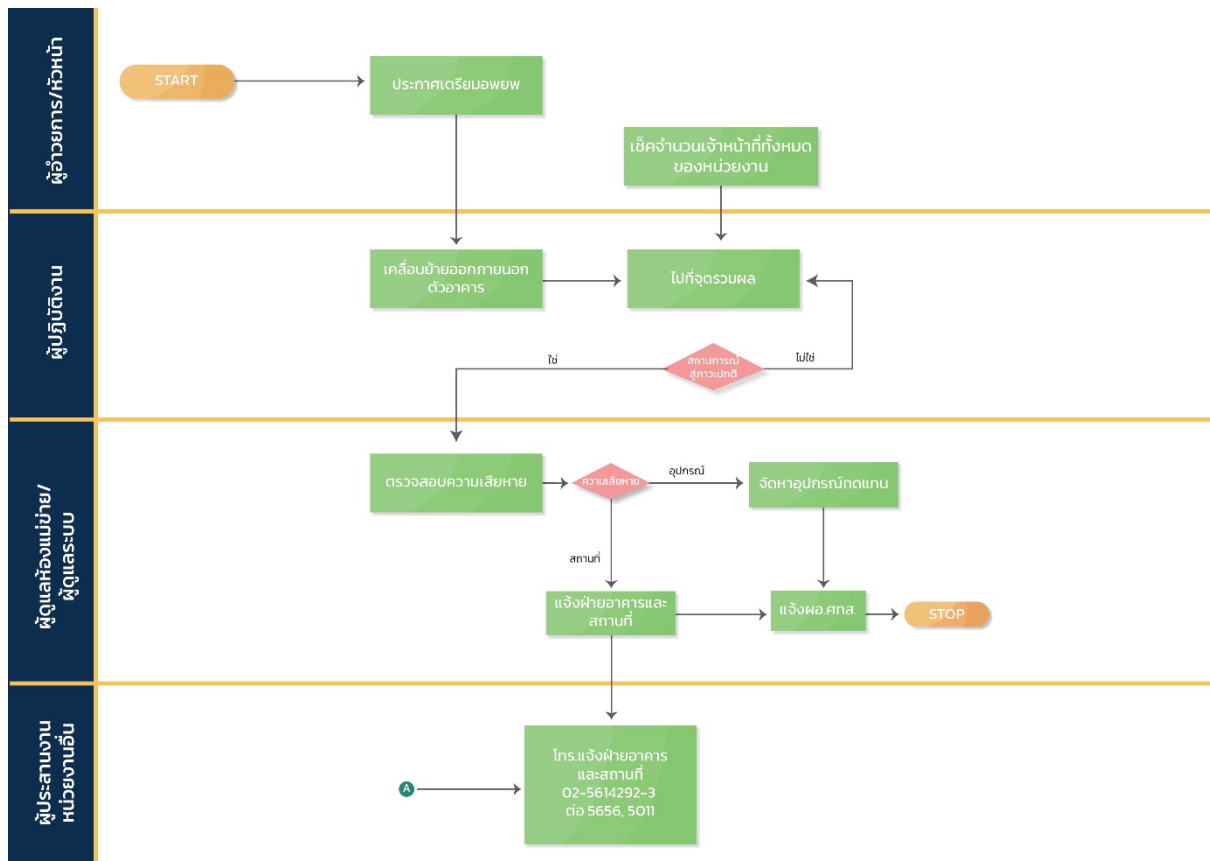


รูปที่ ๓ กรณีเกิดอัคคีภัย (ขณะไม่มีผู้ปฏิบัติงาน)

- กรณีเกิดแผ่นดินไหว

- ๑) ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ๒) ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- ๓) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดแผ่นดินไหว

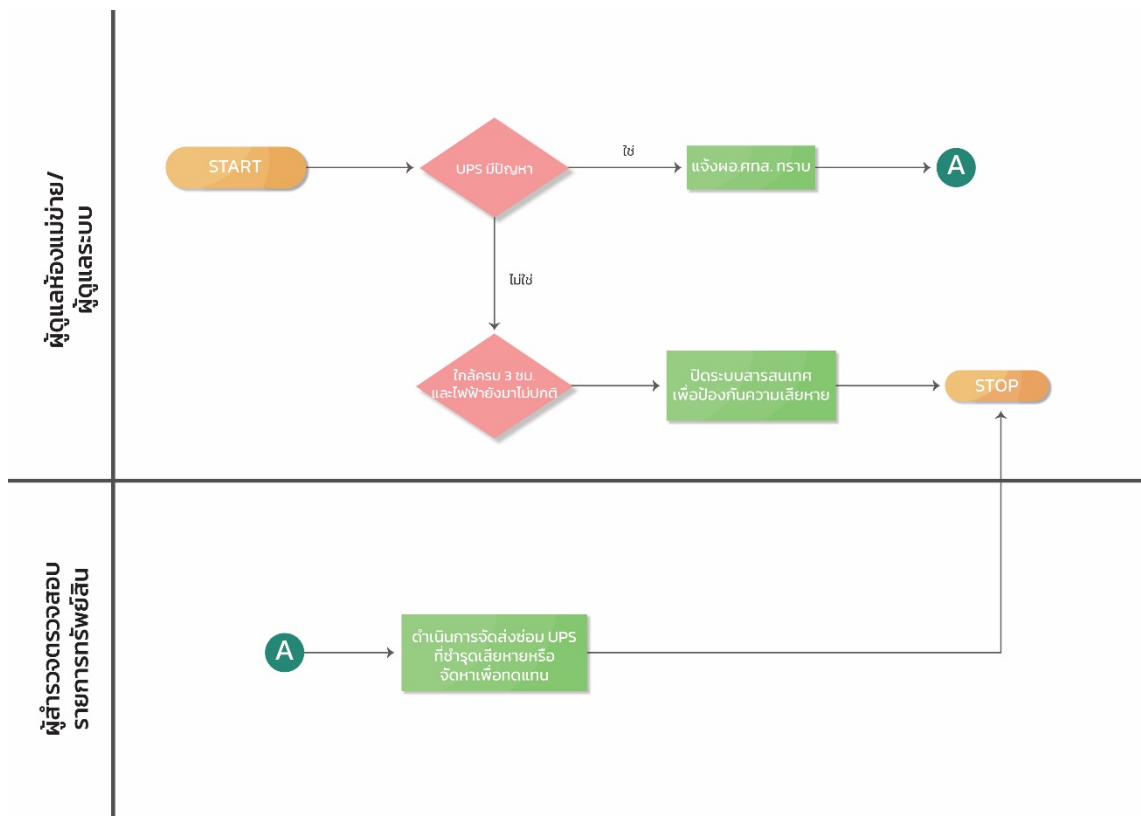


รูปที่ ๔ กรณีเกิดแผ่นดินไหว

- กรณีไฟฟ้าขัดข้อง

- ๑) กรมป่าไม้ มีเครื่อง Generator ที่สามารถปั่นกระแสไฟฟ้าเข้ามาหล่อเลี้ยงอุปกรณ์และระบบในห้อง Data Center
- ๒) ระบบสารสนเทศมีเครื่องสำรองไฟฟ้า (UPS) ซึ่งสามารถสำรองกระแสไฟฟ้าได้
- ๓) ผู้ดูแลระบบดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- ๔) หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟฟ้าขัดข้อง

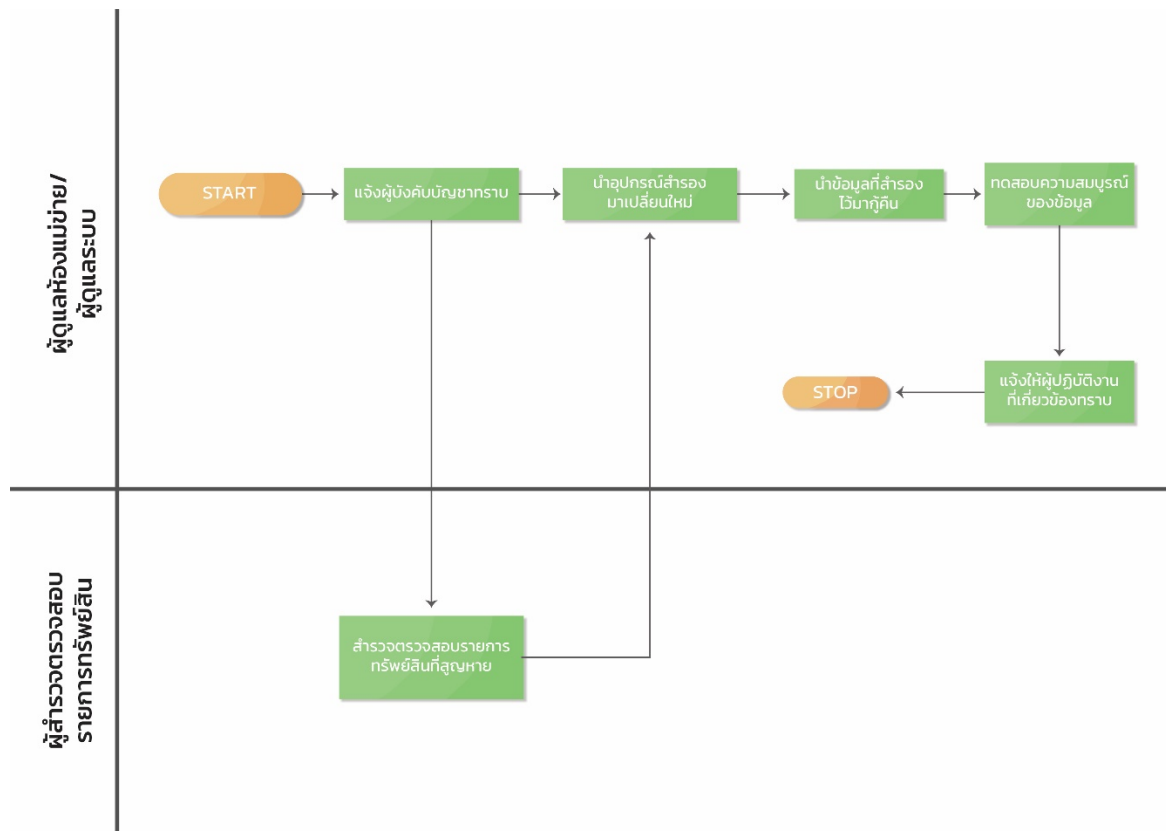


รูปที่ ๕ กรณีไฟฟ้าขัดข้อง

- กรณีโจรกรรม

- ๑) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- ๒) ตรวจสอบรายการทรัพย์สินที่สูญหาย
- ๓) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

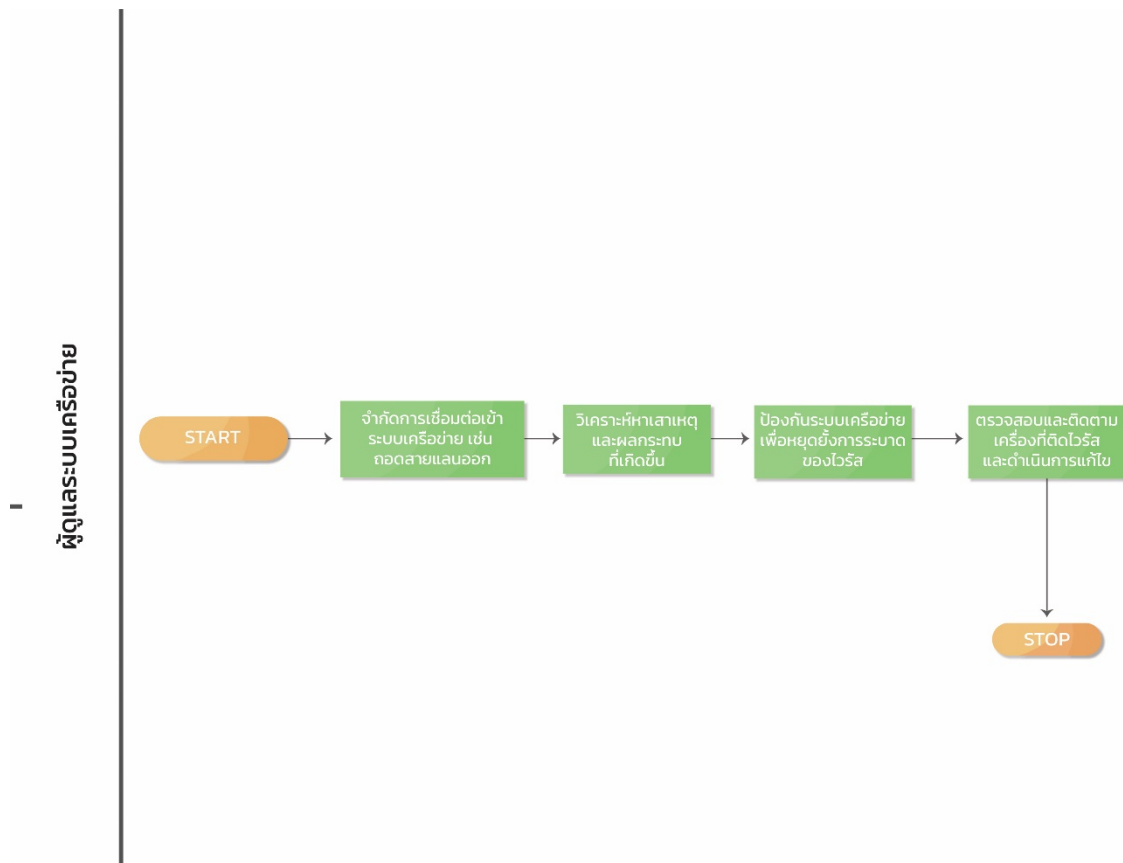


รูปที่ ๖ กรณีโจรกรรม

- กรณีติดไวรัสหรือ Malware

- ๑) กรณีถูกไวรัสหรือ Malware เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมโยงต่อเข้าระบบเครือข่าย
- ๒) ตรวจสอบรายการทรัพย์สินที่สูญหาย
- ๓) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีติดไวรัสหรือ Malware

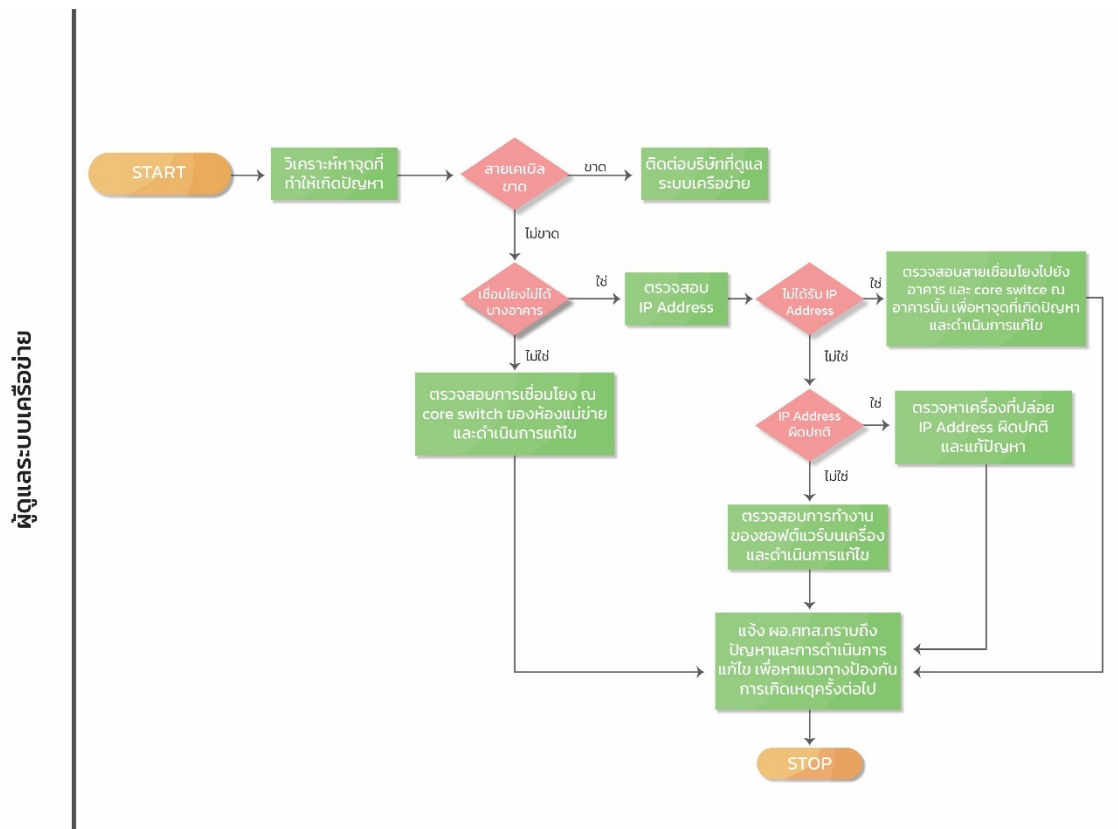


รูปที่ ๗ กรณีติดไวรัสหรือ Malware

- กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- ๑) รับผิดชอบการตรวจสอบหาจุดที่ทำให้เกิดปัญหา
- ๒) หากสายเคเบิลขาด ให้รับผิดชอบบริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิลให้เรียบร้อยโดยเร็ว
- ๓) หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินการเชื่อมโยงเครือข่ายล้มเหลว

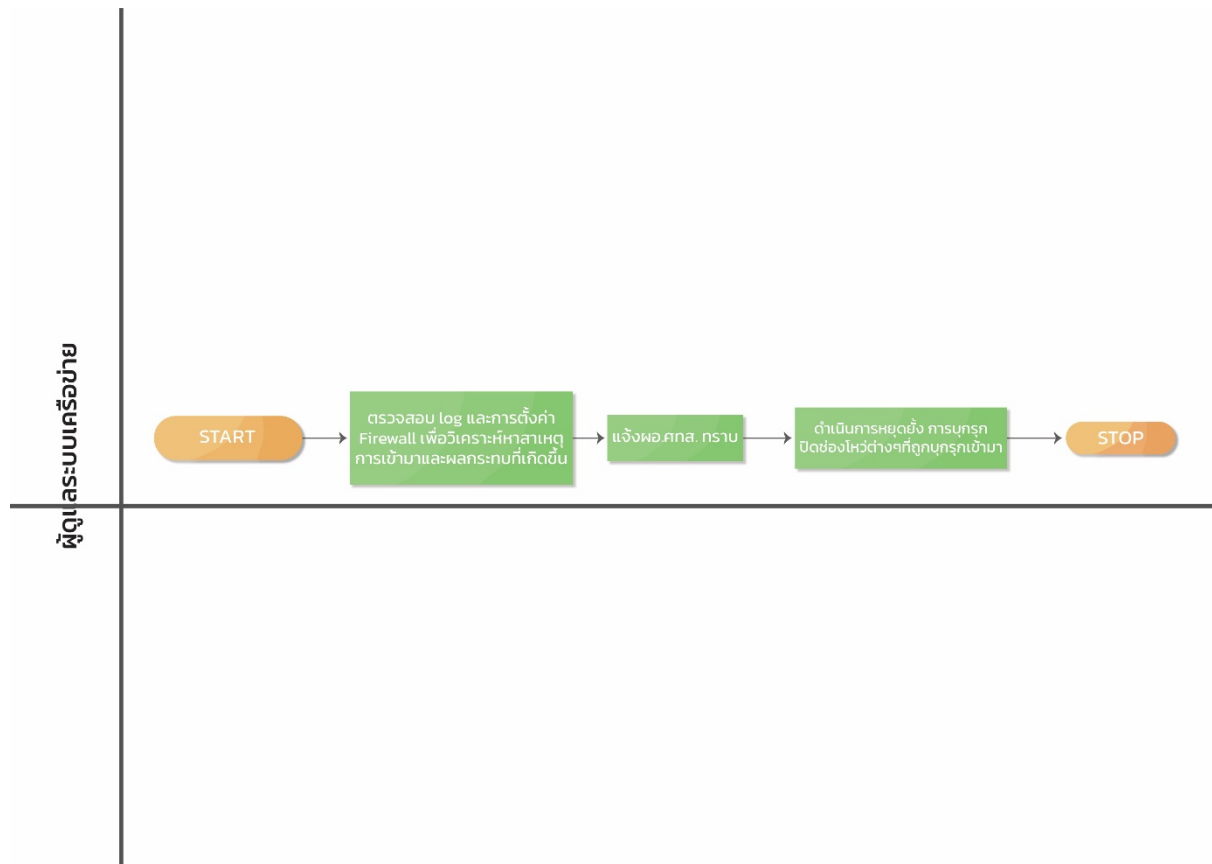


รูปที่ ๘ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- กรณีป้องกันผู้บุกรุกล้มเหลว

- ๑) ผู้ดูแลระบบต้องตรวจสอบหาสาเหตุของการเข้ามาและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่าของ firewall
- ๒) ผู้ดูแลระบบแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารให้ทราบโดยด่วน
- ๓) ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินป้องกันผู้บุกรุกล้มเหลว



รูปที่ ๙ กรณีป้องกันผู้บุกรุกล้มเหลว

๗. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ที่รับผิดชอบรายงานผลการเกิดปัญหา และผลการแก้ไขปัญหาให้ผู้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

๘. การทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฉบับนี้ ต้องได้รับการทบทวนอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจว่าแผนฉบับนี้สามารถรองรับกับสถานการณ์ปัจจุบัน และสามารถนำไปแก้ปัญหาได้จริง เพื่อช่วยแก้ไขปัญหาในกรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติได้อย่างมีประสิทธิภาพ