แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ด้านสารสนเทศ

กรมอู่ทหารเรือ
ปี 2566

สารบัญ

หน้า

๑. หลักการและเหตุผล ๑
๒. วัตถุประสงค์ ๑
๓. ทีมงานบริหารแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศ ของกรมอู่ทหารเรือ ๒
๔. การวิเคราะห์ความเสี่ยง ๓
๕. ลักษณะรายละเอียดของความเสี่ยง ๔
๖. การประมาณความเสี่ยง ๖
๗. การจัดการความเสี่ยง ๑๐
๘. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ ๑๒

แผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน
ด้านระบบเทคโนโลยีสารสนเทศของกรมอู่ทหารเรือ
(IT Contingency Plan)

๑. หลักการและเหตุผล

ปัจจุบัน หน่วยงานราชการมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กร และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา

กรมอู่ทหารเรือ ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการประชาชนได้รับความสะดวกมากยิ่งขึ้น แต่ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจจะได้รับความเสียหายจากการถูกโจมตีจากไวรัสหรือมัลแวร์คอมพิวเตอร์ บุคลากร ระบบไฟฟ้าขัดข้อง อัคคีภัย หรือปัจจัยทั้งภายในและภายนอก รูปแบบต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงานจนไม่สามารถปฏิบัติงานได้อย่างต่อเนื่อง ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องจัดทำแผนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินด้านระบบเทคโนโลยีสารสนเทศที่อาจเกิดขึ้น

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลและระบบสารสนเทศของกรมอู่ทหารเรือ

๖. เพื่อช่วยเพิ่มประสิทธิภาพการตัดสินใจ โดยคำนึงถึงปัจจัยเสี่ยงด้านต่างๆ ที่จะมีผลกระทบกับการดำเนินงาน แล้วพิจารณาหาแนวทางในการป้องกันหรือจัดการปัจจัยเสี่ยง ก่อนเริ่มปฏิบัติงานหรือดำเนินการตามแผนปฏิบัติงานของหน่วย

๓.ขอบเขตการดำเนินการ

การจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศของกรมอู่ทหารเรือ พิจารณาดำเนินการจากการวิเคราะห์ความเสี่ยงที่เกิดจากผู้ปฏิบัติงาน ทางเทคนิค และทางกายภาพ ที่จะส่งผลกระทบ

ต่อระบบสารสนเทศของกรมอู่ทหารเรือ และนำความเสี่ยงที่จะเกิดขึ้นมาประเมินความรุนแรงของเหตุการณ์หรือภัยพิบัติ พร้อมจัดทำแนวคิดในการแก้ไขเหตุการณ์ตั้งแต่ขั้นเกิดเหตุจนถึงขั้นการกู้คืนระบบสารสนเทศให้สามารถใช้งานได้เช่นเดิม

๓. ทีมงานบริหารแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินด้านระบบสารสนเทศของกรมอู่ทหารเรือ

เพื่อให้แผนเตรียมพร้อมกรณีเกิดเหตุฉุกเฉินด้านสารสนเทศ (BCP) ของกรมอู่ทหารเรือ สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล จะต้องจัดตั้งทีมงานบริหารความเสี่ยง (CP TEAM) ขึ้น โดย CP TEAM ประกอบด้วยโครงสร้าง และหน้าที่ดังนี้

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมอู่ทหารเรือ (CIO) มีหน้าที่ บริหารงานด้านสารสนเทศภายในกรมอู่ทหารเรือ ให้สามารถใช้งานระบบคอมพิวเตอร์และระบบสารสนเทศหลักของ ทร. รวมทั้งระบบอินเทอร์เน็ต ได้อย่างมีประสิทธิภาพและมั่นคงปลอดภัย

๒. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศของกรมอู่ทหารเรือ มีหน้าที่ดำเนินการรักษาความมั่นคงปลอดภัย วิเคราะห์และประเมินความเสี่ยงของระบบที่ให้บริการ ตลอดจนกำหนดแนวทางและมาตรการรักษาความมั่นคงปลอดภัย ตรวจสอบและวิเคราะห์สาเหตุของความเสียหายที่เกิดขึ้นจากการโจมตีทางไซเบอร์ พร้อมทั้งให้คำแนะนำในแก้ไขปัญหาของระบบที่เกิดจากการโจมตีทางไซเบอร์

๓. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศของกรมอู่ทหารเรือ มีหน้าที่ ให้บริการติดตั้งระบบเครื่องคอมพิวเตอร์แม่ข่าย คอมพิวเตอร์ลูกข่าย เครื่องพิมพ์ อุปกรณ์เครือข่าย รวมตรวจสอบ ควบคุมการทำงาน สำรองและกู้คืนข้อมูลระบบสารสนเทศในระดับคอมพิวเตอร์แม่ข่ายได้

๔. หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ด้านซอฟท์แวร์ระบบสารสนเทศของกรมอู่ทหารเรือ มีหน้าที่พัฒนา บำรุงรักษา วิเคราะห์ ปรับปรุง แก้ไขปัญหาระบบสารสนเทศที่ติดตั้งภายในหน่วย

โดยทุกตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในส่วนที่รับผิดชอบให้สามารถบริหารแผนฯ และกลับสู่สภาวะปกติได้โดยเร็ว ตามบทบาทหน้าที่ที่กำหนดไว้ของทีมบริหารความเสี่ยง (CP TEAM) และในกรณีที่บุคลากรไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบทาหน้าที่ในหน้าที่ของบุคลากรหลัก ปรากฏดังในตาราง

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ-สกุล	**หมายเลขโทรศัพท์**		**ชื่อ-สกุล**	**หมายเลขโทรศัพท์**
รอง จก.อร.	๗๘๐๐๕	ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมอู่ทหารเรือ		
หน.กรรมวิธีข้อมูลและสถิติ กจก.อร.	๗๘๐๙๖	หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ		

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ-สกุล	หมายเลขโทรศัพท์		ชื่อ-สกุล	หมายเลขโทรศัพท์
นายทหารควบคุมข้อมูล แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.	๗๘๐๘๖	หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศ		
นายทหารวิเคราะห์และพัฒนาระบบแผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.	๗๘๐๖๙	หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ด้านซอฟท์แวร์ระบบสารสนเทศ		
นายทหารควบคุมข้อมูล แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.	๗๘๐๘๖	หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศ		

๔. การวิเคราะห์ความเสี่ยง

เนื่องจากภารกิจของกรมอู่ทหารเรือ มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมอู่ทหารเรือ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด

จากการวิเคราะห์และตรวจสอบความเสี่ยงทางด้านสารสนเทศของกรมอู่ทหารเรือ พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์เอง อาจเกิดถูกโจมตีจากโปรแกรมไม่ประสงค์ดี เช่น ไวรัสคอมพิวเตอร์ หรือ ถูกเจาะทำลายระบบหรือถูกก่อกวนจาก Hacker เป็นต้น

๒. ความเสี่ยงทางกายภาพ เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟฟ้าขัดข้อง น้ำท่วม ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในประเทศ เป็นต้น

๓. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศของกรมอู่ทหารเรือ ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของกรมอู่ทหารเรือ มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของกรมอู่ทหารเรือ

๕. ลักษณะรายละเอียดของความเสี่ยง

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ปัจจัยเสี่ยง/สิ่งคุกคาม	ผลกระทบ/และผู้ได้รับผลกระทบ
๑	การป้องกันโปรแกรมไม่ประสงค์ดีล้มเหลว	T101	ความเสี่ยงด้านเทคนิค	- เครื่องคอมพิวเตอร์ติดโปรแกรมไม่ประสงค์ดี เช่น ไวรัส มัลแวร์	- ไม่ได้ติดตั้งโปรแกรมป้องกันไม่ประสงค์ดี - โปรแกรมป้องกันหมดอายุ	- เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายไม่สามารถใช้งานได้/ข้อมูลสูญหาย - อุปกรณ์เก็บข้อมูลแบบพกพาข้อมูลสูญหาย *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน/ผู้ดูแลระบบ
๒	การป้องกันผู้บุกรุกล้มเหลว	T102	ความเสี่ยงด้านเทคนิค	- การบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี เช่น Hacker เป็นต้น การดักจับข้อมูล การส่งคำสั่งเจตนาร้าย - การเข้าถึงโดยไม่ได้รับอนุญาต	- Hacker - การโจมตีการให้บริการ (Denial of Services) - การดักจับข้อมูล - คำสั่งเจตนาร้าย - ความผิดพลาดของซอฟต์แวร์หรือการเขียนโปรแกรม	- เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายไม่สามารถใช้งานได้/ข้อมูลสูญหาย/ข้อมูลรั่วไหล *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน/ผู้ดูแลระบบ
๓	การเชื่อมต่อเครือข่ายล้มเหลว	T103	ความเสี่ยงด้านเทคนิค	- ไม่สามารถเชื่อมต่อเครื่องแม่ข่ายได้	- อุปกรณ์เครือข่ายขัดข้อง/ชำรุด -สายเคเบิลขาด	ไม่สามารถใช้งานระบบสารสนเทศ *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน/ผู้ดูแลระบบ
๔	อุปกรณ์จัด เก็บข้อมูลเสียหาย	T104	ความเสี่ยงด้านเทคนิค	อุปกรณ์จัดเก็บข้อมูลส่งผลให้ข้อมูลในเครื่องขัดข้อง	- อุปกรณ์จัดเก็บข้อมูลข้อมูลเสีย - ระบบไฟฟ้าขัดข้อง	ไม่สามารถเปิดข้อมูลได้หรือเปิดเครื่องใช้งานไม่ได้ *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน
๕	ระบบไฟฟ้าขัดข้อง	P101	ความเสี่ยงทางกายภาพ	ระบบไฟฟ้าไม่สามารถจ่ายให้เครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ทำเปิดเครื่องใช้งานไม่ได้	แหล่งกำเนิดไฟฟ้าขัดข้องหรือแรงดัน ไฟฟ้าไม่คงที่	ไม่สามารถใช้งานระบบสารสนเทศ *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน/ผู้ดูแลระบบ

๖	ไฟไหม้	P102	ความเสี่ยงทางกายภาพ	การเกิดไฟไหม้อาคารไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลทำให้ระบบคอมพิวเตอร์และระบบเครือข่ายได้รับความเสียหายบางส่วนหรือได้รับ ความเสียหายทั้งหมด	ไฟไหม้จากอุบัติเหตุไฟฟ้าลัดวงจร	- ไม่สามารถใช้งานระบบสารสนเทศ - ไม่สามารถเข้าพื้นที่ทำงาน *ผู้ได้รับผลกระทบ* -ผู้ใช้งาน/ผู้ดูแลระบบ
๗	น้ำท่วม แผ่นดินไหว ภัยธรรมชาติ	P103	ความเสี่ยงทางกายภาพ	- เกิดแผ่นดินไหวในพื้นที่ปฏิบัติงาน ทำให้ตัวอาคารพังเสียหาย - ระบบไฟฟ้าถูกตัดทำให้ - น้ำท่วมในพื้นที่	ภัยธรรมชาติ	- ไม่สามารถใช้งานระบบสารสนเทศ - ไม่สามารถเดินทางมาทำงานได้หรือเข้าพื้นที่ทำงานไม่ได้ *ผู้ได้รับผลกระทบ* -ผู้ใช้งาน/ผู้ดูแลระบบ
๘	การก่อการร้าย การชุมนุมประท้วง	P104	ความเสี่ยงทางกายภาพ	เกิดเหตุการณ์ไม่สงบในพื้นที่ปฏิบัติงาน	- เดินขบวนประท้วง - ก่อวินาศกรรม	ไม่สามารถเดินทางมาทำงานได้หรือเข้าพื้นที่ทำงานไม่ได้ *ผู้ได้รับผลกระทบ* -ผู้ใช้งาน/ผู้ดูแลระบบ
๙	ผู้ใช้งานสารสนเทศขาดความระมัดระวัง และการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ	O101	ความเสี่ยงด้านผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทำให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญหรือการส่งคำสั่งเจตนาร้าย หรือการติดไวรัสคอมพิวเตอร์ ซึ่งส่งผลกระทบต่อระบบงานสารสนเทศของหน่วย		- เครื่องคอมพิวเตอร์แม่ข่ายและลูกข่ายไม่สามารถใช้งานได้/ข้อมูลสูญหาย/ข้อมูลรั่วไหล - ระบบสานเทศใช้งานไม่ได้ *ผู้ได้รับผลกระทบ* - ผู้ใช้งาน/ผู้ดูแลระบบ

๖. การประมาณความเสี่ยง

เป็นการตรวจสอบความเสี่ยงในแง่ของโอกาสการเกิดเหตุ (Incident) หรือเหตุการณ์ (Event) ว่ามีมากน้อยเพียงไรและผลที่ตามมาว่ามีความรุนแรงหรือเสียหายมากน้อยเพียงใด

เกณฑ์การประมาณ เป็นการกำหนดเกณฑ์ที่จะใช้ในการประมาณความเสี่ยง ได้แก่ ระดับโอกาส ที่จะเกิดความเสี่ยง ระดับความรุนแรงของผลกระทบและระดับความเสี่ยง ใช้เกณฑ์ดังนี้

ระดับโอกาสในการเกิดเหตุการณ์		
ระดับ	**โอกาสที่จะเกิด**	**คำอธิบาย**
๕	สูงมาก	> ๔ ครั้ง/ปี
๔	สูง	๔
๓	ปานกลาง	๓
๒	น้อย	๒
๑	น้อยมาก	< ๑ ครั้ง/ปี

ในส่วนการประเมินระดับความรุนแรงของผลกระทบของความเสี่ยง ทั้งที่เป็นตัวเงินและไม่เป็นตัวเงินที่อาจเกิดขึ้น มีแนวทางการประเมินดังนี้

ผลกระทบด้านการเงิน เป็นผลกระทบหรือความเสียหายที่เกิดจากความเสี่ยงและสามารถประเมินค่าเป็นตัวเงินได้ ได้แก่ ค่าความเสียหายในด้านต่างๆต่อทรัพย์สิน

ผลกระทบต่อการดำเนินงาน ความสามารถการบรรลุพันธกิจและวิสัยทัศน์ขององค์กร เป็นผลกระทบที่มีความเสียหายกับการดำเนินงานขององค์กรในภาพโดยรวม ได้แก่

- ผลกระทบจากปัจจัยภายนอกองค์กร นโยบายรัฐบาล และกฎหมาย
- ผลกระทบต่อระบบสารสนเทศ
- ผลกระทบจากการดำเนินงานตามแผนงานหรือโครงการ

ผลกระทบด้านชื่อเสียงขององค์กร เป็นความเสียหายต่อชื่อเสียง ไม่ว่าจะเป็นผลจากการ ดำเนินงานทั้งทางตรงและทางอ้อม ที่ส่งผลต่อภาพลักษณ์และความเชื่อถือขององค์กร เช่น มีการเผยแพร่ข่าวในสื่อมวลชนหรือโซเชียลมีเดีย เป็นต้น

ดังนั้นในแนวทางการประเมินผลกระทบจึงได้เลือกใช้การวิเคราะห์ผลกระทบด้านการเงินหรือผลกระทบต่อระบบเทคโนโลยีสารสนเทศในการจัดระดับความรุนแรงของผลกระทบของความเสี่ยงได้ดังนี้

ระดับความรุนแรงของผลกระทบของความเสี่ยง		
ระดับ	**ผลกระทบ**	**คำอธิบาย**
๕	สูงมาก	>๑๐ ล้านบาท หรือเกิดความสูญเสียต่อระบบสารสนเทศทั้งหมดและเกิดความเสียหายอย่างมากต่อความปลอดภัยของข้อมูลต่างๆ
๔	สูง	> ๕ แสนบาท – ๑๐ ล้านบาท หรือเกิดปัญหากับระบบสารสนเทศที่สำคัญและระบบความปลอดภัยซึ่งส่งผลต่อความถูกต้องของข้อมูลบางส่วน

๓	ปานกลาง	> ๑ แสนบาท – ๕ แสนบาท หรือระบบสารสนเทศทั่วไปมีปัญหาและมีความสูญเสียไม่มาก
๒	น้อย	> ๕ หมื่นบาท – ๑ แสนบาท หรือระบบสารสนเทศเกิดปัญหาเล็กน้อยที่แก้ไขได้
๑	น้อยมาก	ไม่เกิน ๕ หมื่นบาท หรือเกิดเหตุที่ไม่มีความสำคัญ

จากการประมาณความเสี่ยงข้างต้น สามารถประเมินค่าความเสี่ยงเป็นระดับความเสี่ยง(ระดับโอกาสXระดับความรุนแรง) ดังตาราง

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาส/ความถี่	ระดับความรุนแรง	ระดับคะแนน
๑	การป้องกันโปรแกรมไม่ประสงค์ดีล้มเหลว	T101	ความเสี่ยงด้านเทคนิค	- เครื่องคอมพิวเตอร์ติดโปรแกรมไม่ประสงค์ดี เช่นไวรัสคอมพิวเตอร์ ทำให้ไม่สามารถใช้งานได้/ข้อมูลสูญหาย	๕	๔	๒๐
๒	การป้องกันผู้บุกรุกล้มเหลว	T102	ความเสี่ยงด้านเทคนิค	ไม่สามารถเชื่อมต่อไปยังเครื่อง Server ที่ให้บริการระบบสารสนเทศ/ระบบสารสนเทศ/มีการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต	๑	๕	๕
๓	การเชื่อมต่อเครือข่ายล้มเหลว	T103	ความเสี่ยงด้านเทคนิค	ไม่สามารถเชื่อมต่อไปยังเครื่อง Server ที่ให้บริการสารสนเทศ	๕	๓	๑๕
๔	อุปกรณ์จัดเก็บข้อมูลเสียหาย	T104	ความเสี่ยงด้านเทคนิค	อุปกรณ์จัดเก็บข้อมูลข้อมูลในเครื่องขัดข้อง ทำให้ไม่สามารถเปิดข้อมูลได้/เปิดเครื่องใช้งานไม่ได้	๒	๔	๘
๕	ระบบไฟฟ้าขัดข้อง	P101	ความเสี่ยงทางกายภาพ	การเกิดกระแสไฟฟ้าขัดข้อง หรือเกิดแรงดันไฟฟ้าไม่คงที่ ทำให้เครื่องคอมพิวเตอร์และอุปกรณ์อาจได้รับความเสียหายจากแรงดันไฟฟ้าที่ไม่คงที่ หรือเมื่อ	๕	๔	๒๐

				กระแสไฟฟ้าขัดข้อง ทำให้เครื่องคอมพิวเตอร์แม่ข่าย ถูกปิดโดยไม่สมบูรณ์ อาจทำให้ข้อมูลสารสนเทศบางส่วนเกิดการสูญหาย และการให้บริการบางประเภทไม่สามารถเปิดใช้งานได้โดยอัตโนมัติ			
๖	ไฟไหม้	P102	ความเสี่ยงทางกายภาพ	การเกิดไฟไหม้อาคาร ไม่สามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ได้ ส่งผลให้ระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้รับความเสียหายบางส่วน หรือได้รับความเสียหายทั้งหมด ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๑	๕	๕
๗	น้ำท่วม แผ่นดินไหว ภัยธรรมชาติ	P103	ความเสี่ยงทางกายภาพ	อาคารพังเสียหาย หรือระบบไฟฟ้าถูกตัดทำให้ไม่สามารถใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายหลักได้	๑	๕	๕
๘	การก่อการร้าย การชุมนุมประท้วง	P105	ความเสี่ยงทางกายภาพ	เกิดเหตุการณ์ไม่สงบในพื้นที่ปฏิบัติงานทำให้ไม่สามารถเดินทางมาทำงานได้/หรือเข้าไม่สามารถเข้าพื้นที่ทำงาน	๑	๕	๕
๙	ผู้ใช้งานสารสนเทศขาด ความระมัดระวังและการตระหนักถึงความสำคัญของความ	O101	ความเสี่ยงด้านผู้ปฏิบัติงาน	การใช้งานสารสนเทศโดยขาดความระมัดระวัง ทาให้ถูกบุกรุกโจมตีโดยผู้ไม่ประสงค์ดี หรือถูกดักจับข้อมูลสำคัญ หรือการส่งคำสั่งเจตนาร้าย หรือติดไวรัสคอมพิวเตอร์ ซึ่งส่งผล	๓	๕	๑๕

ลำดับ	ชื่อความเสี่ยง	รหัส	ประเภทความเสี่ยง	ลักษณะความเสี่ยง	ระดับโอกาส/ความถี่	ระดับความรุนแรง	ระดับคะแนน
	ปลอดภัยด้านสารสนเทศ			กระทบต่อระบบงานสารสนเทศของหน่วย			

เกณฑ์ในการประเมินค่าความเสี่ยงดังนี้

ระดับคะแนน	จัดระดับความเสี่ยง	กลยุทธ์จัดการความเสี่ยง
๑ - ๘	ต่ำ	ยอมรับความเสี่ยง
๙ - ๑๔	ปานกลาง	ยอมรับความเสี่ยง(มีมาตรการติดตาม)
๑๕-๒๔	สูง	ยอมรับความเสี่ยง(มีแผนควบคุมความเสี่ยง)
๒๕	สูงมาก	ถ่ายโอนความเสี่ยง

๗. การจัดการความเสี่ยง

กำหนดให้ความเสี่ยงที่จำเป็นต้องนำมาดำเนินการจัดการเรียงตามลำดับความเสี่ยงดังนี้

ลำดับ	ความเสี่ยง	ระดับความเสี่ยง	กลยุทธ์การจัดการความเสี่ยง	แนวทางการดำเนินการจัดการความเสี่ยง	ผู้รับผิดชอบ	ระยะเวลาปฏิบัติการ
๑.	การป้องกันโปรแกรมไม่ประสงค์ดีล้มเหลว	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ตัดการเชื่อมต่อกับเครือข่าย - ติดตั้งโปรแกรมป้องกัน/อัพเดทโปรแกรม - ค้นหา(SCAN) และทำลาย(Clean) - ถอดถอน (Uninstall)โปรแกรมที่หน้าสงสัย - กู้คืนข้อมูล/ระบบ - เฝ้าระวัง	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๔ ชั่วโมง
๒	ระบบไฟฟ้าขัดข้อง	๒๐	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ติดตั้งอุปกรณ์สำรองไฟฟ้าให้เครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายที่สำคัญ - กรณีไฟฟ้าดับนานปิดระบบทั้งหมด	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๑ ชั่วโมง
๓	การเชื่อมต่อเครือข่ายล้มเหลว	๑๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดหาระบบเครือข่ายสำรองเพื่อเป็นช่องทางให้ใช้งานได้อย่างต่อเนื่อง - ตรวจสอบการเชื่อมต่อเครือข่าย	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๔ ชั่วโมง
๔	ผู้ใช้งานสารสนเทศขาด ความระมัดระวังและการตระหนักถึงความสำคัญของความ	๑๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนัก ในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของหน่วยอย่างต่อเนื่อง	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๒๔ ชั่วโมง

	ปลอดภัยด้านสารสนเทศ			- กำกับ ดูแล การปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด		
๕	อุปกรณ์จัดเก็บข้อมูลเสียหาย	๘	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- สำรองข้อมูลที่สำคัญไว้ในอุปกรณ์สำรองข้อมูล - จัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้มากู้คืน	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๔ ชั่วโมง
๖	การป้องกันผู้บุกรุกล้มเหลว	๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ตรวจสอบ Log ของ Firewall อย่างสม่ำเสมอ - บริหารจัดการระบบตรวจสอบการบุกรุกเครือข่ายและติดตามเพื่อปรับปรุงอย่างสม่ำเสมอ - ติดตั้งโปรแกรมป้องกันไวรัสและUpdate อย่างสม่ำเสมอ - ติดตั้ง Patch ของระบบปฏิบัติการสม่ำเสมอ	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๔ ชั่วโมง
๗	ไฟไหม้	๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- ตรวจสอบความพร้อมของการใช้งานอุปกรณ์ดับเพลิง - มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ - จัดทำและทดสอบแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง	กธก.อร.	ภายใน ๑ ชั่วโมง
๘	แผ่นดินไหว น้ำท่วม ภัยธรรมชาติ	๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- มีแผนในการเคลื่อนย้ายอุปกรณ์ตามลำดับความสำคัญ	แผนกกรรมวิธีข้อมูลฯ	ภายใน ๒๔ ชั่วโมง

๙	การก่อการร้าย การชุมนุมประท้วง	๕	ควบคุมความเสี่ยง (มีแผนควบคุมความเสี่ยง)	- จัดทำแผนรับสถานการณ์เพื่อให้สามารถดำเนินการได้อย่างต่อเนื่อง - จัดหาระบบสำรองเพื่อให้ระบบสารสนเทศสามารถทำงานได้ - สำรองข้อมูลระบบ และฐานข้อมูลเก็บไว้ในสถานที่อื่นอีกหนึ่งชุด	กธก.อร.	ภายใน ๒๔ ชั่วโมง

๘. แนวทางการปฏิบัติรองรับสถานการณ์ฉุกเฉินด้านสารสนเทศ

๘.๑ การป้องกันโปรแกรมไม่ประสงค์ดีล้มเหลว รายละเอียดตาม ผนวก ก

๘.๒ ระบบไฟฟ้าขัดข้อง รายละเอียดตาม ผนวก ข

๘.๓ การเชื่อมต่อเครือข่ายล้มเหลว รายละเอียดตาม ผนวก ค

๘.๔ ผู้ใช้งานสารสนเทศขาด ความระมัดระวัง และการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ รายละเอียดตาม ผนวก ง

๘.๕ อุปกรณ์จัดเก็บข้อมูลเสียหาย รายละเอียดตาม ผนวก จ

๘.๖ การป้องกันผู้บุกรุกล้มเหลว รายละเอียดตาม ผนวก ฉ

๘.๗ ไฟไหม้ รายละเอียดตาม ผนวก ช

๘.๘ แผ่นดินไหว น้ำท่วม ภัยธรรมชาติ รายละเอียดตาม ผนวก ซ

๘.๙ การก่อการร้าย การชุมนุมประท้วง รายละเอียดตาม ผนวก ฌ

ผนวก ก
มาตรการรองรับการการป้องกันโปรแกรมไม่ประสงค์ดีล้มเหลว

๑. ผู้สั่งการในที่เกิดเหตุ: แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

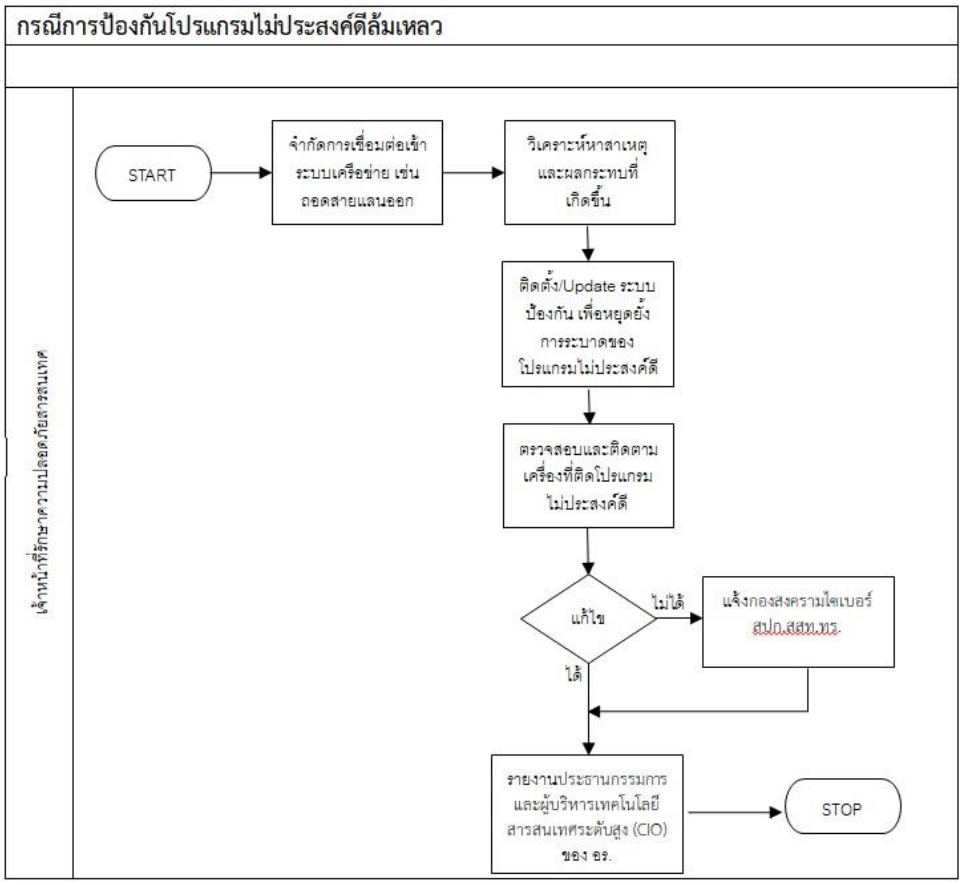
๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ/เวรประจำวัน)
- ตรวจสอบความเสียหายเบื้องต้น (หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ)
- ตรวจสอบประวัติการใช้งาน(LOG)เพื่อหาแหล่งที่มา
- ประสานขอรับการสนับสนุนการวิเคราะห์ LOG จาก ศูนย์ไซเบอร์ สสท.ทร. (ถ้าจำเป็น)

๓. การรายงานเหตุ

- วิเคราะห์หาสาเหตุและเสนอแนะหนทางการแก้ไขปัญหา
- รายงานการตรวจสอบ สรุปหาสาเหตุและผลการปฏิบัติ ให้ CIO ของ อร.

๔. ขั้นตอนการปฏิบัติ



ผนวก ข
มาตรการรองรับระบบไฟฟ้าขัดข้อง

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

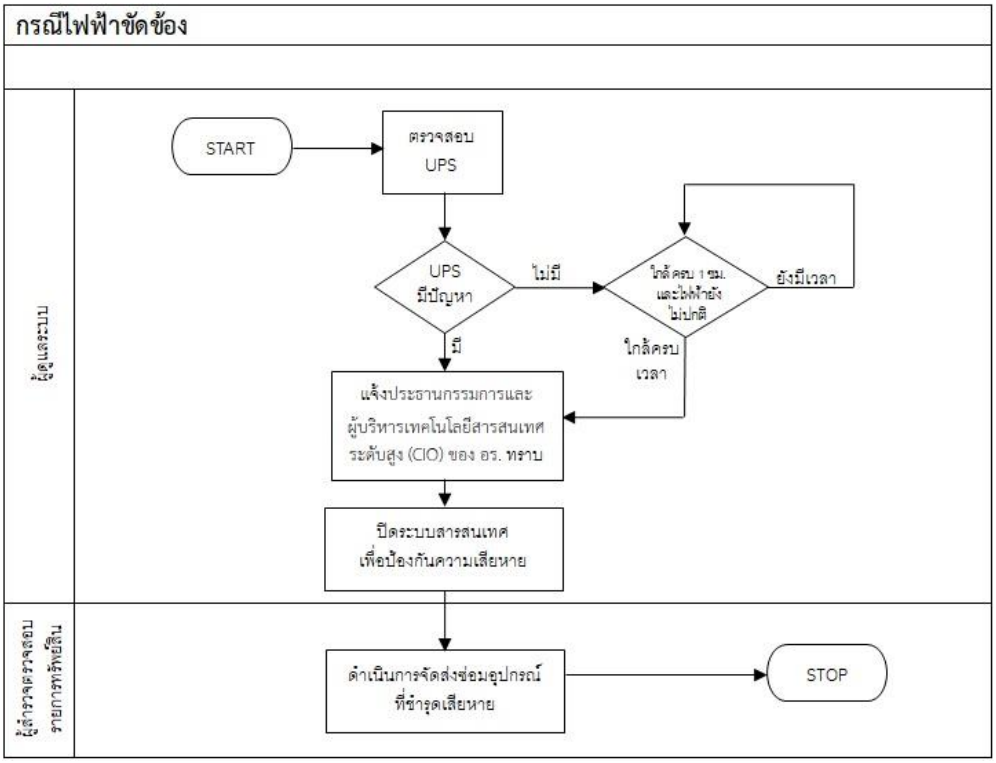
๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เวรประจำวัน)
- ตรวจสอบความเสียหายเบื้องต้น (หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่ควบคุมระบบสารสนเทศ)
- ตรวจสอบระบบสำรองไฟฟ้า
- ตรวจสอบสาเหตุและแจ้งผู้ที่เกี่ยวข้อง

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ และผลการปฏิบัติ ให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**



ผนวก ค
มาตรการรองรับการเชื่อมต่อเครือข่ายล้มเหลว

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

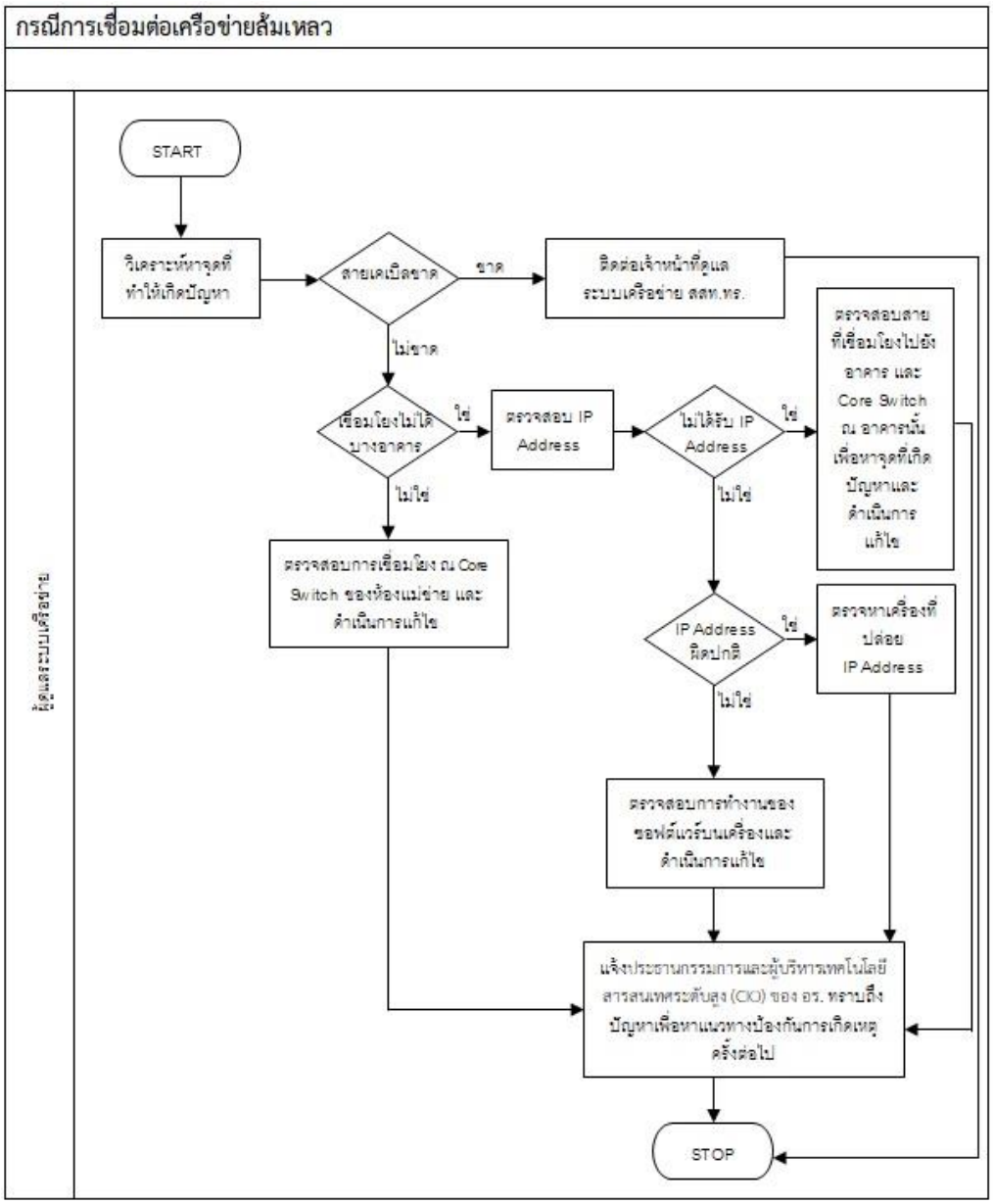
๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ/เวรประจำวัน)
- ตรวจสอบเหตุขัดข้องเบื้องต้น (หัวหน้าเจ้าหน้าที่/ผู้ดูแลระบบเครือข่าย)
- แจ้ง สสท.ทร. กรณีหาข้อขัดข้องไม่ได้เพื่อหาสาเหตุ

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**



ผนวก ง
มาตรการรองรับผู้ใช้งานสารสนเทศขาด ความระมัดระวัง และการตระหนักถึงความสำคัญของความปลอดภัยด้านสารสนเทศ

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- ตรวจสอบความเสียหายเบื้องต้น (หัวหน้าเจ้าหน้าที่/เจ้าหน้าที่รักษาความปลอดภัยระบบสารสนเทศ)
- ตรวจสอบผู้ที่กระทำจากประวัติผู้ใช้งานเพื่อหาสาเหตุ

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**

- ฝึกอบรม เผยแพร่และประชาสัมพันธ์ข้อมูลเพื่อสร้างความตระหนัก ในเรื่องของความมั่นคงปลอดภัยสารสนเทศให้กับบุคลากรของ อร. อย่างต่อเนื่อง
- กำกับ ดูแลการปฏิบัติตามแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยสารสนเทศอย่างเคร่งครัด

ผนวก จ
มาตรการรองรับอุปกรณ์จัดเก็บข้อมูลเสียหาย

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

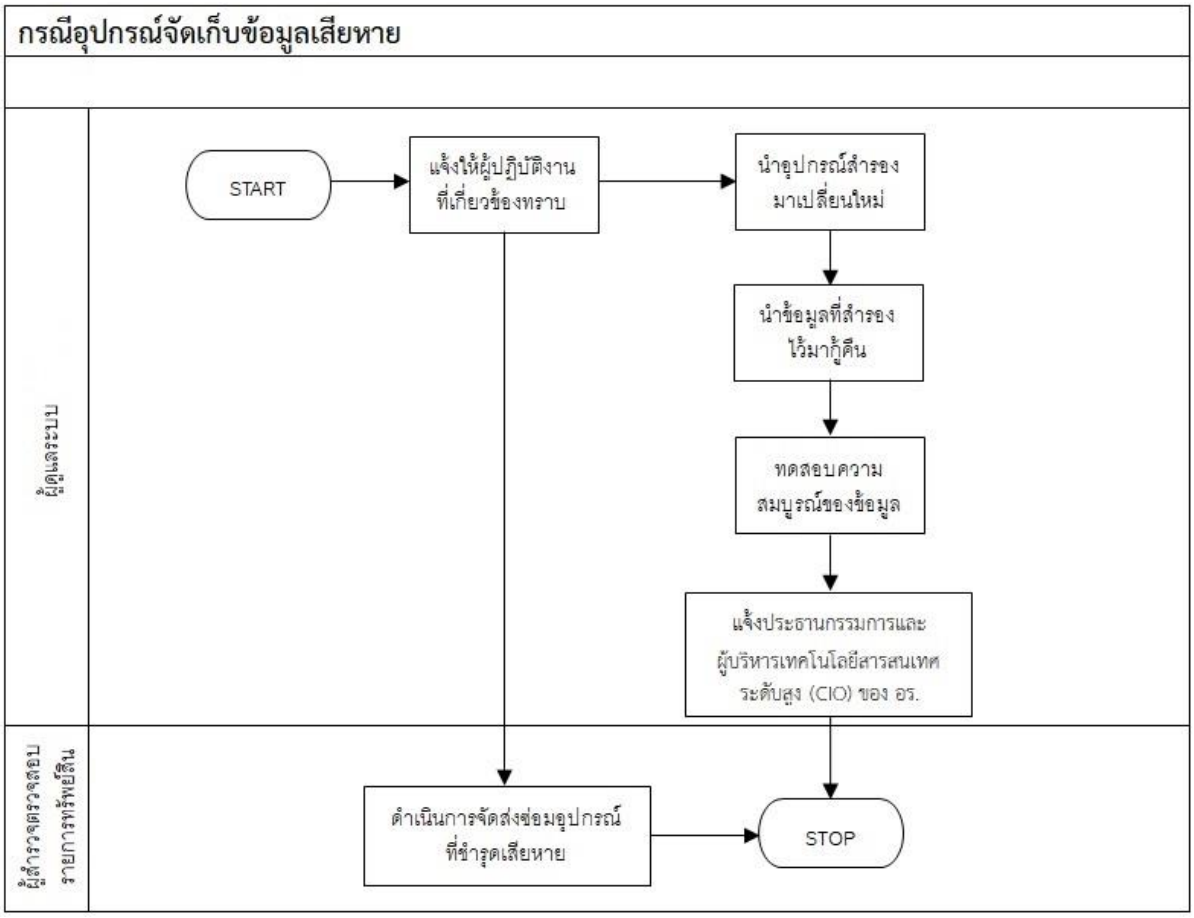
๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ/เวรประจำวัน)
- ตรวจสอบหาสาเหตุและความเสียหายเบื้องต้น (หัวหน้าเจ้าหน้าที่/ผู้ดูแลระบบ)

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**



ผนวก ฉ
มาตรการรองรับการป้องกันบุกรุกล้มเหลว

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

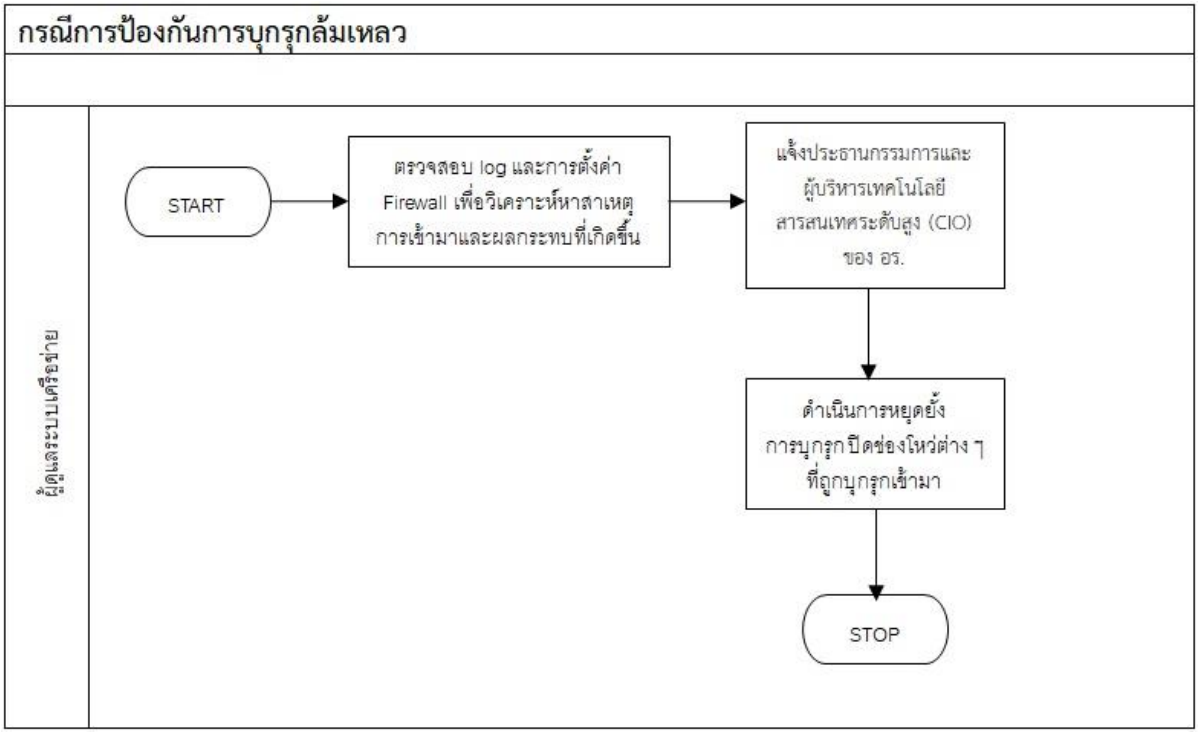
๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ)
- ตรวจสอบความเสียหายเบื้องต้น (หัวหน้าเจ้าหน้าที่/ผู้ดูแลระบบเครือข่าย)
- ตรวจสอบประวัติการใช้งาน(LOG)เพื่อหาผู้บุกรุก

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**



ผนวก ช
มาตรการรองรับไฟไหม้

๑. ผู้สั่งการในที่เกิดเหตุ: ธก.อร.

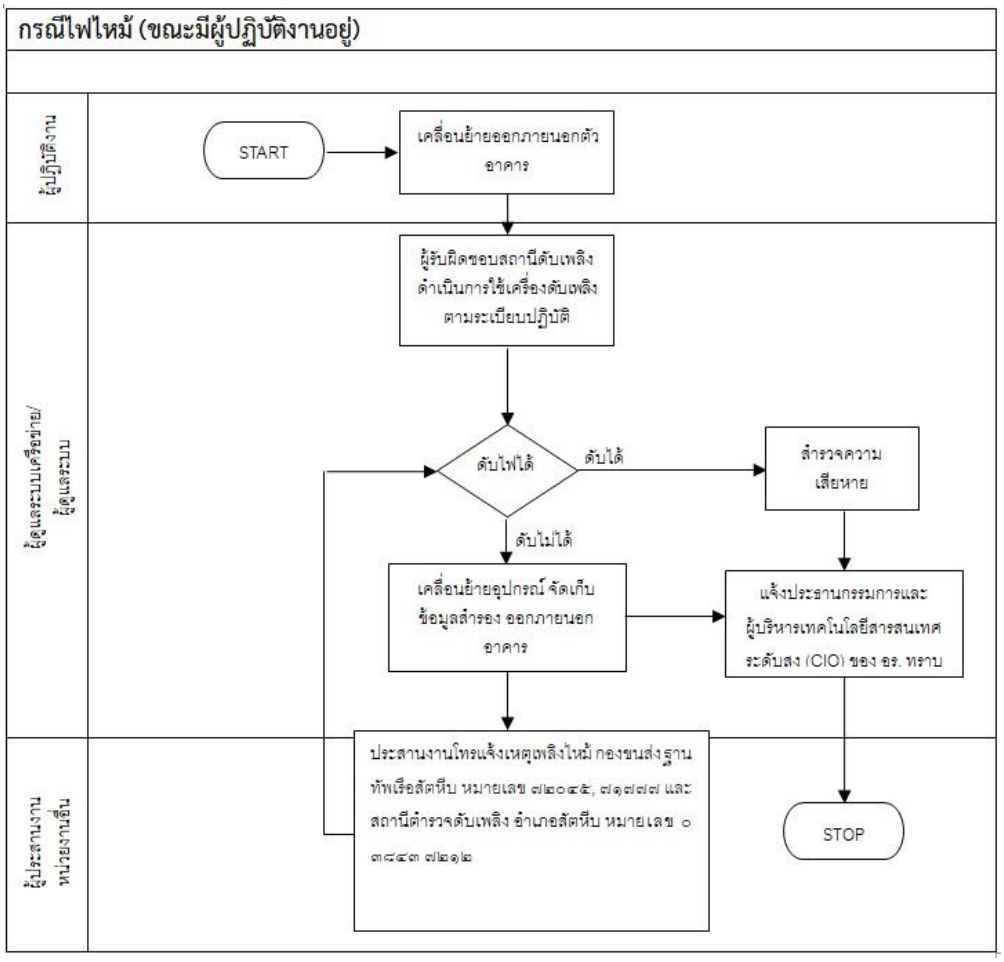
๒. การตรวจสอบและสรุปหาสาเหตุเบื้องต้น

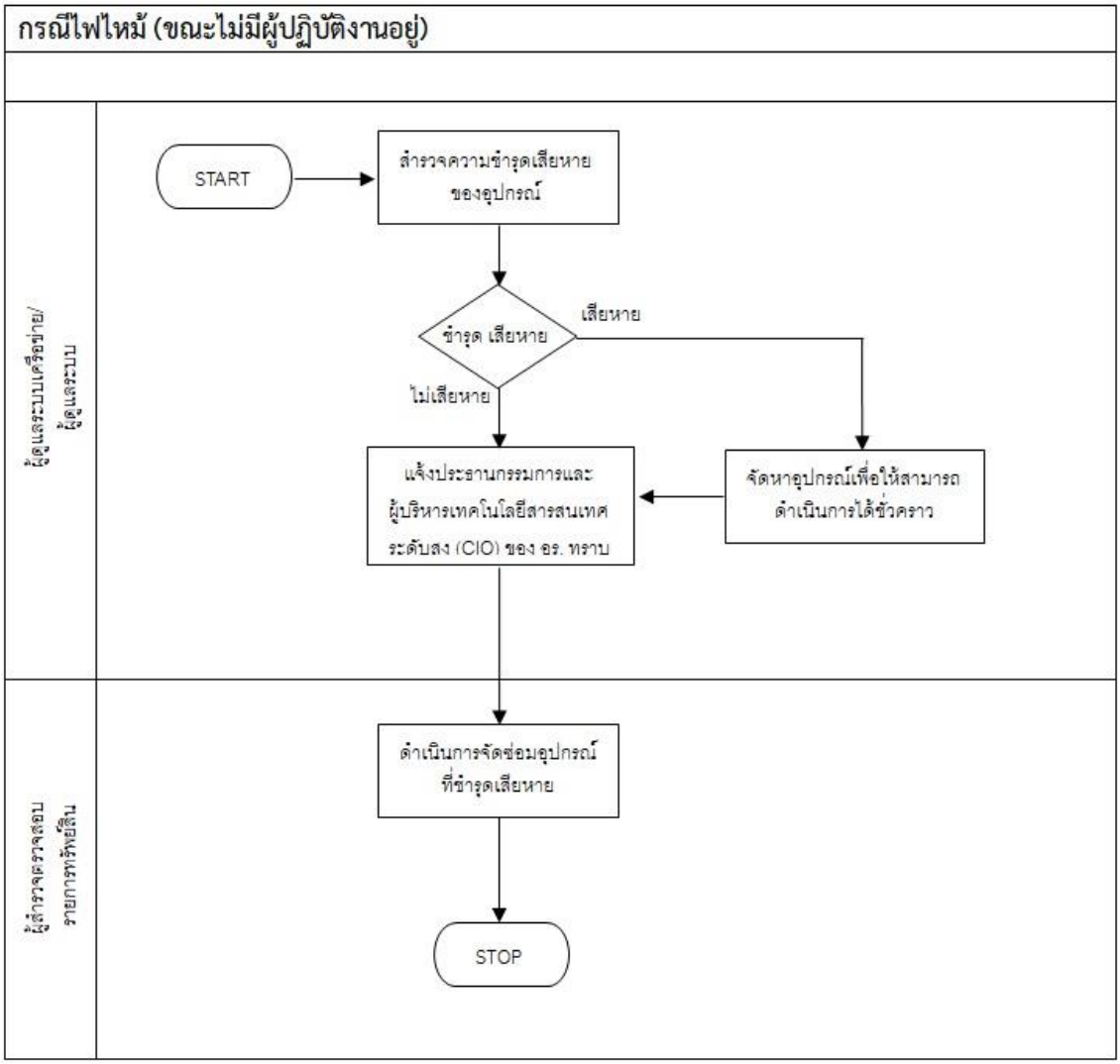
- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เวรประจำวัน)
- ตรวจสอบระบบแจ้งเตือนภัย(ระบบอัตโนมัติ/เวรประจำวัน)
- ตรวจสอบแหล่งหรือสถานที่เกิดไฟไหม้
- ตรวจสอบอุปกรณ์สำหรับดับเพลิง

๓. การรายงานเหตุ

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. ขั้นตอนการปฏิบัติ




กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)
ผู้ดูแลระบบเครือข่าย/ ผู้ดูแลระบบ
START
สำรวจความชำรุดเสียหาย ของอุปกรณ์
ชำรุด เสียหาย
เสียหาย
ไม่เสียหาย
แจ้งประธานกรรมการและ ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง (CIO) ของ อร. ทราบ
จัดหาอุปกรณ์เพื่อให้สามารถ ดำเนินการได้ชั่วคราว
ผู้สำรวจตรวจสอบ รายการทรัพย์สิน
ดำเนินการจัดซ่อมอุปกรณ์ ที่ชำรุดเสียหาย
STOP

ผนวก ซ
มาตรการรองรับแผ่นดินไหว น้ำท่วม ภัยธรรมชาติ

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

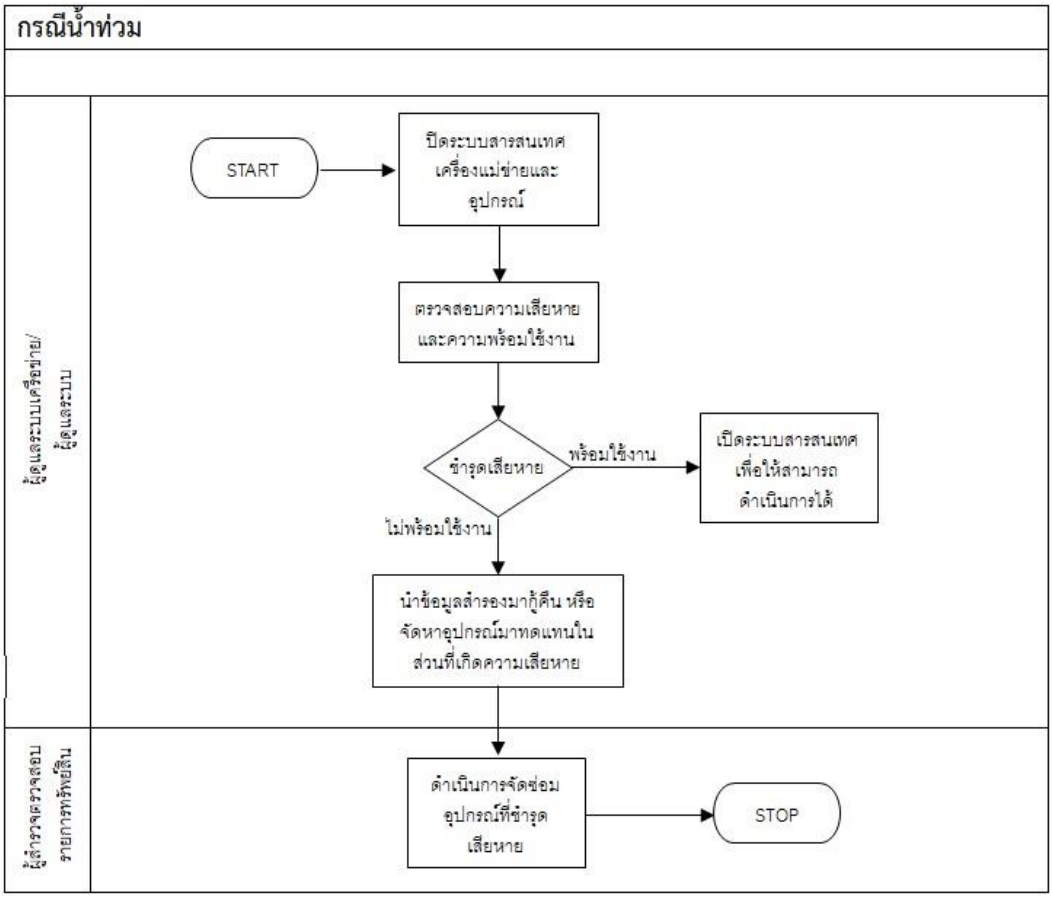
๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

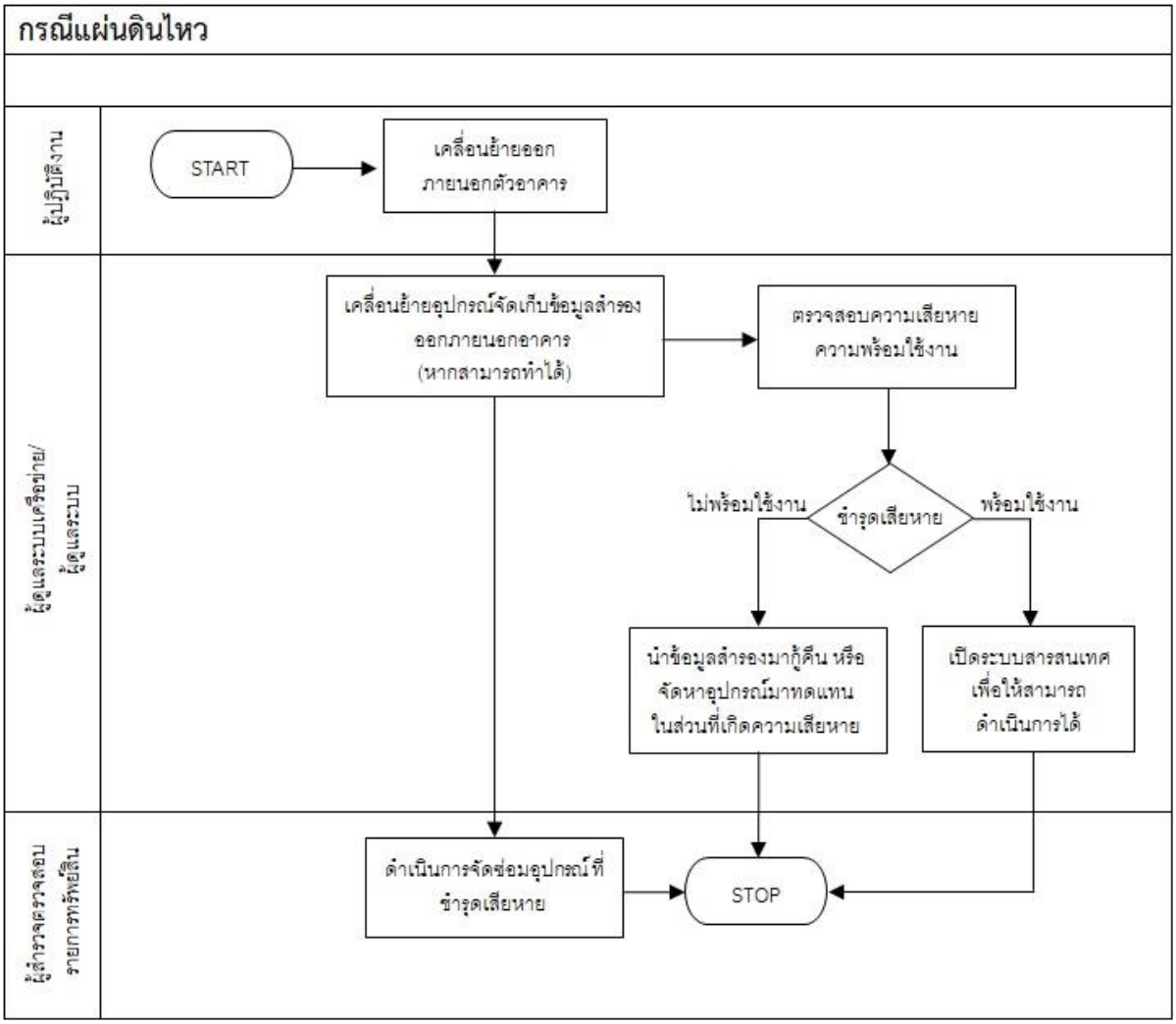
- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ/เวรประจำวัน)
- ตรวจสอบความเสียหาย

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**




กรณีแผ่นดินไหว
ผู้ปฏิบัติงาน
ผู้ดูแลระบบเครือข่าย/ ผู้ดูแลระบบ
ผู้สำรวจตรวจสอบรายการทรัพย์สิน
START
เคลื่อนย้ายออก ภายนอกตัวอาคาร
เคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรอง ออกภายนอกอาคาร (หากสามารถทำได้)
ตรวจสอบความเสียหาย ความพร้อมใช้งาน
ชำรุดเสียหาย
ไม่พร้อมใช้งาน
พร้อมใช้งาน
นำข้อมูลสำรองมากู้คืน หรือ จัดหาอุปกรณ์มาทดแทน ในส่วนที่เกิดความเสียหาย
เปิดระบบสารสนเทศ เพื่อให้สามารถ ดำเนินการได้
ดำเนินการจัดซ่อมอุปกรณ์ที่ ชำรุดเสียหาย
STOP

ผนวก ฌ
มาตรการรองรับการก่อการร้าย การชุมนุม

๑. **ผู้สั่งการในที่เกิดเหตุ:** แผนกกรรมวิธีข้อมูลและสถิติ กจก.อร.

๒. **การตรวจสอบและสรุปหาสาเหตุเบื้องต้น**

- ได้รับการแจ้งเตือนจากผู้ประสบเหตุ (ทั้งผู้ใช้ทั่วไป/เจ้าของระบบ/ผู้ดูแลระบบ/เวรประจำวัน)
- ตรวจสอบผลกระทบกับการปฏิบัติงาน

๓. **การรายงานเหตุ**

- รายงานการตรวจสอบ สรุปหาสาเหตุและการปฏิบัติให้ CIO ของ อร.

๔. **ขั้นตอนการปฏิบัติ**