THAITEX

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ

ระบบเทคโนโลยีสารสนเทศ

บริษัท ไทยรับเบอร์ลาเท็คซ์กรุ๊ป จำกัด (มหาชน)

คำนำ

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของ บริษัท ไทยรับเบอร์ลาเท็คซ์กรุ๊ป จำกัด (มหาชน) จำเป็นต้องได้รับการดูแลรักษา เพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ ฝ่ายเทคโนโลยีสารสนเทศได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศของบริษัทฯ ซึ่งอาจมีปัจจัยจากภายนอก และปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้

ดังนั้น จึงได้จัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ บริษัท ไทยรับเบอร์ลาเท็คซ์กรุ๊ป จำกัด (มหาชน)

สารบัญ

คำนำ 1
สารบัญ 2
วัตถุประสงค์ 3
ขอบเขตการดำเนินงาน
1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ 3
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น 5
3. การเตรียมความพร้อม 6
4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน 10
5. แผนการกู้คืนระบบและข้อมูล 10
6. การติดตามและรายงานผล 11
ภาคผนวก ก 12
เบอร์โทรศัพท์หน่วยงาน 12
ภาคผนวก ข 13
ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ 13

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร
2. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร
3. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
4. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้สถานกรณ์ได้อย่างทันท่วงที

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติที่อาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่ฝ่ายเทคโนโลยีสารสนเทศ จัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของบริษัทฯ ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. การเตรียมความพร้อม
4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
5. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ
6. แผนการกู้คืนข้อมูลและข้อมูล
7. การติดตามและรายงานผล

1. <u>การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ</u>

1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

<u>ภัยพิบัติจากภายนอก</u>

- ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ การจลาจล ชุมนุมประท้วง แผ่นดินไหว ฯลฯ
- ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง
- การบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
- ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ /ไฟกระชาก
- ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

- ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย
- ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในบริษัทฯ
- เจ้าหน้าที่หรือบุคลากรของบริษัทฯ ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ หรือหยุดการทำงาน

1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อบริษัทฯ มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ (Security log Management System) โดยเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ เพื่อนำมาสรุปเป็นข้อมูล ดังนี้

สถานการณ์หรือภาวะฉุกเฉิน	**ระดับความรุนแรง ต่ำสุด (1) – สูงสุด (5)**			**รวม**	**จัดลำดับ**
	ต่อ ระบบงาน	ต่อ พันธกิจ	ต่อ ประชาชน		
กรณีไฟไหม้	5	5	5	15	1
กรณีแผ่นดินไหว	4	1	5	10	2
กรณีจลาจล การชุมนุม/เหตุการณ์ความไม่สงบ/ สถานการทางการเมือง	2	3	4	9	3
กรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์	4	3	2	9	3
กรณีการบุกรุก และภัยคุกคามทางคอมพิวเตอร์	5	3	1	9	3
กรณีน้ำท่วม/น้ำรั่วซึม	3	2	3	8	4
กรณีไวรัสคอมพิวเตอร์	3	1	1	7	5
กรณีไฟฟ้าดับ/หม้อไฟระเบิด	3	1	3	7	5
กรณีภัยแล้ง/คลื่นความร้อน	2	1	4	7	5
กรณีพายุ	1	1	4	6	6
กรณีโรคระบาด	1	1	4	6	6

ตารางแสดงผลการประเมินสถานการ์และระดับความรุนแรง

2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

บริษัท ไทยรับเบอร์ลาเท็คซ์กรุ๊ป จำกัด (มหาชน) มีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน กรรมการผู้จัดการใหญ่ (CEO) จะสั่งการให้ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูงของบริษัทฯ ทราบเพื่อพิจารณาประกาศใช้แผนต่อไป

2.2 กำหนดขั้นตอนการดำเนินงาน

ฝ่ายเทคโนโลยีสารสนเทศจั ดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติภายในบริษัทฯ โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้นรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

2.3 การป้องกันการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์

เพื่อเป็นการป้องกันการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์ มีแนวทางดังนี้

1) มีการควบคลุมการเข้า-ออก ของพนักงาน และผู้ที่มาติดต่อ โดยมีการกำหนดช่วงเวลาที่อนุญาตตลอดจนพื้นที่ที่อนุญาตในการถึงตามสิทธิ์หรืออำนาจหน้าที่
2) มีการควบคุมการนำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ เข้า – ออก อาคาร
3) มีการติดตั้งกล้องโทรทัศน์วงจรปิดตามจุดต่างๆ อย่างทั่วถึง
4) มีการติดตั้งไฟส่องสว่างอย่างทั่วถึง
5) มีการจัดเจ้าหน้าที่รักษาความปลอดภัย ค่อยตรวจตราอย่างเพียงพอและทั่วถึง

2.4 การป้องกันการบุกรุก และคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและเครือข่ายมีแนวทางดังนี้

1) กำหนดมาตรการควบคุมดารเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้เจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศที่เป็นผู้รับผิดชอบพาเข้าไปในห้องควบคุม (Access Control) และอนุญาตเฉพาะผู้ที่เกี่ยวข้องเท่านั้น
2) มีการติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) ภายในห้องควบคุมระบบเครือข่าย เพื่อป้องกันการโจรกรรม
3) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสาสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า – ออกห้องควบคุมการรับ – ส่งข้อมูล ในระบบเครือข่าย
4) มีการติดตั้ง IPS (Intrusion Prevention System) เพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้าย ๆ กับ IDS (Intrusion Detection System) แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรม หรือ Hardware ตัวอื่นๆ
5) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ตของบริษัท เพื่อตรวจสอบการใช้งานเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้งานระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป
6) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยจัดหา

ระบบบริหารจัดเก็บข้อมูล Log (Central log Management) เพื่อตรวจสอบติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในเครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของบริษัทให้ดียิ่งขึ้น

7) มีระบบยืนยันตัวตนในการเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้งานระบบเครือข่ายหรืออินเตอร์เน็ต ตามอำนาจหน้าที่และความรับผิดชอบ

2.5 การป้องกันและกำจัดไวรัส

เพื่อเป็นการป้องกันและกำจัดไวรัสที่อาจเข้ามาทำลายหรือสร้างความเสียหายแก่ข้อมูลหรือระบบสารสนเทศ มีแนวทางดังนี้

1) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)
2) อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอวันละ 1 ครั้ง เป็นอย่างน้อย สั่งสแกนไวรัสสัปดาห์ละ 1 ครั้ง
3) ผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเตอร์เน็ตหรือการใช้งานอีเมล เพื่อไม่ให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

2.6 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 2 ชั่วโมง
2) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
3) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

3. <u>การเตรียมความพร้อม</u>

3.1 การจัดเตรียมอุปกรณ์

ฝ่ายเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือ ข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC/ เครื่องคอมพิวเตอร์ Notebook
- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการของเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus
- แผ่น Driver อุปกรณ์ต่าง ๆ
- ระบบสำรองไฟฟ้าอัตโนมัติ (UPS)
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

3.2 การติดต่อประสานงาน

คณะกรรมการความปลอดภัย อาชีวอนามัย และสภาพแวดล้อมในการทำงานของบริษัท ฯ การติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่ความจำเป็นฉุกเฉิน เช่น ไฟฟ้า, สถานีดับเพลิง, สถานีตำรวจ เป็นต้น

3.3 สำรองข้อมูล

เพื่อเป็นการเตรียมความพร้อม ในการรับมือต่อความบกพร่องอันเกิดจากกการทำงานและภัยพิบัติ เมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุกแทรกแซงเปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ บริษัทจึงได้มีการจัดทำระบบสำรองข้อมูล ในนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ส่วนที่ 9

3.4 การเตรียมความพร้อมกรณีเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้
2) ติดตั้งถังดับเพลิง ไว้ในห้องควบคุมระบบเครือข่าย
3) ติดตั้งถังดับเพลิงในทุกชั้นของอาคาร เพื่อควบคุมเพลิงไหม้เบื้องต้น สำหรับห้องปฏิบัติงานคอมพิวเตอร์การติดตั้งถังดับเพลิงประเภท C โดยไม่ทำความเสียหายแก่อุปกรณ์หรือเครื่องคอมพิวเตอร์ (อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์)

3.5 การเตรียมความพร้อมกรณีแผ่นดินไหว

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นไหวที่เกิดขึ้น เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยแผ่นดินไหว

1) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/ แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ได้แก่
   - กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)
   - ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า(http://ndwc.disaster.go.th/in.ndwc-9.283/)
   - กองเฝ้าระวังแผ่นดินไหว : ข้อมูลการเกิดแผ่นดินไหว (www.earthquake.tmd.go.th)
   - กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม/ แผ่นดินไหว (www.dmr.go.th)
   - กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการและแนวทางปฏิบัติ (www.disaster.go.th)
2) การเตรียมคน สถานที่อพยพ และวัสดุอุปกรณ์
   - ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
   - ประสานการเตรียมการกับส่วนราชการเกี่ยวข้อง ในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
   - สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร
   - สำรวจ จัดทำบัญชียานพาหนะ และเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยคได้อย่างมีประสิทธิภาพ เมื่อเกิดภัย
   - จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและขนส่งสิ่งของที่จำเป็นต่าง ๆ

3) การจัดเตรียมอุปกรณ์วัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้
   - เตรียมอุปกรณ์ยังชีพ เช่น ไฟฉาย น้ำดื่ม อุปกรณ์ทำแผล และยา ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ
   - ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
   - ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง
   - ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง
   - ศึกษาแผน/ ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน
4) การจัดเตรียมมาจรการเพื่อความปลอดภัยของอาคาร
   - สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลอาคารตามความเหมาะสม
   - เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้นถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน
5) การปฏิบัติขั้นเตรียมการ
   - มีการซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
   - ทำสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ
   - อบรมให้ความรู้การปฏิวัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่ บุคลากรในองค์กร
   - รายงานสรุปผลการปฏิบัติการขั้นตอนการเตรียม

3.6 กรณีชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวยรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจลเตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยจากการชุมนุมประท้วงและก่อจลาจล

1) จัดทำแผนเตรียมความพร้อมรับสถานการณ์การชุมนุมทางการเมืองด้านเทคโนโลยีสารสนเทศ
2) จัดทำแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (Business Continuity Planning) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานในพื้นที่ได้ ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง
3) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม
4) ตรวจสอบระบบไฟฟ้า ระบบปั้มน้ำ ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน
5) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย
6) จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไหล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงานที่บริษัท

7) จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

3.7 การเตรียมความพร้อมกรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย /อุปกรณ์

เพื่อเป็นการป้องกันและเตรียมความพร้อม

1) ติดตามข่าวสารการโจรกรรมจากสื่อ หรือจากบุคคลในชุมชน
2) มีการตรวจสอบการทำงานของระบบกล้องวงจรปิด สัปดาห์ละ 1 ครั้ง เป็นอย่างน้อย
3) มีการตรวจสอบระบบรักษาความปลอดภัย สัปดาห์ละ 1 ครั้ง เป็นอย่างน้อย
4) มีการตรวจสอบระบบไฟส่องสว่าง เดือนละ 1 ครั้ง เป็นอย่างน้อย
5) มีการตรวจสอบสภาพโดยรอบของตัวอาคาร ห้องควบคุมระบบเครือข่าย และห้องปฏิบัติการ เดือนละ 1 ครั้ง เป็นอย่างน้อย

3.8 การเตรียมความพร้อมกรณีเกิดเหตุน้ำท่วม/ น้ำรั่วซึม

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่วซึม ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินเกิดจากน้ำท่วม/ น้ำรั่วซึม
2) มีการตรวจสอบน้ำท่วม/น้ำรั่วซึม ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างน้อยสัปดาห์ละ 1 ครั้ง และควรตรวจสอบถี่ขึ้นในช่วงที่มีฝนตก

3.9 การเตรียมความพร้อมกรณีไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้า ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้น เพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ / หม้อไฟระเบิด
2) ติดตั้งเครื่องสำรองไฟฟ้าและหรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์ (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 30 นาที
3) ตรวจสอบระบบไฟฟ้าและอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ
4) จัดทำ Checklist ระยะเวลาในการเปิด / ปิด ระบบสารสนเทศเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย กรณีที่ระบบไฟฟ้าดับหรือถูกตัด
5) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ
6) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

4. <u>การกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน</u>

องค์กรมอบหมายหน้าที่ความรับผิดชอบ เพื่อรองรัยภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

4.1 รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ได้แก่

กรรมการผู้จัดการใหญ่ (Chief Executive Officer : CEO)

ผู้จัดการฝ่ายเทคโนโลยีสารสนเทศ (IT Manager)

4.2 รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องแม่ข่าย และแอปพลิเคชั่น ได้แก่

คุณอุไรรัตน์ สุระเสน	เบอร์โทรศัพท์ติดต่อ	มือถือ (081) 732 4247
คุณอรนุช นาสมบูรณ์	เบอร์โทรศัพท์ติดต่อ	มือถือ (092) 535 9244
คุณกิตติศักดิ์ รัตนตระกูลไทย	เบอร์โทรศัพท์ติดต่อ	มือถือ (062) 496 6244
คุณนฤมล สายพรหม	เบอร์โทรศัพท์ติดต่อ	มือถือ (062) 292 6144
คุณภูวนาถ สำแดง	เบอร์โทรศัพท์ติดต่อ	มือถือ (090) 963 4708

4.3 รับผิดชอบการประสานงาน หน่วยงานภายในและภายนอกที่เกี่ยวข้องกับระบบไฟฟ้า กรณีไฟดับ/ หม้อระเบิด/ ไฟไหม้ และอาคารสถานที่ กรณีน้ำท่วม/ รั่วซึม ได้แก่

คุณปัณณรุจน์ ทองนพเก้า	เบอร์โทรศัพท์ติดต่อ	มือถือ (099) 326 4632
คุณไชยณรงค์ อุ่นนุช	เบอร์โทรศัพท์ติดต่อ	มือถือ (081) 865 5165

4.4 รับผิดชอบการสำรวจตรวจสอบทรัพย์สิน ได้แก่

คุณธัญพร พลายงาม	เบอร์โทรศัพท์ติดต่อ	มือถือ (081) 720 6809
คุณอรนุช นาสมบูรณ์	เบอร์โทรศัพท์ติดต่อ	มือถือ (092) 535 9244
คุณภูวนาถ สำแดง	เบอร์โทรศัพท์ติดต่อ	มือถือ (090) 963 4708

4.5 รับผิดชอบการสำรอง / กู้คืนข้อมูล ปัญหาจากการโดนเจาะระบบหรือภัยคุกคามทางคอมพิวเตอร์ ได้แก่

คุณอุไรรัตน์ สุระเสน	เบอร์โทรศัพท์ติดต่อ	มือถือ (081) 732 4247
คุณกิตติศักดิ์ รัตนตระกูลไทย	เบอร์โทรศัพท์ติดต่อ	มือถือ (062) 496 6244

5. <u>แผนการกู้คืนระบบและข้อมูล</u>

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครือข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานและรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลาและรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนโดยเร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

1) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4) ขอยืมอุปกรณ์คอมพิวเตอร์ของหน่วยงานอื่นมาใช้ชั่วคราว

5) นำ Backup Device / CD-ROM / Hard Disk ที่ได้สำรองข้อมูลไว้กลับมา Restore กลับมาโดยเร็วภายใน 72 ชั่วโมง
6) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูล และระบบอื่น ๆ ที่เกี่ยวข้อง

6. <u>การติดตามและรายงานผล</u>

กำหนดให้มีผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ระบุไว้

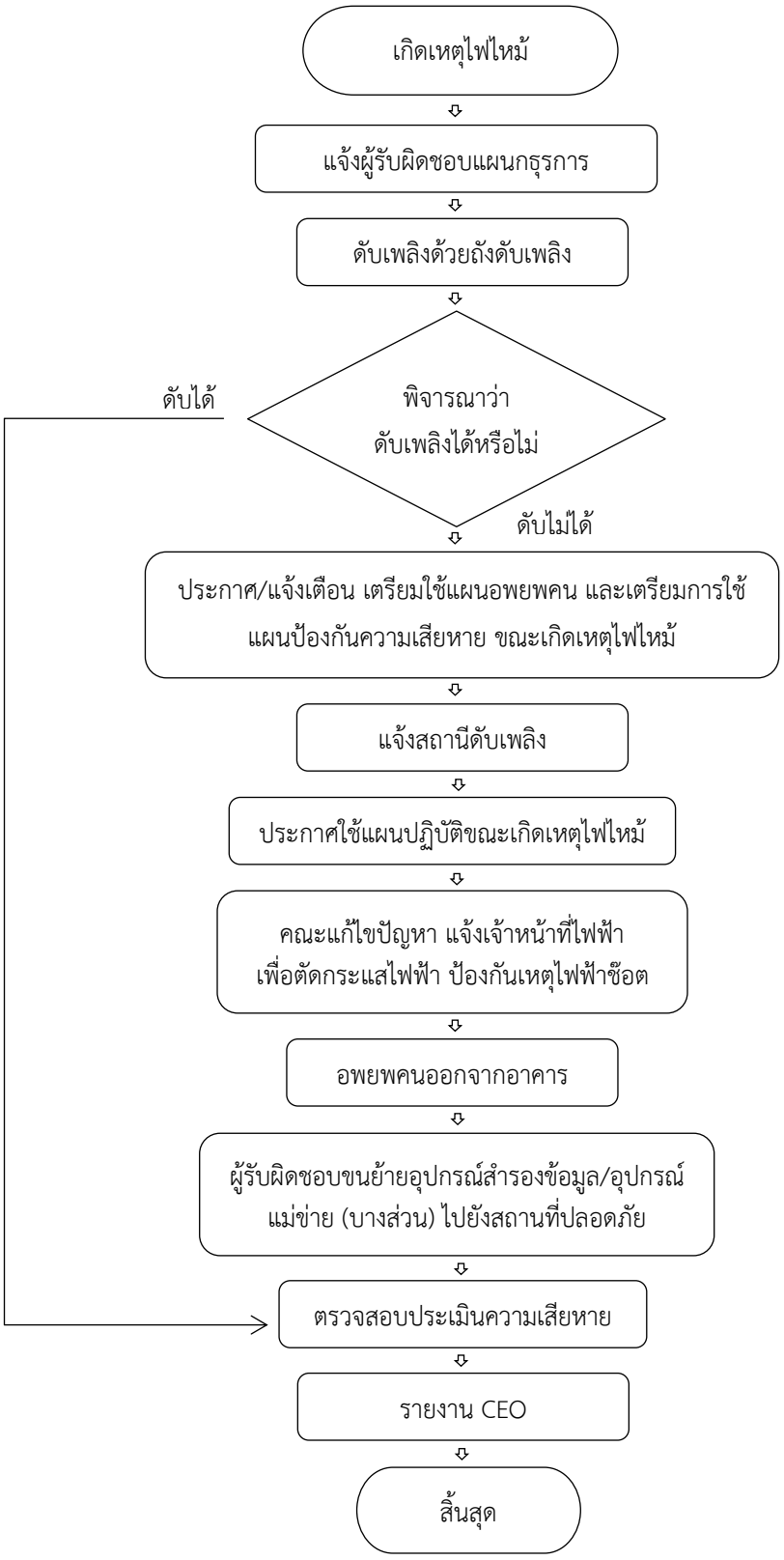
ภาคผนวก
เบอร์โทรศัพท์หน่วยแจ้งเหตุฉุกเฉิน

191	:	เหตุด่วนเหตุร้าย
1646	:	ศูนย์เอราวัณ
192	:	ศูนย์เตือนภัยพิบัติแห่งชาติ
1784	:	สายด่วนนิรภัย
1418	:	มูลนิธิป่อเต็กตึ๊ง
02 226 4444-8	:	มูลนิธิร่วมกตัญญู
02 337 3497	:	สถานีดับเพลิงบางพลี
02 328 1161-63	:	สถานีดับเพลิงและกู้ภัยเฉลิมพระเกียรติ
02 740 3211	:	สถานีตำรวจภูธรบางแก้ว
09 3112 2275	:	สถานีตำรวจนครบาลบางนา
02 769 5200	:	การไฟฟ้านครหลวงเขตบางพลี

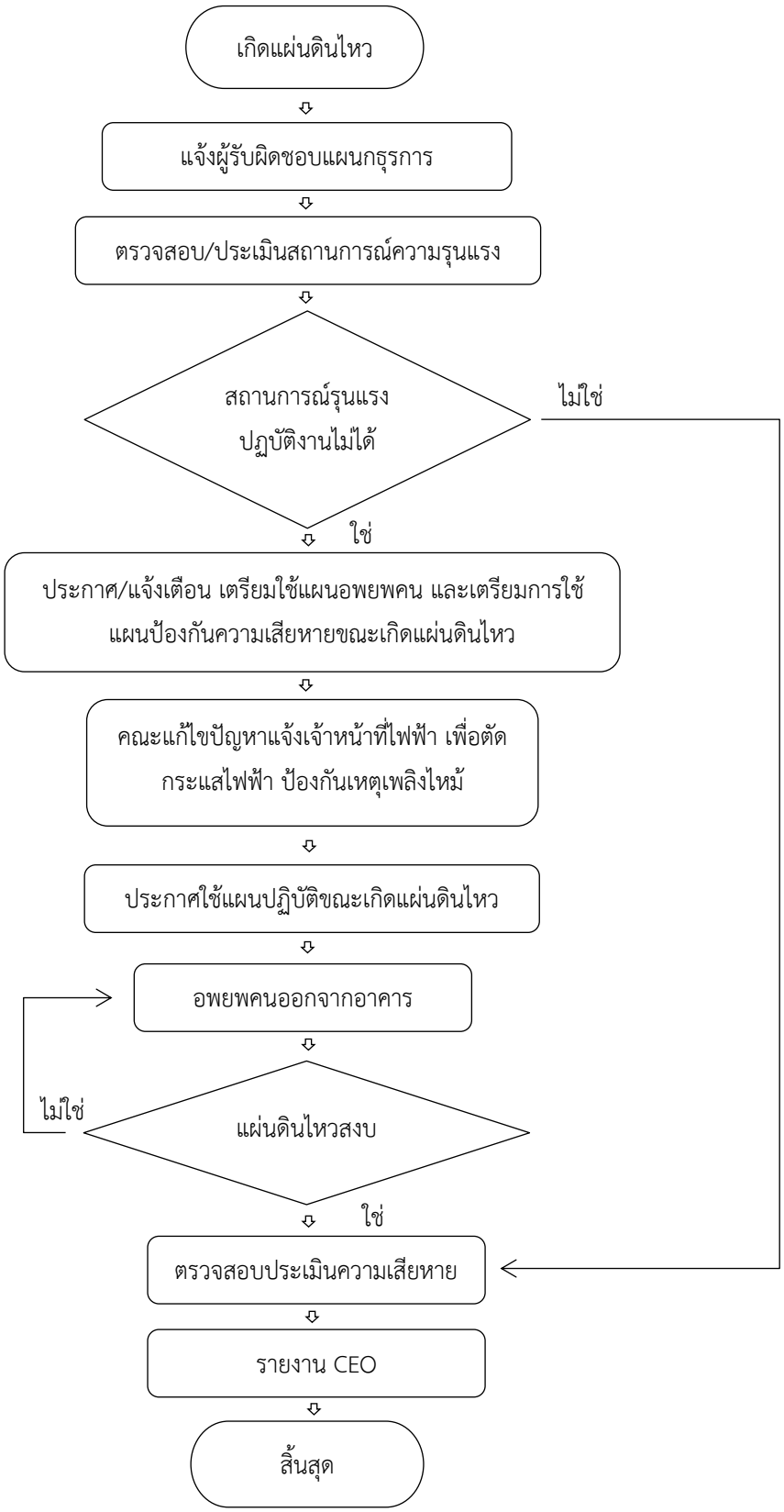
ภาคผนวก ข

ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ

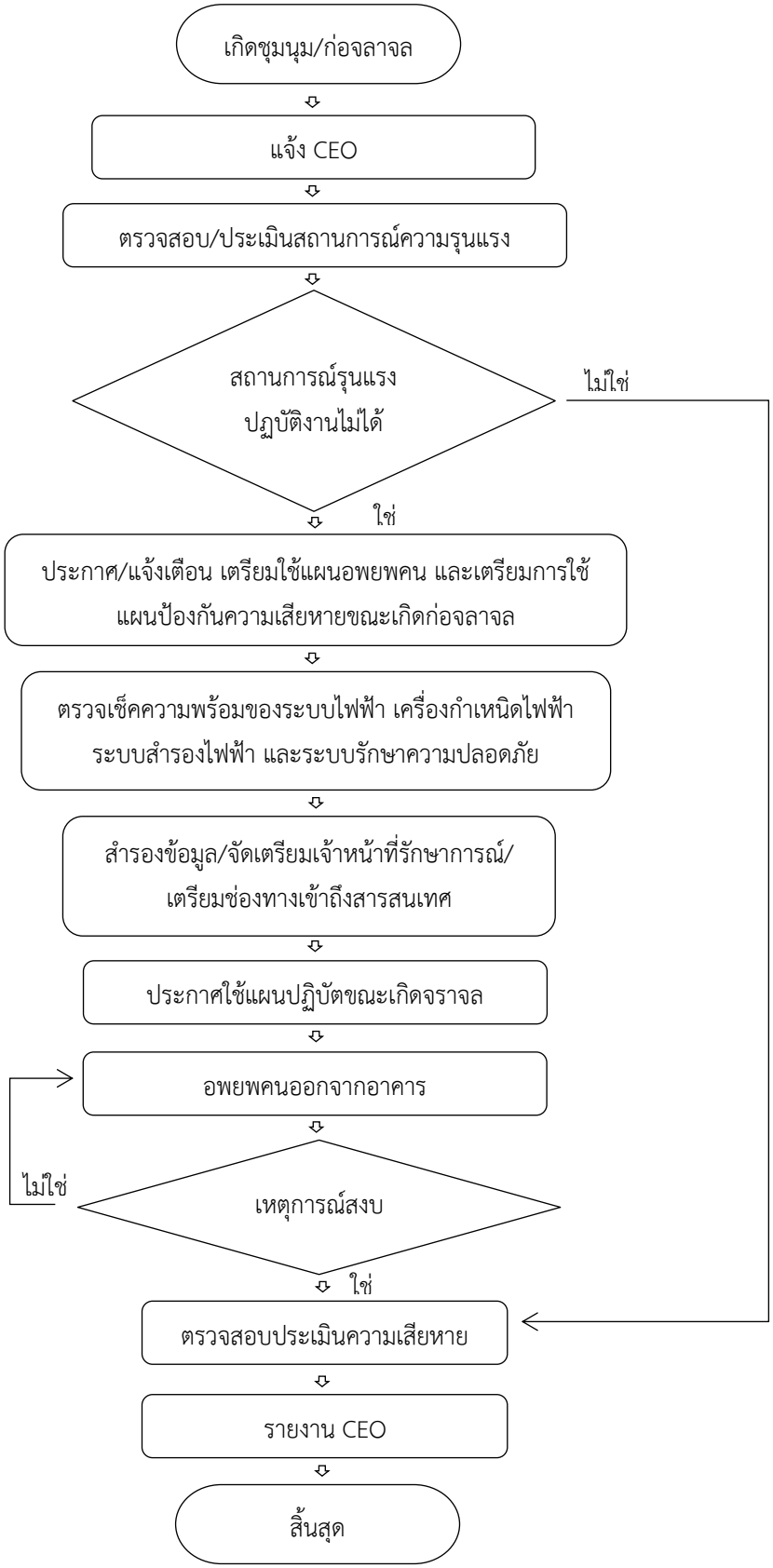
1. กรณีเกิดเหตุไฟไหม้



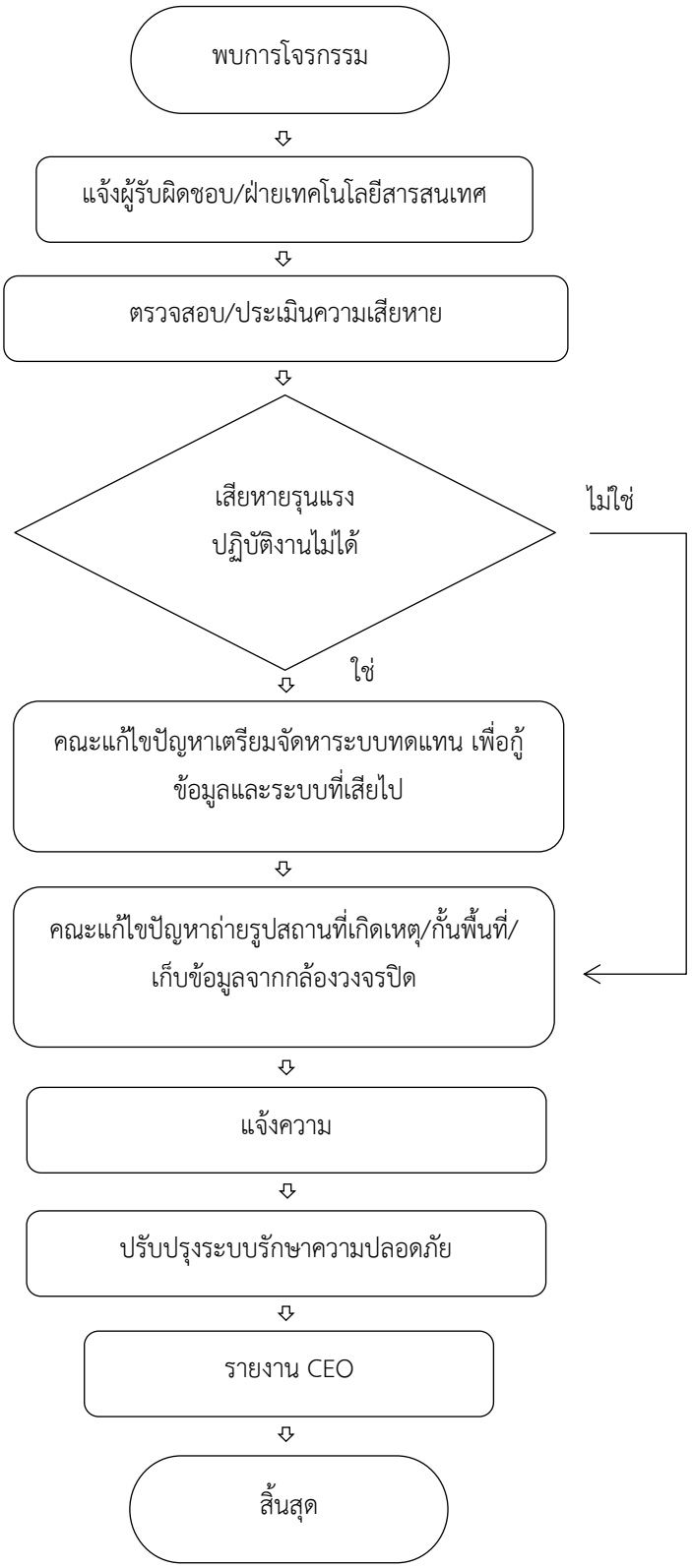
2. กรณีแผ่นดินไหว



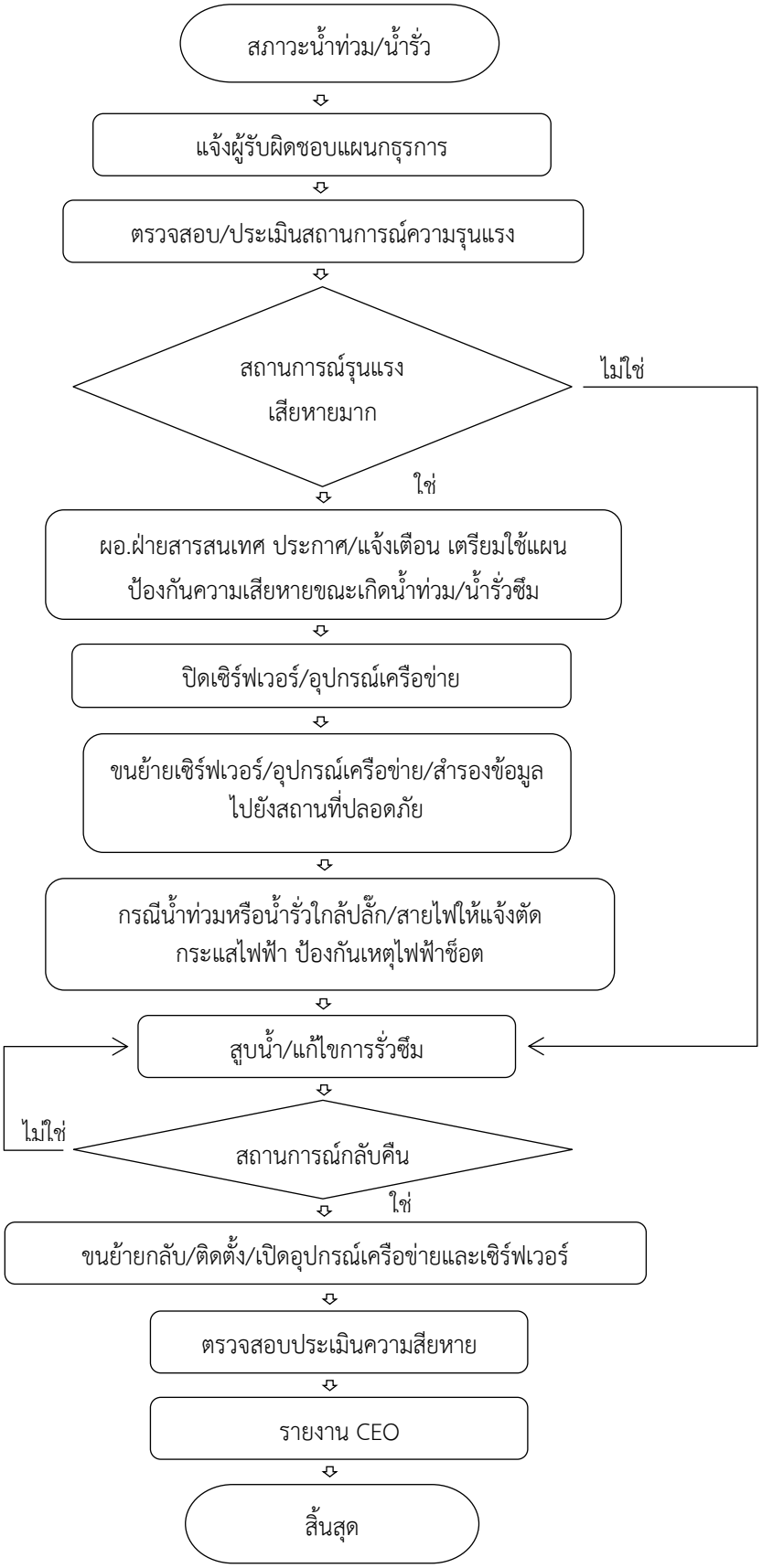
3. กรณีชุมนุมประท้วงและก่อจลาจล



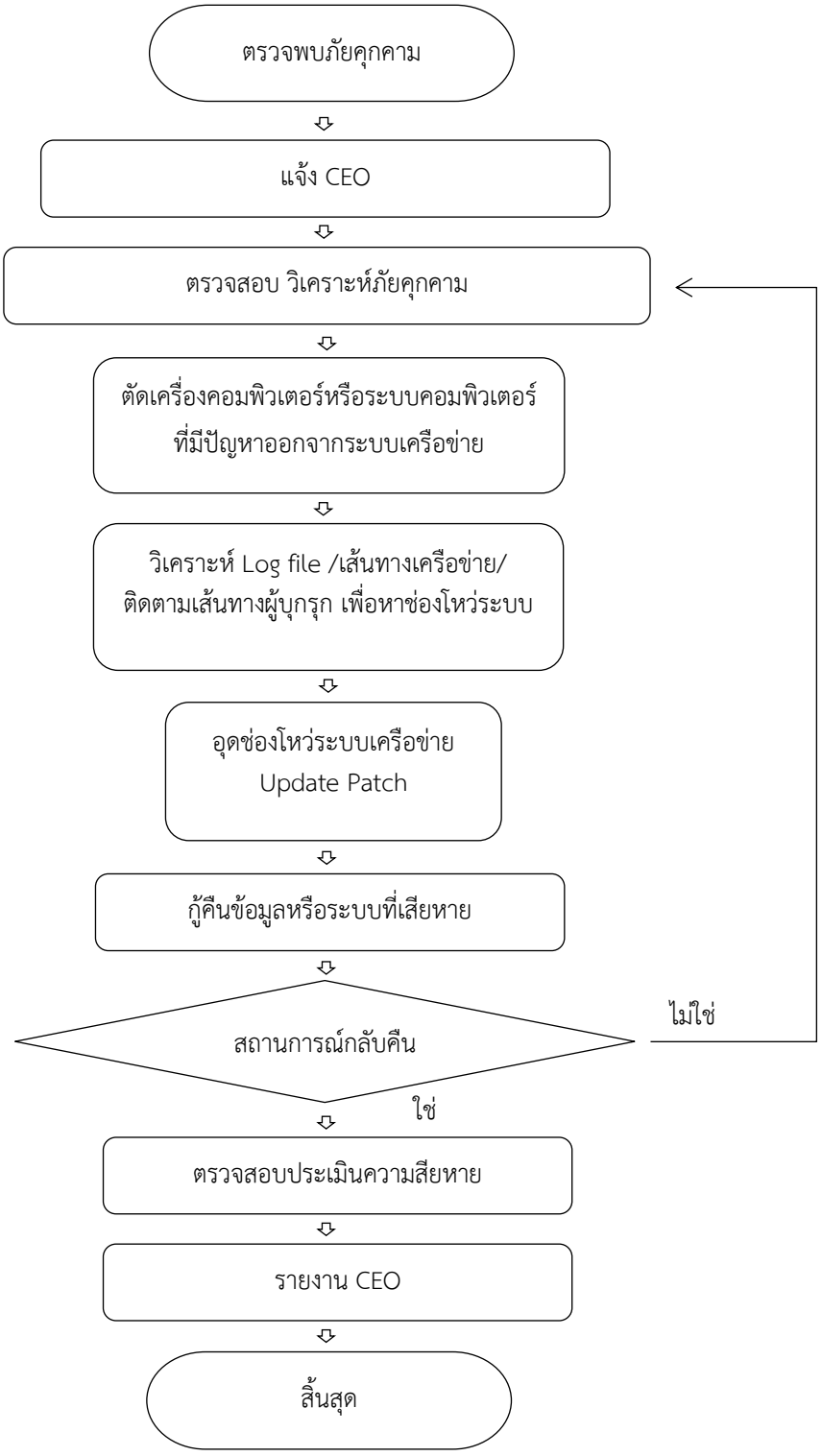
4. กรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์



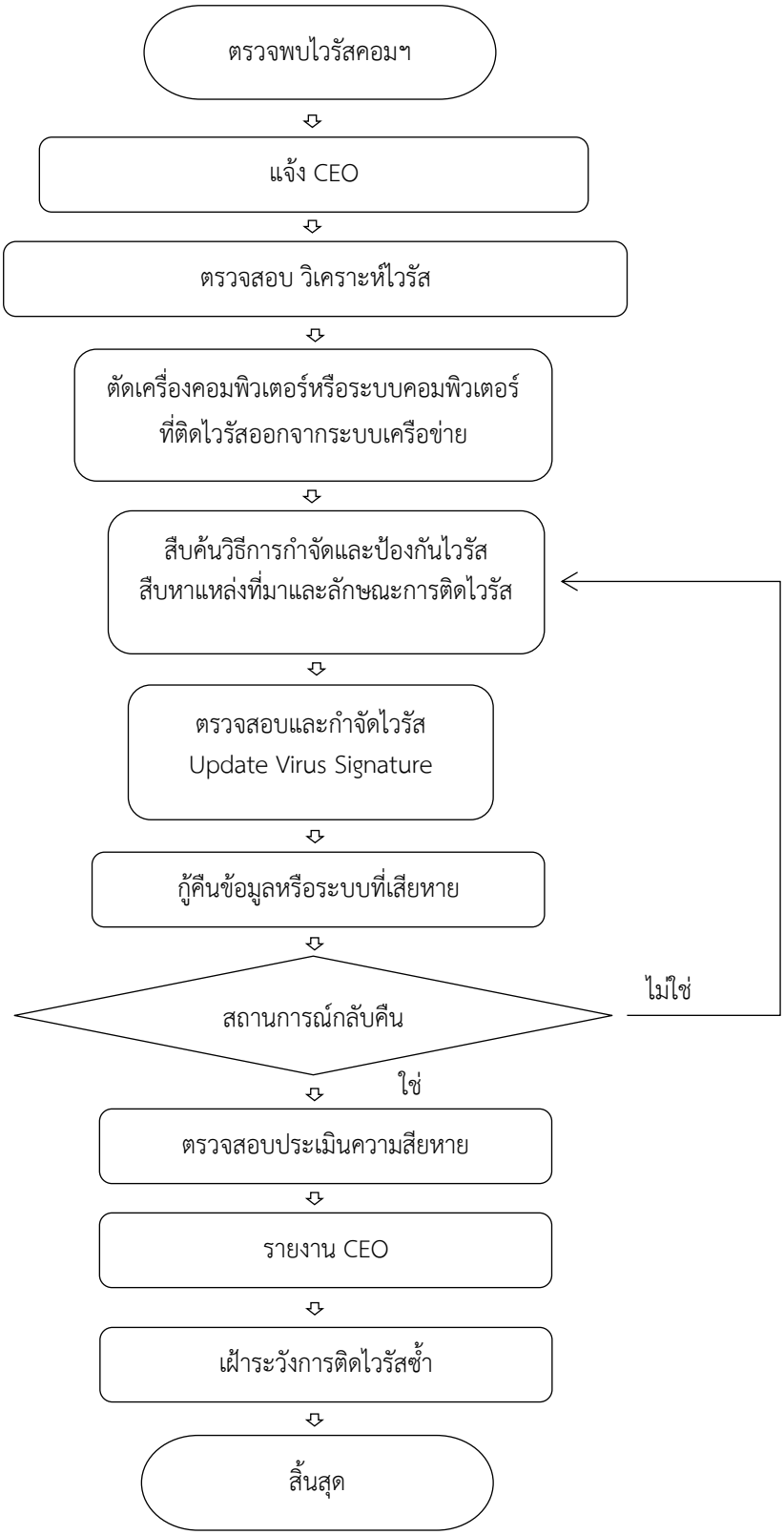
5. กรณีน้ำท่วม-น้ำรั่วซึม



6. กรณีการบุกรุก และภัยคุกคามทางคอมพิวเตอร์



7. กรณีไวรัสคอมพิวเตอร์



8. กรณีไฟฟ้าดับ/หม้อไฟระเบิด