TRITON

ประกาศที่ 002/2563

เรื่อง แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

โดยมติที่ประชุมคณะกรรมการบริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) ครั้งที่ 1/2563 เมื่อวันที่ 24 มกราคม 2563 ได้มีมติอนุมัติ แผนรับสถานะการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ รายละเอียดตามเอกสารที่แนบมานี้

ฝ่ายบริหารจึงเห็นควรประกาศแจ้งมาเพื่อให้พนักงานในกลุ่มบริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย รับทราบเพื่อนำไปใช้ปฏิบัติให้เป็นแนวทางเดียวกันทั่วทั้งองค์กร ทั้งนี้ ให้มีผลบังคับใช้ ตั้งแต่วันที่ 1 กุมภาพันธ์ 2563 เป็นต้นไป

ประกาศมา ณ วันที่ 27 มกราคม 2563

.....

นายเชิดศักดิ์ กู้เกียรตินันท์

ประธานเจ้าหน้าที่บริหาร

TRITON

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ

บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน) และบริษัทย่อย

จัดทำโดย ฝ่ายสารสนเทศ

บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน)

ประจำปี 2563

คำนำ

ข้อมูลสารสนเทศถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานของบุคลากรในองค์กร ฝ่ายสารสนเทศได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศขององค์กรซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศรวมทั้งระบบอุปกรณ์ต่าง ๆ เสียหายได้ ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร สามารถแก้ไขปัญหาและลดความเสี่ยงที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศรวมถึงระบบอุปกรณ์ต่าง ๆ

สารบัญ

วัตถุประสงค์

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

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) ที่ฝ่ายสารสนเทศจัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหา ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. การเตรียมความพร้อม
4. การกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
5. แผนการกู้คืนระบบและข้อมูล
6. การติดตามและรายงานผล

1 การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศขององค์กรสามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

- ภัยธรรมชาติที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายได้แก่ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ
- การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล
- ระบบการสื่อสารของเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง
- ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ
- การบุกรุกหรือโจมตีจากภายนอกเพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล
- ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

- ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลาย
- ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร
- เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์และซอฟต์แวร์อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้หรือหยุดการทำงาน

1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation Assessment)

เมื่อองค์กรมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้วจะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่าง ๆ (Security Log Management System) โดยเจ้าหน้าที่เทคโนโลยีสารสนเทศเพื่อนำมาสรุปเป็นข้อมูลดังนี้

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (1 รุนแรงต่ำสุด, 5 รุนแรงสูงสุด)			รวม	จัดลำดับ
	ต่อระบบงาน	ต่อพันธกิจตามกฎหมาย	ต่อประชาชน		
กรณีไฟไหม้	5	5	5	15	1
กรณีแผ่นดินไหว	4	1	5	10	2
กรณีจลาจล การชุมนุม/เหตุการณ์ความไม่สงบ/สถานการณ์ทางการเมือง	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	3	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

ตารางแสดงผลการประเมินสถานการณ์และระดับความรุนแรง

2 ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

ฝ่ายสารสนเทศมีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ประธานเจ้าหน้าที่บริหาร (CEO) จะสั่งการให้ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูงของบริษัทเพื่อประกาศใช้แผนต่อไป

2.2 กำหนดขั้นตอนการดำเนินงาน

ฝ่ายสารสนเทศจัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือผิดปกติ โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่าง ๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

2.3 การป้องกันการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์

เพื่อเป็นการป้องกันการโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์ มีแนวทางดังนี้

1) มีการควบคุมการเข้า–ออก ของพนักงาน และผู้ที่มาติดต่อ โดยมีการกำหนดช่วงเวลาที่อนุญาต ตลอดจนพื้นที่ที่อนุญาตในการเข้าถึงตามสิทธิ์หรืออำนาจหน้าที่
2) มีการควบคุมการนำอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ เข้า–ออก อาคาร
3) มีการติดตั้งกล้องโทรทัศน์วงจรปิดตามจุดต่าง ๆ อย่างทั่วถึง
4) มีการติดตั้งไฟส่องสว่างอย่างทั่วถึง
5) มีการจัดเจ้าหน้าที่รักษาความปลอดภัยประจำจุดและมีการลาดตระเวนตรวจตราอย่างเพียงพอและทั่วถึง

2.4 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

1) กำหนดมาตรการควบคุมการเข้า–ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็นให้เจ้าหน้าที่ของฝ่ายสารสนเทศที่เป็นผู้รับผิดชอบพาเข้าไปในห้องควบคุม ควรมีการติดตั้งระบบควบคุมการเข้า-ออกห้องควบคุม (Access Control) และอนุญาตเฉพาะผู้ที่เกี่ยวข้องเท่านั้น
2) มีการติดตั้งกล้องโทรทัศน์วงจรปิด (CCTV) ภายในห้องควบคุมระบบเครือข่าย เพื่อป้องกันการโจรกรรม
3) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย
4) มีการติดตั้ง IPS (Intrusion Prevention System) เพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้าย ๆ กับ IDS (Intrusion Detection System) แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ Hardware ตัวอื่น ๆ
5) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเทอร์เน็ตของบริษัท เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

6) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยจัดหาระบบบริหารจัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในเครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของบริษัทให้ดียิ่งขึ้น

7) มีระบบยืนยันตัวตนในการเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้งานระบบเครือข่ายหรืออินเทอร์เน็ต ตามอำนาจหน้าที่และความรับผิดชอบ

2.5 การป้องกันและกำจัดไวรัส

เพื่อเป็นการป้องกันและกำจัดไวรัสที่อาจเข้ามาทำลายหรือสร้างความเสียหายแก่ข้อมูลหรือระบบสารสนเทศ มีแนวทางดังนี้

1) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

2) อัปเดตข้อมูลไวรัสอย่างสม่ำเสมอ ทุก 1 เดือน เป็นอย่างน้อย

3) ผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเทอร์เน็ต หรือการใช้งานอีเมล เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

2.6 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 30 นาที

2) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Generator) ที่เป็นระบบอัตโนมัติ ซึ่งจะทำงานทันทีเมื่อเกิดไฟฟ้าดับ

3) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

4) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

3 การเตรียมความพร้อม

3.1 การจัดเตรียมอุปกรณ์

ฝ่ายสารสนเทศ ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

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

3.2 การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น

3.3 การสำรองข้อมูล

เพื่อเป็นการเตรียมความพร้อมในการรับมือต่อความบกพร่องอันเกิดจากการทำงานและภัยพิบัติ เมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุกแทรกแซงเปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลกลับมาใช้งานได้ บริษัทจึงได้มีการกำหนดนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ไว้ในนโยบายด้านความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ หัวข้อที่ 6 ข้อย่อยที่ 7

3.4 การเตรียมความพร้อมกรณีเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟไหม้
2) ติดตั้งระบบดับเพลิงอัตโนมัติ (Fire Suppression System) ในห้องควบคุมระบบเครือข่าย
3) ติดตั้งเครื่องดับเพลิงในทุกชั้นของอาคารเพื่อการควบคุมเพลิงในเบื้องต้น สำหรับห้องปฏิบัติงานคอมพิวเตอร์ควรติดตั้งถังดับเพลิงชนิดหูหิ้วที่สามารถดับไฟประเภท C ได้ โดยไม่ทำความเสียหายแก่อุปกรณ์หรือเครื่องคอมพิวเตอร์ (อุปกรณ์ไฟฟ้า อิเล็กทรอนิกส์ คอมพิวเตอร์)

3.5 การเตรียมความพร้อมกรณีแผ่นดินไหว

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัยแผ่นดินไหว

1) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่าง ๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่
    - กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)

- ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (http://122.155.1.141/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) การสังเกตพฤติกรรมของสัตว์ สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

- สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู
- แมลงสาบจำนวนมากวิ่งเพ่นพ่าน
- หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน
- ปลากระโดดขึ้นมาจากผิวน้ำ

3) การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

- ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน
- ประสานการเตรียมการกับส่วนราชการเกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
- สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร
- สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย
- จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

4) การจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

- เตรียมอุปกรณ์ยังชีพ เช่น ไฟฉาย น้ำดื่ม อุปกรณ์ทำแผลและยา ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ
- ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า
- ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง
- ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง
- ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

5) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

- สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม
- เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไข หรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

6) การปฏิบัติขั้นเตรียมการ

- การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม
- การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญและกำหนดมาตรการในการเผชิญภัย
- อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่ บุคลากรในองค์กร
- รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

3.6 กรณีชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ 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 ระบบปั๊มน้ำ ระบบสำรองไฟฟ้า เครื่องกำเนิดไฟฟ้า และระบบรักษาความปลอดภัยสำหรับห้องควบคุมระบบเครือข่าย ให้อยู่ในสภาพที่พร้อมใช้งาน
5) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย
6) จัดเตรียมช่องทางการเข้าใช้งานระบบจากระยะไกล (Remote) กรณีที่มีเหตุขัดข้องเจ้าหน้าที่สามารถ Remote เข้ามาแก้ไขปัญหาได้ทันที โดยไม่ต้องเดินทางมาปฏิบัติงานที่บริษัท
7) จัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ เป็นต้น

3.7 การเตรียมความพร้อมกรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์

เพื่อเป็นการป้องกันและเตรียมความพร้อม

1) ติดตามข่าวสารการโจรกรรมจากสื่อ หรือ จากบุคคลในชุมชน
2) มีการตรวจสอบการทำงานของระบบกล้องวงจรปิด สัปดาห์ละ 1 ครั้งเป็นอย่างน้อย
3) มีการตรวจสอบระบบรักษาความปลอดภัย สัปดาห์ละ 1 ครั้งเป็นอย่างน้อย
4) มีการตรวจสอบระบบไฟส่องสว่าง เดือนละ 1 ครั้งเป็นอย่างน้อย
5) มีการตรวจสอบสภาพโดยรอบของตัวอาคาร ห้องควบคุมระบบเครือข่าย และห้องปฏิบัติการ เดือนละ 1 ครั้งเป็นอย่างน้อย

3.8 การเตรียมความพร้อมกรณีเกิดเหตุน้ำท่วม/น้ำรั่วซึม

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่วซึม ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม/น้ำรั่วซึม
2) ติดตั้งระบบตรวจจับการรั่วซึมของน้ำ (Water Leak Detection System) ในห้องควบคุมระบบเครือข่าย
3) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบเครือข่าย เพื่อให้ปลอดภัยต่อการรั่วซึม อย่างน้อยสัปดาห์ละ 1 ครั้ง และควรตรวจสอบถี่ขึ้นในช่วงที่มีฝนตก

3.9 การเตรียมความพร้อมกรณีไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

1) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ/หม้อไฟระเบิด
2) ติดตั้งเครื่องกำเนิดไฟฟ้า (Generator) และตรวจเช็คความพร้อมอยู่เสมอ ได้แก่ ปริมาณน้ำมัน แบตเตอรี่ และตั้งเวลาทดสอบการทำงานอัตโนมัติสัปดาห์ละ 1 ครั้งเป็นอย่างน้อย ซึ่งเมื่อระบบไฟฟ้าถูกตัด เครื่องกำเนิดไฟฟ้าจะทำงานทันทีโดยจ่ายกระแสไฟฟ้าเข้าห้องควบคุมระบบเครือข่ายเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่องเป็นระยะเวลาประมาณ 8 ชั่วโมง
3) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 30 นาที
4) ตรวจสอบระบบไฟฟ้าและอุปกรณ์ไฟฟ้าให้พร้อมใช้งานอยู่เสมอ
5) จัดทำ Checklist ระยะเวลาในการปิด/เปิด ระบบสารสนเทศเครื่องคอมพิวเตอร์แม่ข่ายติดตั้งอยู่ในห้องควบคุมระบบเครือข่าย กรณีที่ระบบไฟฟ้าดับหรือถูกตัด
6) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
7) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

4 การกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

องค์กรมอบหมายหน้าที่ความรับผิดชอบ เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

4.1 **รับผิดชอบในการกำหนดนโยบาย** ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแลควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติงาน ผู้รับผิดชอบ ได้แก่

ประธานเจ้าหน้าที่บริหาร (Chief Executive Officer : CEO)

ผู้จัดการอาวุโสฝ่ายสารสนเทศ (Senior IT Manager)

4.2 **รับผิดชอบการปฏิบัติงาน** ดูแลระบบ ดูและห้องแม่ข่าย และแอปพลิเคชัน ได้แก่

คุณฉัตรชัย ศุภนาม	เบอร์โทรศัพท์ติดต่อ	081-383-0996
คุณนพพร สุขเจริญ	เบอร์โทรศัพท์ติดต่อ	086-381-8242

4.3 **รับผิดชอบการประสานงาน** หน่วยงานภายในและภายนอกที่เกี่ยวข้องกับระบบไฟฟ้า กรณีไฟดับ/หม้อไฟระเบิด/ไฟไหม้ และอาคารสถานที่ กรณีน้ำท่วม/รั่วซึม ได้แก่

คุณเพ็ญศรี สืบสุวงศ์	เบอร์โทรศัพท์ติดต่อ	094-948-9812
คุณจิตติมา กินกิ่ง	เบอร์โทรศัพท์ติดต่อ	065-594-9178

4.4 **รับผิดชอบการสำรวจตรวจสอบทรัพย์สิน** ได้แก่

คุณประภาวดี สมมาตร	เบอร์โทรศัพท์ติดต่อ	063-189-6985
คุณเพ็ญศรี สืบสุวงศ์	เบอร์โทรศัพท์ติดต่อ	094-948-9812
คุณฉัตรชัย ศุภนาม	เบอร์โทรศัพท์ติดต่อ	081-383-0996

4.5 **รับผิดชอบการสำรอง/กู้คืนข้อมูล** ปัญหาจากการโดนเจาะระบบหรือภัยคุกคามทางคอมพิวเตอร์ ได้แก่

คุณฉัตรชัย ศุภนาม	เบอร์โทรศัพท์ติดต่อ	081-383-0996
คุณนพพร สุขเจริญ	เบอร์โทรศัพท์ติดต่อ	086-381-8242

5 แผนการกู้คืนระบบและข้อมูล

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) โดยปกติระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ จะต้องอยู่ในสภาพพร้อมใช้งานและรองรับการให้บริการกับเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนโดยเร็วที่สุดหรือเท่าที่จะดำเนินการได้ ซึ่งแผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงานโดยดำเนินการดังนี้

1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4. ขอยืมอุปกรณ์คอมพิวเตอร์จากหน่วยงานอื่นมาใช้ชั่วคราว
5. นำ Backup Device / CD-ROM / Hard Disk ที่ได้สำรองข้อมูลไว้นำกลับมา Restore โดยใช้คณะกู้ระบบร่วมกันกู้ระบบกลับมาโดยเร็วภายใน 48 ชั่วโมง
6. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

จากภัยพิบัติดังกล่าวไม่เฉพาะทาง Hardware เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว การก่อวินาศกรรม แต่ยังรวมถึงการถูกเจาะระบบหรือไวรัสคอมพิวเตอร์ ซึ่งอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ จึงมีแผนจัดตั้งศูนย์สำรองข้อมูล (DR and Backup Site) ที่ปลอดภัยและอยู่คนละสถานที่กัน เพื่อเตรียมการบริการด้านเทคโนโลยีสารสนเทศให้มีความต่อเนื่องอยู่เสมอ

ขั้นตอนการดำเนินการ

1. สำรวจความต้องการของระบบสำรอง
2. สำรวจไซต์สำรองที่เหมาะสม
3. การประเมินความเสี่ยงจากสิ่งต่าง ๆ รวมถึงการจัดหามาตรการในการลดความเสี่ยง
4. การจัดลำดับผลกระทบขององค์กร
5. การจัดทำไซต์สำรอง
6. การจัดทำแผนกู้คืน
7. การวางแผน การแต่งตั้งคณะทำงาน ลำดับการทำงานหลังระบบได้รับความเสียหาย
8. การฝึกอบรมให้แก่บุคลากร เพื่อรับทราบหน้าที่ รวมถึงการฝึกอบรมทางด้านเทคนิค
9. การทดสอบแผนกู้คืน อาจทดสอบกับระบบจำลองก่อนการทดสอบกับระบบจริง และทดสอบอย่างน้อยปีละ 1 ครั้ง

6 การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการฝ่ายทรัพยากรบุคคลและธุรการทราบ เพื่อนำเสนอรายงานสรุปให้ CEO เป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้ เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรับสถานการณ์ฉุกเฉินและแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันท่วงทีในกรณีที่เกิดภัยพิบัติต่อไป

ประกาศ ณ วันที่ 1 กุมภาพันธ์ 2563

(นายเชิดศักดิ์ กู้เกียรตินันท์)
ประธานเจ้าหน้าที่บริหาร
บริษัท ไทรทัน โฮลดิ้ง จำกัด (มหาชน)

ภาคผนวก ก

เบอร์โทรศัพท์หน่วยงานแจ้งเหตุฉุกเฉิน

ศูนย์เอราวัณ
1646

ศูนย์นเรนทร
1669

มูลนิธิร่วมกตัญญู
0-2226-4444-8

มูลนิธิป่อเต็กตึ๊ง
1418

SOS
เหตุด่วนเหตุร้าย
191

ศูนย์วิทยุรามา
0-2354-6999


สน.โชคชัย
0-2538-1599

ศูนย์วิทยุพระราม
199


สถานีดับเพลิงลาดพร้าว
0-2511-0032


สถานีดับเพลิงหัวหมาก
0-2314-0071

การไฟฟ้านครหลวง
Metropolitan Electricity Authority
การไฟฟ้านครหลวง
1130

การประปานครหลวง
สนง.ประปาสาขาลาดพร้าว
0-2934-4432-6

สนง.เขตลาดพร้าว
0-2530-6641-5

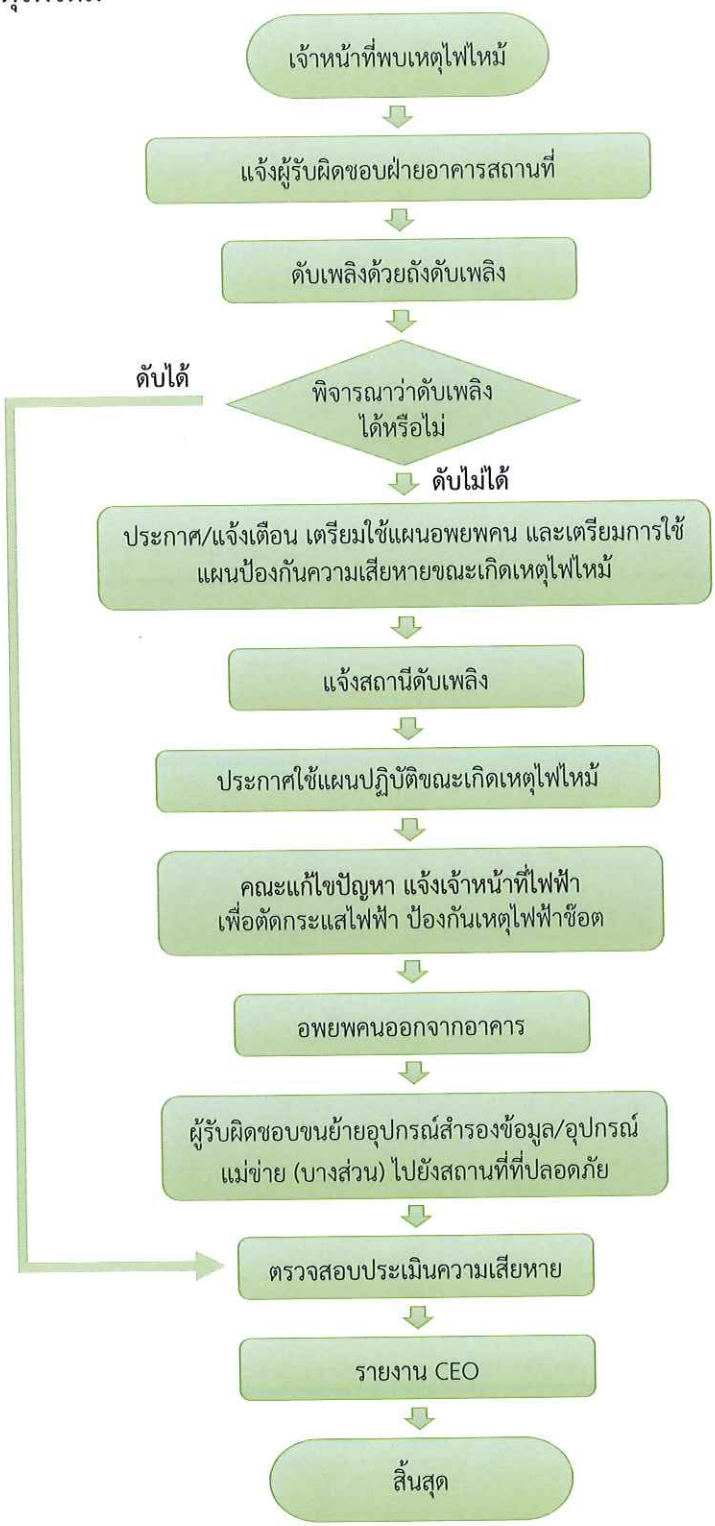
ศูนย์เตือนภัยพิบัติแห่งชาติ
192

บภ.
สายด่วนนิรภัย
1784

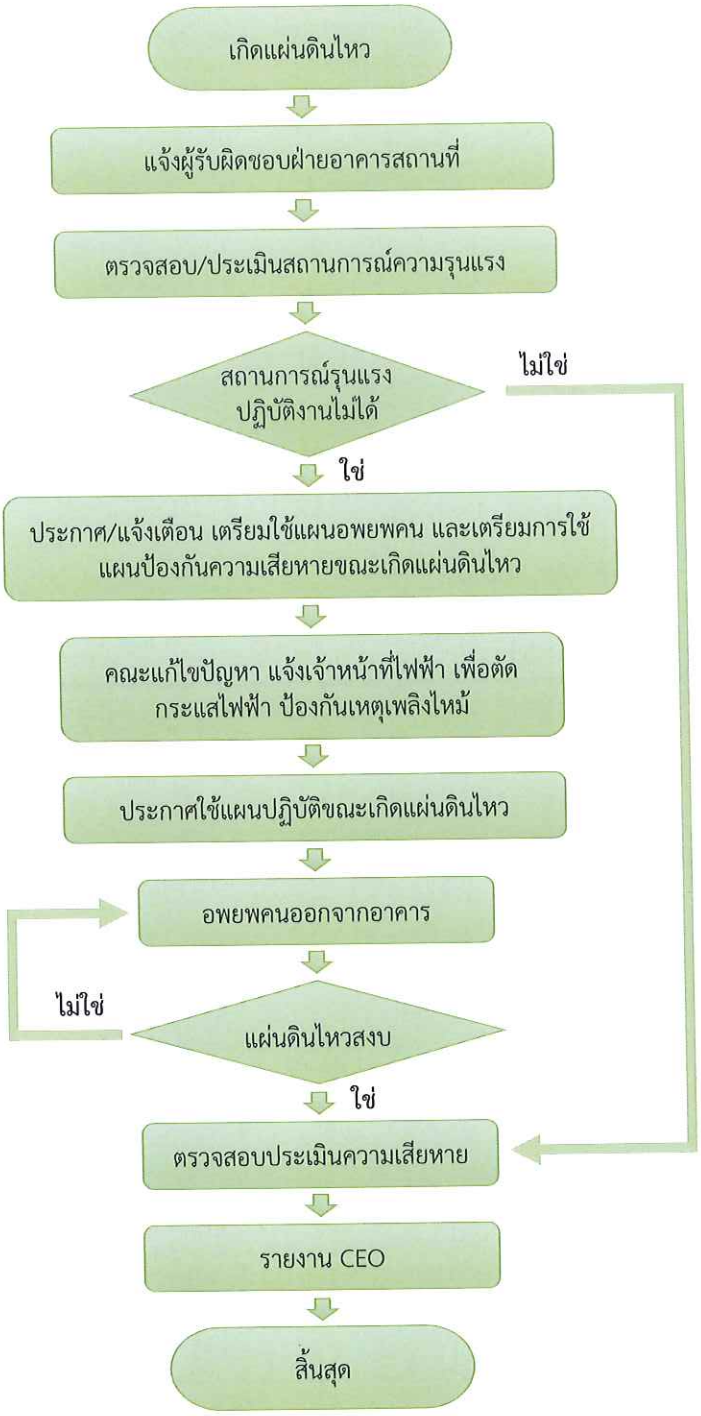
ภาคผนวก ข

ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ

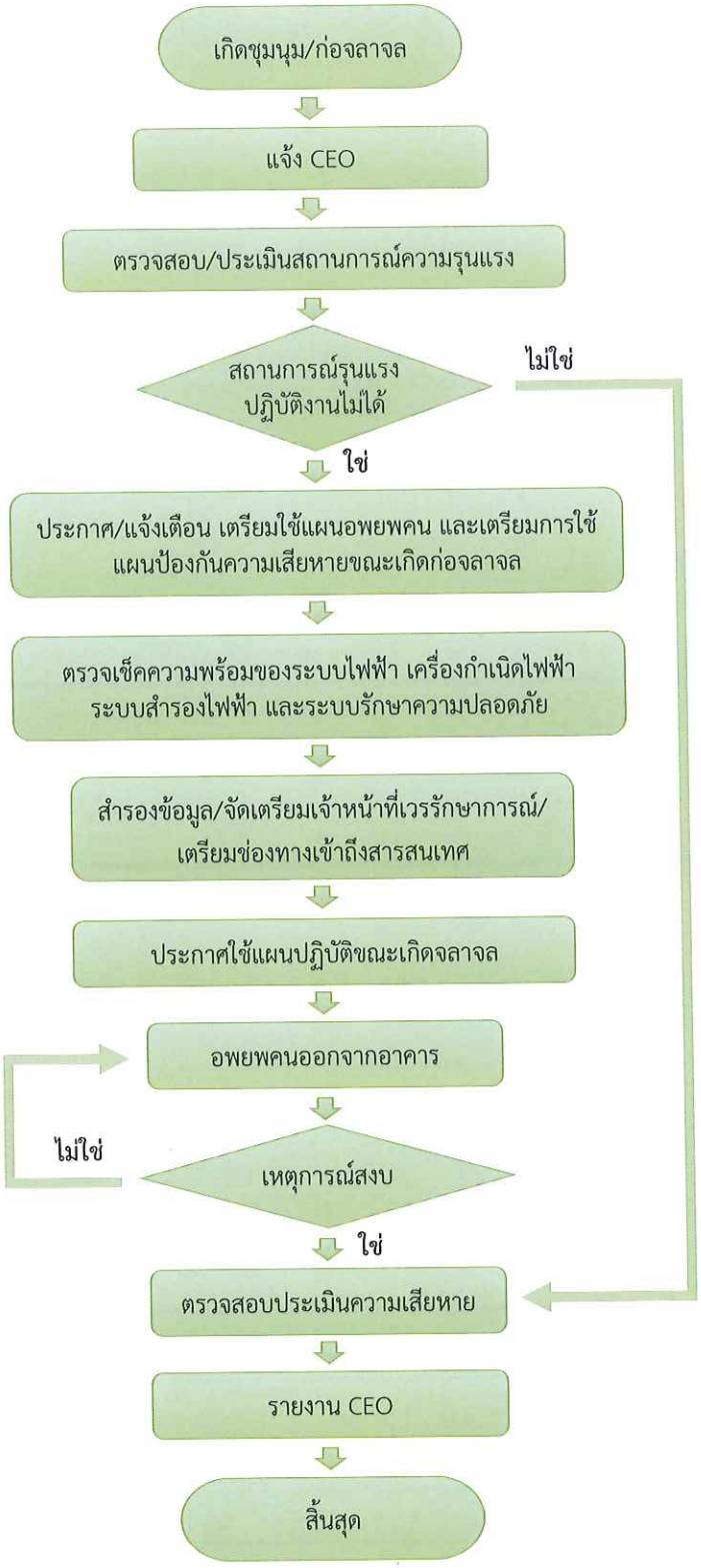
1. กรณีเกิดเหตุไฟไหม้



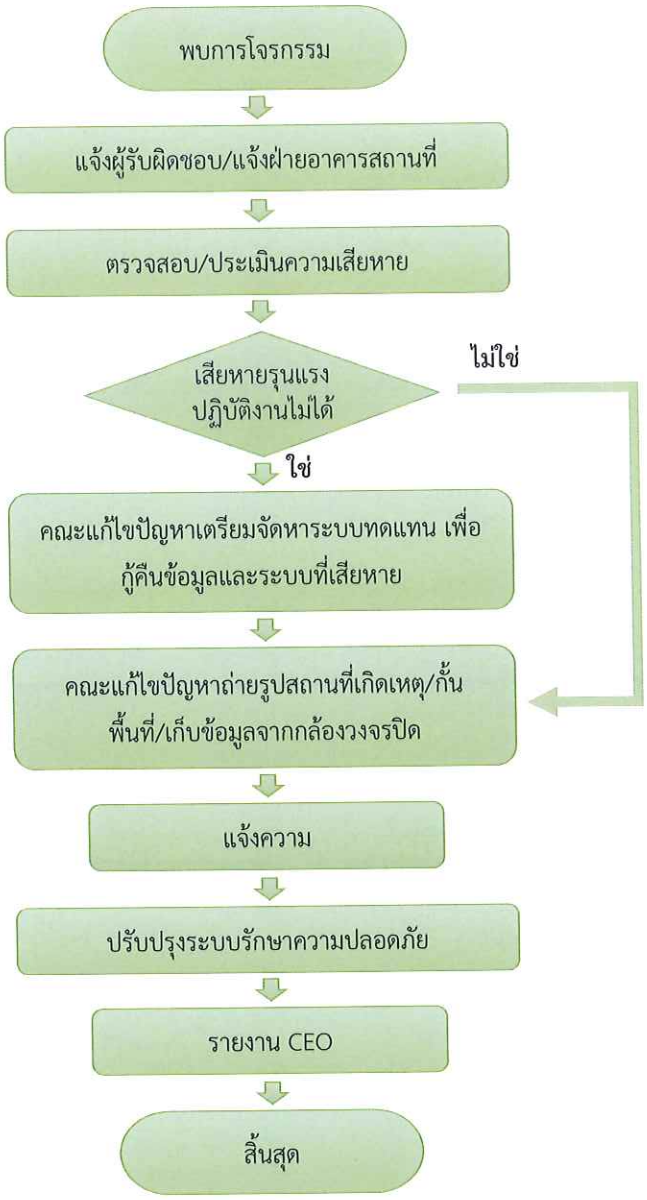
2. กรณีกรณีแผ่นดินไหว



3. กรณีซุมนุมประท้วงและก่อจลาจล

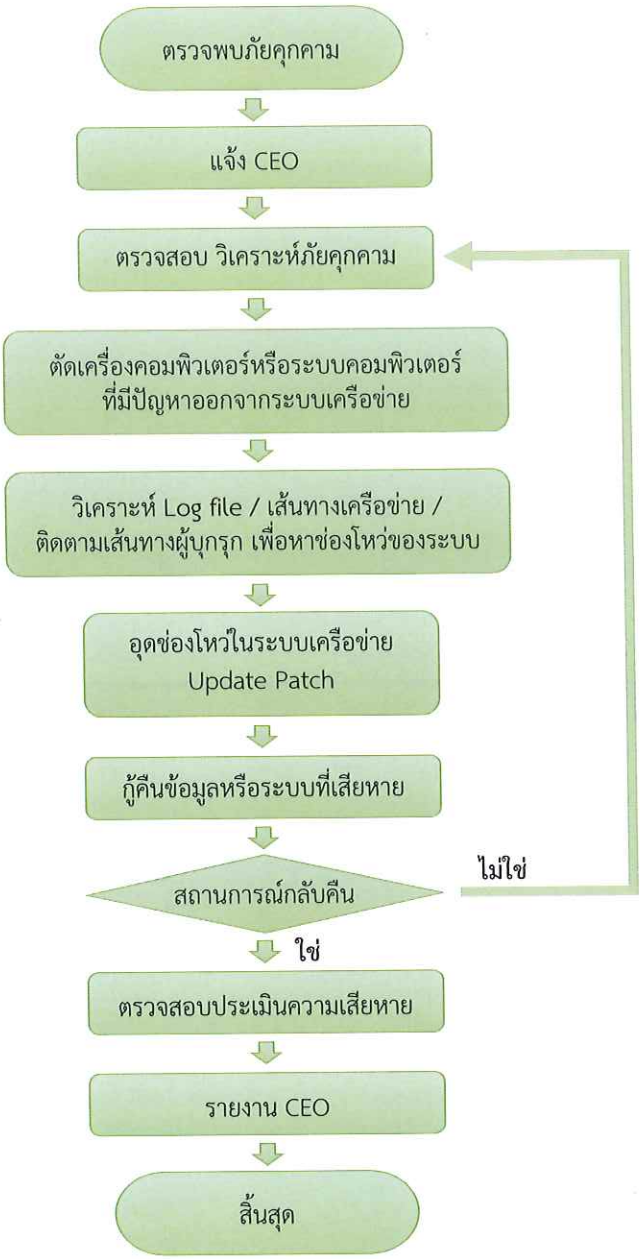


4. กรณีโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่าย/อุปกรณ์

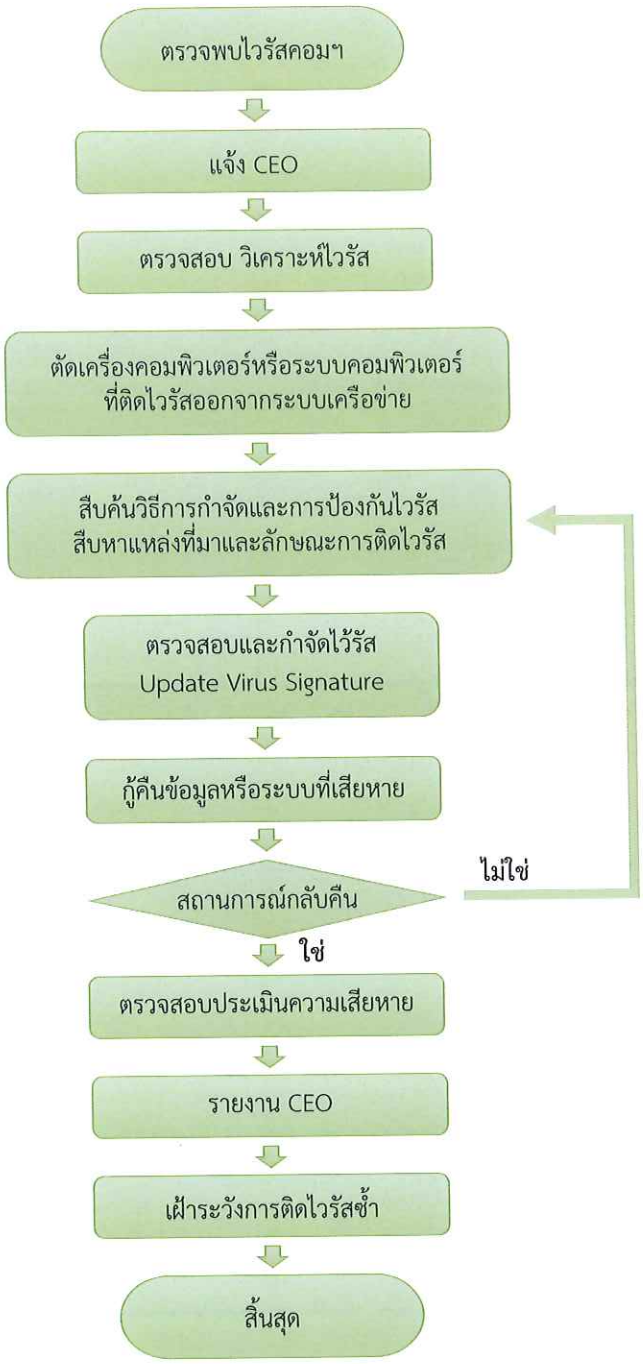


5. กรณีน้ำท่วม/น้ำรั่วซึม

6. กรณีการบุกรุก และภัยคุกคามทางคอมพิวเตอร์



7. กรณีไวรัสคอมพิวเตอร์



8. กรณีไฟฟ้าดับ/หม้อไฟระเบิด