JTS

Jasmine Technology Solution

IT CONTINUITY PLAN

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบสารสนเทศ

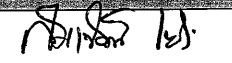
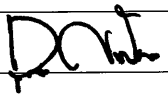
บริษัท จัสมิน เทคโนโลยี โซลูชั่น จำกัด (มหาชน)

รหัสเอกสาร :	[ITGS-CP-001]
หมายเลขปรับปรุงเอกสาร :	1.0
วันที่เอกสารมีผลบังคับใช้ :	01/06/2565
เจ้าของเอกสาร :	สมเจตน์ แซ่จัง
ผู้อนุมัติเอกสาร :	ดุสิต ศรีสง่าโอฬาร

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	คำอธิบายและเหตุผลในการแก้ไข	ผู้แก้ไข	วันที่
1.0	เอกสารเผยแพร่ฉบับแรก	สมเจตน์ แซ่จัง	01/06/2565

ลายเซ็นรับรองเอกสาร

หน้าที่	ชื่อ	ลายเซ็น	ตำแหน่ง	วันที่
จัดทำโดย	สมเจตน์ แซ่จัง		Senior Manager	01/06/2565
อนุมัติโดย	ดุสิต ศรีสง่าโอฬาร		President	01/06/2565

สารบัญ

หลักการและเหตุผล 4
วัตถุประสงค์ 4
ขอบเขตการดำเนินงาน 4
1. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ 5
1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ 5
1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง 6
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น 6
2.1 การประกาศใช้แผน 6
2.2 กำหนดขั้นตอนการดำเนินงาน 6
2.3 การติดต่อประสานงาน 7
2.4 การจัดเตรียมอุปกรณ์ 7
2.5 การสำรองข้อมูล 7
2.6 การป้องกันและกำจัดไวรัส 7
2.7 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ 8
2.8 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง 9
3. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัต 10
3.1 กรณีไฟไหม้ 10
3.2 กรณีไฟฟ้าดับ 11
3.3 กรณีโดนแทรกแซงระบบ 12
3.4 กรณีแผ่นดินไหว 13
4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน 14
4.1 ระดับนโยบาย 14
4.2 ระดับปฏิบัติ 14
5. การติดตามและรายงานผล 14

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ

(IT Continuity Plan)

หลักการและเหตุผล

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานของบริษัทฯ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ หน่วยงานเทคโนโลยีสารสนเทศได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศของบริษัทฯ อาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบ ทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้น จึงได้จัดทำแผน รับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Continuity Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ ระบบเทคโนโลยีสารสนเทศสามารถดำนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของบริษัทฯ

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของบริษัทฯ
2. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศของบริษัทฯ
3. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ของบริษัทฯให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Continuity Plan) จัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะ ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัต
4. การกำหนดผู้รับผิดชอบ
5. การติดตามและรายงานผล

1. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยี สารสนเทศของบริษัทฯ จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

<u>ภัยพิบัติจากภายนอก</u>

1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย แผ่นดินไหว ฯลฯ
2) ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง
3) การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยสีารสนเทศจากภายนอก เพื่อสร้างความเสียหาย หรือ ทำลายระบบข้อมูล
4) ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ /ไฟกระชาก
5) ไวรัสคอมพิวเตอร์

<u>ภัยพิบัติจากภายใน</u>

1) ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย
2) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในบริษัทฯ
3) เจ้าหน้าที่หรือบุคลากรของบริษัทฯ ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ ทั้งด้าน ฮาร์ดแวร์ และซอฟต์แวร์ อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง

เมื่อมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยเจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศ นำมาสรุปเป็นข้อมูล ดังนี้

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)		จัดเรียงลำดับ	
	ต่อระบบงาน	คู่ค้า/ผู้ที่ให้และ รับบริการ/ผู้มีส่วนได้ส่วนเสีย	รวม	จัดลำดับ
กรณีไฟไหม้	5	5	10	1
กรณีโดนแทรกแซงระบบ	5	4	9	2
กรณีไฟฟ้าดับ	4	4	8	3
กรณีแผ่นดินไหว	3	2	5	4

2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

หน่วยงานเทคโนโลยีสารสนเทศ มีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Continuity) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่าง เคร่งครัด

2.2 กำหนดขั้นตอนการดำเนินงาน

หน่วยงานเทคโนโลยีสารสนเทศ จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉิน โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้ บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืน ระบบ

2.3 การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ เป็นต้น

2.4 การจัดเตรียมอุปกรณ์

จัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิด ขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC/เครื่องคอมพิวเตอร์ Notebook
- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการของเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

2.5 การสำรองข้อมูล

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุก แทรกแซง เปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยมีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และแผนการสำรองข้อมูล ดังนี้

1) การสำรองระบบงานต่าง ๆ
2) การสำรองข้อมูลเครือข่าย (Configuration)

2.6 การป้องกันและกำจัดไวรัส

1) ติดตั้งโปรแกรมป้องกันไวรัสและกำจัดไวรัส โดยมีการอัพเดทข้อมูลไวรัสอยู่เสมอ
2) มีการตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูล และมีการตั้งเวลาตรวจหาไวรัสเป็นสม่ำเสมอ
3) พนักงานของบริษัทฯควรปฏิบัติตามเอกสาร"นโยบายด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Policy)" อย่างเคร่งครัดในการใช้งานระบบเทคโนโลยีสารสนเทศของระบบบริษัทฯ เช่น ระมัดระวังในการดาวน์โหลดไฟล์ต่าง ๆ จากอินเตอร์เน็ต หรือใช้ความระมัดระวังในการเปิด e-mail ที่ไม่ทราบแหล่งที่มา เป็นต้น

4) มีรายงานสรุปผลความผิดปกติของเครื่องลูกข่ายโดยจะจัดส่งผ่าน email ให้กับเจ้าหน้าที่เทคโนโลยีสารสนเทศเพื่อดำเนินการตรวจสอบ ป้องกัน และแก้ไขต่อไป

2.7 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

1) กำหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปใน ห้องควบคุม ต้องลงชื่อเบิกกุญแจ และ keycard ในสมุดควบคุมการเข้า – ออก ห้ามบุคคลที่ไม่มีอำนาจหน้าที่ เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้เจ้าหน้าที่ของหน่วยงานเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบพาเข้าไป
2) มีการติดตั้งระบบป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบ เครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย และเปิดใช้งานตลอดเวลา
3) มีการติดตั้ง IPS (Intrusion Prevention System) Fail2ban บน Proxy Server เพื่อให้ตรวจสอบการบุกรุกและยุดยั้งผู้บุกรุก
4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเตอร์เน็ต เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป
5) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกา าหนดหลักเกณฑ์และวิธีการทำ ธุรกรรมทางอิเล็กทรอนิกส์ โดยได้จัดหาระบบบริหาร จัดเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของบริษัทฯให้ดียิ่งขึ้น
6) หน่วยงานเทคโนโลยีสารสนเทศมีแผนในการปรับปรุงระบบ ป้องกันการบุกรุก (Firewall) และ IPS (Intrusion Prevention System) โดยอยู่ในระหว่างการปรับเปลี่ยนชุดอุปกรณ์ ระบบ

ป้องกันการบุกรุก (Firewall) และ IPS (Intrusion Prevention System) ให้มีประสิทธิภาพและความสามารถมากขึ้น

2.8 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยี สารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 60 นาที

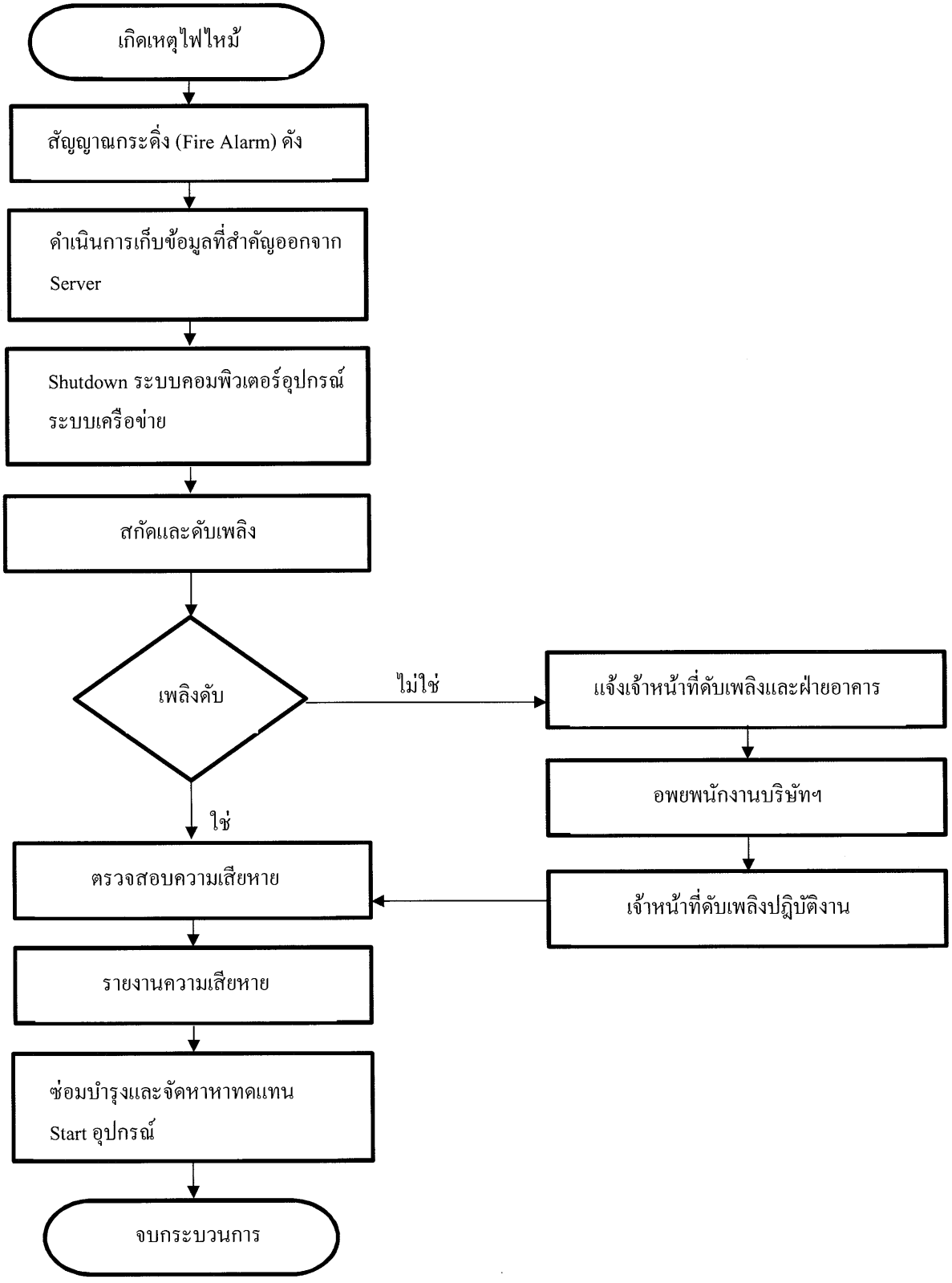
2) มีเครื่องกำเนิดไฟฟ้าสำรอง (Generator) ของอาคารจ่ายไฟให้อัตโนมัติกับระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์

3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษา เครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

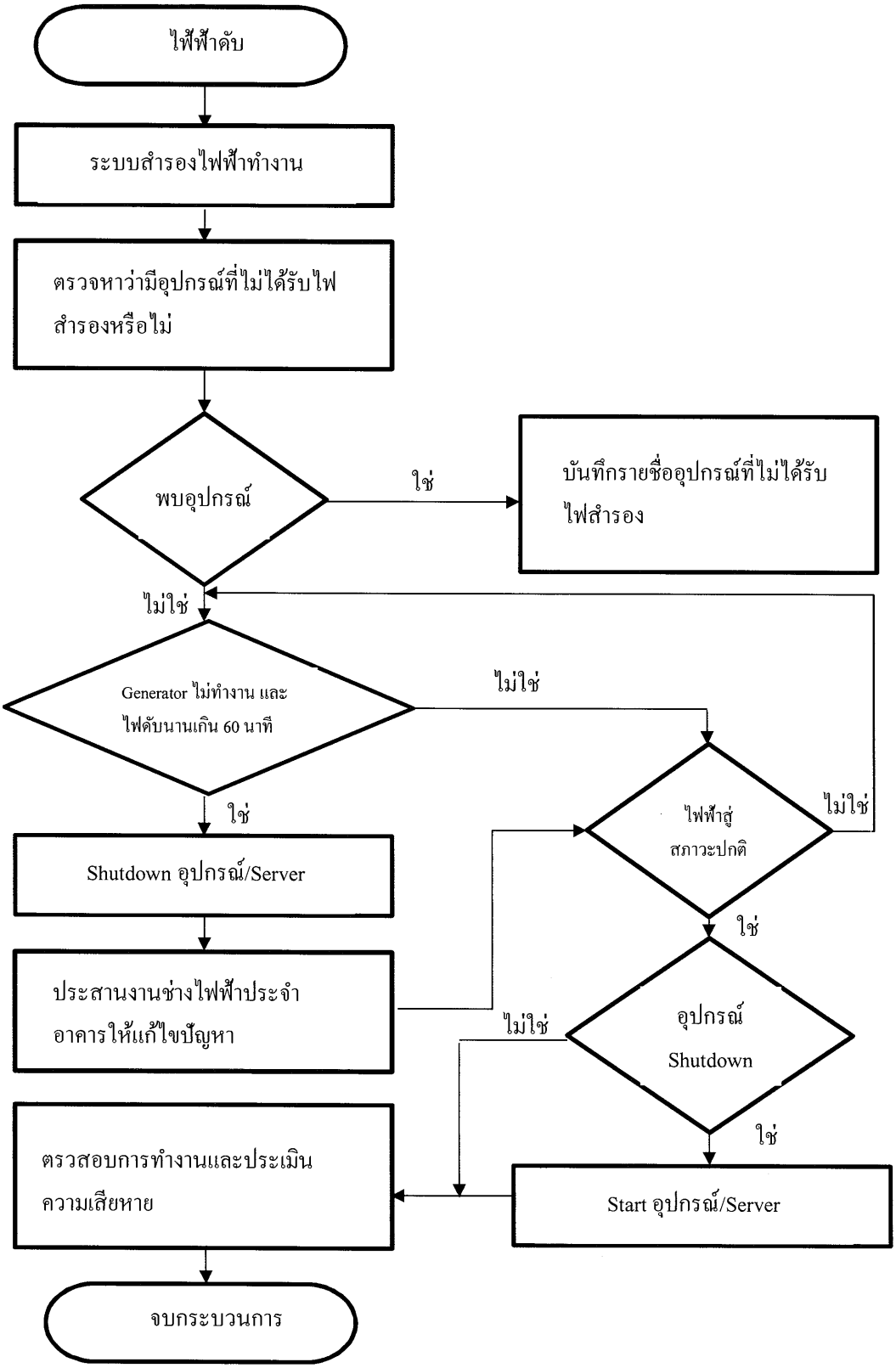
4) เมื่อเกิดกระแสไฟฟ้าดับและผู้ใช้งานมีการติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ ให้ผู้ใช้รีบบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

3. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

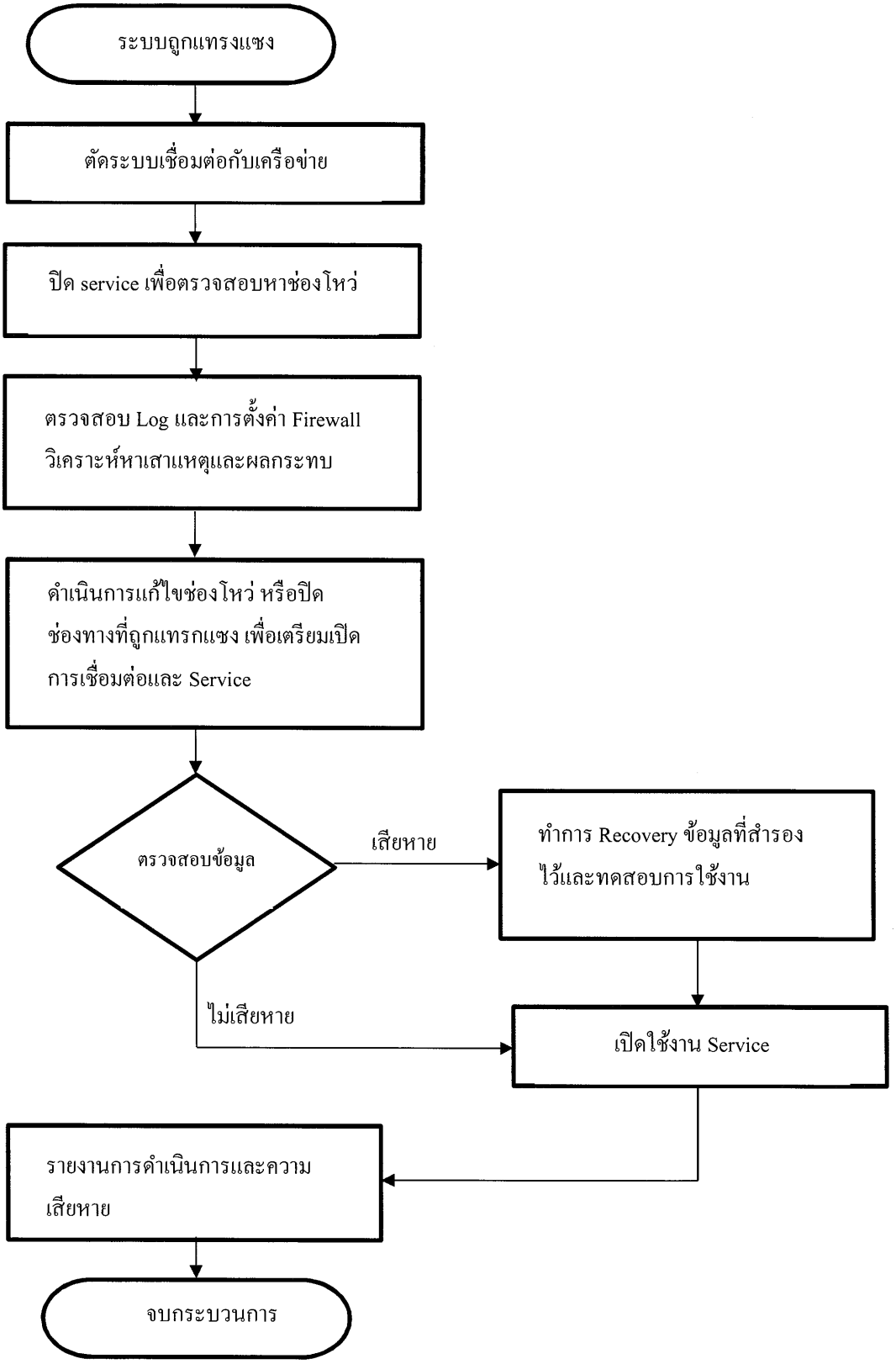
3.1 กรณีไฟไหม้



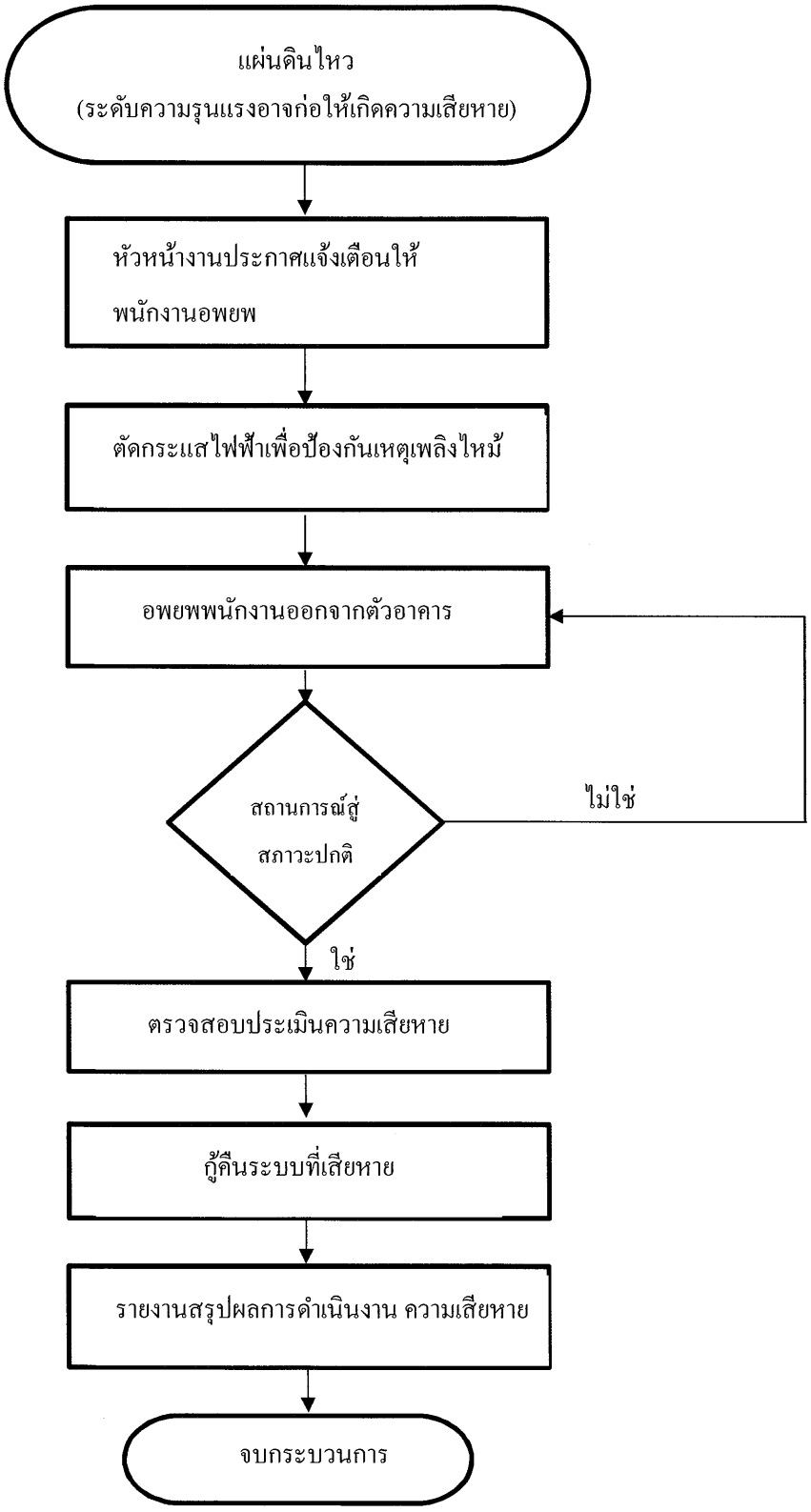
3.2 กรณีไฟฟ้าดับ



3.3 กรณีโดนแทรกแซงระบบ



3.4 กรณีแผ่นดินไหว



4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

4.1 ระดับนโยบาย

กรรมการผู้จัดการ รับผิดชอบในการกำหนดนโยบาย ให้คำเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ

เป็นผู้รับผิดชอบในการสั่งการตามนโยบายของบริษัทฯ ติดตามและกำกับดูแล ควบคุม ตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ในระดับปฏิบัติ

4.2 ระดับปฏิบัติ

หัวหน้างฝ่ายเทคโนโลยีสารสนเทศ รับผิดชอบประสานงาน กับผู้ปฏิบัติและทีมงานด้านเทคโนโลยีสารสนเทศ ให้ความคิดเห็น เสนอแนะวิธีการ แนวทางแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการป้องกันและแก้ไขปัญหา และตรวจสอบระบบมั่นคงและความปลอดภัยของระบบเทคโนโลยีสารสนเทศ พร้อมรายงานผลการดำเนินการ

5. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศทราบ เพื่อนาเสนอรายงานสรุปให้ผู้บริหารระดับสูง เพื่อที่จะนามาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนามาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Continuity) ฉบับนี้ ได้ผ่านการพิจารณาจากคณะทางานบริหารและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของบริษัทฯ เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศต่อไป