แผนรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)

แผนรองรับสถานการณ์ฉุกเฉิน
(IT Contingency Plan)

1. บทนำ

ระบบเทคโนโลยีสารสนเทศถือเป็นทรัพย์สินที่มีความสำคัญ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยต่อการปฏิบัติงานและให้บริการประชาชน ตลอดจนเตรียมความพร้อมรองรับสถานการณ์ฉุกเฉินของหน่วยงานให้มีประสิทธิภาพและส่งผลต่อการดำเนินงานตามภารกิจของหน่วยงานอย่างสูงสุด

กรมกิจการสตรีและสถาบันครอบครัว ได้ตระหนักถึงความสำคัญของข้อมูลและสารสนเทศของหน่วยงาน จึงได้จัดทำแผนป้องกันและแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) กรมกิจการสตรีและสถาบันครอบครัว กระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์

2. วัตถุประสงค์

2.1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.2 เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

2.3 เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2.4 เพื่อสร้างความเข้าใจร่วมกันในการดูแลรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของหน่วยงาน

3. การวิเคราะห์และประเมินความรุนแรงของเหตุภัยพิบัติ

จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมกิจการสตรีและสถาบันครอบครัว พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

3.1 วิเคราะห์เหตุการณ์ภัยพิบัติ

กรมกิจการสตรีและสถาบันครอบครัว ได้ดำเนินการวิเคราะห์เหตุการณ์ที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ โดยสามารถจำแนกประเภทของภัยพิบัติออกเป็น 2 ประเภทหลัก ดังนี้

3.1.1 ภัยพิบัติจากภายนอก

(1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่าย เช่น อัคคีภัย อุทกภัย แผ่นดินไหว จลาจล ชุมนุมประท้วง หรือสถานการณ์ความไม่สงบ ซึ่งอาจส่งผลกระทบต่อสถานที่ตั้งของศูนย์ข้อมูล (Data Center) และระบบสารสนเทศของหน่วยงาน

(2) ความขัดข้องของระบบสื่อสารและเครือข่าย เช่น ระบบอินเทอร์เน็ตขัดข้อง การเชื่อมโยงเครือข่ายล้มเหลว หรือผู้ให้บริการเครือข่าย (ISP) ไม่สามารถให้บริการได้ตามปกติ

(3) ภัยคุกคามทางไซเบอร์ เช่น การโจมตีจากภายนอก (Cyber Attack) ได้แก่ DDoS, Malware, Ransomware, Phishing หรือการบุกรุกระบบ (Unauthorized Access) เพื่อเข้าถึง ทำลาย หรือแก้ไขข้อมูลโดยมิชอบ

(4) ความขัดข้องของระบบไฟฟ้า เช่น ไฟฟ้าดับ ไฟตก ระบบไฟฟ้าไม่เสถียร ซึ่งส่งผลต่อการทำงานของอุปกรณ์ IT และระบบเครือข่าย

(5) ไวรัสคอมพิวเตอร์ ซึ่งอาจแพร่กระจายผ่านเครือข่าย อินเทอร์เน็ต หรืออุปกรณ์จัดเก็บข้อมูลภายนอก และส่งผลให้ระบบหยุดชะงักหรือข้อมูลเสียหาย

(6) ความล้มเหลวของผู้ให้บริการภายนอก เช่น Cloud Provider, Data Center ภายนอก, ระบบ SaaS หรือผู้ให้บริการโครงสร้างพื้นฐานไม่สามารถให้บริการได้ตาม SLA

3.1.2 ภัยพิบัติจากภายใน

(1) ความเสียหายของระบบแม่ข่ายและอุปกรณ์สารสนเทศ เช่น Hardware Failure Disk เสีย ระบบฐานข้อมูลเสียหาย หรือระบบล่ม

(2) ความผิดพลาดจากการปฏิบัติงานของบุคลากร เช่น การลบข้อมูลโดยไม่ตั้งใจ การตั้งค่าระบบผิดพลาด หรือการใช้งานระบบไม่ถูกต้อง

(3) การเข้าถึงข้อมูลโดยมิชอบจากบุคลากรภายใน เช่น การใช้สิทธิ์เกินขอบเขต การนำข้อมูลออกโดยไม่ได้รับอนุญาต หรือการกระทำที่ก่อให้เกิดความเสียหายต่อข้อมูลของหน่วยงาน

(4) การบริหารจัดการสิทธิ์การเข้าถึงไม่เหมาะสม เช่น การกำหนดสิทธิ์ผู้ใช้งานไม่ถูกต้อง ไม่มีการทบทวนสิทธิ์ หรือไม่มีการควบคุมการเข้าถึงข้อมูลสำคัญ

(5) การขาดการบำรุงรักษาและอัปเดตระบบ (Patch Management) เช่น ไม่อัปเดตระบบปฏิบัติการหรือซอฟต์แวร์ ทำให้เกิดช่องโหว่ด้านความมั่นคงปลอดภัย

(6) การสำรองข้อมูลไม่เพียงพอหรือไม่สามารถกู้คืนได้ เช่น ไม่มีการทดสอบการกู้คืนข้อมูลหรือข้อมูลสำรองเสียหาย

3.2 การประเมินความเสี่ยงและจัดลำดับความสำคัญ

เพื่อให้สามารถบริหารจัดการความเสี่ยงได้อย่างมีประสิทธิภาพ กรมกิจการสตรีและสถาบันครอบครัวได้กำหนดหลักเกณฑ์การประเมินความเสี่ยงโดยพิจารณาจาก 2 ปัจจัยหลัก ได้แก่ โอกาสเกิด (Likelihood) ระดับ 1–5 และผลกระทบ (Impact) ระดับ 1–5 โดยคำนวณระดับความเสี่ยง (Risk Level) จากสูตร: Risk Score = Likelihood × Impact

(1) เกณฑ์การประเมิน

ระดับ	โอกาสเกิด (Likelihood)	ผลกระทบ (Impact)
1	น้อยมาก	มีผลกระทบต่อการดำเนินงานในระดับน้อยมาก - ระบบใช้งานได้ตามปกติ - ข้อมูลไม่สูญหาย - ไม่กระทบต่อการให้บริการ
2	น้อย	มีผลกระทบต่อการดำเนินงานในระดับน้อย

		- ระบบสามารถให้บริการได้ตามปกติ แต่มีประสิทธิภาพในการทำงานลดลงเล็กน้อย - ข้อมูลบางส่วนมีความไม่ถูกต้องในระดับเล็กน้อย แต่ไม่ส่งผลกระทบต่อการดำเนินงานโดยรวม - กระทบต่อการให้บริการเล็กน้อย แต่สามารถแก้ไขได้ทันที
3	ปานกลาง	มีผลกระทบต่อการดำเนินงานในระดับปานกลาง - ระบบบางส่วนไม่สามารถใช้งานได้ - ข้อมูลบางส่วนสูญหายหรือมีความไม่ถูกต้อง ส่งผลกระทบต่อการดำเนินงานบางส่วน และต้องใช้เวลาในการตรวจสอบและแก้ไข - การให้บริการล่าช้า
4	สูง	มีผลกระทบต่อการดำเนินงานในระดับมาก - ระบบหลักหยุดให้บริการชั่วคราว - ข้อมูลสำคัญบางส่วนสูญหายหรือเสียหาย ส่งผลกระทบต่อการดำเนินงานหลัก และไม่สามารถกู้คืนได้ในทันที - ไม่สามารถให้บริการบางบริการได้
5	สูงมาก	มีผลกระทบต่อการดำเนินงานในระดับรุนแรง - ระบบทั้งหมดไม่สามารถใช้งานได้ - ข้อมูลสำคัญสูญหายหรือรั่วไหล - ไม่สามารถให้บริการได้ และกระทบภาพลักษณ์องค์กร

(2) การจัดระดับความเสี่ยง

ระดับ	**ระดับ**	**แนวทางการดำเนินการ**
1 – 5	ต่ำ	เฝ้าระวัง
6 – 10	ปานกลาง	ควบคุมความเสี่ยง
11 – 15	สูง	เร่งดำเนินการ
16 - 25	วิกฤต	ดำเนินการทันที

(3) ประเมินสถานการณ์

ลำดับ	**สถานการณ์/ภาวะฉุกเฉิน**	**โอกาสเกิด**	**ผลกระทบ**	**รวม**	**ระดับความเสี่ยง**
1	ไฟไหม้	3	5	15	สูง
2	บุกรุก/ภัยคุกคาม/ไวรัส	5	5	25	วิกฤต
3	ระบบเครือข่ายล้มเหลว	4	4	16	วิกฤต
4	ระบบไฟฟ้าขัดข้อง	3	4	12	สูง
5	คอมพิวเตอร์แม่ข่ายขัดข้อง	4	5	20	วิกฤต
6	ข้อมูลรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล	4	5	20	วิกฤต
7	ความผิดพลาดจากการปฏิบัติงานของบุคลากร	4	4	16	วิกฤต
8	การหยุดชะงักของผู้ให้บริการภายนอก	3	5	15	สูง
9	เหตุการณ์ความไม่สงบ	3	5	15	สูง

10	น้ำท่วม	3	5	15	สูง
11	แผ่นดินไหว	3	5	15	สูง
12	โรคระบาด	3	4	12	สูง
13	โจรกรรม/การสูญหายของทรัพย์สิน	3	3	9	ปานกลาง

(4) การกำหนดระดับความรุนแรงและแนวทางรองรับ

ลำดับ	**สถานการณ์/ภาวะฉุกเฉิน**	**ระดับความเสี่ยง**	**RTO**	**RPO**	**แนวทาง/แผนรองรับ**
1	ไฟไหม้	สูง	≤ 24 ชม.	≤ 1 ชม.	จัดให้มีศูนย์สำรองข้อมูล (Disaster Recovery Site) และการสำรองข้อมูลนอกสถานที่ พร้อมทั้งทดสอบและซ้อมแผนความต่อเนื่องทางธุรกิจ (BCP) อย่างสม่ำเสมอ
2	บุกรุก/ภัยคุกคาม/ไวรัส	วิกฤต	≤ 4 ชม.	≤ 1 ชม.	จัดทำแผนตอบสนองต่อเหตุการณ์ (Incident Response Plan) พร้อมระบบเฝ้าระวังและตรวจจับภัยคุกคาม (SOC/EDR) และดำเนินการกู้คืนระบบจากข้อมูลสำรอง
3	ระบบเครือข่ายล้มเหลว	วิกฤต	≤ 2 ชม.	≤ 4 ชม.	จัดให้มีระบบเครือข่ายสำรอง (Redundant Network) และการสลับใช้งานเส้นทางสื่อสาร (Failover) โดยอัตโนมัติ
4	ระบบไฟฟ้าขัดข้อง	สูง	≤ 2 ชม.	≤ 4 ชม.	จัดให้มีระบบสำรองไฟฟ้า เช่น UPS และเครื่องกำเนิดไฟฟ้า (Generator) พร้อมทั้งการบริหารจัดการพลังงานอย่างต่อเนื่อง
5	คอมพิวเตอร์แม่ข่ายขัดข้อง	วิกฤต	≤ 4 ชม.	≤ 1 ชม.	จัดให้มีระบบสำรองแบบ High Availability และ Virtualization พร้อมทั้งการสำรองและกู้คืนข้อมูลอย่างเป็นระบบ
6	ข้อมูลรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล	วิกฤต	≤ 4 ชม.	≤ 1 ชม.	ดำเนินการตามแผนตอบสนองเหตุละเมิดข้อมูลส่วนบุคคล (PDPA) พร้อมกำหนดสิทธิ์การเข้าถึงข้อมูลและการตรวจสอบการใช้งาน (Audit Log)
7	ความผิดพลาดจากการ	วิกฤต	≤ 8 ชม.	≤ 4 ชม.	จัดให้มีคู่มือการปฏิบัติงาน (SOP) การอบรมบุคลากรอย่างต่อเนื่อง

ลำดับ	สถานการณ์/ภาวะฉุกเฉิน	ระดับความเสี่ยง	RTO	RPO	แนวทาง/แผนรองรับ
	ปฏิบัติงานของบุคลากร				และระบบตรวจสอบย้อนกลับ (Log) รวมถึงการกู้คืนข้อมูล (Rollback)
8	การหยุดชะงักของผู้ให้บริการภายนอก	สูง	≤ 8 ชม.	≤ 4 ชม.	จัดให้มีผู้ให้บริการสำรอง (Multi-Cloud / Multi-ISP) และช่องทางสื่อสารสำรอง พร้อมรองรับการทำงานในโหมดออฟไลน์
9	เหตุการณ์ความไม่สงบ	สูง	≤ 24 ชม.	≤ 8 ชม.	จัดให้มีแผนการปฏิบัติงานจากระยะไกล (Remote Work) และแผนย้ายสถานที่ปฏิบัติงานสำรอง
10	น้ำท่วม	สูง	≤ 24 ชม.	≤ 1 ชม.	จัดให้มีศูนย์สำรองข้อมูล การสำรองข้อมูลบนระบบ Cloud และแผนการย้ายระบบไปยังสถานที่สำรอง
11	แผ่นดินไหว	สูง	≤ 24 ชม.	≤ 1 ชม.	จัดให้มีศูนย์สำรองข้อมูลและการสำรองข้อมูลนอกสถานที่ พร้อมแผนฟื้นฟูระบบจากภัยพิบัติ
12	โรคระบาด	สูง	≤ 24 ชม.	≤ 1 ชม.	จัดให้มีศูนย์สำรองข้อมูลและการสำรองข้อมูลนอกสถานที่ พร้อมแผนฟื้นฟูระบบจากภัยพิบัติ
13	โจรกรรม/การสูญหายของทรัพย์สิน	ปานกลาง	≤ 24 ชม.	≤ 8 ชม.	จัดให้มีมาตรการควบคุมทรัพย์สิน การเข้ารหัสข้อมูล (Encryption) และระบบเฝ้าระวังความปลอดภัย

หมายเหตุ

- RTO (Recovery Time Objective) = ระยะเวลาสูงสุดที่ยอมให้ระบบหยุดชะงัก
- RPO (Recovery Point Objective) = ระยะเวลาข้อมูลสูญหายที่ยอมรับได้

4. ขั้นตอนและแนวทางการป้องกันและรักษาความปลอดภัย

4.1 การประกาศใช้แผน

กรมกิจการสตรีและสถาบันครอบครัว มีการประกาศใช้แผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency plan) เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ จะทำการแจ้งให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมฯ ทราบ เพื่อพิจารณาประกาศใช้แผนต่อไป

4.2 กำหนดขั้นตอนการดำเนินการ

กลุ่มเทคโนโลยีสารสนเทศ กองยุทธศาสตร์และแผนงาน จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุฉุกเฉินในกรมฯ โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่าง ๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุก เพื่อให้สามารถยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ ซึ่งประกอบด้วย

4.2.1 การเตรียมความพร้อม

(1) แจ้งให้เจ้าหน้าที่ทราบถึงแผนแก้ไขปัญหาสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(2) แจ้งให้เจ้าหน้าที่สำรองข้อมูลจากเครื่องคอมพิวเตอร์ที่ใช้ปฏิบัติงานอยู่อย่างสม่ำเสมอ

(3) ให้ผู้ดูแลระบบสำรองระบบและฐานข้อมูลบนเครื่องคอมพิวเตอร์แม่ข่ายตามระยะเวลาที่กำหนด

(4) ให้เจ้าหน้าที่สำรวจระบบและอุปกรณ์ที่มีอยู่ พร้อมปรับปรุงทะเบียนครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ให้ถูกต้องเป็นปัจจุบันอยู่เสมอ

(5) ปรับปรุงและติดตั้งแผนผังการเชื่อมโยงระบบเครือข่ายไว้ในห้องเครื่องคอมพิวเตอร์

(6) ดูแลบำรุงรักษา ซ่อมแซมแก้ไข เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง

(7) จัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า สถานีดับเพลิง สถานีตำรวจ ผู้ให้บริการอินเตอร์เน็ต ฯลฯ

4.2.2 แนวทางการปฏิบัติกรณีเกิดภัยพิบัติ

(1) กรณีไฟไหม้

- หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานอาคารสถานที่ สำนักงานเลขานุการกรมทันที และโทรแจ้งสถานีดับเพลิง
- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง (ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ
- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมออย่างน้อยปีละ 1 ครั้ง

(2) กรณีบุกรุก/ภัยคุกคาม/ไวรัส

- ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น
    - กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall
    - กรณีถูกไวรัสหรือภัยคุกคาม เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบ

เครือข่าย และวิเคราะห์หาสาเหตุและผลกระทบ ที่เกิดจากไวรัสที่ระบาด

- ผู้ดูแลระบบแจ้งผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศให้ทราบโดยด่วน
- ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัสตรวจสอบและติดตามเครื่องที่ติดไวรัส/หยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆที่ทำให้ผู้บุกรุกเข้ามาได้
- ดำเนินการแก้ไข หากไม่สามารถแก้ไขให้ใช้งานได้ตามปกติ หรือไม่สามารถดำเนินการให้บริการเครือข่ายได้ กลุ่มเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

(3) กรณีระบบเครือข่ายล้มเหลว

- ดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา
- หากสายสัญญาณขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่ายเพื่อดำเนินการซ่อมแซมสายสัญญาณให้เสร็จเรียบร้อยโดยเร็ว
- หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางจุด ให้ดำเนินการตรวจสอบสายสัญญาณที่เชื่อมต่อไปยังจุด และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

(4) ระบบไฟฟ้าขัดข้อง

- เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหายของระบบสารสนเทศ
- กำหนดให้มีการสำรองฐานข้อมูล และระบบงานต่าง ๆ อย่างน้อยทุกเดือน

(5) กรณีคอมพิวเตอร์แม่ข่ายขัดข้อง

- ตรวจสอบสถานะระบบจากเครื่องมือ Monitoring หรือการแจ้งเตือน
- วิเคราะห์สาเหตุเบื้องต้น (Hardware / Software / Network)
- ดำเนินการแก้ไขเบื้องต้น เช่น Restart ระบบหรือ Service ที่เกี่ยวข้อง
- หากไม่สามารถแก้ไขได้ ให้ดำเนินการสลับไปใช้ระบบสำรอง
- ตรวจสอบความถูกต้องของฐานข้อมูลและความสมบูรณ์ของระบบ
- แจ้งผู้ใช้งานและผู้บริหารเกี่ยวกับสถานการณ์และระยะเวลาการกู้คืน
- บันทึกเหตุการณ์และจัดทำรายงานสรุป (Incident Report)
- ทบทวนและปรับปรุงมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ

(6) กรณีข้อมูลรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล

- ตรวจสอบและยืนยันเหตุการณ์การรั่วไหลของข้อมูล
- ระงับการเข้าถึงระบบหรือข้อมูลที่เกี่ยวข้องทันที
- ประเมินขอบเขตและประเภทของข้อมูลที่ได้รับผลกระทบ
- แจ้งผู้บริหารและเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

- ดำเนินการตามกฎหมายที่เกี่ยวข้อง โดยแจ้งหน่วยงานกำกับภายในระยะเวลาที่กำหนด
- แจ้งเจ้าของข้อมูล (Data Subject) หากมีความเสี่ยงสูง
- ดำเนินการแก้ไขช่องโหว่และเสริมมาตรการความมั่นคงปลอดภัย
- จัดทำรายงานเหตุการณ์และสรุปบทเรียน

(7) กรณีความผิดพลาดจากการปฏิบัติงานของบุคลากร

- ตรวจสอบเหตุการณ์และระบุสาเหตุของความผิดพลาด
- ระงับการดำเนินการที่อาจก่อให้เกิดความเสียหายเพิ่มเติม
- กู้คืนข้อมูลหรือระบบจาก Backup (หากมีความเสียหาย)
- ตรวจสอบ Log การใช้งานเพื่อยืนยันความถูกต้อง
- แจ้งผู้บังคับบัญชาและผู้เกี่ยวข้อง
- ดำเนินการแก้ไขระบบหรือข้อมูลให้กลับสู่สภาพปกติ
- จัดให้มีการอบรมหรือทบทวนแนวปฏิบัติ (SOP) แก่บุคลากร
- ปรับปรุงมาตรการควบคุม เช่น การกำหนดสิทธิ์การเข้าถึง (Access Control)

(8) กรณีการหยุดชะงักของผู้ให้บริการภายนอก

- ตรวจสอบสถานะของผู้ให้บริการ (Cloud / Internet / Vendor)
- ประเมินผลกระทบต่อระบบและการให้บริการของหน่วยงาน
- ติดต่อผู้ให้บริการเพื่อรับทราบสาเหตุและระยะเวลาในการแก้ไข
- ดำเนินการใช้ระบบหรือช่องทางสำรอง (Backup System / Secondary Link)
- แจ้งผู้ใช้งานเกี่ยวกับสถานการณ์และแนวทางการใช้งานชั่วคราว
- ติดตามสถานการณ์อย่างต่อเนื่องจนกว่าจะกลับสู่ภาวะปกติ
- บันทึกเหตุการณ์และประเมินประสิทธิภาพของผู้ให้บริการ (SLA)
- ทบทวนและปรับปรุงแผนรองรับ เช่น การใช้ Multi-Vendor หรือ Multi-Cloud

(9) กรณีจลาจล/ชุมนุม/เหตุการณ์ความไม่สงบ

- เมื่อเกิดเหตุการณ์จลาจล/ชุมนุม/เหตุการณ์ความไม่สงบ บริเวณกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์ หรือบ้านราชวิถี
- เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศผู้รับผิดชอบ สำรองรองข้อมูลที่จำเป็น และปิดเครื่องแม่ข่าย
- อพยพเจ้าหน้าที่ออกจากตัวอาคาร ปิดล็อกประตูห้อง Server และห้องทำงาน
- เมื่อสถานการณ์กลับสู่ภาวะปกติ ให้ดำเนินการตรวจสอบและประเมินความเสียหาย
- ติดตั้ง/กู้คืนระบบสารสนเทศที่ได้รับความเสียหาย ทดสอบความสมบูรณ์ พร้อมรายงานผลการดำเนินการ

(10) กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ห้อง Data Center ชั้น 8 อาคารกระทรวงการพัฒนาสังคมและความมั่นคงของมนุษย์
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืนในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

(11) กรณีแผ่นดินไหว

- ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง
- เตรียมบุคลากร วัสดุอุปกรณ์ สถานที่อพยพ
    - ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหว
    - ประสานการเตรียมการกับหน่วยงานที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม
    - สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สาหรับบุคลากรขององค์กร
    - จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ
- อบรม ให้ความรู้เกี่ยวกับการปฏิบัติเมื่อเกิดแผ่นดินไหวแก่เจ้าหน้าที่บุคลากรภายในองค์กร

(12) กรณีโรคระบาด

- หากเกิดโรคระบาด และกรมฯ มีคำสั่งให้ปฏิบัติงานที่บ้าน หรือสลับกันมาปฏิบัติงาน
- ให้ปฏิบัติงานที่บ้านโดยใช้เทคโนโลยีในการสื่อสารและปฏิบัติงาน เช่น การประชุมทางไกลออนไลน์ การควบคุมระยะไกล (Remote) โทรศัพท์ Line ฯลฯ
- เจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ จัดเตรียมอุปกรณ์เพื่อสนับสนุนการปฏิบัติงานของบุคลากร
- ผู้ที่ปฏิบัติงานที่บ้านให้ส่งผลการปฏิบัติงานให้ผู้อำนวยการกอง/สำนัก/กลุ่มขึ้นตรงผู้รับผิดชอบดำเนินการสรุปผลการปฏิบัติงานเพื่อนำเสนอผู้บริหาร

(13) กรณีโจรกรรม/การสูญหายของทรัพย์สิน

- เมื่อเกิดการโจรกรรม ให้แจ้งผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ
- เจ้าหน้าที่ที่รับผิดชอบสำรวจ ตรวจสอบรายการทรัพย์สินที่สูญหาย

- เจ้าหน้าที่ที่รับผิดชอบนำอุปกรณ์สำรองมาทดแทน/กู้คืนระบบ/ทดสอบความสมบูรณ์
- รายงานผลการดำเนินการ

5. การกำหนดบทบาทหน้าที่และผู้รับผิดชอบ

หน่วยงานกำหนดบทบาทหน้าที่และความรับผิดชอบในการบริหารจัดการเหตุการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศอย่างชัดเจน โดยครอบคลุมทั้งระดับนโยบาย การบริหารจัดการ และการปฏิบัติงาน เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและสามารถตอบสนองต่อสถานการณ์ได้อย่างทันท่วงที ดังนี้

(1) ผู้บริหารระดับสูง

ประกอบด้วย อธิบดีกรมกิจการสตรีและสถาบันครอบครัว และรองอธิบดีกรมกิจการสตรีและสถาบันครอบครัว รับผิดชอบเชิงนโยบายและการกำกับดูแล กำหนดนโยบาย แนวทาง และมาตรการด้านความมั่นคงปลอดภัยสารสนเทศ ให้ข้อเสนอแนะ คำปรึกษา และสนับสนุนทรัพยากร/งบประมาณ สั่งการและตัดสินใจในกรณีเกิดเหตุการณ์ระดับวิกฤต กำกับ ติดตาม และประเมินผลการดำเนินงาน พิจารณาอนุมัติแผน BCP/DRP

(2) ผู้บริหารด้านเทคโนโลยีสารสนเทศระดับสูง (DCIO)

รับผิดชอบการบริหารจัดการและควบคุมการดำเนินงานด้าน IT วางแผน ควบคุม และกำกับการดำเนินงานด้านระบบสารสนเทศ ประเมินความเสี่ยงและกำหนดมาตรการป้องกัน ควบคุมการตอบสนองเหตุการณ์ (Incident Response) ประสานงานกับหน่วยงานภายในและภายนอก รายงานสถานการณ์ต่อผู้บริหารระดับสูง

(3) ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ

ประกอบด้วย ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศ และเจ้าหน้าที่กลุ่มเทคโนโลยีสารสนเทศ รับผิดชอบในการดำเนินงานเชิงปฏิบัติการ ดูแลและบริหารจัดการระบบเครือข่าย ระบบแม่ข่าย ระบบสารสนเทศและฐานข้อมูล ตรวจสอบ เฝ้าระวัง และตอบสนองต่อเหตุการณ์ผิดปกติ ดำเนินการแก้ไขปัญหา กู้คืนระบบ และสำรองข้อมูล ตรวจสอบความมั่นคงปลอดภัยของระบบ (Security Monitoring) บันทึกเหตุการณ์และจัดทำรายงาน (Incident Report) ปฏิบัติตามแผนฯ พร้อมรายงานผลการดำเนินการ

(4) ผู้ใช้งานระบบ (End Users)

รับผิดชอบการใช้งานระบบอย่างถูกต้องและปลอดภัย ปฏิบัติตามนโยบายและแนวทางด้าน IT Security แจ้งเหตุการณ์ผิดปกติหรือความเสี่ยงต่อผู้ดูแลระบบทันที และไม่กระทำการที่ก่อให้เกิดความเสี่ยงต่อระบบสารสนเทศ

(5) เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)

รับผิดชอบด้านข้อมูลส่วนบุคคล ให้คำแนะนำด้านการคุ้มครองข้อมูลส่วนบุคคล ตรวจสอบและกำกับการปฏิบัติตาม PDPA ดำเนินการเมื่อเกิดเหตุข้อมูลรั่วไหล (Data Breach) และประสานงานกับหน่วยงานกำกับดูแล

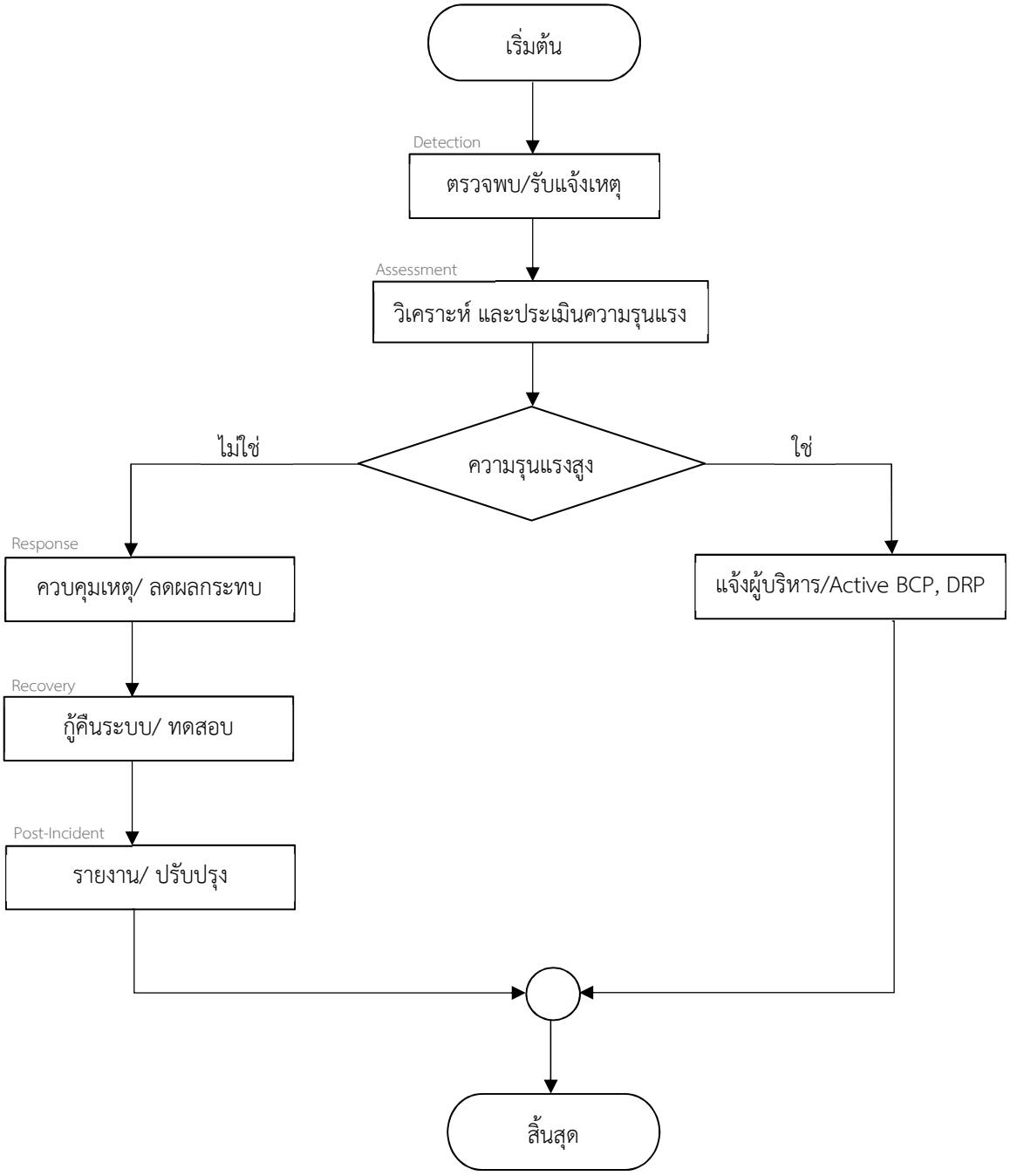
(6) ผู้ให้บริการภายนอก (Vendor/ Service Provider)

รับผิดชอบตามขอบเขตสัญญา (SLA) ให้บริการระบบ Cloud / Network / Software สนับสนุนการแก้ไขเหตุการณ์ แจ้งสถานะระบบและเหตุขัดข้อง และปฏิบัติตามข้อตกลงด้านความมั่นคงปลอดภัย

6. ผังกระบวนงาน

6.1 สำหรับใช้ร่วมทุกเหตุการณ์

- ผังกระบวนงานหลัก (ใช้ร่วมทุกเหตุการณ์)



- ขั้นตอนการปฏิบัติงานหลัก (ใช้ร่วมทุกเหตุการณ์)
    - การตรวจพบเหตุการณ์ (Detection)

        เมื่อเกิดเหตุการณ์ที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศหน่วยงาน ต้องดำเนินการตรวจจับและรับแจ้งเหตุผ่านระบบเฝ้าระวังหรือจากผู้ใช้งาน พร้อมทั้งบันทึกรายละเอียดเหตุการณ์เบื้องต้น เช่น วัน เวลา ระบบที่ได้รับผลกระทบ และลักษณะเหตุการณ์ และดำเนินการแจ้งทีมเทคโนโลยีสารสนเทศหรือผู้รับผิดชอบทันทีตามช่องทางที่กำหนด
    - การประเมินสถานการณ์ (Assessment)

        กลุ่มเทคโนโลยีสารสนเทศต้องดำเนินการวิเคราะห์สาเหตุและลักษณะของเหตุการณ์ที่เกิดขึ้น รวมทั้งประเมินระดับความรุนแรงและผลกระทบต่อระบบ ภารกิจของหน่วยงาน และผู้รับบริการ เพื่อกำหนดแนวทางการตอบสนองที่เหมาะสม ในกรณีที่เหตุการณ์มีความรุนแรงสูง ให้รายงานผู้บริหารและพิจารณาใช้แผนความต่อเนื่องทางธุรกิจ (BCP) หรือแผนกู้คืนระบบ (DRP) ตามความเหมาะสม
    - การตอบสนองเหตุการณ์ (Response)

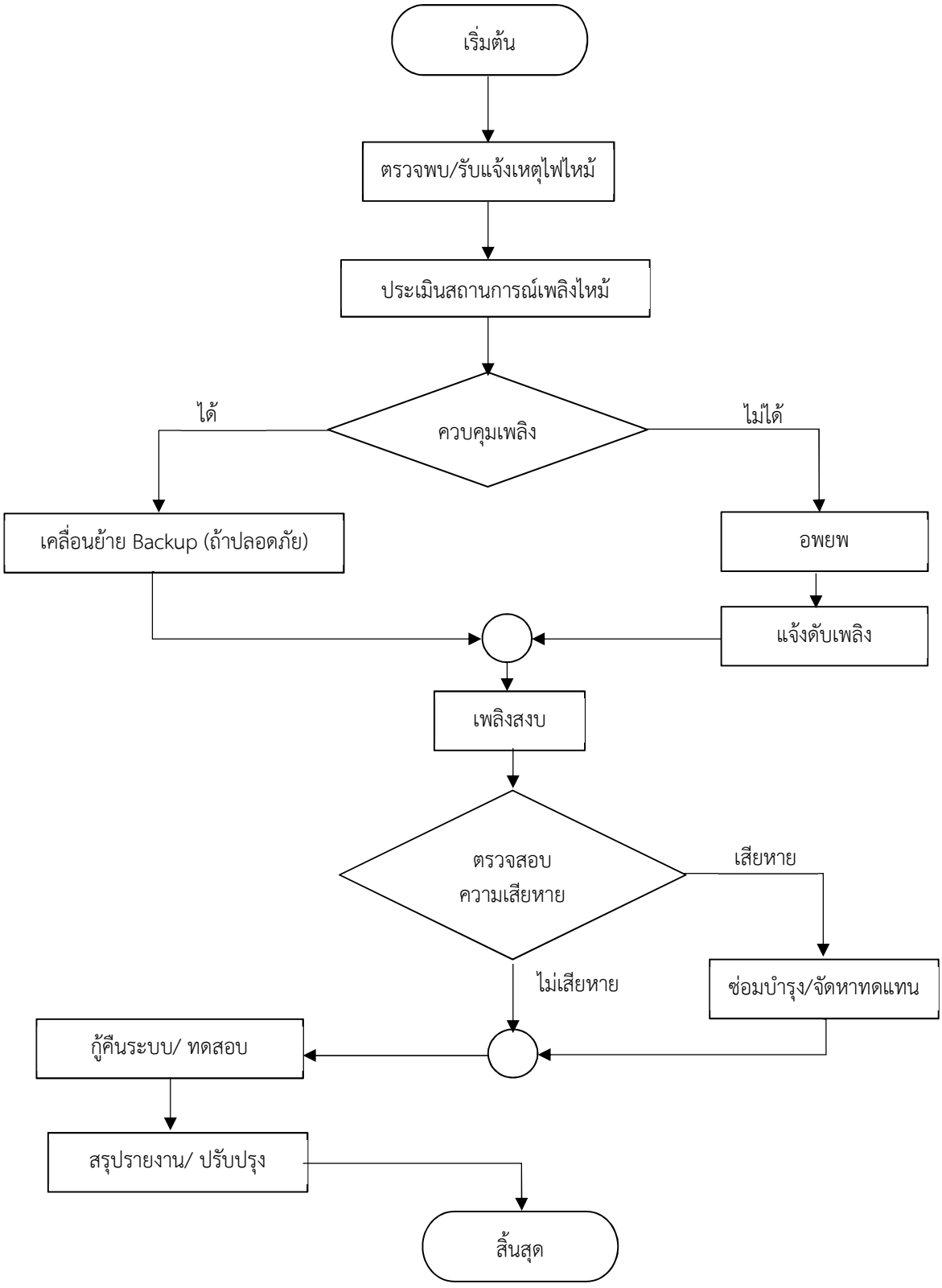
        หน่วยงานต้องดำเนินการควบคุมสถานการณ์โดยทันที เพื่อลดผลกระทบและป้องกันการขยายวงกว้างของปัญหาโดยอาจดำเนินการ เช่น การจำกัดสิทธิ์การเข้าถึง การหยุดการทำงานของระบบที่ได้รับผลกระทบ หรือการแยกระบบออกจากเครือข่าย (Isolation) พร้อมทั้งดำเนินการแก้ไขปัญหาเฉพาะหน้า และประสานงานกับหน่วยงานที่เกี่ยวข้อง รวมถึงผู้ให้บริการภายนอก (Vendor) หากจำเป็น
    - การกู้คืนระบบ (Recovery)

        ภายหลังจากสามารถควบคุมสถานการณ์ได้แล้ว ให้ดำเนินการกู้คืนระบบและข้อมูลจากแหล่งสำรอง (Backup) หรือระบบสำรอง (Disaster Recovery Site) ตามลำดับความสำคัญของระบบที่กำหนดไว้ในแผน ทั้งนี้ ต้องตรวจสอบความถูกต้องครบถ้วนของข้อมูล และทดสอบการทำงานของระบบให้สามารถกลับมาใช้งานได้ตามปกติก่อนเปิดให้บริการแก่ผู้ใช้งาน
    - การดำเนินการภายหลังเหตุการณ์ (Post-Incident)

        เมื่อสถานการณ์กลับสู่ภาวะปกติ ให้จัดทำรายงานสรุปเหตุการณ์อย่างเป็นทางการ พร้อมทั้งวิเคราะห์สาเหตุของปัญหา (Root Cause Analysis) และประเมินประสิทธิภาพของการดำเนินการตามแผน รวมทั้งนำผลการวิเคราะห์ไปใช้ในการปรับปรุงมาตรการ แนวปฏิบัติ และแผนความต่อเนื่องด้านเทคโนโลยีสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น เพื่อป้องกันไม่ให้เกิดเหตุการณ์ซ้ำในอนาคต

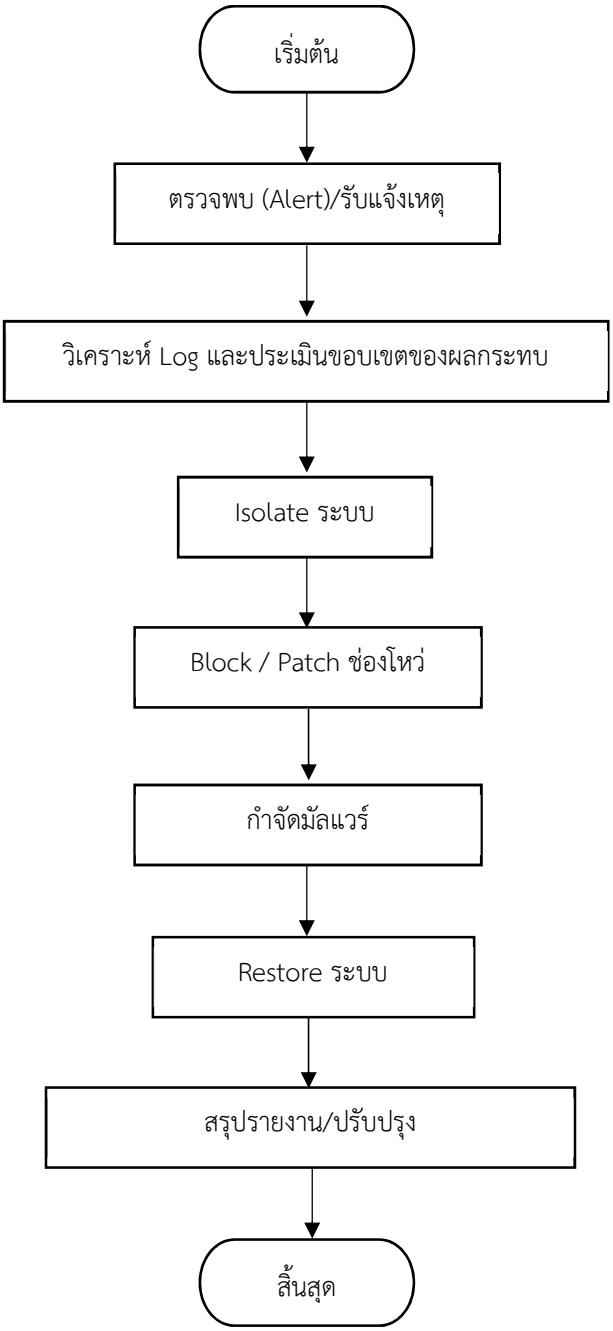
6.2 ผังรายกรณี

(1) ไฟไหม้

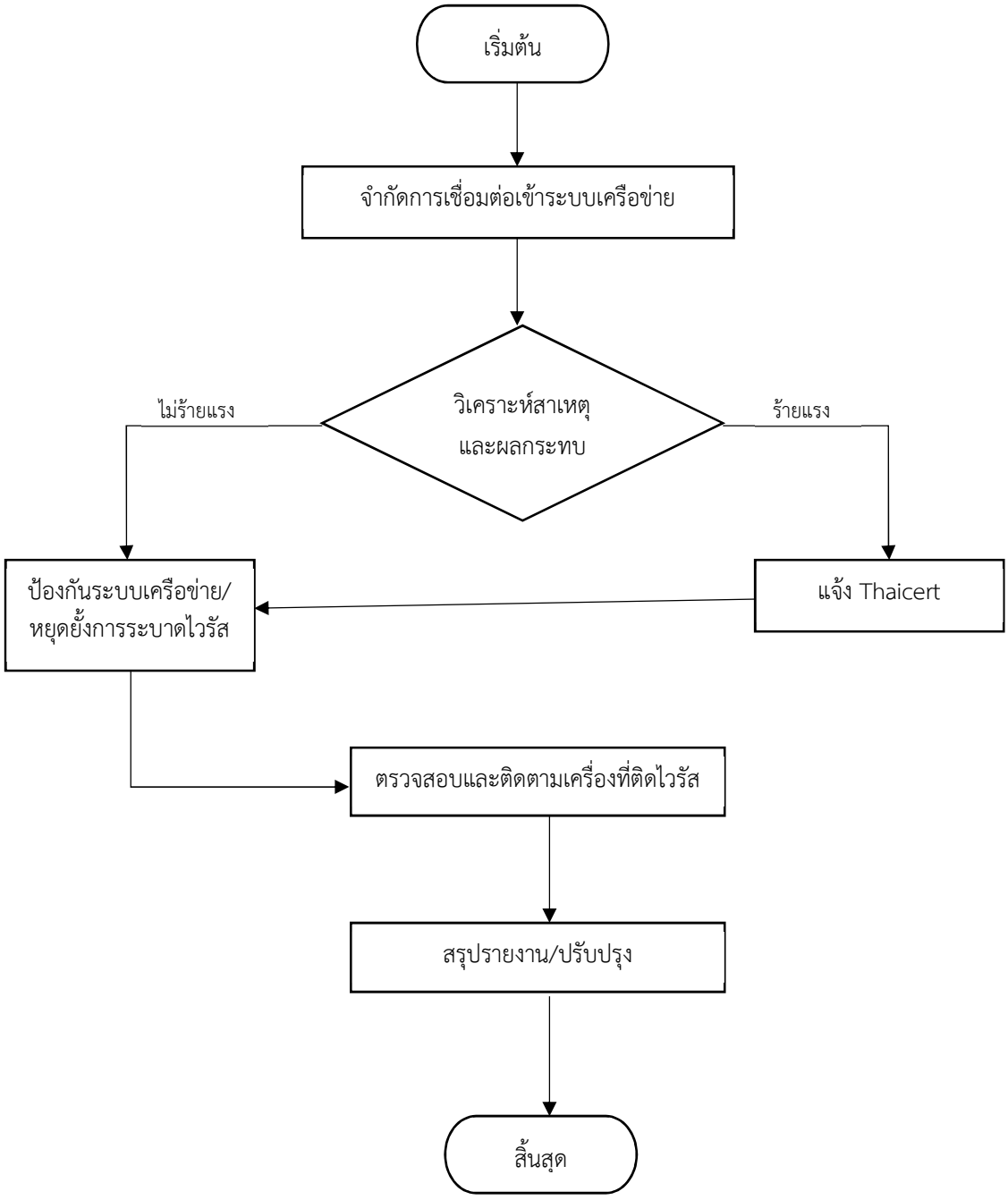


(2) บุกรุก/ภัยคุกคาม/ไวรัส

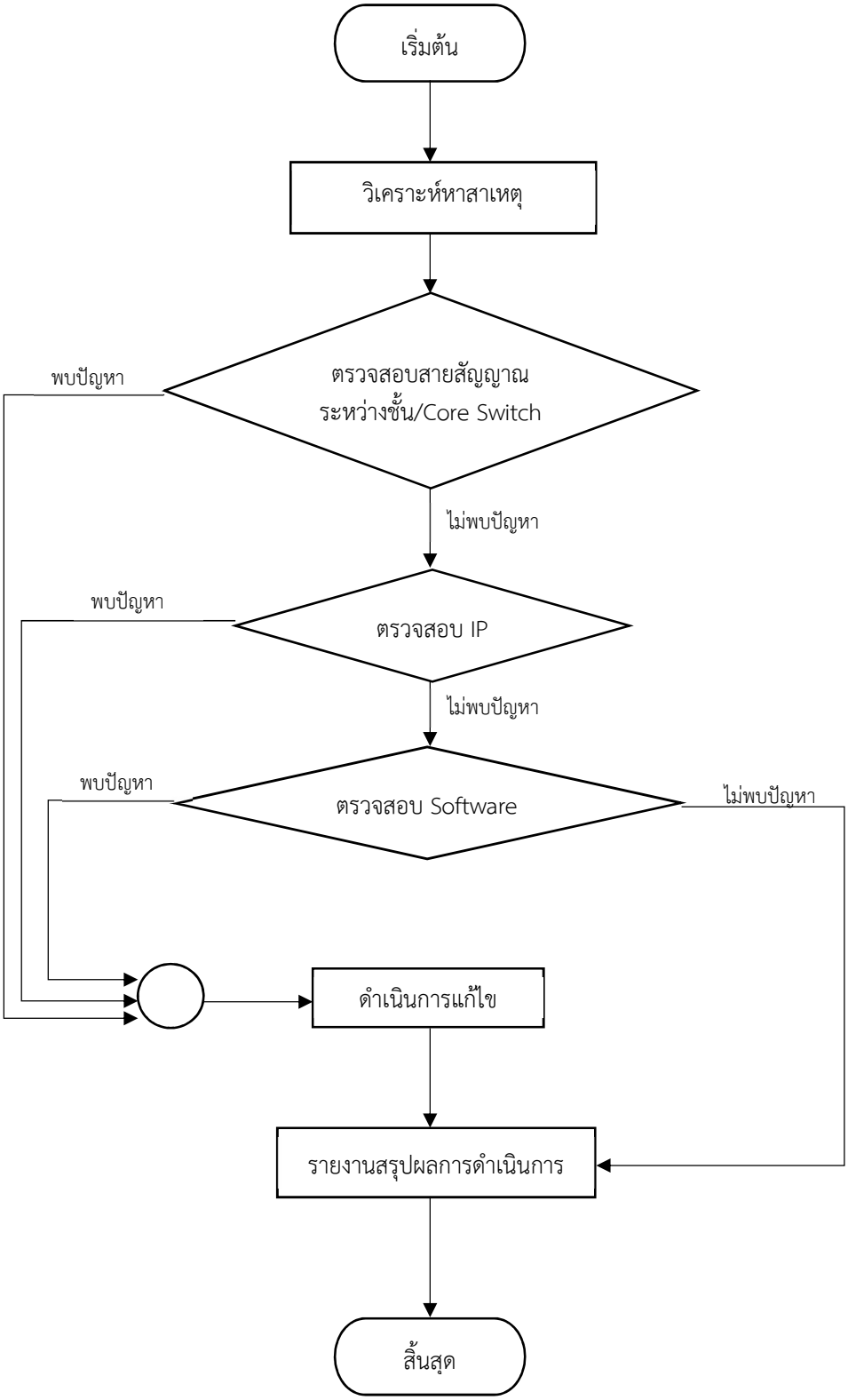
- บุกรุก/ภัยคุกคาม



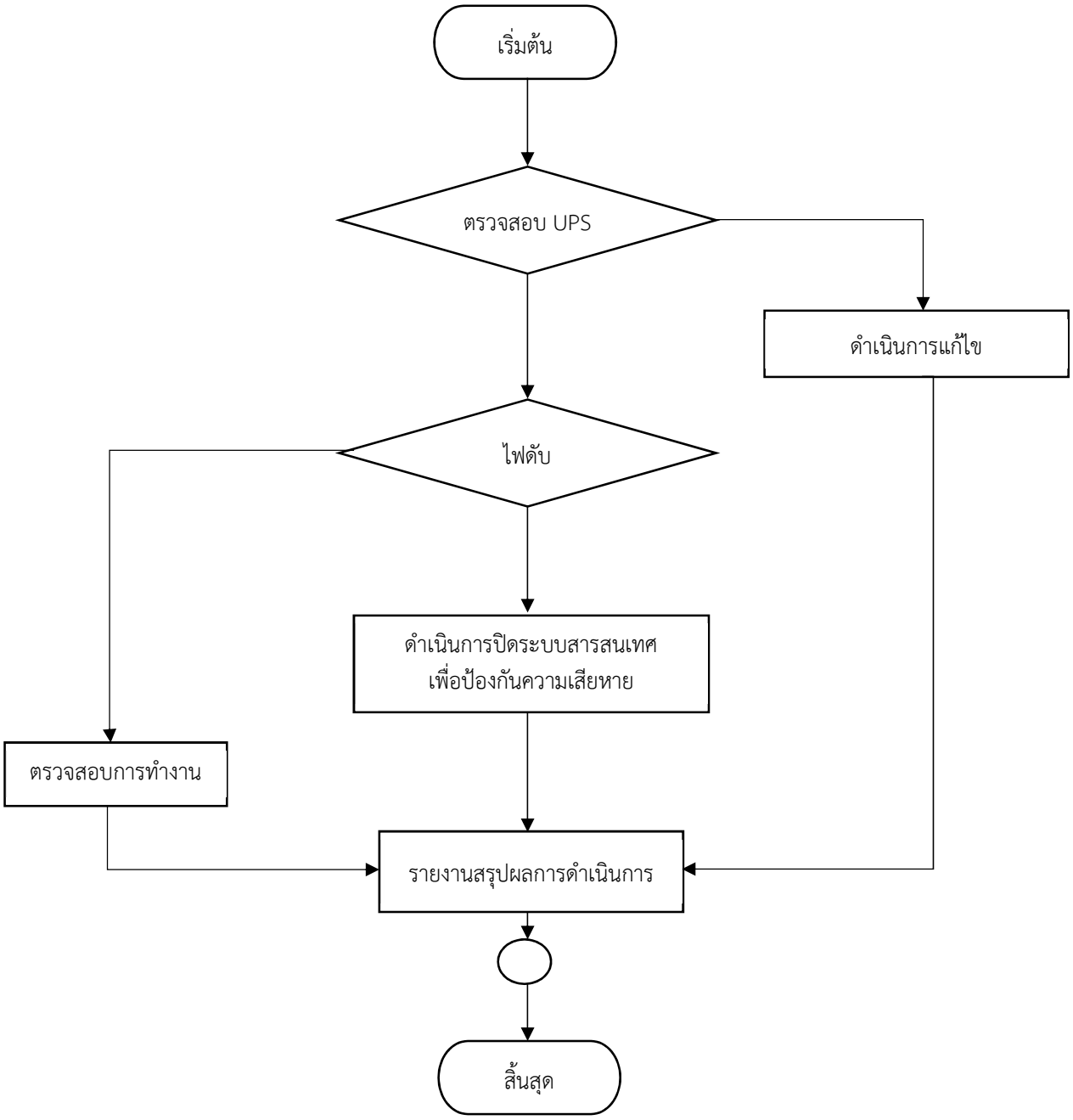
- ไวรัส


เริ่มต้น
จำกัดการเชื่อมต่อเข้าระบบเครือข่าย
วิเคราะห์สาเหตุ
และผลกระทบ
ไม่ร้ายแรง
ร้ายแรง
ป้องกันระบบเครือข่าย/
หยุดยั้งการระบาดไวรัส
แจ้ง Thaicert
ตรวจสอบและติดตามเครื่องที่ติดไวรัส
สรุปรายงาน/ปรับปรุง
สิ้นสุด

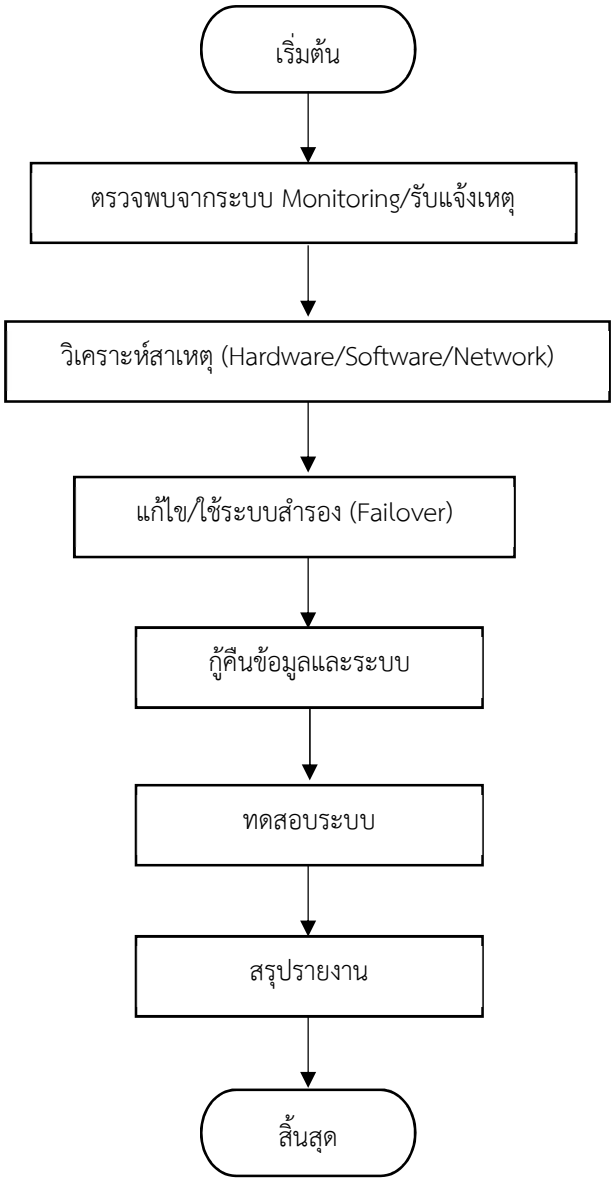
(3) ระบบเครือข่ายล้มเหลว



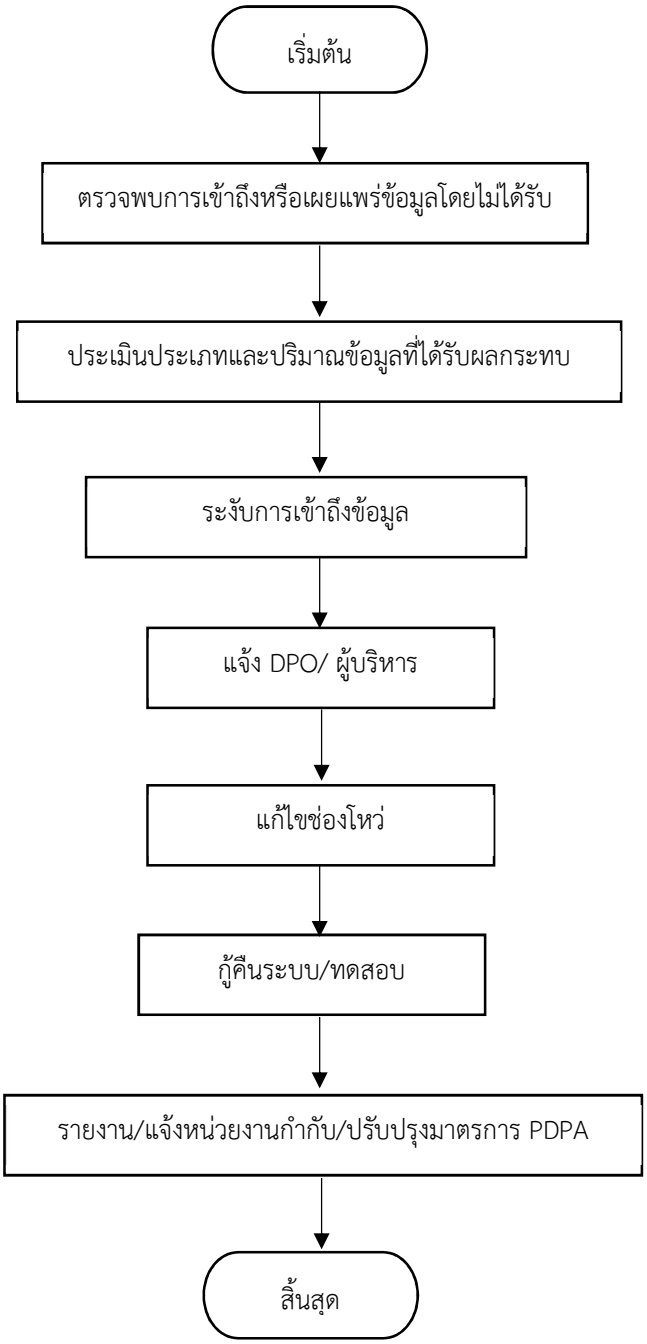
(4) ระบบไฟฟ้าขัดข้อง



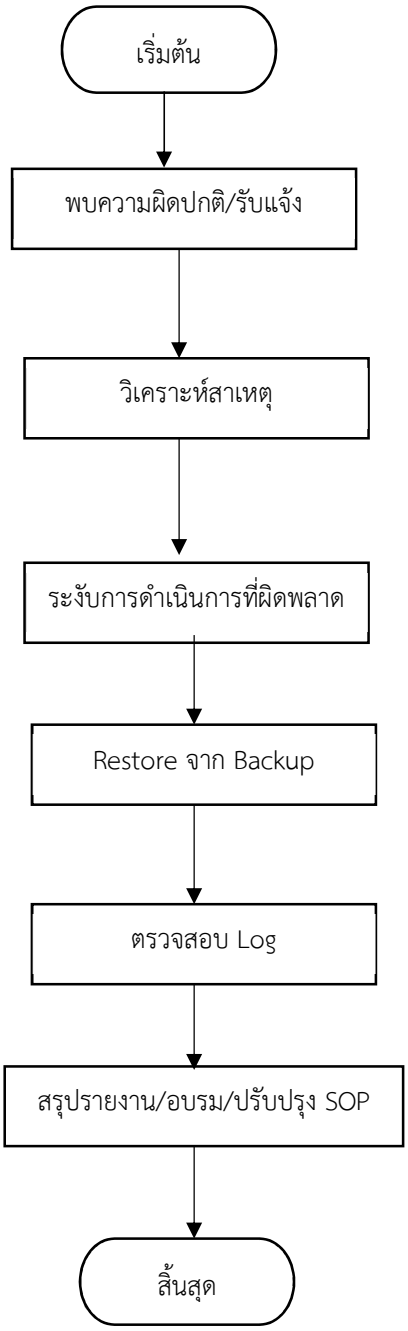
(5) คอมพิวเตอร์แม่ข่ายขัดข้อง



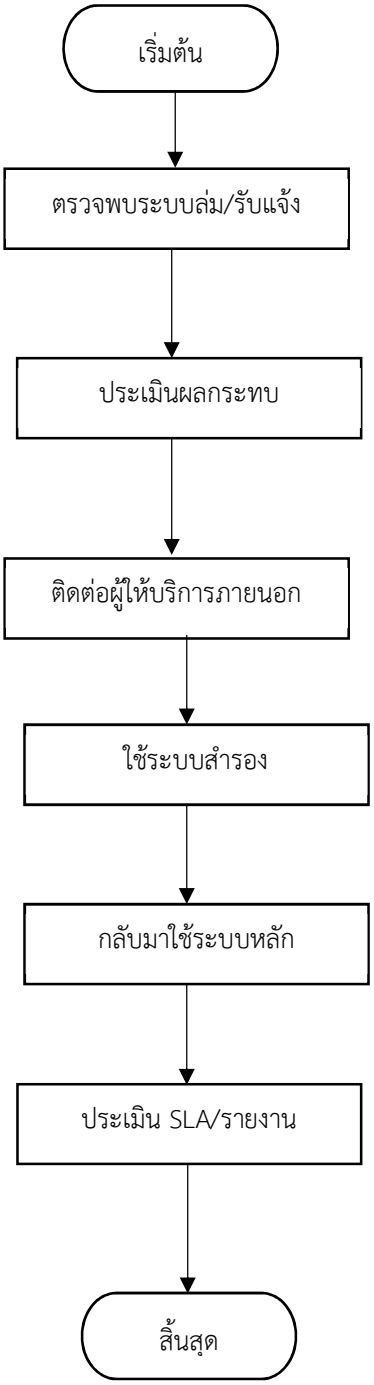
(6) ข้อมูลรั่วไหลหรือการละเมิดข้อมูลส่วนบุคคล



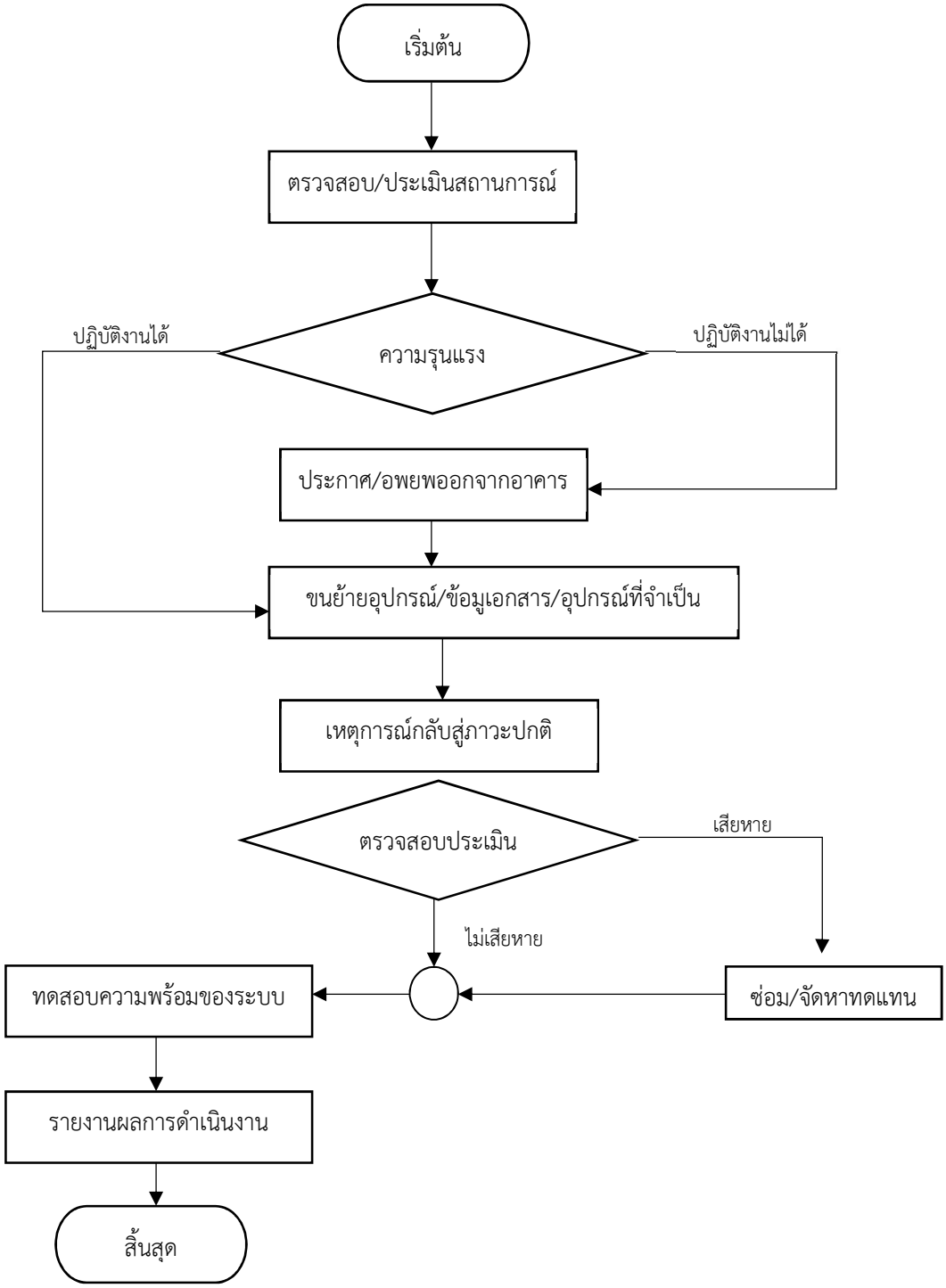
(7) ความผิดพลาดจากการปฏิบัติงานของบุคลากร



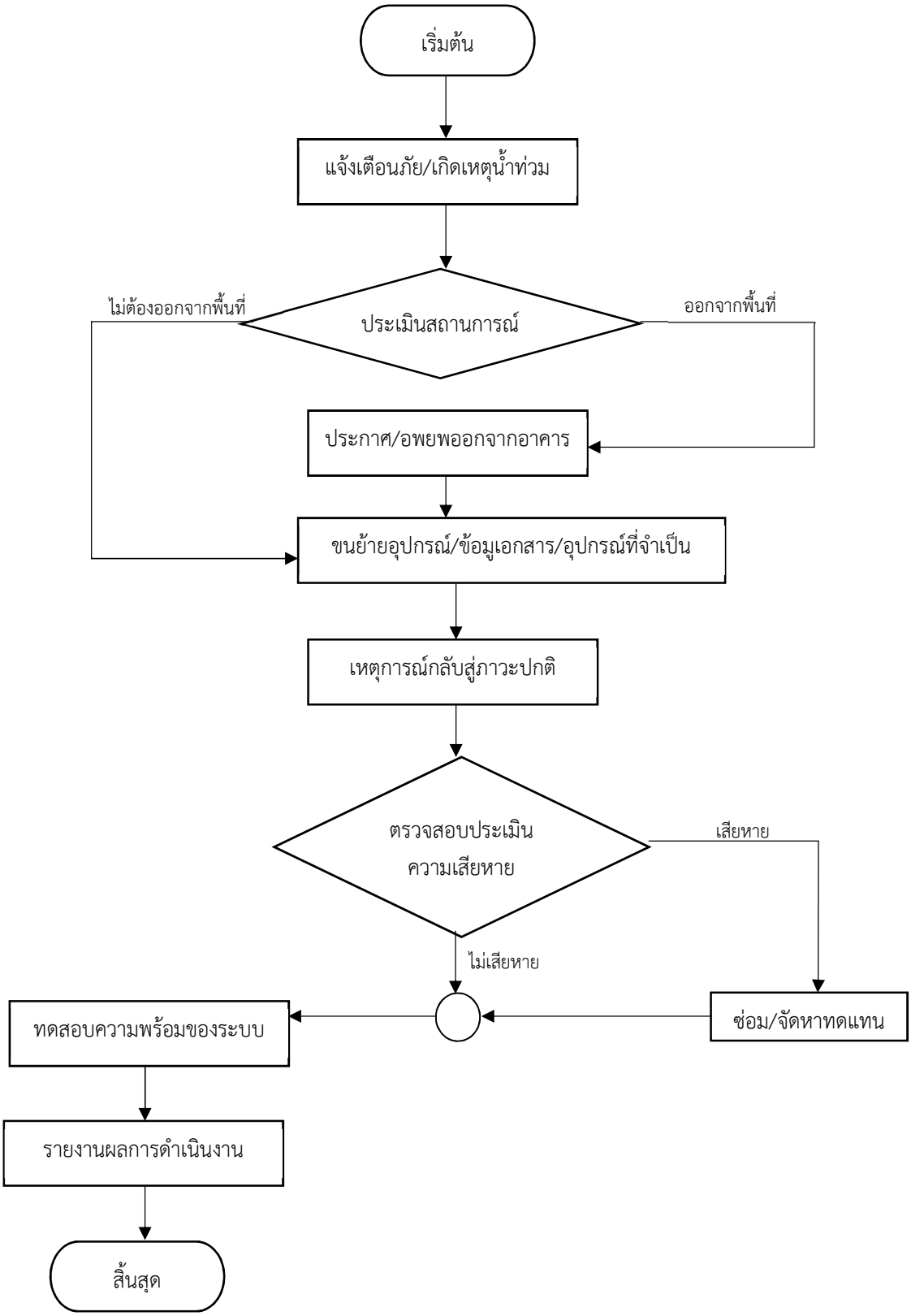
(8) การหยุดชะงักของผู้ให้บริการภายนอก



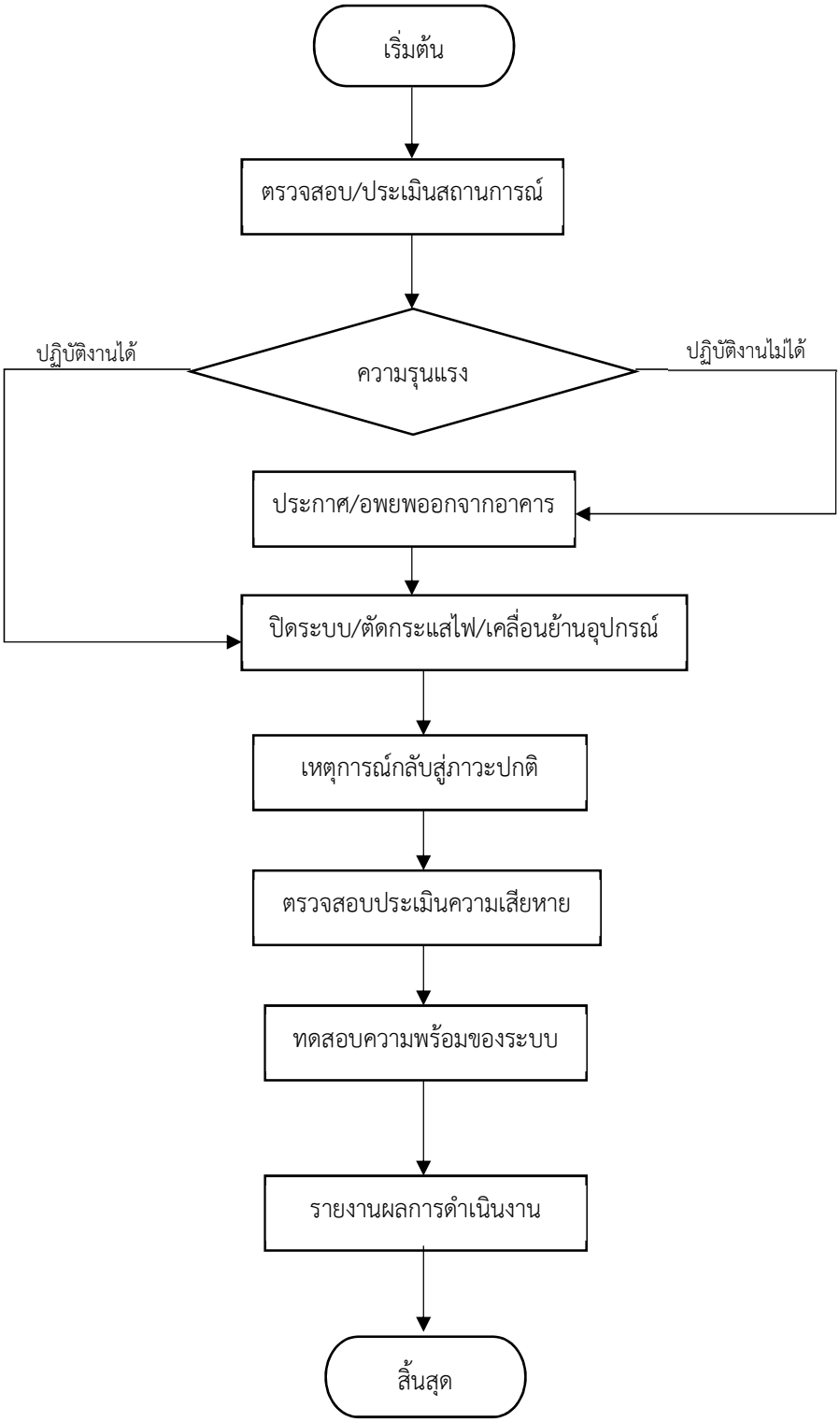
(9) เหตุการณ์ความไม่สงบ



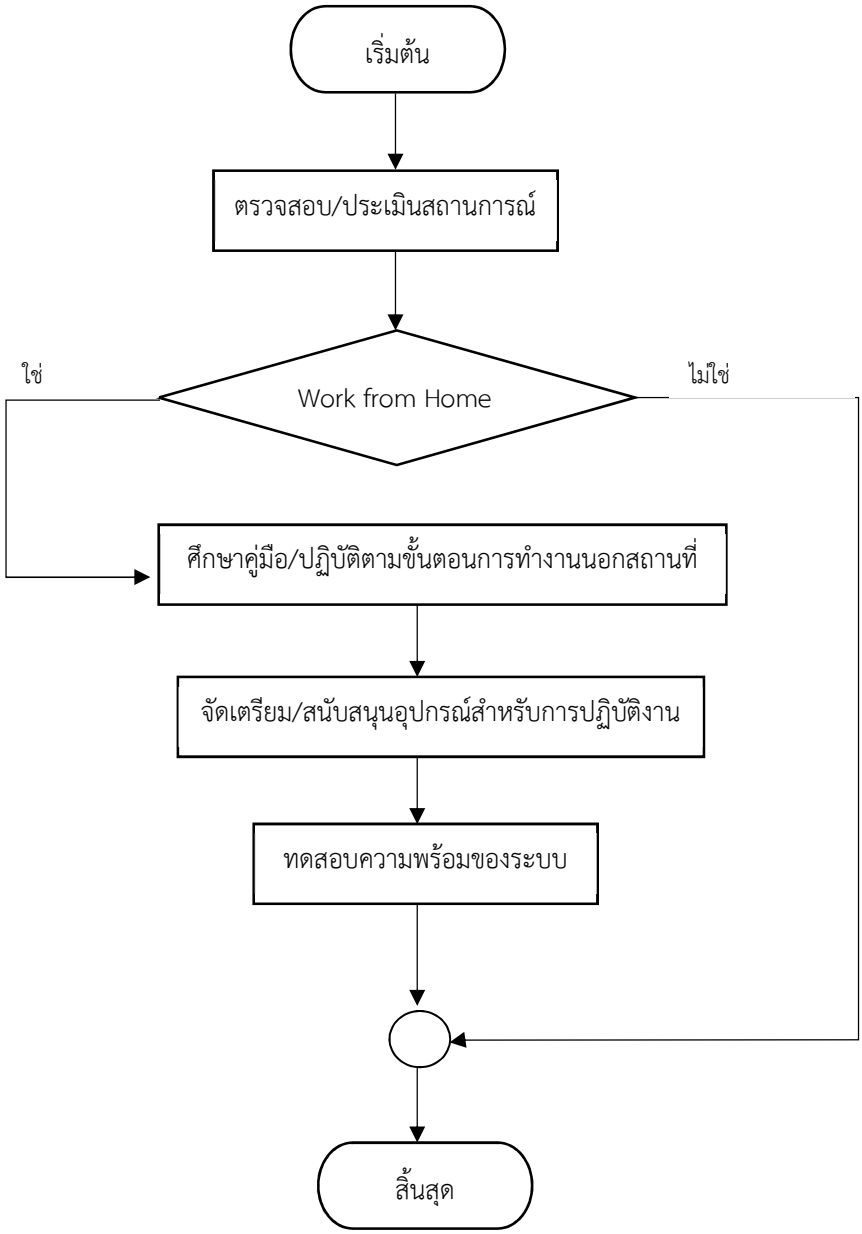
(10) น้ำท่วม


เริ่มต้น
แจ้งเตือนภัย/เกิดเหตุน้ำท่วม
ประเมินสถานการณ์
ไม่ต้องออกจากพื้นที่
ออกจากพื้นที่
ประกาศ/อพยพออกจากอาคาร
ขนย้ายอุปกรณ์/ข้อมูเอกสาร/อุปกรณ์ที่จำเป็น
เหตุการณ์กลับสู่ภาวะปกติ
ตรวจสอบประเมิน
ความเสียหาย
เสียหาย
ไม่เสียหาย
ทดสอบความพร้อมของระบบ
ซ่อม/จัดหาทดแทน
รายงานผลการดำเนินงาน
สิ้นสุด

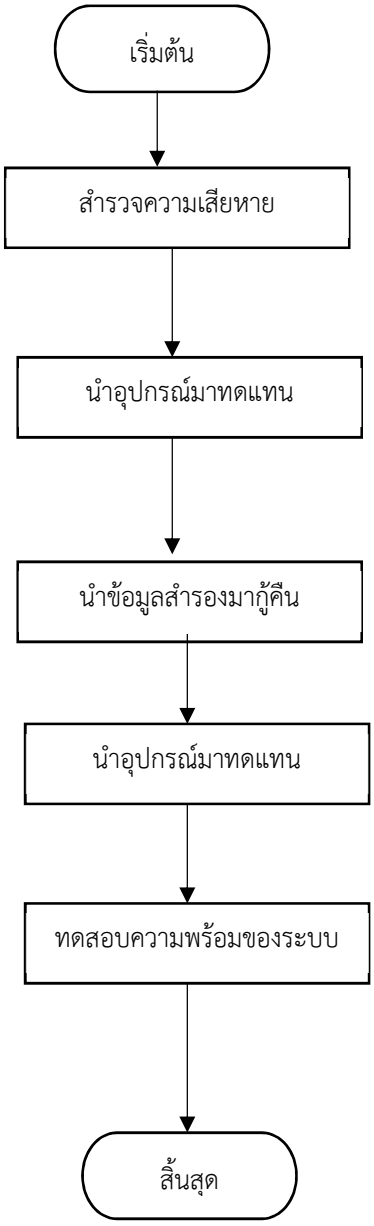
(11) แผ่นดินไหว


เริ่มต้น
ตรวจสอบ/ประเมินสถานการณ์
ความรุนแรง
ปฏิบัติงานได้
ปฏิบัติงานไม่ได้
ประกาศ/อพยพออกจากอาคาร
ปิดระบบ/ตัดกระแสไฟ/เคลื่อนย้านอุปกรณ์
เหตุการณ์กลับสู่ภาวะปกติ
ตรวจสอบประเมินความเสียหาย
ทดสอบความพร้อมของระบบ
รายงานผลการดำเนินงาน
สิ้นสุด

(12) โรคระบาด


เริ่มต้น
ตรวจสอบ/ประเมินสถานการณ์
Work from Home
ใช่
ไม่ใช่
ศึกษาคู่มือ/ปฏิบัติตามขั้นตอนการทำงานนอกสถานที่
จัดเตรียม/สนับสนุนอุปกรณ์สำหรับการปฏิบัติงาน
ทดสอบความพร้อมของระบบ
สิ้นสุด

(13) โจรกรรม/การสูญหายของทรัพย์สิน



7. แผนการกู้คืนระบบและข้อมูล

เพื่อกำหนดแนวทางและขั้นตอนในการกู้คืนระบบสารสนเทศและข้อมูลของหน่วยงานให้สามารถกลับมาใช้งานได้อย่างรวดเร็ว ถูกต้อง และปลอดภัย ภายหลังเกิดเหตุการณ์ที่ส่งผลกระทบต่อเครื่องแม่ข่ายหรือระบบสารสนเทศ โดยครอบคลุมระบบสารสนเทศที่สำคัญ ได้แก่ ระบบเครื่องแม่ข่าย (Server/ Virtual Machine/ Cloud) ระบบฐานข้อมูล (Database) ระบบเครือข่าย (Network Configuration) ระบบสารสนเทศภารกิจหลักของหน่วยงาน และข้อมูลสำคัญและข้อมูลส่วนบุคคล (PDPA)

7.1 การสำรองข้อมูล

หน่วยงานกำหนดนโยบายการสำรองข้อมูล เพื่อให้ข้อมูลและระบบสารสนเทศที่สำคัญได้รับการปกป้อง และสามารถกู้คืนได้อย่างมีประสิทธิภาพเมื่อเกิดเหตุการณ์ผิดปกติ โดยมีรายละเอียดดังนี้

(1) การสำรองข้อมูลการตั้งค่าเครือข่าย (Configuration Backup)

หน่วยงานต้องดำเนินการสำรองค่าการตั้งค่าของอุปกรณ์และระบบเครือข่ายที่สำคัญ เช่น Firewall, Router, Switch และ Server Configuration อย่างสม่ำเสมอ ดังนี้

- ต้องสำรองข้อมูลทุกครั้งเมื่อมีการเปลี่ยนแปลงการตั้งค่า และอย่างน้อยวันละ 1 ครั้ง
- ไฟล์สำรองต้องอยู่ในรูปแบบที่สามารถนำกลับมาใช้งานได้ทันที (Restorable Format)
- จัดเก็บข้อมูลสำรองไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย เช่น ระบบจัดเก็บข้อมูลส่วนกลาง (NAS), Storage กลาง หรือระบบ Cloud
- ต้องมีการควบคุมการเข้าถึงไฟล์ Configuration อย่างเหมาะสม

(2) การสำรองข้อมูลฐานข้อมูล (Database Backup)

หน่วยงานต้องดำเนินการสำรองข้อมูลฐานข้อมูลอย่างเป็นระบบและต่อเนื่อง ดังนี้

- ดำเนินการสำรองข้อมูลแบบเต็ม (Full Backup) เป็นประจำทุกวัน
- ใช้เทคนิคการบีบอัดข้อมูล (Compression) เพื่อเพิ่มประสิทธิภาพในการจัดเก็บและการโอนถ่ายข้อมูล
- พิจารณาใช้การสำรองข้อมูลแบบ Incremental หรือ Differential เพื่อเพิ่มความรวดเร็วและลดภาระของระบบ
- ตรวจสอบความสมบูรณ์ของข้อมูลสำรองทุกครั้ง (Backup Verification)
- จัดเก็บข้อมูลสำรองแยกจากระบบหลัก (Off-site Storage หรือ Cloud) เพื่อป้องกันความเสียหายจากเหตุเดียวกัน

(3) การสำรองระบบและแอปพลิเคชัน (System / Application Backup)

เพื่อรองรับการกู้คืนระบบในกรณีเกิดเหตุฉุกเฉิน หน่วยงานต้องดำเนินการดังนี้

- สำรองข้อมูลในระดับระบบ (System Image) หรือ Snapshot ของเครื่องเสมือน (Virtual Machine)
- สำรองโปรแกรมประยุกต์ (Application) และค่าการตั้งค่าที่สำคัญ
- จัดเตรียมระบบสำรอง เช่น Standby Server หรือ Disaster Recovery Site เพื่อรองรับการกู้คืนระบบ
- ตรวจสอบความพร้อมของระบบสำรองอย่างสม่ำเสมอ

(4) การกำหนดรอบเวลาในการสำรองข้อมูล (Backup Schedule)

หน่วยงานต้องกำหนดรอบระยะเวลาการสำรองข้อมูลให้เหมาะสมกับความสำคัญของระบบ โดยมีแนวทางดังนี้

- Full Backup: รายวัน
- Incremental Backup: รายชั่วโมง หรือรายวัน
- Configuration Backup: ทุกครั้งที่มีการเปลี่ยนแปลง
- Off-site Backup: รายวัน หรือ รายสัปดาห์

ทั้งนี้ การกำหนดรอบเวลาต้องสอดคล้องกับค่า RPO (Recovery Point Objective) ที่กำหนดไว้ในแผน

(5) มาตรการความมั่นคงปลอดภัยของข้อมูลสำรอง (Backup Security Control)

หน่วยงานต้องกำหนดมาตรการควบคุมเพื่อปกป้องข้อมูลสำรอง ดังนี้

- เข้ารหัสข้อมูลสำรอง (Encryption) ทั้งในระหว่างจัดเก็บและการรับ-ส่งข้อมูล
- กำหนดสิทธิ์การเข้าถึงข้อมูล (Access Control) ตามหลักการ Least Privilege
- จัดเก็บข้อมูลสำรองในสถานที่ที่แยกจากระบบหลัก (Off-site / Cloud Storage)
- จัดให้มีการบันทึกและตรวจสอบ Log การเข้าถึงข้อมูลสำรองอย่างสม่ำเสมอ
- ทดสอบการกู้คืนข้อมูลจาก Backup (Restore Test) อย่างน้อยปีละ 1 ครั้ง

7.2 การกู้คืนระบบและข้อมูล

(1) การประเมินสถานการณ์

หน่วยงานต้องดำเนินการตรวจสอบและประเมินสถานการณ์โดยทันทีเมื่อเกิดเหตุการณ์ โดยมีรายละเอียดดังนี้

- ตรวจสอบลักษณะและขอบเขตความเสียหายของระบบสารสนเทศ รวมถึงอุปกรณ์ที่เกี่ยวข้อง
- ระบุระบบ แอปพลิเคชัน และข้อมูลที่ได้รับผลกระทบอย่างชัดเจน
- ประเมินผลกระทบต่อภารกิจหลักของหน่วยงานและผู้รับบริการ
- จัดลำดับความสำคัญของระบบ (Priority) เพื่อกำหนดลำดับการกู้คืนให้สอดคล้องกับความจำเป็นเร่งด่วน
- รายงานสถานการณ์ต่อผู้บริหารหรือผู้มีอำนาจสั่งการตามลำดับ

(2) การเตรียมระบบ

ภายหลังการประเมินสถานการณ์ ให้ดำเนินการเตรียมความพร้อมของระบบสำหรับการกู้คืน ดังนี้

- จัดเตรียมเครื่องแม่ข่ายสำรอง (Standby Server) หรือสภาพแวดล้อมบนระบบ Cloud ตามที่กำหนดในแผน
- ติดตั้งระบบปฏิบัติการ (Operating System) และโปรแกรมพื้นฐานที่จำเป็นให้พร้อมใช้งาน
- ตรวจสอบและกำหนดค่าระบบเครือข่าย (Network Configuration) ให้สามารถรองรับการกู้คืนและการเชื่อมต่อได้อย่างถูกต้อง
- ตรวจสอบความพร้อมของทรัพยากร เช่น พื้นที่จัดเก็บ (Storage), หน่วยความจำ (Memory) และสิทธิ์การเข้าถึงระบบ

(3) การกู้คืนข้อมูล

เมื่อระบบมีความพร้อม ให้ดำเนินการกู้คืนข้อมูลตามลำดับความสำคัญ ดังนี้

- นำข้อมูลสำรองล่าสุด (Latest Backup) ที่ผ่านการตรวจสอบแล้ว มาใช้ในการกู้คืน
- ดำเนินการกู้คืนฐานข้อมูล (Database Restore) และระบบงานที่เกี่ยวข้อง
- นำค่าการตั้งค่าระบบ (Configuration) กลับมาใช้งาน เพื่อให้ระบบสามารถทำงานได้ตามปกติ
- ตรวจสอบความครบถ้วน ถูกต้อง และความสอดคล้องของข้อมูล (Data Integrity)
- บันทึกขั้นตอนและผลการดำเนินงานเพื่อใช้เป็นหลักฐานและการตรวจสอบย้อนหลัง

(4) การทดสอบระบบ

ภายหลังการกู้คืนข้อมูล ให้ดำเนินการทดสอบระบบก่อนเปิดใช้งานจริง ดังนี้

- ทดสอบการทำงานของระบบ (Functional Test) เพื่อยืนยันว่าระบบสามารถให้บริการได้ตามปกติ
- ตรวจสอบความถูกต้องของข้อมูล และความสัมพันธ์ของข้อมูลในระบบ
- ทดสอบด้านความมั่นคงปลอดภัย เช่น การตรวจสอบสิทธิ์การเข้าถึง และการป้องกันช่องโหว่
- ให้ผู้ใช้งานหรือหน่วยงานที่เกี่ยวข้องร่วมทดสอบ (User Acceptance Test: UAT) ตามความเหมาะสม

(5) การเปิดใช้งานระบบ

เมื่อระบบผ่านการทดสอบเรียบร้อยแล้ว ให้ดำเนินการเปิดใช้งานระบบตามขั้นตอน ดังนี้

- เปิดให้บริการระบบตามลำดับความสำคัญของภารกิจ (Priority-based Service Restoration)
- แจ้งผู้ใช้งานและหน่วยงานที่เกี่ยวข้องให้ทราบถึงสถานะการกลับมาให้บริการของระบบ
- เฝ้าระวังและติดตามการทำงานของระบบอย่างใกล้ชิดในช่วงระยะเวลาเริ่มต้น (Monitoring Period)
- บันทึกเหตุการณ์และผลการดำเนินงานเพื่อใช้ในการรายงานและปรับปรุงแผนในอนาคต

8. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉินให้ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศทราบ เพื่อนำเสนอรายงานสรุปให้อธิบดีกรมกิจการสตรีและสถาบันครอบครัว และผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม เพื่อนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพยิ่งขึ้น และสามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

****