

IT CONTINGENCY PLAN



**แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ
ระบบเทคโนโลยีสารสนเทศ**





แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ
ระบบเทคโนโลยีสารสนเทศ
IT CONTINGENCY PLAN

สารบัญ

	หน้า
วัตถุประสงค์ ขอบเขตการดำเนินงาน	4
การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ	5
การประเมินสถานการณ์และกำหนดระดับความรุนแรง	5
ขั้นตอนและแนวทางการป้องกันเบื้องต้น	5-7
การเตรียมความพร้อม	7-13
การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน	14-18
ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ	19-30
การตรวจสอบการทำงานของเครื่องแม่ข่าย	31-32
แผนการกู้คืนข้อมูล	33-34
การติดตามและรายงานผล	35

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan)

ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศ ถือเป็นสิ่งที่มีความสำคัญต่อการดำเนินงานตามภารกิจของกรมส่งเสริมคุณภาพสิ่งแวดล้อม จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัยสามารถนำไปใช้ประโยชน์ต่อการปฏิบัติงานได้อย่างมีประสิทธิภาพ ศูนย์สารสนเทศสิ่งแวดล้อม ได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศของกรมฯ ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์เครือข่ายได้รับความเสียหายได้ ดังนั้น ศูนย์สารสนเทศสิ่งแวดล้อม จึงได้จัดทำแผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเตรียมความพร้อม และสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที ลดความเสี่ยงที่อาจเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม

วัตถุประสงค์

1. เพื่อเตรียมความพร้อมรับมือสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศขององค์กร
2. เพื่อสร้างความรู้ความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร
3. เพื่อใช้เป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กรให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

ขอบเขตการดำเนินงาน

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) ที่ศูนย์สารสนเทศสิ่งแวดล้อม จัดทำขึ้นสำหรับเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของกรมฯ ประกอบด้วย

1. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น
3. การเตรียมความพร้อม
4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน
5. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ อาคารกรมส่งเสริมคุณภาพสิ่งแวดล้อม
6. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ อาคารศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม
7. การตรวจสอบการทำงานของเครื่องแม่ข่าย
8. แผนการกู้คืนข้อมูล
9. การติดตามและรายงานผล

1. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

1.1 วิเคราะห์เหตุการณ์ภัยพิบัติ ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของกรมฯ จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว โรคระบาด ฯลฯ

2) ระบบเครื่องแม่ข่ายที่เชื่อมต่อบริเวณอินเทอร์เน็ตเกิดความขัดข้อง

3) การบุกรุกหรือโจมตีระบบควบคุมเทคโนโลยีสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล

4) ระบบกระแสไฟฟ้าขัดข้อง ไฟฟ้าดับ ไฟกระชาก

5) ไวรัสมัลแวร์

ภัยพิบัติจากภายใน

1) ระบบเครื่องแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย

2) ไวรัสมัลแวร์จากผู้ใช้งานภายในกรมฯ

3) เจ้าหน้าที่หรือบุคลากรของกรมฯ ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย

1.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง

เมื่อกรมฯ มีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรงภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ โดยเจ้าหน้าที่ศูนย์สารสนเทศสิ่งแวดล้อม นำมาสรุปเป็นข้อมูล ดังนี้

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)			จัดเรียงลำดับ	
	ต่อระบบงาน	ต่อพันธกิจ	ต่อประชาชน	รวม	จัดลำดับ
กรณีไฟไหม้	5	5	4	14	1
กรณีโดนแทรกแซงระบบ	5	4	3	12	2
กรณีไฟฟ้าดับ	5	3	2	10	3
กรณีแผ่นดินไหว	3	2	3	8	4
กรณีจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	2	2	3	7	5
กรณีเกิดโรคระบาด	1	5	5	11	3

2. ขั้นตอนและแนวทางการป้องกันเบื้องต้น

2.1 การประกาศใช้แผน

กรมส่งเสริมคุณภาพสิ่งแวดล้อม มีการประกาศใช้แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency) อย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมจะทำการแจ้งให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของกรมฯ ทราบ เพื่อพิจารณาประกาศใช้แผนต่อไป

2.2 กำหนดขั้นตอนการดำเนินงาน

ศูนย์สารสนเทศสิ่งแวดล้อม จัดเตรียมขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์ฉุกเฉินหรือความผิดปกติ โดยกำหนดขั้นตอนการปฏิบัติที่เหมาะสมต่อสถานการณ์ต่างๆ ที่เกิดขึ้น รวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกหรือสถานการณ์ฉุกเฉิน เพื่อให้สามารถแก้ปัญหา หรือยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลา รวมถึงการเตรียมอุปกรณ์สำรองเพื่อใช้ในการกู้คืนระบบ

2.3 การติดต่อประสานงาน

มีการจัดทำข้อมูลรายชื่อหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัย กรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า , สถานีดับเพลิง , สถานีตำรวจ, หน่วยงานด้านสาธารณสุข, สำนักข่าวที่มีความน่าเชื่อถือ เป็นต้น

2.4 การจัดเตรียมอุปกรณ์

ศูนย์สารสนเทศสิ่งแวดล้อม ซึ่งเป็นหน่วยงานหลักที่ดูแลระบบเทคโนโลยีสารสนเทศ ระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์หรืออุปกรณ์เครือข่ายเกิดขัดข้องใช้งานไม่ได้ ดังนี้

- เครื่องคอมพิวเตอร์ PC/เครื่องคอมพิวเตอร์ Notebook/Tablet /Pocket Wi-Fi
- โปรแกรมระบบปฏิบัติการ/ ระบบปฏิบัติการของเครือข่าย/ ระบบงานที่สำคัญ
- อุปกรณ์สำรองข้อมูลและระบบงานที่สำคัญ
- โปรแกรม antivirus
- Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฟ้าอัตโนมัติ
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์
- อุปกรณ์ และโปรแกรม สำหรับการติดต่อสื่อสารออนไลน์ (VDO Conference)
- ระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการปฏิบัติงาน (Cloud Server)

2.5 การสำรองข้อมูล

เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเกิดความเสียหาย ถูกทำลายจากไวรัส หรือผู้บุกรุกแทรกแซง เปลี่ยนแปลงข้อมูล และสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยกรมฯ มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์ และแผนการสำรองข้อมูล ดังนี้

- 1) การสำรองข้อมูลเว็บไซต์ และระบบงานต่าง ๆ ของกรมส่งเสริมคุณภาพสิ่งแวดล้อม
- 2) การสำรองข้อมูลเครือข่าย (Configuration)

2.6 การป้องกันและกำจัดไวรัส

มีการติดตั้งซอฟต์แวร์ป้องกันและกำจัดไวรัส สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อในระบบเครือข่าย โดยผู้ใช้งานต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่ออินเทอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้บุกรุกสามารถเข้ามาทำลายระบบได้

2.7 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

- 1) กำหนดมาตรการควบคุมการเข้า – ออก ห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้องควบคุมจะมีกุญแจ และ keycard ส่วนกลางเพียง 1 ชุดเท่านั้น กรณีที่ผู้เกี่ยวข้องต้องการเข้าไปในห้องควบคุม ต้องลงชื่อเบิกกุญแจ และ keycard ในสมุดควบคุมการเข้า – ออก ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากจำเป็น ให้เจ้าหน้าที่ของศูนย์สารสนเทศสิ่งแวดล้อมเป็นผู้รับผิดชอบพาเข้าไป ในห้องควบคุมมีการติดตั้งกล้องโทรทัศน์วงจรปิด

2) มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยกำหนดให้ Firewall ควบคุมการเข้า-ออก หรือการควบคุมการรับ-ส่งข้อมูล ในระบบเครือข่าย และเปิดใช้งานตลอดเวลา

3) มีการติดตั้ง IPS (Intrusion Prevention System) เพื่อให้ตรวจสอบการบุกรุกโดยจะทำงานคล้ายๆกับ IDS แต่จะมีคุณสมบัติพิเศษในการจู่โจมกลับหรือหยุดยั้งผู้บุกรุกได้ด้วยตัวเองโดยที่ไม่จำเป็นต้องอาศัยโปรแกรมหรือ Hardware ตัวอื่นๆ

4) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบการใช้งานข้อมูลบนเครือข่ายอินเทอร์เน็ตของกรมฯ เพื่อตรวจสอบการใช้งานบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและหาวิธีการป้องกันต่อไป

5) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยได้จัดหาระบบบริหารจัดการเก็บข้อมูล Log (Central Log Management) เพื่อตรวจสอบ ติดตามการวิเคราะห์ (Log File) และการเฝ้าระวังในเครือข่าย (Network Monitoring) เพื่อเพิ่มประสิทธิภาพในการดูแลระบบเครือข่ายของกรมส่งเสริมคุณภาพสิ่งแวดล้อมให้ดียิ่งขึ้น

2.8 การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว จลาจล ชุมชนุประท้วง

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นดินไหว โดยเตรียมอุปกรณ์ดังนี้

- 1) เตรียมอุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงแหล่งที่เก็บ
- 2) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน
- 3) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน

2.9 การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เพื่อเป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบเทคโนโลยีสารสนเทศและอุปกรณ์เครือข่ายคอมพิวเตอร์ ได้กำหนดแนวทาง ดังนี้

- 1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์เครือข่าย หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ 120 นาที
- 2) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Generator)
- 3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
- 4) ติดตั้งอุปกรณ์ตรวจวัดอุณหภูมิและความชื้น สำหรับห้อง Server
- 5) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

3. การเตรียมความพร้อม

3.1 การเตรียมความพร้อมกรณีเกิดการแทรกแซงเว็บไซต์

เมื่อเกิดเหตุโจมตี บุกรุก ผ่านทางเว็บไซต์ให้ดำเนินการ ดังนี้

- 1) สกัดกั้นการเข้าถึงเครื่องให้บริการ เพื่อไม่ให้เกิดการเปลี่ยนแปลงของข้อมูล ด้วยการถอดสาย Network ออกจากเครื่อง
- 2) ตรวจสอบความเปลี่ยนแปลงของข้อมูลในระบบ
- 3) ตรวจสอบ Log File หรือ แฟ้มกิจกรรมของระบบ เพื่อดูพฤติกรรมที่น่าสงสัย
- 4) ดำเนินการปิดช่องโหว่บนหน้าเว็บไซต์ โดยให้คำนึงถึงสิ่งต่างๆ ดังนี้

- การตรวจสอบการป้อนข้อมูล
- SQL Injection
- XSS (Cross Site Scripting)

5) หากไม่สามารถดำเนินการแก้ไขได้โดยเร็ว ให้ทำการปิดการใช้งานในส่วนที่เกิดปัญหา ก่อนปรับปรุงซอฟต์แวร์ที่เกี่ยวข้องให้เป็นรุ่นล่าสุดที่มีความมั่นคงปลอดภัยสูง

แผนปฏิบัติการกรณีเกิดการแทรกแซงเว็บไซต์

กลุ่มระบบคอมพิวเตอร์ทำการซ้อมปฏิบัติตามแผนการแทรกแซงเว็บไซต์ ดังนี้

- 1) เจ้าหน้าที่ได้รับแจ้งทางอีเมลหรือโทรศัพท์ว่า เว็บไซต์ www.deqp.go.th ถูกแทรกแซงเปลี่ยนหน้าเว็บไซต์
- 2) ทดลองเข้าเว็บไซต์ www.deqp.go.th เพื่อตรวจสอบหน้าเว็บไซต์อีกครั้ง
- 3) หลังจากตรวจสอบเป็นที่แน่ชัดว่าหน้าเว็บไซต์ถูกเปลี่ยนแปลง ให้รีบเก็บหลักฐานโดยการ copy หน้าเว็บไซต์ไว้
- 4) ติดต่อสำนักงานพัฒนารัฐบาลดิจิทัล (สปร.) เพื่อแจ้งเหตุและดำเนินการตัดการเชื่อมต่อจากเครือข่ายอินเทอร์เน็ตชั่วคราวเพื่อดำเนินการแก้ไข
- 5) ตรวจสอบหาร่องรอยการเข้าโจมตี ตรวจสอบ log เพื่อหา IP ที่เข้าเปลี่ยนหน้าเว็บไซต์
- 6) แก้ไขข้อบกพร่อง ช่องโหว่ทางเครือข่าย ที่เป็นสาเหตุให้ถูกโจมตี เปลี่ยน Password การเข้าใช้เครื่องแม่ข่ายหากจำเป็น
- 7) เปลี่ยนหน้าเว็บไซต์กลับเป็นแบบเดิมพร้อมเชื่อมต่อเครือข่ายอินเทอร์เน็ต เข้ากับเครื่องให้บริการเว็บไซต์ เปิดการเชื่อมต่อให้สามารถใช้งานเครื่องแม่ข่ายได้ตามปกติ
- 8) กรณีเกิดความเสียหายร้ายแรง ให้นำหลักฐานที่ได้ทั้งหมดเข้าแจ้งความกับตำรวจ

3.2 การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากกรณีไฟฟ้าดับ ไฟกระชาก

กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศฯ ดังนี้

- 1) ติดตั้งเครื่องสำรองไฟฟ้าอัตโนมัติ เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาในการสำรองไฟฟ้าโดยประมาณ 120 นาที
- 2) ติดตั้งเครื่องกำเนิดไฟฟ้าสำรอง (Generator)
- 3) เปิดเครื่องสำรองไฟฟ้า (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และ บำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ
- 4) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รับทำการบันทึกข้อมูลที่ค้างอยู่ที่และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ
- 5) กำหนดให้มีการสำรองฐานข้อมูล และระบบงานต่าง ๆ ทุก 1 เดือนเป็นอย่างน้อย

3.3 การเตรียมความพร้อมรับสถานการณ์ภัยจากแผ่นดินไหว

เตรียมความพร้อม โดยติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น ดังนี้

- 1) ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณสุขภัยจากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทาง

ปฏิบัติในการป้องกันและแก้ไขปัญหาสาธารณสุข ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์/แอปพลิเคชัน ของหน่วยงานต่างๆ เช่น กรมอุตุนิยมวิทยา ศูนย์เตือนภัยพิบัติแห่งชาติ กรมป้องกันและบรรเทาสาธารณภัย

2) การเตรียมบุคลากร วัสดุอุปกรณ์ สถานที่อพยพ

- ประสานการเตรียมการกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหว

- ประสานการเตรียมการกับหน่วยงานที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

- สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรขององค์กร

- จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

3) การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการให้ดำเนินการแก้ไข เพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

4) อบรม ให้ความรู้เกี่ยวกับการปฏิบัติเมื่อเกิดแผ่นดินไหว แก่เจ้าหน้าที่ บุคลากรภายในองค์กร

3.4 การเตรียมความพร้อมรับสถานการณ์ภัยจากการชุมนุมประท้วงและก่อกบฏจลาจล

ติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อกบฏจลาจล

1) ดำเนินการค้นหาข่าวจากแหล่งข่าวต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

2) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสาร ยานพาหนะ และมอบหมายหน้าที่ความรับผิดชอบ

3) ติดตั้งระบบกล้องวงจรปิดเพื่อรักษาความปลอดภัย

3.5 การเตรียมความพร้อมเพื่อรับมือกรณีเกิดโรคระบาด

1) กำหนดให้มีผู้ประสานงานหลักและทีมงานที่รับผิดชอบ ติดตามข้อมูล รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากผลกระทบของโรคระบาด จากหน่วยงานด้านสาธารณสุข สำนักข่าว ประกาศจากหน่วยงานภาครัฐ เป็นต้น

2) ติดต่อสื่อสารให้ความรู้แก่บุคลากร เจ้าหน้าที่ รวมถึงต้องเผยแพร่แผนการรับมือของหน่วยงานในทางเดียวกัน เพื่อลดความตื่นตระหนกของบุคลากร

3) การกำหนดแนวทางในการปฏิบัติงานระหว่างเกิดการแพร่ระบาด

3.1) กำหนดแนวทางในการปฏิบัติงาน โดยคำนึงถึงมาตรการทางสาธารณสุข มีความยืดหยุ่น คล่องตัวต่อเจ้าหน้าที่ผู้ปฏิบัติงาน

3.2) มอบหมายงานตามบทบาท ภารกิจ

* กรณีปฏิบัติงานในสถานที่ตั้งได้ เช่น กำหนดห้วงระยะเวลา และรูปแบบการทำงานที่เหมาะสม

* กรณีไม่สามารถปฏิบัติงานในสถานที่ตั้งได้ เช่น ปฏิบัติงานในที่พักอาศัย หรือพื้นที่ที่หน่วยงานกำหนดที่มีมาตรการสุขภาพและความปลอดภัย โดยการใช้เทคโนโลยีสนับสนุนการปฏิบัติงานตามความเหมาะสม และมีการรายงานผลการปฏิบัติงานต่อผู้บังคับบัญชา

4) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ยานพาหนะ รวมถึงระบบการสื่อสารออนไลน์ (VDO Conference, line group) ระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุนการปฏิบัติงาน (Cloud Server) และมอบหมายหน้าที่ความรับผิดชอบ (กรณีไม่สามารถปฏิบัติงานในสถานที่ตั้งได้)

3.6 เตรียมความพร้อมในการเสริมสร้างความมั่นคงปลอดภัยให้กับระบบระบบเครือข่าย

ติดตั้งโปรแกรมสำหรับติดตามการทำงานของระบบคอมพิวเตอร์ และบริหารจัดการอุปกรณ์เครือข่าย (Solar Winds Network Monitoring) โดยอาศัยโปรโตคอล SNMP เพื่อตรวจสอบสถานะของอุปกรณ์เครือข่ายในระบบ ซึ่งจะช่วยให้ผู้ดูแลระบบนั้นสามารถที่จะพบปัญหาหรือตรวจสอบปัญหาได้อย่างรวดเร็ว และประสานหน่วยงานศูนย์ประสานงานด้านความมั่นคงปลอดภัย Thai-CERT กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม เพื่อเข้ามาดำเนินการติดตั้งอุปกรณ์และซอฟต์แวร์สำหรับติดตามและเฝ้าระวังการบุกรุกจากภายนอก

การใช้งานโดยทั่วไป

สำหรับผู้ใช้งานเครือข่าย

1. จัดให้มีการอบรมเพื่อเสริมสร้างสมรรถนะในการใช้งานเทคโนโลยีสารสนเทศ เพื่อพัฒนาทักษะความรู้ ความเข้าใจ ในด้านเทคโนโลยีสารสนเทศให้แก่บุคลากรของกรมส่งเสริมคุณภาพสิ่งแวดล้อม เพื่อให้เจ้าหน้าที่ที่ได้รับการฝึกอบรมสามารถนำไปใช้ในการปฏิบัติงานได้อย่างเหมาะสมและมีประสิทธิภาพมากยิ่งขึ้น

2. สร้างความรู้ ความเข้าใจ แก่เจ้าหน้าที่กรมส่งเสริมคุณภาพสิ่งแวดล้อม ให้มีความตระหนักในการใช้งานเทคโนโลยีสารสนเทศอย่างปลอดภัย โดยกำหนดให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม หมวด ๔ แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน¹

ข้อ 1¹ ผู้ใช้งาน ปฏิบัติตามแนวทางการใช้งานหรือห้ามใช้งานโปรแกรมคอมพิวเตอร์

ข้อ 2¹ ผู้ใช้งาน ปฏิบัติตามเงื่อนไขการใช้งานและไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น

ข้อ 3¹ ผู้ใช้งาน กำหนดหรือใช้งานรหัสผ่านโดยปฏิบัติ (แนวปฏิบัติสำหรับการตั้งและใช้งานรหัสผ่าน)

ข้อ 4¹ ผู้ใช้งาน ตรวจสอบและป้องกันไวรัสโดยปฏิบัติ (แนวปฏิบัติสำหรับการป้องกันไวรัส)

ข้อ 5¹ ผู้ใช้งาน ป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การขโมย การสูญหาย หรือการเสียหายของข้อมูล เอกสาร คอมพิวเตอร์ หรืออุปกรณ์คอมพิวเตอร์ของกรมฯ

ข้อ 6¹ ผู้ใช้งาน ป้องกันอุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพาซึ่งสินทรัพย์เป็นของกรมฯ (แนวปฏิบัติสำหรับการใช้อุปกรณ์หรือเครื่องคอมพิวเตอร์แบบพกพา)

ข้อ 7¹ ผู้ใช้งาน ใช้ระบบงานของกรมฯ

ข้อ 8¹ ผู้ใช้งาน ทำบันทึกข้อความขอใช้งาน VPN เพื่อขออนุมัติจาก ผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมสำหรับการเข้าถึงระบบงานของกรมฯ จากระยะไกล โดยต้องแสดงเหตุผลหรือความจำเป็นในการใช้งาน พร้อมระบุระยะเวลาการใช้งานตามที่ต้องการ (แนวปฏิบัติในการเข้าถึงระบบงานจากระยะไกล)

ข้อ 9¹ ผู้ใช้งาน ห้ามใช้งานระบบเทคโนโลยีสารสนเทศ อินเทอร์เน็ต และเครือข่ายของกรมฯ ในลักษณะที่ผิดวัตถุประสงค์ (แนวปฏิบัติสำหรับการป้องกันการใช้งานระบบเทคโนโลยีสารสนเทศผิดวัตถุประสงค์)

ข้อ 10¹ ผู้ใช้งาน ใช้ระบบงานอีเมล

ข้อ 11¹ ในการจัดการกับข้อมูลของกรมฯ ตามชั้นความลับ ผู้ใช้งานข้อมูล ปฏิบัติตามแนวปฏิบัติในการบริหารจัดการข้อมูลตามระดับชั้นความลับ ที่กรมฯ ได้กำหนดไว้

ข้อ 12¹ เมื่อผู้ใช้งานพบเหตุการณ์หรือจุดอ่อนด้านความมั่นคงปลอดภัย ให้รีบแจ้งไปยังกลุ่มระบบคอมพิวเตอร์ หรือศูนย์สารสนเทศสิ่งแวดล้อมโดยทันทีที่พบเห็น

ข้อ 13¹ ผู้บังคับบัญชา ต้องดำเนินการตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานที่ลาออกก่อนวันที่มาปฏิบัติงานวันสุดท้ายเพื่อดูว่ายังอยู่ในสภาพที่ใช้งานได้ตามปกติหรือไม่ หากเกิดการชำรุดหรือเสียหาย ให้ตรวจสอบว่าเป็นการเสียหายตามสภาพการใช้งานหรือไม่ หากเป็นการชำรุดหรือเสียหายโดยประมาทหรือเลินเล่อ ให้แจ้งหน่วยงานพัสดุเพื่อดำเนินการสอบสวนต่อไป

¹ หมวด 4 แนวปฏิบัติที่เกี่ยวข้องกับหน้าที่และความรับผิดชอบของผู้ใช้งาน (แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมส่งเสริมคุณภาพสิ่งแวดล้อม)

การใช้งานเครือข่าย

สำหรับผู้ดูแลระบบ กำหนดให้ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศของกรมส่งเสริมคุณภาพสิ่งแวดล้อม หมวด 6 แนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย²

1) ข้อ 34² ผู้รับผิดชอบระบบสารสนเทศ ต้องบริหารจัดการความมั่นคงปลอดภัยบนเครือข่ายของกรมฯ

2) ข้อ 35² ผู้รับผิดชอบระบบสารสนเทศ กำหนดมาตรการความมั่นคงปลอดภัยสำหรับการใช้งาน VPN เพื่อเข้าถึงระบบงานของกรมฯ จากระยะไกล (แนวปฏิบัติสำหรับการบริหารจัดการการเข้าถึงเครือข่ายจากระยะไกล)

3) ข้อ 36² ผู้รับผิดชอบระบบสารสนเทศ ควบคุมการเข้าถึงและใช้งานระบบเครือข่ายไร้สายภายในกรมฯ

สำหรับผู้ใช้งาน กลุ่มระบบคอมพิวเตอร์ได้ดำเนินการติดตั้งโปรแกรมป้องกันและกำจัดไวรัสให้กับเครื่องคอมพิวเตอร์ลูกข่ายภายในกรมฯ โปรแกรมป้องกันและกำจัดไวรัสจะทำการสแกนข้อมูลที่มีการรับ - ส่งผ่านเครือข่ายก่อนมีการใช้งาน โดยแจ้งให้ผู้ใช้งานปฏิบัติดังนี้

- 1) ไม่ควรเปิดให้ผู้อื่นสามารถเข้าถึงข้อมูลในเครื่องคอมพิวเตอร์
- 2) ไม่ควรเปิดการเข้าถึงข้อมูลในเครื่องแบบ Full Control
- 3) ควรตรวจสอบข้อมูลที่รับ - ส่ง มาจากระบบเครือข่าย
- 4) ไม่ควรทำการ Download ข้อมูลใดๆ จากเครือข่ายภายนอก

3.6 การเตรียมความพร้อมในการดำเนินการเกี่ยวกับโปรแกรมป้องกันและกำจัดไวรัส

1) ดำเนินการติดตั้งโปรแกรมป้องกันและกำจัดไวรัส โดยติดตั้งโปรแกรมป้องกันและกำจัดไวรัสให้กับเครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องภายในกรมฯ อย่างเพียงพอ และได้ต่ออายุลิขสิทธิ์ของโปรแกรมทุกปี

2) ดำเนินการปรับปรุงรุ่นของโปรแกรมให้เป็นปัจจุบันอยู่เสมอ

3) ดำเนินการปรับปรุงฐานข้อมูลของไวรัสอย่างสม่ำเสมอ

4) โปรแกรมป้องกันและกำจัดไวรัสที่ใช้งานอยู่ต้องมีการตรวจสอบแบบทันทีทันใด

5) โปรแกรมป้องกันและกำจัดไวรัสที่ใช้งานอยู่ มีความสามารถในการตรวจสอบการ โจมตีจากไวรัสในรูปแบบต่างๆ ได้แก่ ตรวจสอบเมื่อเข้าใช้งานแฟ้มข้อมูล, ตรวจสอบเมื่อเข้าใช้งานโปรแกรมดูเว็บไซต์ และตรวจสอบเมื่อมีการใช้งาน E-mail

² หมวด 6 แนวปฏิบัติในการบริหารจัดการความมั่นคงปลอดภัยของเครือข่าย (แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกรมส่งเสริมคุณภาพสิ่งแวดล้อม)

3.7 การเตรียมความพร้อม แผนปฏิบัติการณเกิดไฟไหม้/การทดสอบแผนปฏิบัติการณเพลิงไหม้ ห้อง Server

เจ้าหน้าที่ศูนย์สารสนเทศสิ่งแวดล้อม ได้เข้าร่วมฝึกอบรมหลักสูตรป้องกันและระงับอัคคีภัยประจำปีของหน่วยงาน เพื่อให้เจ้าหน้าที่ที่ปฏิบัติงานภายในอาคารมีความรู้ ความเข้าใจเกี่ยวกับความปลอดภัยในอาคาร พร้อมรับสถานการณ์ฉุกเฉินกรณีเกิดเหตุเพลิงไหม้ โดยในกรณีเกิดเหตุไฟไหม้ห้อง Server ให้ปฏิบัติดังนี้

- 1) เมื่อได้รับแจ้งเหตุไฟไหม้ ในกรณีปฏิบัติงานอยู่ในห้อง Server ควรรีบออกจากห้อง Server และลงจากอาคารอย่างเป็นระเบียบโดยเร็วที่สุด และไม่ควรกลับเข้าไปในอาคารอีก
- 2) ในกรณีอพยพออกจากห้อง Server ควรใช้มือสัมผัสบริเวณผนังหรืออั้งไถ่ๆ ประตู ถ้ามีความร้อนสูง แสดงว่าเกิดเพลิงไหม้บริเวณไถ่ๆ
- 3) หนีไฟลงด้านล่างของอาคาร โดยใช้บันไดหนีไฟด้านนอกอาคาร เนื่องจากลักษณะบันไดภายในอาคารเป็นเหมือนช่อง โพรง ที่เสริมให้เปลวไฟพุ่งขึ้น และลุกลามอย่างรวดเร็ว แต่ถ้าลงทางบันไดไม่ได้ ให้ลงทางหน้าต่าง โดยใช้เชือก หรือผ้ายาวผูกโรยตัวลงมา ส่วนการกระโดดลงจากอาคาร ควรมีเบาะหรือฟูกที่นอนรองรับ
- 4) ห้ามใช้ลิฟต์ เพราะขณะเกิดเพลิงไหม้ ไฟฟ้าจะดับ ทำให้ลิฟต์ค้าง จะทำให้ด้านในของตัวลิฟต์ไม่มีอากาศ
- 5) หากเส้นทางหนีไฟเต็มไปด้วยกลุ่มควันให้ใช้ผ้าชุบน้ำมาคลุมตัว และปิดจมูกป้องกันการสำลักควันแล้วหมอบคลานเนื่องจากอากาศบริสุทธิ์จะอยู่ด้านล่าง (เหนือพื้น)
- 6) ห้ามหนีไฟเข้าไปหลบในห้องต่างๆ ที่เป็นจุดอับภายในอาคาร เช่น ห้องน้ำ ที่แม้ในช่วงแรกจะปลอดภัย แต่เมื่อไฟลุกลาม น้ำที่อยู่ในห้องอาจไม่เพียงพอสำหรับดับไฟ และความร้อนของไฟจะส่งผลให้น้ำมีความร้อนสูงขึ้นจนสามารถวกให้เสียชีวิตได้ สิ่งสำคัญที่สุดของการหนีรอดจากเหตุอัคคีภัย คือ การมีสติเป็นอันดับแรก เพราะจะทำให้เจ้าหน้าที่กรมฯ สามารถหนีเอาตัวรอด และช่วยเหลือผู้อื่นได้อย่างปลอดภัย ซึ่งกรมฯ อยู่ในเขตพื้นที่ของสถานีดับเพลิงดุสิต 41/11 ถนนเศรษฐศิริ แขวงถนนนครไชยศรี เขตดุสิต กรุงเทพมหานคร 10300

การทดสอบแผนปฏิบัติการณเพลิงไหม้ ห้อง Server

- 1) หลังได้ยื่นกริ่งสัญญาเพลิงไหม้ดั่งขึ้น รับผิดชอบที่มาของกริ่งสัญญาณ
- 2) เจ้าหน้าที่รีบออกจากห้อง Sever ตามผู้นำถ้อธงไป
- 3) เจ้าหน้าที่ทุกคนรีบวิ่งไปทางบันไดหนีไฟและลงบันไดโดยเร็ว
- 4) ผู้นำตรวจสอบอีกครั้งว่าไม่มีผู้ตกค้าง และลงบันไดเป็นคนสุดท้าย เมื่อทุกลงมารวมตัวกันบริเวณชั้นล่างของอาคาร เริ่มทำการตรวจนับเจ้าหน้าที่แต่ละกอง หลังตรวจนับเจ้าหน้าที่และแจ้งจำนวนเรียบร้อยเป็นอันเสร็จขั้นตอนการซ้อมหนีไฟ

4. การกำหนดหน้าที่และผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน จัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบ ดังนี้

4.1 ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้คำแนะนำ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

อธิบดีกรมส่งเสริมคุณภาพสิ่งแวดล้อม

รองอธิบดีกรมส่งเสริมคุณภาพสิ่งแวดล้อม

ผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อม

ผู้อำนวยการศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม

4.2 ระดับปฏิบัติ เทคโนโลยีสารสนเทศและเครือข่าย อาคารกรมส่งเสริมคุณภาพสิ่งแวดล้อม

เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงาน รับผิดชอบการปฏิบัติงาน การบริหารจัดการศึกษา ทบสวน วางแผน ติดตาม และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้

ทีมกู้คืนระบบ ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนระบบต่างๆ ให้สามารถกลับมาใช้งานได้ตามปกติ

นายธนาพันธ์ สุภสอาด เบอร์โทรศัพท์ 081-7014843

นายวิทยา ขำศิริ เบอร์โทรศัพท์ 089-7803040

นายโชคดี มั่นคง เบอร์โทรศัพท์ 082-4214093

นางสาวไพลิน พันธุ์แน่น เบอร์โทรศัพท์ 089-6823335

ทีมกู้คืนเครือข่าย ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนให้เครือข่ายกลับมาใช้งานได้ตามปกติ

นายธนาพันธ์ สุภสอาด เบอร์โทรศัพท์ 081-7014843

นายอรุณ ทรัพย์ประเสริฐ เบอร์โทรศัพท์ 089-4861446

นางสาวอรอุมา กลางประพันธ์ เบอร์โทรศัพท์ 086-3588256

ทีมกู้คืนระบบปฏิบัติการ ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งานได้ตามปกติ

นายธนาพันธ์ สุภสอาด เบอร์โทรศัพท์ 081-7014843

นายอภิศักดิ์ วัฒนพงษ์ เบอร์โทรศัพท์ 086-3726808

นายอรุณ ทรัพย์ประเสริฐ เบอร์โทรศัพท์ 089-4861446

นางวรรณภา ตันติวิศาลเกษตร เบอร์โทรศัพท์ 089-6395939

ทีมแก้ไขกรณีฉุกเฉินของระบบ ทำหน้าที่ค้นหาสาเหตุและวิธีอุดช่องโหว่ในระบบเครือข่าย และแก้ไขให้ระบบสามารถใช้งานได้เป็นปกติ

นายธนาพันธ์ สุภสอาด เบอร์โทรศัพท์ 081-7014843

นายอภิศักดิ์ วัฒนพงษ์ เบอร์โทรศัพท์ 086-3726808

นายโชคดี มั่นคง เบอร์โทรศัพท์ 082-4214093

นางสาวไพลิน พันธุ์แน่น เบอร์โทรศัพท์ 089-6823335

ทีมประเมินความเสียหาย ทำหน้าที่ประเมินความเสียหายและให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

นายธนาพันธ์ สุภสอาด เบอร์โทรศัพท์ 081-7014843

นายอรุณ ทรัพย์ประเสริฐ เบอร์โทรศัพท์ 089-4861446

นางสาวหฤทัย ศักดิ์สีลากุล เบอร์โทรศัพท์ 095-5959224

4.3 ระดับปฏิบัติ ด้านอาคารสถานที่ อาคารกรมส่งเสริมคุณภาพสิ่งแวดล้อม ทำหน้าที่ควบคุม
ประสานงาน แก้ไขปัญหาเบื้องต้น จัดเตรียมสถานที่สำหรับปฏิบัติงานสำรอง ระบบไฟฟ้า ระบบการสื่อสาร
ระบบปรับอากาศ ให้พร้อมใช้งานกรณีเกิดภัยพิบัติฉุกเฉิน และการจราจรต่างๆ

นายบัญชา พันธุ์ลี	เบอร์โทรศัพท์	096-8898012
นายชรินทร์ เดชโชติ	เบอร์โทรศัพท์	086-7658694
นายเกียรติศักดิ์ อ่อนศรี	เบอร์โทรศัพท์	090-2280601
นายอดุลวิทย์ จันทร์ศรี	เบอร์โทรศัพท์	083-9642496

ทีมแก้ไขกรณีเกิดไฟไหม้ (ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการแก้ไขปัญหา
เบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์สารสนเทศสิ่งแวดล้อมได้จัดหาไว้

นายธนาพันธ์ สุขสะอาด	เบอร์โทรศัพท์	081-7014843
นายอรุณ ทรัพย์ประเสริฐ	เบอร์โทรศัพท์	089-4861446
นายสยาม วงศ์ศรีธาตุ	เบอร์โทรศัพท์	083-9253352
นายเกรียงไกร ยงยศรุ่งเรือง	เบอร์โทรศัพท์	083-7070661

ทีมแก้ไขกรณีไฟฟ้าดับ ไฟกระชาก (ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการ
แก้ไขปัญหาเบื้องต้น จัดหาระบบป้องกันไม่ให้เกิดความเสียหายต่อระบบและอุปกรณ์เครือข่าย

นายธนาพันธ์ สุขสะอาด	เบอร์โทรศัพท์	081-7014843
นายบัญชา พันธุ์ลี	เบอร์โทรศัพท์	096-8898012
นายอรุณ ทรัพย์ประเสริฐ	เบอร์โทรศัพท์	089-4861446
นายเกียรติศักดิ์ อ่อนศรี	เบอร์โทรศัพท์	090-2280601
นายเกรียงไกร ยงยศรุ่งเรือง	เบอร์โทรศัพท์	083-7070661

ทีมแก้ไขกรณีแผ่นดินไหว ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อ
ผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

นายธนาพันธ์ สุขสะอาด	เบอร์โทรศัพท์	081-7014843
นายธนภฤต จันทร์ขำ	เบอร์โทรศัพท์	099-4050599
นายภูเนศ ส้ารวมสุข	เบอร์โทรศัพท์	062-3419555
นางสาวหฤทัย ศักดิ์ลีลากุล	เบอร์โทรศัพท์	095-5959224

ทีมแก้ไขกรณีเกิดการจราจร ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อ
ผู้ควบคุมและผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

นายชรินทร์ เดชโชติ	เบอร์โทรศัพท์	086-7658694
นางจิรพรรณ เมืองปลื้ม	เบอร์โทรศัพท์	082-2993396
นายอดุลวิทย์ จันทร์ศรี	เบอร์โทรศัพท์	083-9642496
นายสยาม วงศ์ศรีธาตุ	เบอร์โทรศัพท์	083-9253352

ทีมแก้ไขกรณีเกิดโรคระบาด ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบข้อมูล
ติดต่อสื่อสาร จัดหาเครื่องมือ วัสดุ อุปกรณ์ ระบบการติดต่อสื่อสารออนไลน์ และระบบเทคโนโลยีสารสนเทศ
เพื่อสนับสนุนการปฏิบัติงานให้แก่เจ้าหน้าที่ รายงานผลต่อผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

นายธนาพันธ์ สุขสอาด	เบอร์โทรศัพท์	081-7014843
นายชรินทร์ เดชโชติ	เบอร์โทรศัพท์	086-7658694
นายปวิช สนั่นเมือง	เบอร์โทรศัพท์	081-3365036
นายชัยยุทธ์ มณีงาม	เบอร์โทรศัพท์	081-2532983
นายเกียรติศักดิ์ อ่อนศรี	เบอร์โทรศัพท์	090-2280601
นางสาวอรอุมา กลางประพันธ์	เบอร์โทรศัพท์	086-3588256
นายภูเนศ ส้ารวมสุข	เบอร์โทรศัพท์	062-3419555

4.4 ระดับปฏิบัติ เทคโนโลยีสารสนเทศและเครือข่าย อาคารศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม
เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงาน รับผิดชอบการปฏิบัติงาน การบริหารจัดการศึกษา ทบทวน วางแผน ติดตาม และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ โดยแบ่งทีมงาน ดังนี้

ทีมกู้คืนระบบ ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนระบบต่างๆ ให้สามารถกลับมาใช้งานได้ตามปกติ

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นางกัลยา กาญจนนัชฐิติ	เบอร์โทรศัพท์	086-9855231
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมกู้คืนเครือข่าย ทำหน้าที่บริหารจัดการ ประสานงานการกู้คืนให้เครือข่ายกลับมาใช้งานได้ตามปกติ

นางจินดารัตน์ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นางกัลยา กาญจนนัชฐิติ	เบอร์โทรศัพท์	086-9855231
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมกู้คืนระบบปฏิบัติการ ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งานได้ตามปกติ

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นางกัลยา กาญจนนัชฐิติ	เบอร์โทรศัพท์	086-9855231
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมแก้ไขกรณีถูกแทรกแซงระบบ ทำหน้าที่ค้นหาสาเหตุและวิธีอุดช่องโหว่ในระบบเครือข่าย และแก้ไขให้ระบบสามารถใช้งานได้เป็นปกติ

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นางกัลยา กาญจนนัชฐิติ	เบอร์โทรศัพท์	086-9855231
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมประเมินความเสียหาย ทำหน้าที่ประเมินความเสียหายและให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นางกัลยา กาญจนนัชฐิติ	เบอร์โทรศัพท์	086-9855231
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

4.5 ระดับปฏิบัติด้านอาคารสถานที่ อาคารศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม ทำหน้าที่ควบคุม ประสานงาน แก้ไขปัญหาเบื้องต้น จัดเตรียมสถานที่สำหรับปฏิบัติงานสำรอง ระบบไฟฟ้า ระบบการสื่อสาร ระบบปรับอากาศ ให้พร้อมใช้งานกรณีเกิดภัยพิบัติฉุกเฉิน และการจลาจลต่างๆ

นางจินดารัตน์ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5905553
นายซัชชัย โอมแก้ว	เบอร์โทรศัพท์	084-1223143
นายโอภาส งามพริ้ง	เบอร์โทรศัพท์	089-5194602
นายอุดร แสนเกษม	เบอร์โทรศัพท์	081-2537311
นายไพโรจน์ ไทยลี	เบอร์โทรศัพท์	081-3429010
นายวุฒิชัย เปรินทร์	เบอร์โทรศัพท์	097-2285718

ทีมแก้ไขกรณีเกิดไฟไหม้ (ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการแก้ไข ปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง โดยใช้อุปกรณ์ที่ศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม ได้จัดหาไว้

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นายชัชชัย โอมแก้ว	เบอร์โทรศัพท์	084-1223143
นายไพโรจน์ ไทยลี	เบอร์โทรศัพท์	081-3429010
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมแก้ไขกรณีไฟฟ้าดับ ไฟกระชาก (ห้องควบคุมระบบ) ทำหน้าที่แจ้งเหตุ ประสานงาน ดำเนินการ แก้ไขปัญหาเบื้องต้น จัดหาระบบป้องกันไม่ให้เกิดความเสียหายต่อระบบและอุปกรณ์เครือข่าย

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นายโอภาส งามพริ้ง	เบอร์โทรศัพท์	089-5194602
นายอุดร แสนเกษม	เบอร์โทรศัพท์	081-2537311
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

ทีมแก้ไขกรณีแผ่นดินไหว ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผลต่อ ผู้ควบคุมและผู้อำนวยการศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อมทราบ

นายรัฐ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5954000
นายวุฒิชัย เปรินทร์	เบอร์โทรศัพท์	097-2285718
นายไพโรจน์ ไทยลี	เบอร์โทรศัพท์	081-3429010
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

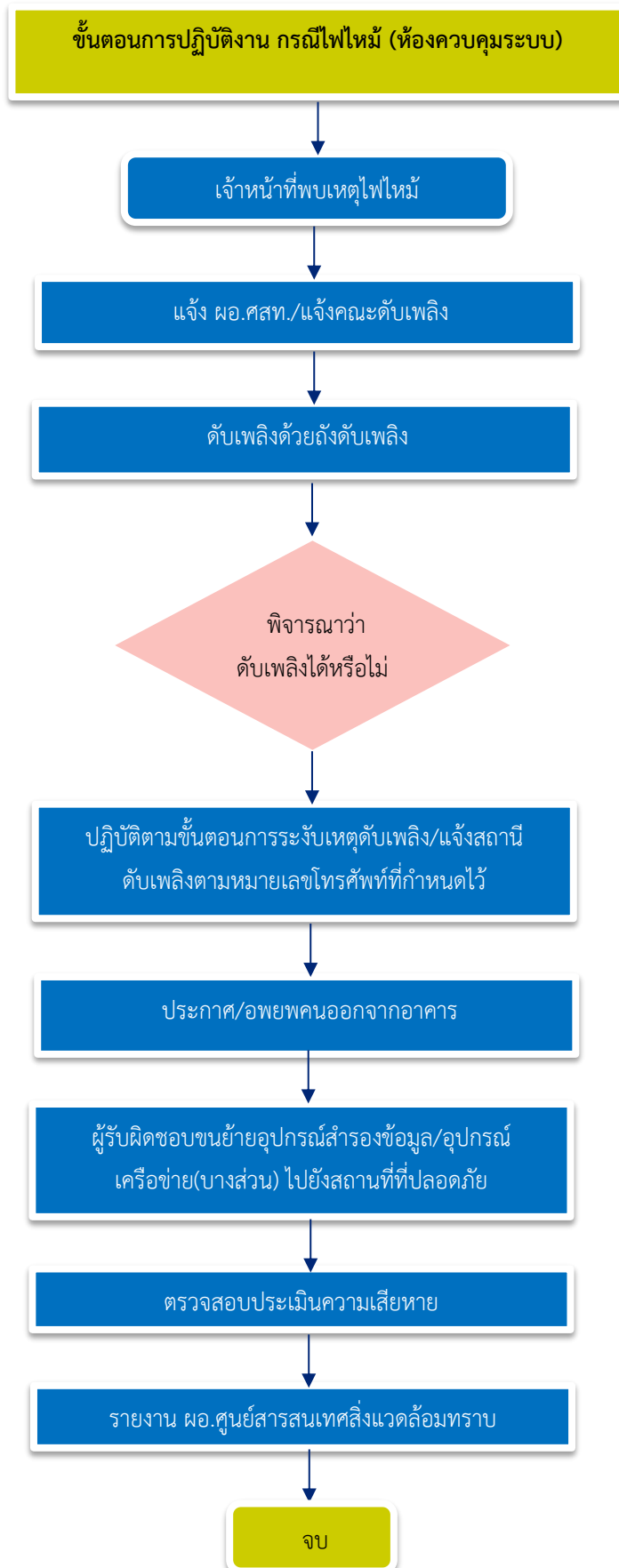
ทีมแก้ไขกรณีเกิดการจลาจล ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบ รายงานผล ต่อผู้ควบคุมและผู้อำนวยการศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อมทราบ

นางจินดารัตน์ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5905553
นายชัชชัย โอมแก้ว	เบอร์โทรศัพท์	084-1223143
นายโอภาส งามพริ้ง	เบอร์โทรศัพท์	089-5194602
นายอุดร แสนเกษม	เบอร์โทรศัพท์	081-2537311
นายไพโรจน์ ไทยลี	เบอร์โทรศัพท์	081-3429010
นายวุฒิชัย เปรินทร์	เบอร์โทรศัพท์	097-2285718

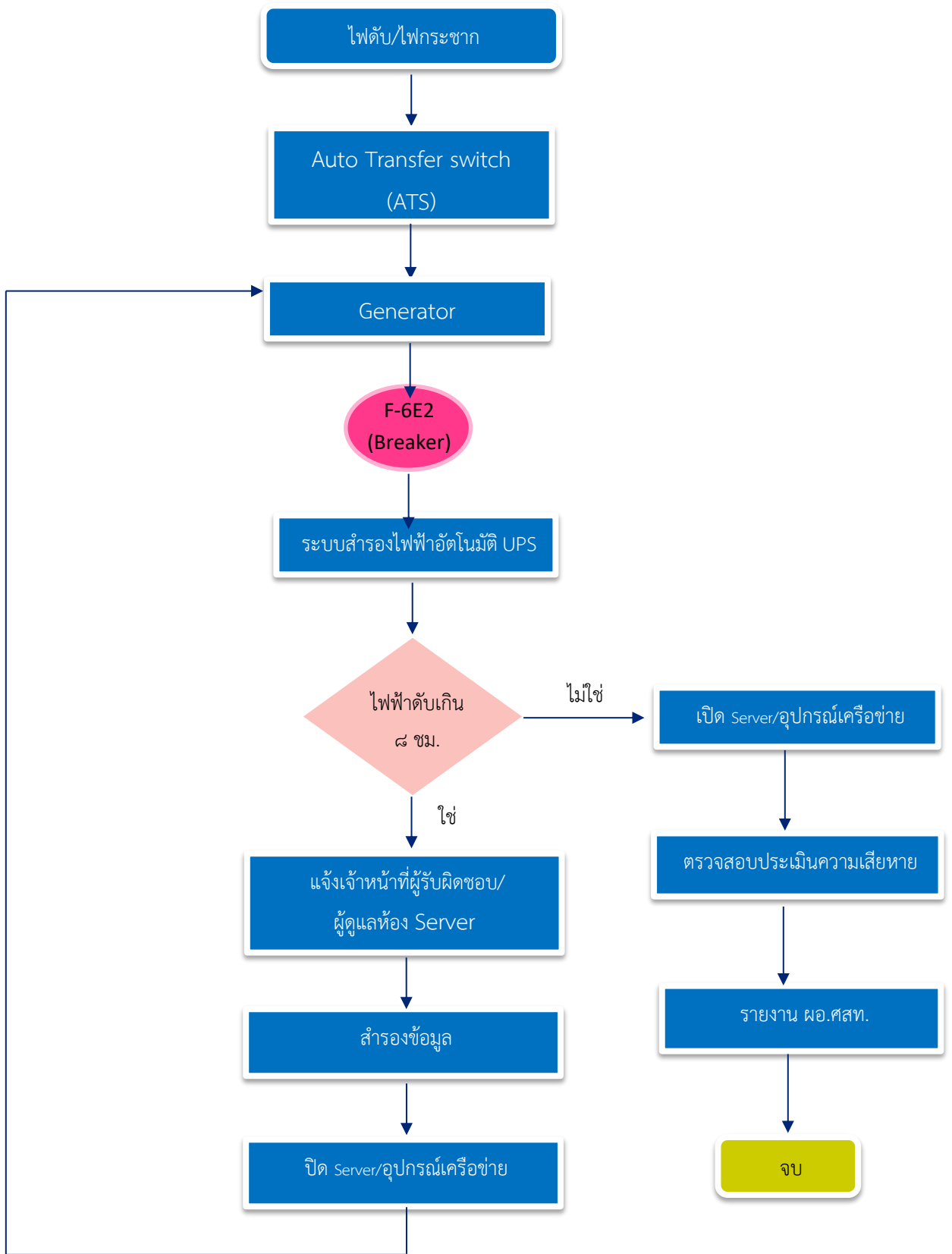
ทีมแก้ไขกรณีเกิดโรคระบาด ทำหน้าที่แจ้งเหตุ ประสานงานตามคำสั่งการ ตรวจสอบข้อมูล ติดต่อสื่อสาร จัดหาเครื่องมือ วัสดุ อุปกรณ์ ระบบการติดต่อสื่อสารออนไลน์ และระบบเทคโนโลยีสารสนเทศเพื่อสนับสนุน การปฏิบัติงานให้แก่เจ้าหน้าที่ รายงานผลต่อผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ

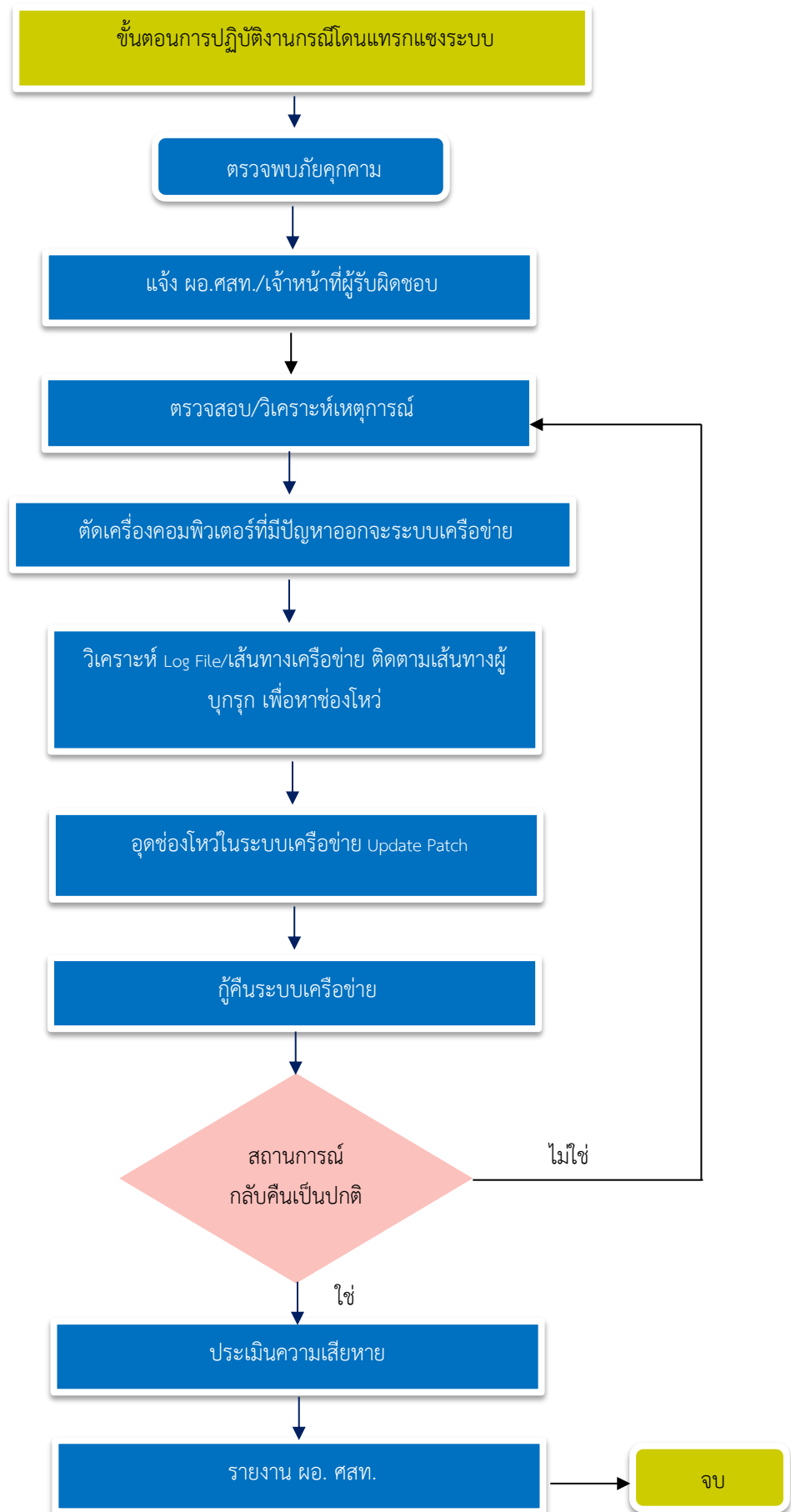
นางจินดารัตน์ เรืองโชติวิทย์	เบอร์โทรศัพท์	062-5905553
นางสาวอารีรัตน์ จากสกุล	เบอร์โทรศัพท์	089-6894061
นางสาวอุไร เกษมศรี	เบอร์โทรศัพท์	089-9875459
นางสาวเนาวรัตน์ วีระชน	เบอร์โทรศัพท์	089-6830967
นางสาวอาทิตย์ยา พามี	เบอร์โทรศัพท์	089-2349004
นางอามัสนา เอกคม	เบอร์โทรศัพท์	086-8706500
นางสาวพรรณทิพา พุ่มน้ำเย็น	เบอร์โทรศัพท์	089-9101778
นายบรรดิษฐ์ สารีบุญ	เบอร์โทรศัพท์	081-9653740

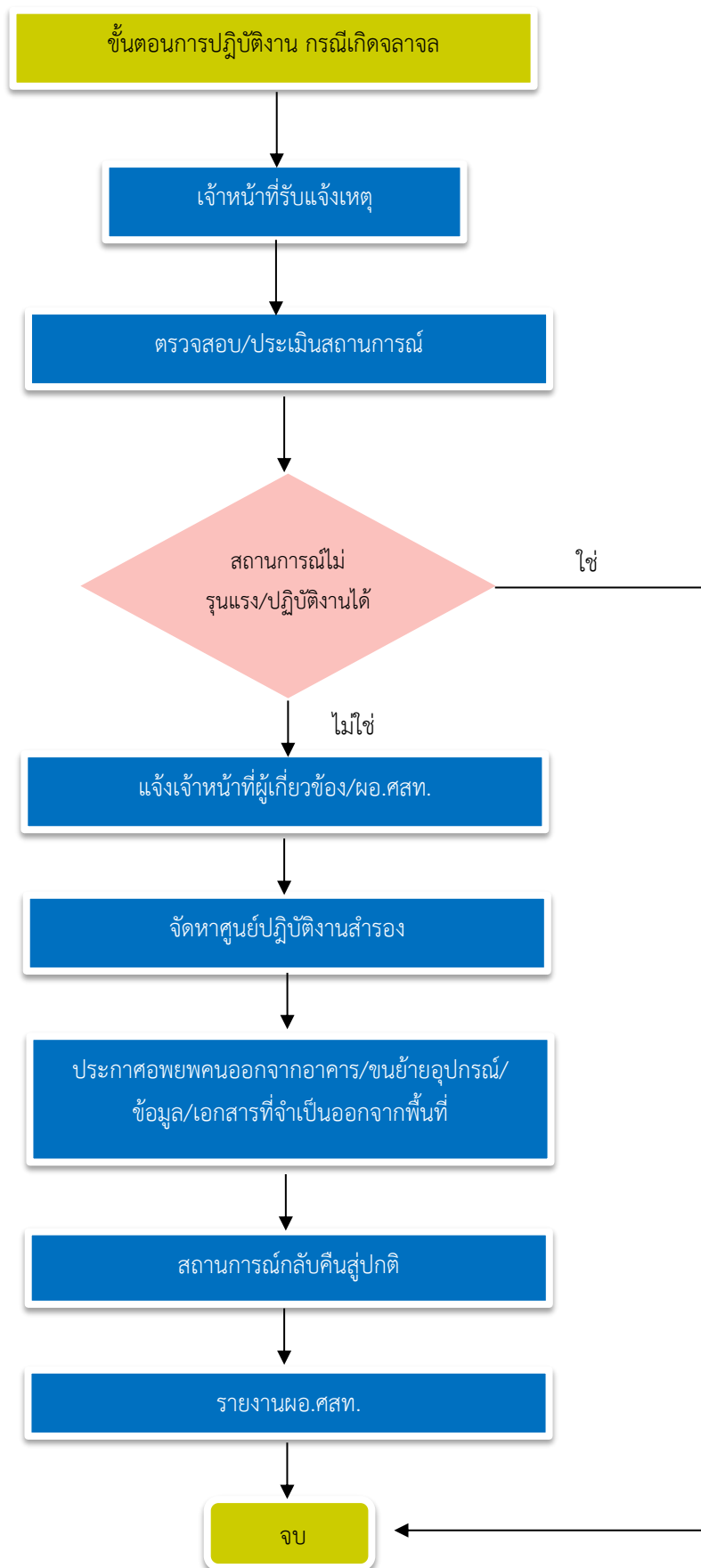
5. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ อาคารกรมส่งเสริมคุณภาพสิ่งแวดล้อม

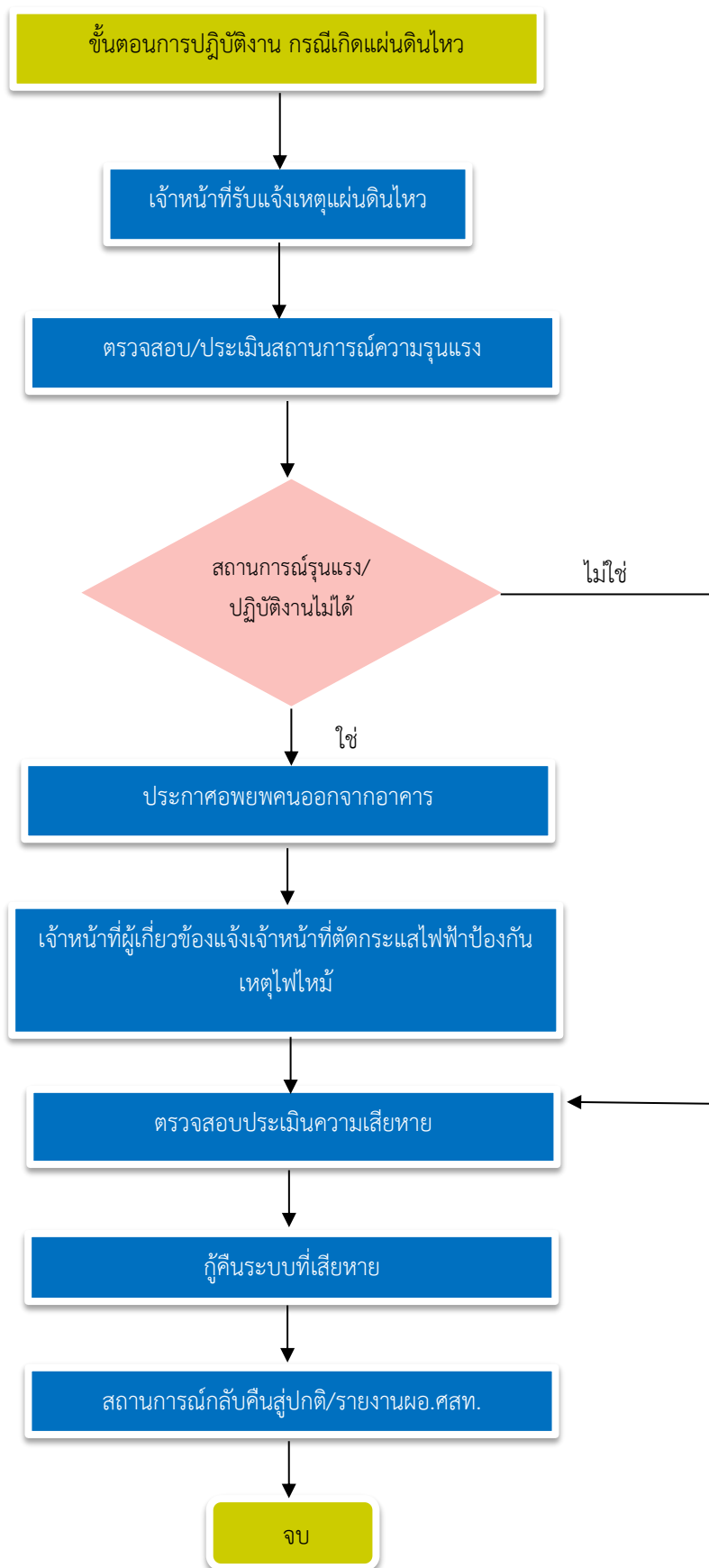


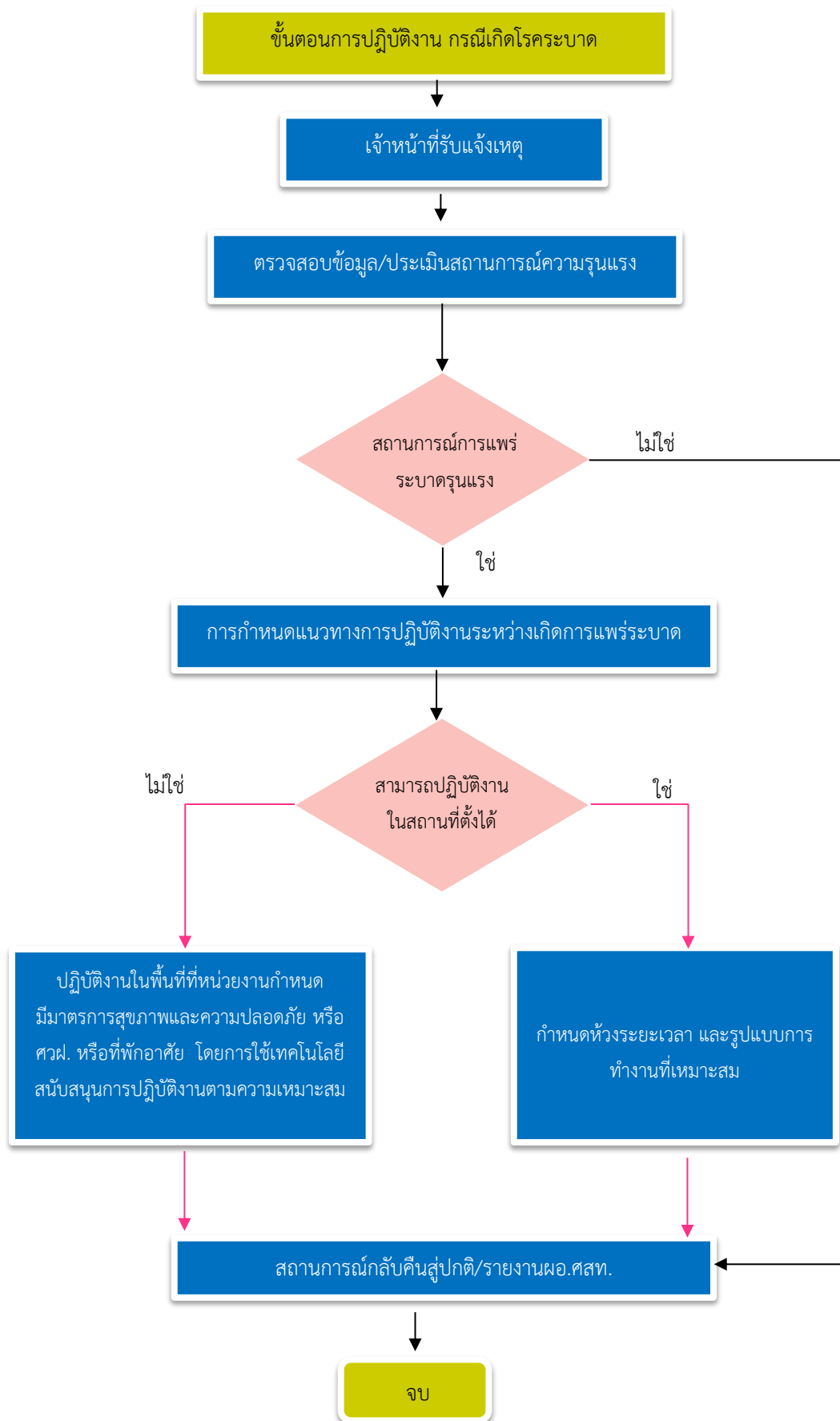
ขั้นตอนการปฏิบัติงาน กรณีไฟฟ้าดับ /ไฟกระชาก/หม้อไพระเบิด



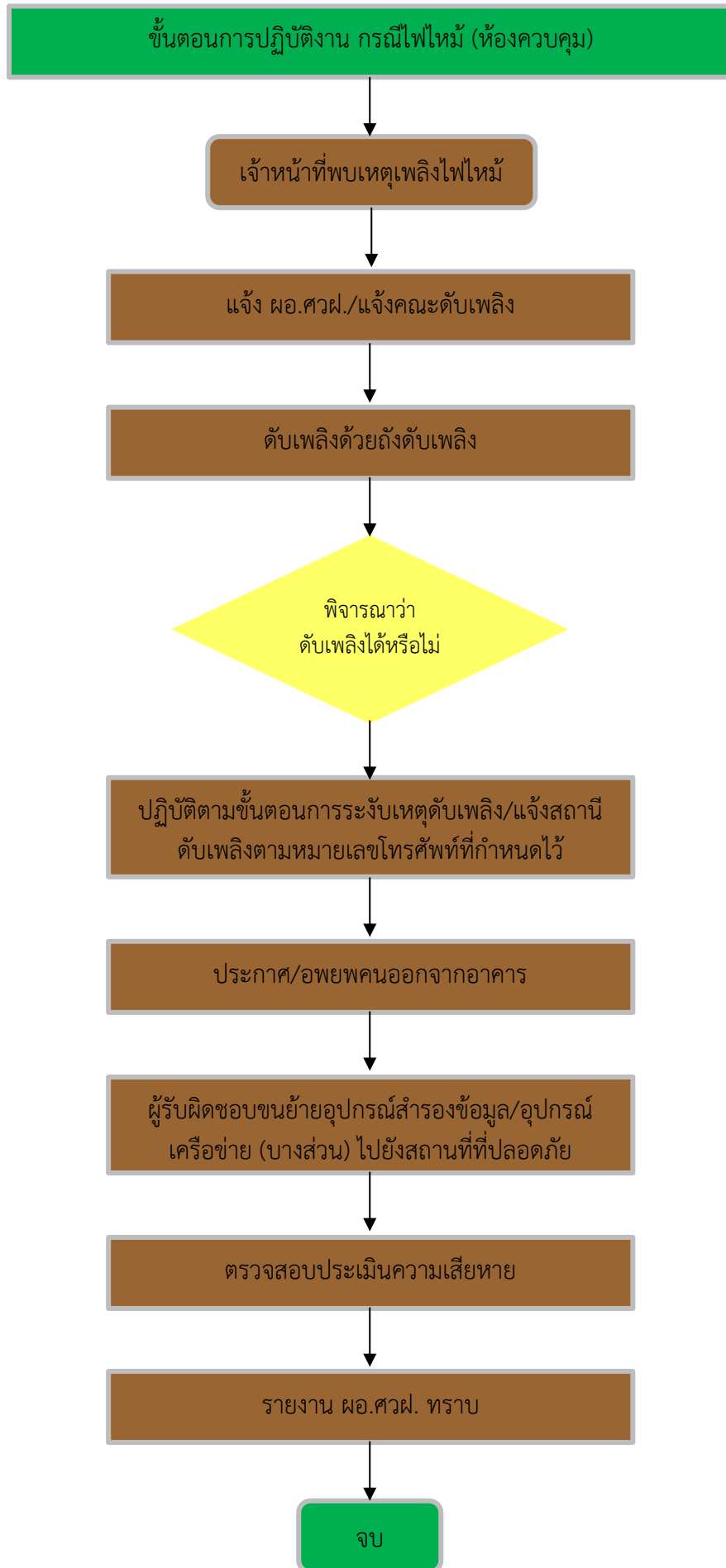


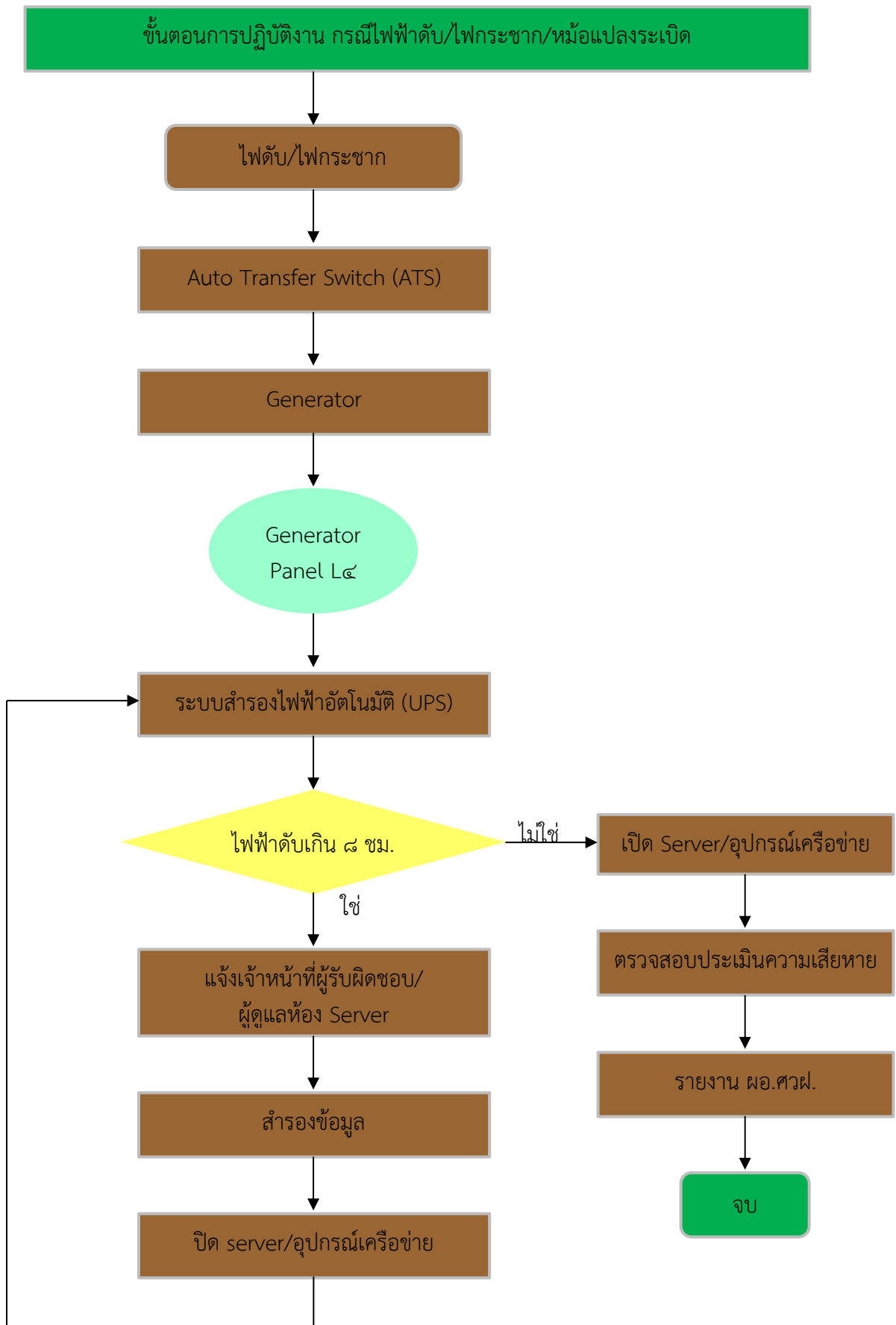


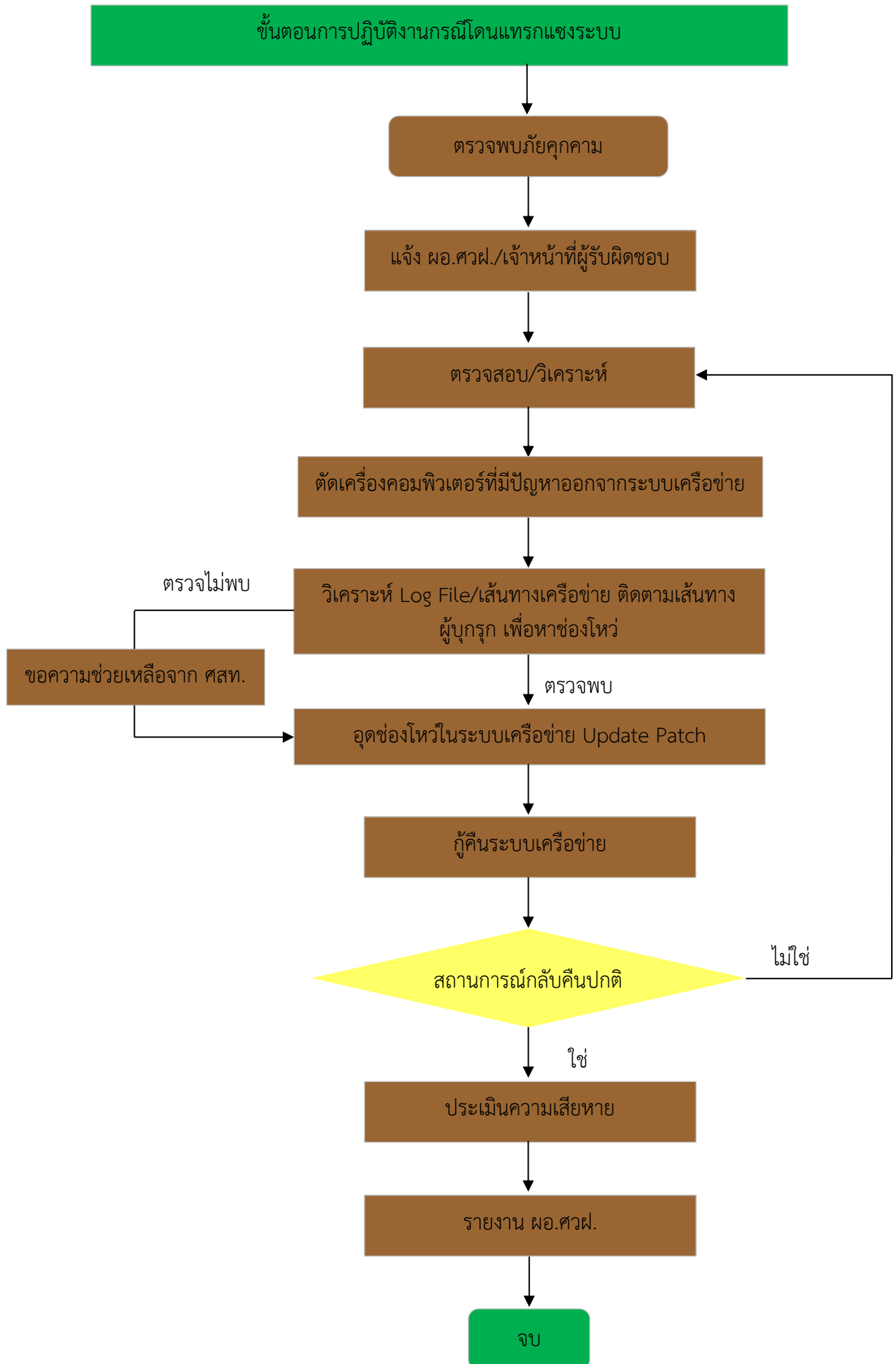


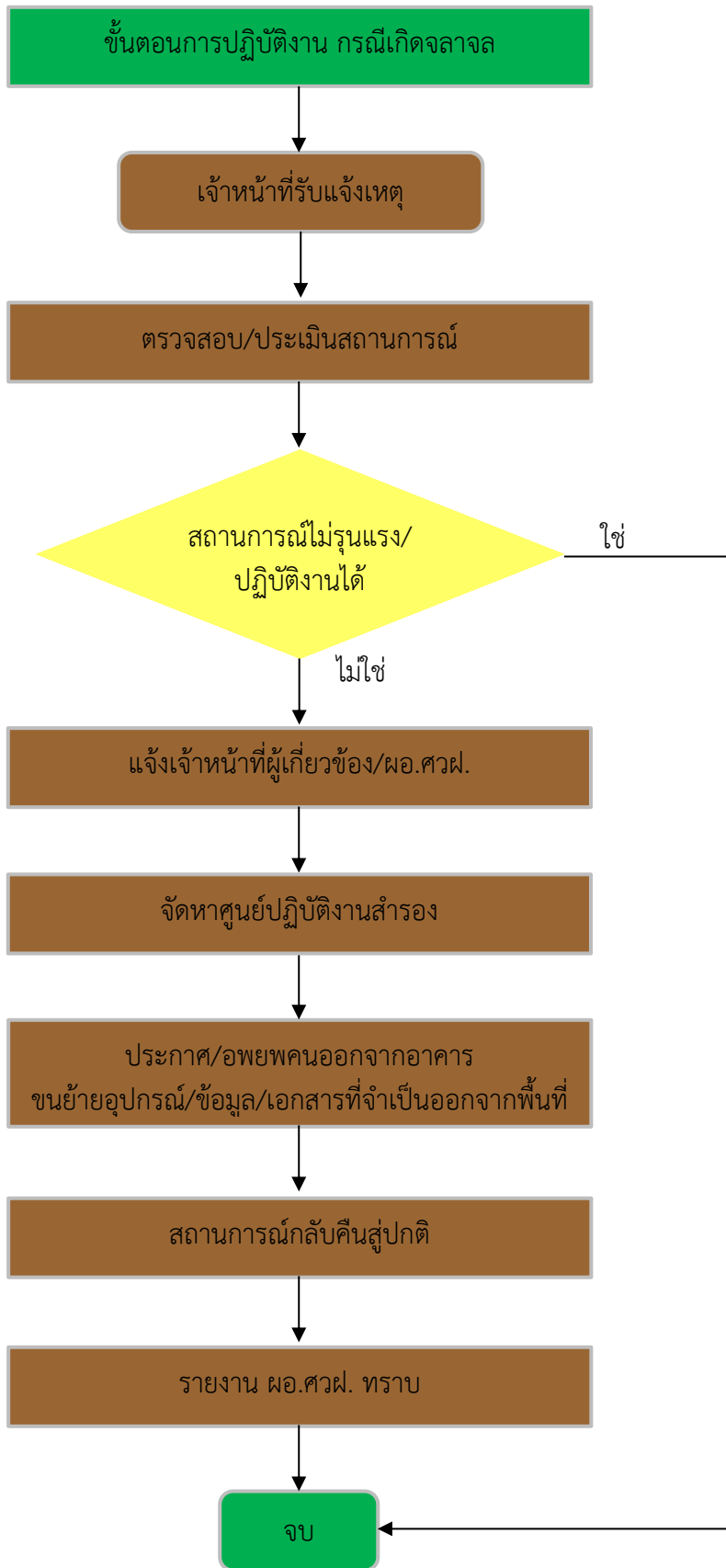


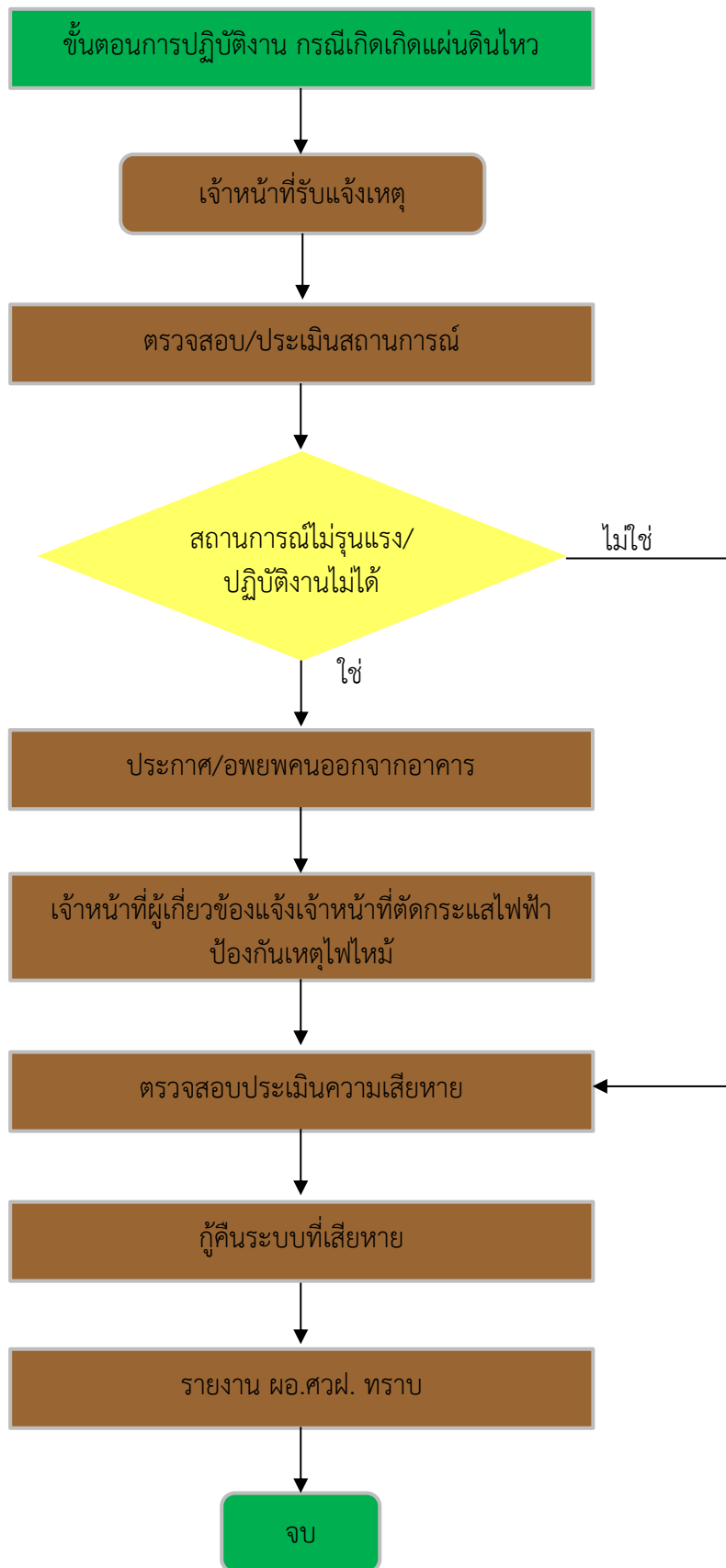
6. ผังกระบวนการแก้ไขปัญหาและสถานการณ์ภัยพิบัติ อาคารศูนย์วิจัยและฝึกอบรมด้านสิ่งแวดล้อม

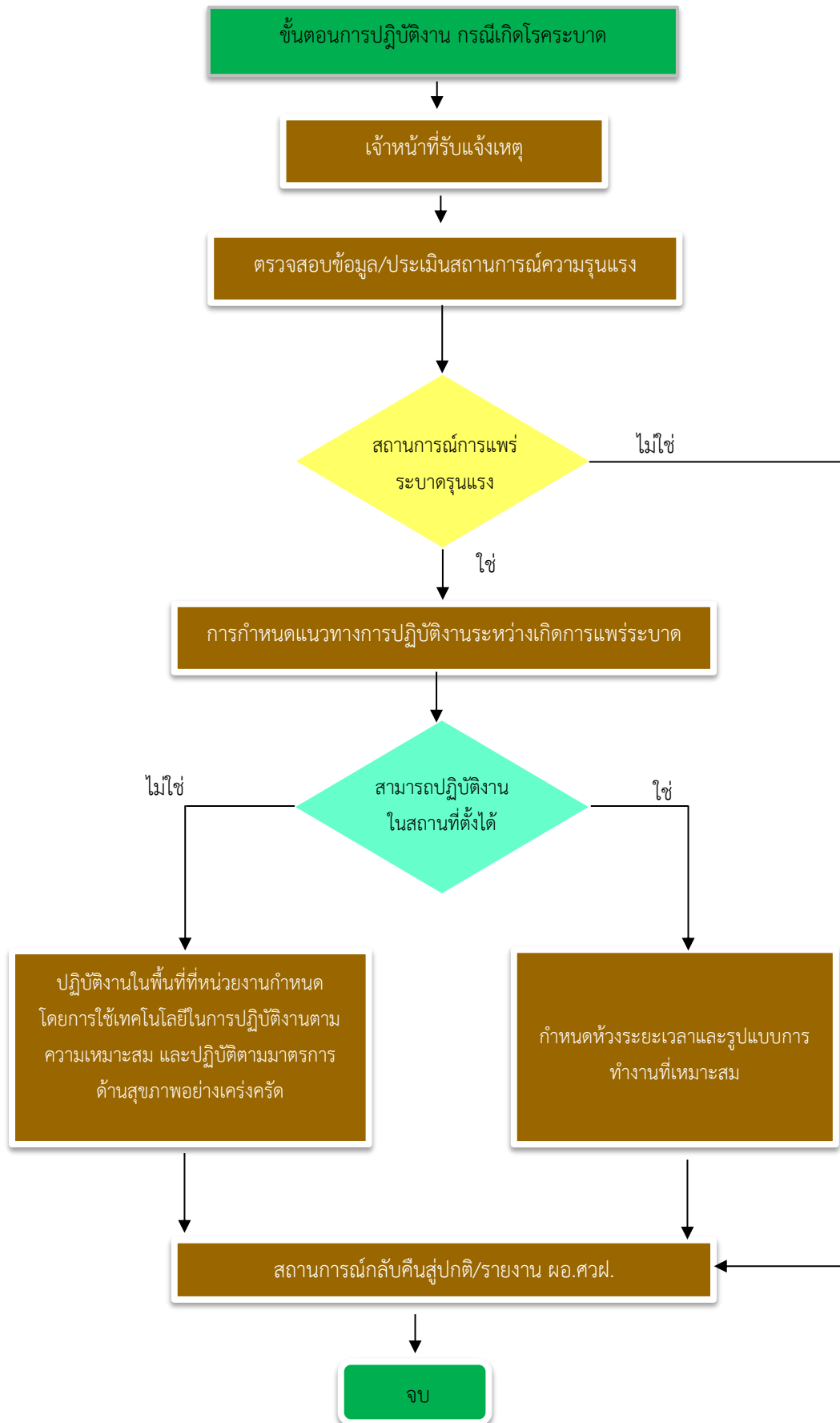










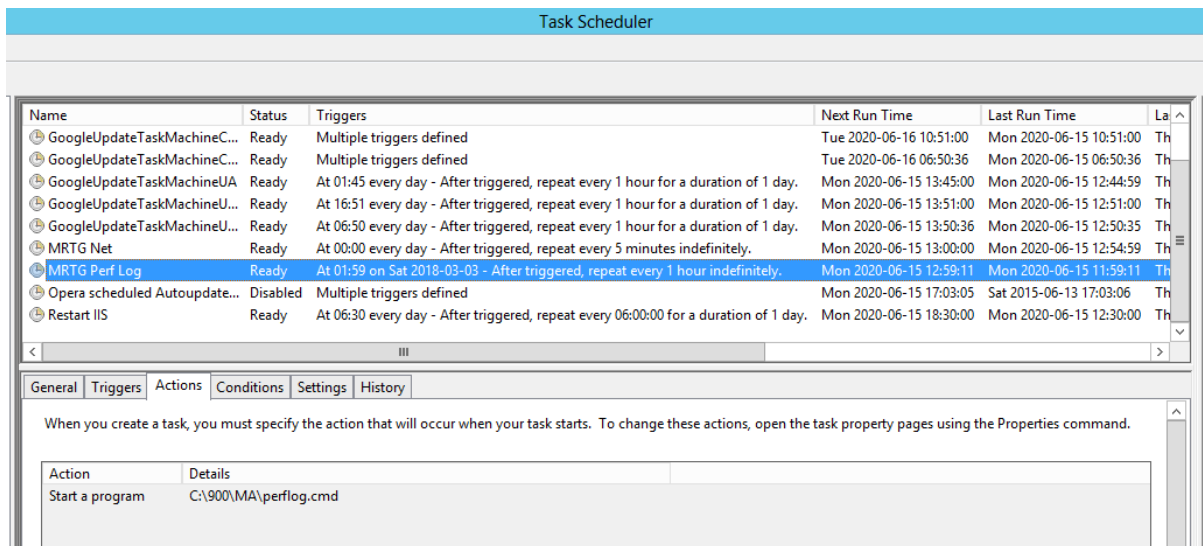


7. การตรวจสอบการทำงานของเครื่องแม่ข่าย (Server Monitoring System)

การตรวจสอบการทำงานของเครื่องแม่ข่าย (Server Monitoring System) ผ่านทางโปรโตคอล SNMP เพื่อบันทึกการจราจรการใช้งานทางระบบเครือข่าย และบันทึกการเข้าใช้งานของเว็บเซิร์ฟเวอร์ (Web Server Log Files) โดยใช้ซอฟต์แวร์ MRTG และ AWSTATS เพื่อตรวจสอบการใช้งานจราจรทางเครือข่าย การใช้งานเว็บไซต์และทรัพยากรของระบบ โดยมีรายละเอียด ดังนี้

7.1 การเข้าดูจราจรของเครือข่ายและการใช้งานทรัพยากรของเครื่อง

ผู้ดูแลสามารถเข้าดูปริมาณการใช้งานเครือข่ายและทรัพยากร ได้ผ่านทางเว็บไซต์ <http://datacenter.deqp.go.th/mrtg/index.html> โดยระบบจะประมวลผลและบันทึกข้อมูลทุก ๆ 5 นาที โดยประมวลผลจาก Log ข้อมูลที่มีการตั้งเวลาให้บันทึกข้อมูลไว้ทุก ๆ 1 ชม. ดังภาพที่ 1 ด้วยชุดสคริปต์ในโฟลเดอร์ C:\900\MA\mrtg ดังภาพที่ 2



ภาพที่ 1 การตั้งเวลาทุก 1 ชม. ในการเปลี่ยนชื่อไฟล์สำหรับการเก็บข้อมูลเพื่อบันทึกการใช้งานทรัพยากร

สคริปต์การเปลี่ยนชื่อไฟล์ทุก 1 ชม. C:\900\MA\perflog.cmd

```
@echo off

logman stop MRTG

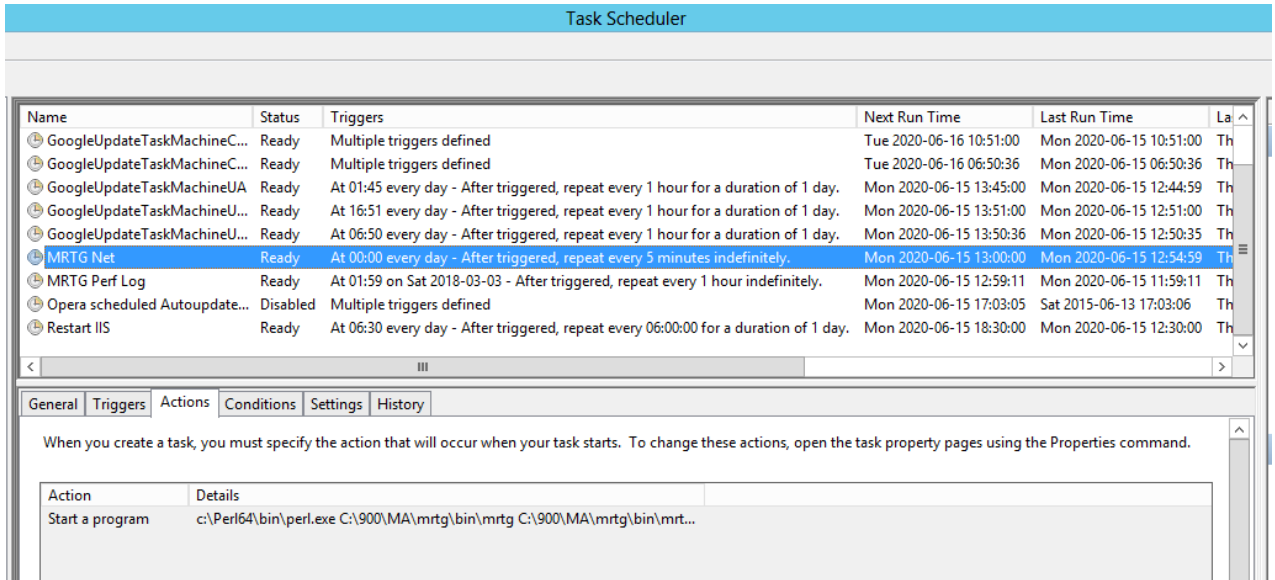
set a=C:\PerfLogs\Admin\MRTG\resource-%date:~4,4%%date:~9,2%.csv

set b=resource-%date:~4%_%time:~0,2%-time:~3,2%-time:~6,2%.csv

ren %a% %b%

if exist %a% del %a%

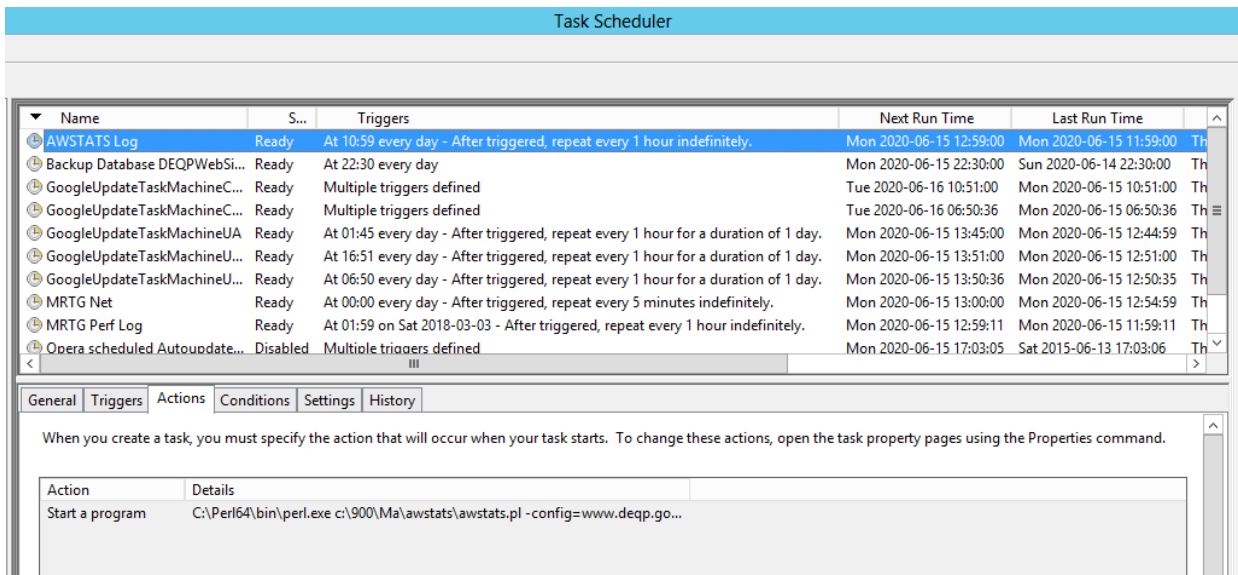
logman start MRTG
```



ภาพที่ 2 การตั้งเวลาทุก 5 นาทีในการสร้างข้อมูลกราฟจราจรเครือข่ายและทรัพยากรของเครื่อง

7.2 การเข้าดูการเข้าถึงระบบของผู้ใช้งาน

ผู้ดูแลสามารถเข้าดูประวัติการใช้งานหน้าระบบต่าง ๆ ของผู้ใช้งานแบบออนไลน์ ได้ผ่านทางเว็บไซต์ <http://datacenter.deqp.go.th/stats/awstats.pl?config=www.deqp.go.th> โดยระบบจะประมวลผล Log การเข้าใช้งาน ด้วยชุดสคริปต์ในโฟลเดอร์ C:\900\MA\awstats ทุก ๆ 1 ชม. ดังภาพที่ 3



ภาพที่ 3 การตั้งเวลาทุก 1 ชม. ในการประมวลผลข้อมูล Log ของผู้เข้าใช้งาน

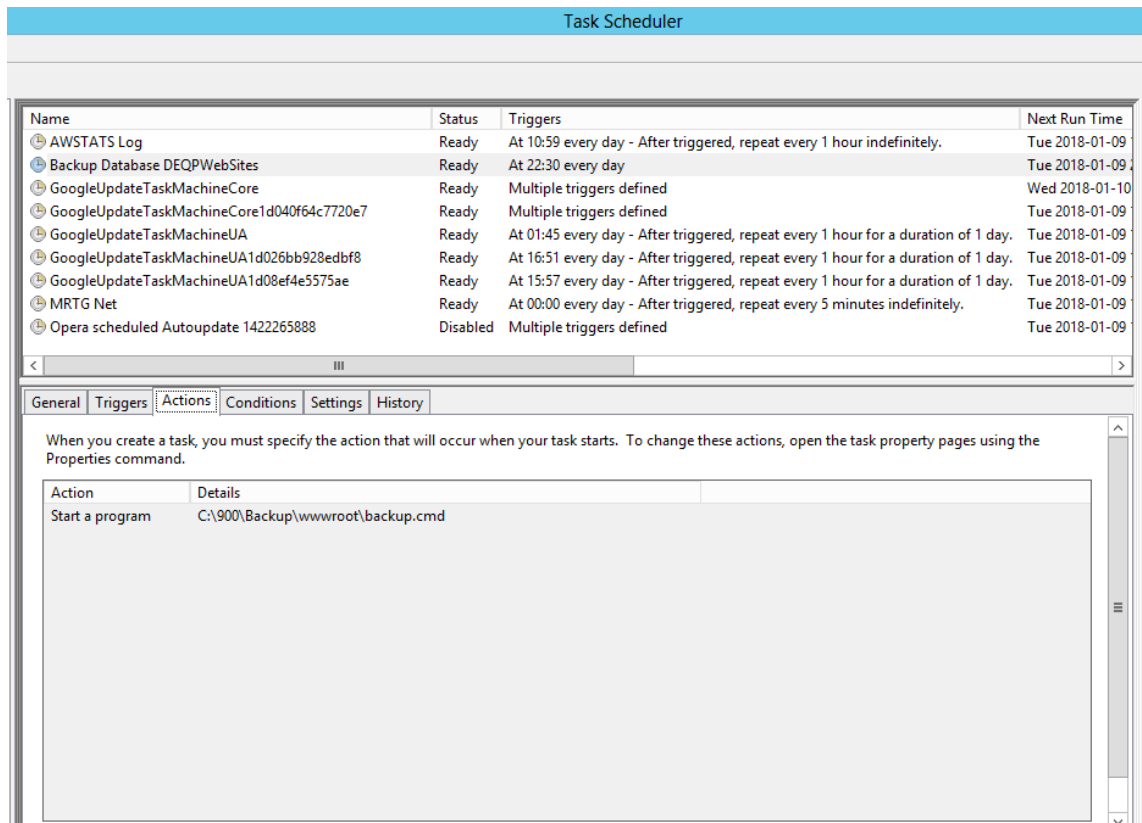
8. แผนการกู้คืนข้อมูล

กรณีเกิดเหตุฉุกเฉินทำให้เครื่องแม่ข่ายเสียหายไม่อาจใช้งานต่อไปได้ จำเป็นต้องมีการสำรองข้อมูล (Backup) ข้อมูลในเครื่องแม่ข่ายไว้ โดยมีแผนปฏิบัติ ดังนี้

8.1 ทำการสำรองข้อมูลเครือข่าย (Configuration) เป็นประจำทุกเดือน

8.2 สำรองฐานข้อมูล

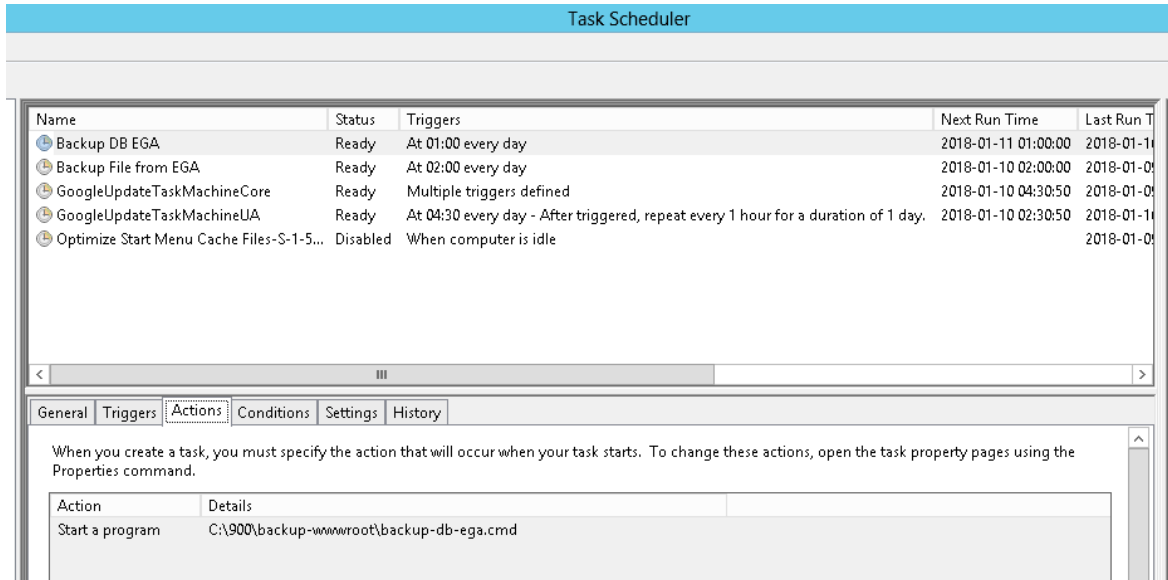
ดำเนินการเขียนสคริปต์สำรองข้อมูล (Full Backup) และบีบอัดไฟล์ฐานข้อมูลไว้เพื่อประหยัดพื้นที่และเวลาในการจัดเก็บรวมถึงการโอนถ่ายข้อมูล ดังภาพที่ 1 โดยจะสำรองข้อมูลไว้ทุก ๆ วัน เวลา 22:30 น.



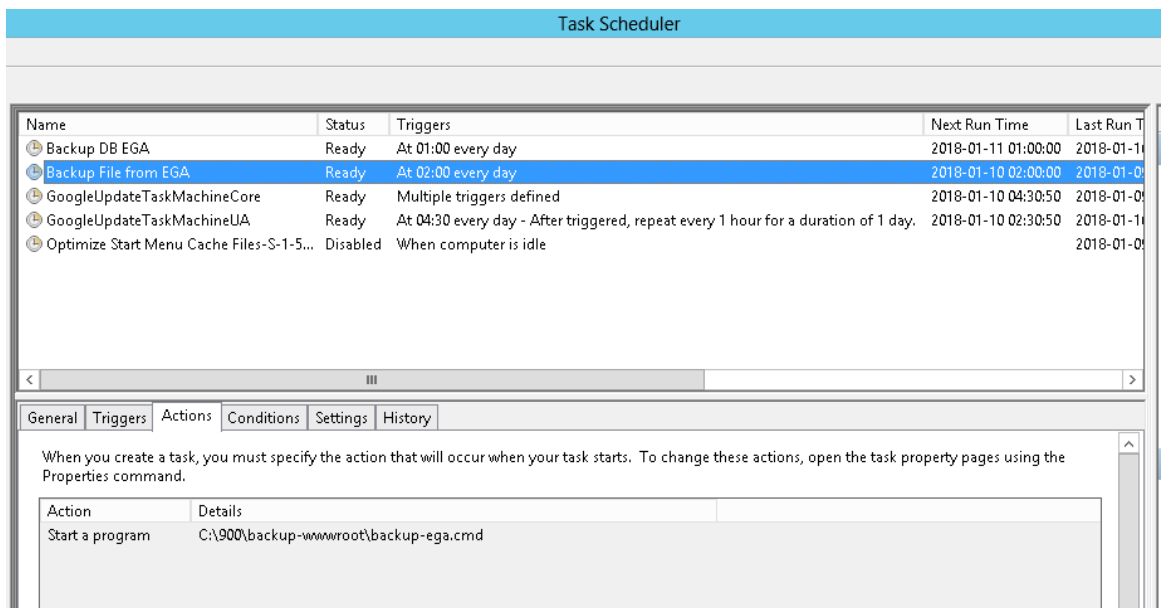
ภาพที่ 1 Task Schedule สำหรับสำรองฐานข้อมูล

8.3 สำรองข้อมูลเว็บไซต์

ติดตั้งและคอนฟิกพีอาร์ชอพท์แวร์ (FTP Server) เพื่อใช้สำหรับโอนถ่ายข้อมูลระหว่างเครื่องแม่ข่ายที่โครงการพัฒนาระบบคลาวด์กลางภาครัฐ (Government Data Center and Cloud service : GDCC) ภายใต้กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม และเครื่องแม่ข่ายที่สำนักงานกรมส่งเสริมคุณภาพสิ่งแวดล้อม โดยเครื่องแม่ข่ายที่ GDCC จะใช้เป็นเซิร์ฟเวอร์หลัก และส่วนเครื่องที่สำนักงานกรมส่งเสริมคุณภาพสิ่งแวดล้อมจะเป็นเซิร์ฟเวอร์สำรอง โดยที่เครื่องแม่ข่ายที่กรมฯ จะทำหน้าที่สำรองข้อมูลเฉพาะส่วนที่ใหม่กว่าหรือมีการเปลี่ยนแปลงจาก GDCC มาที่กรมทุกวัน เริ่มที่เวลา 01.00 น. โดยชุดสคริปต์จะสำรองทั้งข้อมูล Database และข้อมูลเนื้อหาเว็บ ดังภาพที่ 2 และ 3



ภาพที่ 2 ชุดสคริปต์ที่ใช้ในการดาวน์โหลดและนำกลับคืนฐานข้อมูล



ภาพที่ 3 ชุดสคริปต์สำหรับอัปเดตเนื้อหาข้อมูลเว็บให้ตรงกันระหว่างเครื่องที่ สพร. และ กรมฯ

9. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบเมื่อเกิดเหตุการณ์หรือภัยพิบัติฉุกเฉิน ให้ผู้อำนวยการศูนย์สารสนเทศสิ่งแวดล้อมทราบ เพื่อนำเสนอรายงานสรุปให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง เพื่อที่จะนำมาปรับปรุงพัฒนาแผนรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศให้มีประสิทธิภาพ สามารถนำมาใช้งานได้ทันที ในกรณีที่เกิดภัยพิบัติต่อไป

แผนรับมือสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศ (IT Contingency) ฉบับนี้ได้ผ่านการพิจารณาจากคณะทำงานบริหารและประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของกรมส่งเสริมคุณภาพสิ่งแวดล้อม เพื่อเตรียมความพร้อมและสร้างความรู้ความเข้าใจ ตลอดจนเป็นแนวทางในการดูแลรักษา ระบบเทคโนโลยีสารสนเทศต่อไป

(ลงชื่อ) 

(นายวรพล จันทร์งาม)

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกรม (DCIO)

ชื่อหน่วยงาน กรมส่งเสริมคุณภาพสิ่งแวดล้อม

๒๗ / ก.ม. / ๒๕๖๔