องค์การจัดการน้ำเสีย
WASTEWATER MANAGEMENT AUTHORITY

แผนบริหารความต่อเนื่องทางธุรกิจ

(Business Continuity Plan: BCP)

องค์การจัดการน้ำเสีย ประจำปีงบประมาณ พ.ศ. 2567

(ทบทวนครั้งที่ 1)

กองบริหารความเสี่ยงและควบคุมภายใน

ฝ่ายพัฒนาองค์กร สายงานวิชาการและแผน

คำนำ

ปัจจุบันประเทศไทยกำลังเผชิญกับสภาวการณ์ที่โลกเกิดภัยพิบัติต่างๆ อย่างไม่คาดคิด และมีความรุนแรงมากยิ่งขึ้นทุกปี เช่น วิกฤตเศรษฐกิจ อุทกภัย วาตภัย อัคคีภัย แผ่นดินไหว การจลาจล การประท้วง โรคระบาด เป็นต้น ซึ่งส่งผลกระทบต่อวิถีชีวิตของคนทั่วโลก รวมทั้งทำให้ระบบและกลไกของรัฐหลายประการมีปัญหา โดยไม่สามารถดำเนินภารกิจในสภาวะวิกฤตได้อย่างมีประสิทธิภาพ องค์การจัดการน้ำเสีย รัฐวิสาหกิจ ภายใต้สังกัดกระทรวงมหาดไทย ในฐานะหน่วยงานที่มีภารกิจในการออกแบบ ก่อสร้าง และบริหารจัดการระบบบำบัดน้ำเสียรวมและบำบัดน้ำเสียชุมชนทั่วประเทศ การปรับปรุงฟื้นฟู และบริหารจัดการระบบรวบรวมและบำบัดน้ำเสียชุมชนทั่วประเทศและให้บริการหรือกิจการต่อเนื่องที่เกี่ยวข้องกับการจัดการน้ำเสียอย่างมีประสิทธิภาพในเชิงเศรษฐกิจ รวมถึงการพัฒนานวัตกรรมระบบบำบัดน้ำเสียที่เป็นมิตรต่อสิ่งแวดล้อมเพื่อสังคมอย่างต่อเนื่อง ซึ่งอาจได้รับผลกระทบจากเหตุการณ์ความเสี่ยงด้านต่างๆ ซึ่งเป็นอุปสรรคในการปฏิบัติภารกิจขององค์การจัดการน้ำเสีย และส่งผลกระทบต่อการให้บริการประชาชน

ดังนั้น เพื่อให้องค์การจัดการน้ำเสียมีการเตรียมความพร้อมและสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพภายใต้สภาวะวิกฤตต่างๆ รวมถึงเป็นไปตามหลักเกณฑ์การวัดและประเมินผลการดำเนินงานของสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ ในหัวข้อการบริหารความเสี่ยงและควบคุมภายใน จึงได้จัดทำแผนบริหารความต่อเนื่องทางธุรกิจสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต หรือ Business Continuity Plan (BCP) ขึ้น เพื่อใช้เป็นแนวทางในการปฏิบัติงานของเจ้าหน้าที่และผู้ที่เกี่ยวข้องในการดำเนินงานตามบทบาท ภารกิจ และลดความเสียหายอันเกิดจากการสูญเสียของบุคลากรและทรัพย์สินของทางราชการให้น้อยที่สุด และเพื่อให้มั่นใจว่าภารกิจหลักที่สำคัญขององค์กรสามารถดำเนินการได้อย่างต่อเนื่องแม้ว่าจะประสบกับวิกฤตการณ์ หรือภัยพิบัติต่างๆ ดังนั้น บุคลากรทุกคนจะต้องศึกษาและทำความเข้าใจในหน้าที่ของตนเอง และปฏิบัติตามคู่มืออย่างเคร่งครัด รวมทั้งมีการซักซ้อมเป็นประจำอย่างต่อเนื่อง เพื่อให้ไม่สับสนและสามารถควบคุมสถานการณ์ได้หากเกิดเหตุการณ์จริง ตลอดจนทบทวนแผนให้ทันต่อสภาวะวิกฤตที่อาจเกิดขึ้นใหม่ในอนาคต องค์การจัดการน้ำเสียหวังว่าแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤตฉบับนี้ จะเป็นประโยชน์ต่อการปฏิบัติงานของหน่วยงานต่อไป

กองบริหารความเสี่ยงและควบคุมภายใน

สิงหาคม 2566

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

ภาคผนวก

หน้า

ภาคผนวก (ต่อ)

หน้า

สารบัญตาราง

หน้า

บทที่ 1

บทนำ

การบริหารความต่อเนื่องทางธุรกิจ หรือต่อไปนี้จะเรียกว่า “Business Continuity Manangement (BCM)” นั่นต้องประกอบไปด้วย แผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plans: BCP) จัดทำขึ้นเพื่อให้องค์การจัดการน้ำเสียสามารถนำไปใช้ในการตอบสนอง และปฏิบัติงานในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่างๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร โดยไม่ให้สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินดังกล่าวส่งผลให้หน่วยงานต้องหยุดการดำเนินงานหรือไม่สามารถให้บริการได้อย่างต่อเนื่อง

หากองค์การจัดการน้ำเสียไม่มีกระบวนการรองรับให้การดำเนินงานเป็นไปอย่างต่อเนื่อง อาจส่งผลกระทบต่อองค์การจัดการน้ำเสียในด้านต่างๆ เช่น ด้านเศรษฐกิจ การเงิน การให้บริการ สังคม ชุมชน สิ่งแวดล้อม ตลอดจนชีวิตและความเป็นอยู่ของประชาชน เป็นต้น ดังนั้นการจัดทำแผนบริหารความต่อเนื่องทางธุรกิจ จึงเป็นสิ่งสำคัญที่จะช่วยให้หน่วยงานสามารถรับมือกับเหตุการณ์ฉุกเฉินที่ไม่คาดคิด และทำให้กระบวนการที่สำคัญ (Critical Business Process) สามารถกลับมาดำเนินการได้อย่างปกติหรือตามระดับการให้บริการที่กำหนดไว้ ซึ่งจะช่วยให้สามารถลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อหน่วยงานได้

วัตถุประสงค์ (Objectives)

1. เพื่อกำหนดทรัพยากรที่จำเป็นให้สามารถปฏิบัติงานได้ต่อเนื่องและกำหนดขั้นตอนวิธีการในกรณีที่เกิดเหตุการณ์ที่ไม่ปกติหรือเหตุการณ์ฉุกเฉิน

2. เพื่อให้การหยุดชะงักของการปฏิบัติงานมีผลกระทบน้อยที่สุดไม่ว่าจะหยุดชะงักด้วยสาเหตุใดก็ตาม และเพื่อให้สามารถดำเนินปฏิบัติงานต่อไปในระดับที่ยอมรับได้

3. เพื่อให้สอดคล้องกับวัตถุประสงค์การกู้คืนของภารกิจต่างๆ ขององค์กรในช่วงที่เกิดวิกฤติ โดยหน่วยงานต่างๆ จะมุ่งเน้นไปที่การกู้คืนและสนับสนุนกระบวนการที่สำคัญ

4. เพื่อให้ประชาชน เจ้าหน้าที่ ลูกค้า และผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของหน่วยงานแม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

5. เพื่อให้มีการปฏิบัติตามกฎระเบียบข้อบังคับขององค์กร ข้อตกลงกับผู้รับบริการ

6. เพื่อจำกัดความเสียหายต่อทรัพย์สิน ทรัพยากร ชื่อเสียง ภาพลักษณ์ขององค์กร

7. องค์กรสามารถปฏิบัติภารกิจหลักที่สำคัญต่อไปได้ในช่วงภาวะวิกฤต

8. องค์กรสามารถให้บริการหรือดำเนินกิจกรรมต่อไปได้อย่างต่อเนื่อง

9. องค์กรสามารถฟื้นกลับงานหรือกิจกรรมที่สำคัญต่อภารกิจหลักสู่ภาวะปกติ

10. เพื่อจัดระบบการดำเนินงานและเตรียมความพร้อมในด้านต่างๆ ไว้รองรับสถานการณ์ภัยพิบัติตามลักษณะความเสี่ยงภัยในทุกขั้นตอนทั้งในช่วงก่อนเกิดภัย ขณะเกิดภัย และภายหลังที่ภัยได้ผ่านพ้นไปแล้ว

11. เพื่อพัฒนาขีดความสามารถในการป้องกัน การเตรียมความพร้อม การระงับและบรรเทาและการฟื้นฟูบูรณะ ให้มีประสิทธิภาพและประสิทธิผลสูงสุดในทุกสถานการณ์

หลักการเตรียมความพร้อมในภาวะวิกฤตตามพระราชกฤษฎีกาว่าด้วยหลักเกณฑ์และวิธีการบริหารกิจการบ้านเมืองที่ดี พ.ศ. 2546 คือการที่องค์กรสามารถนำบทเรียนสถานการณ์ความรุนแรงสำคัญที่ผ่านมาปรับกระบวนการทำงานใหม่ โดยเฉพาะในเรื่องการบริการประชาชน เพื่อให้มั่นใจว่าภารกิจหลักของราชการ หรืองานบริการประชาชนที่สำคัญสามารถดำเนินงาน หรือให้บริการได้อย่างต่อเนื่องไม่สะดุดหยุดลงแม้ว่าจะประสบกับวิกฤตการณ์ หรือภัยพิบัติต่างๆ ซึ่งที่ประชุมคณะรัฐมนตรีเมื่อวันที่ 24 เมษายน 2555 ได้มีมติเห็นชอบกรอบแนวทางการดำเนินการเตรียมความพร้อมต่อสภาวะวิกฤต 4 ขั้นตอน คือ

1. การสร้างความรู้ความเข้าใจให้กับองค์กร

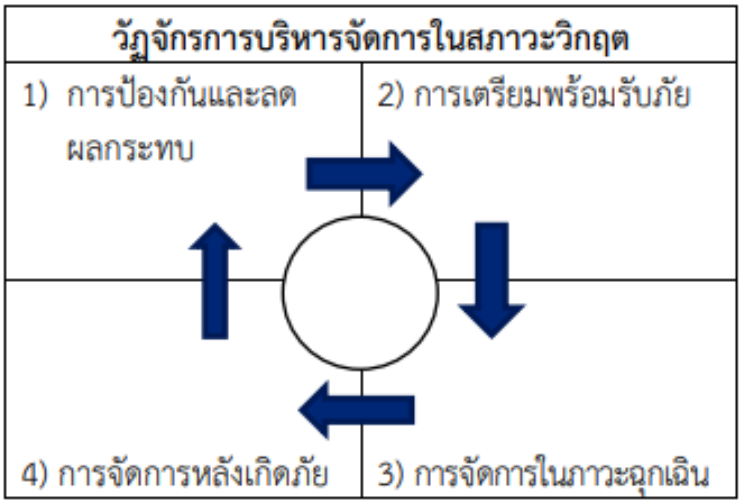
2. เตรียมความพร้อมขององค์กรในการจัดทำแผนรองรับการดำเนินภารกิจการให้บริการประชาชนได้อย่างต่อเนื่อง (Business Continuity Plans)

3. การซักซ้อมแผนและนำไปปฏิบัติได้จริง

4. การส่งเสริมให้มีการบริหารจัดการอย่างยั่งยืนในสภาวะวิกฤต

การบริหารจัดการองค์กรในสภาวะวิกฤต/เหตุการณ์ฉุกเฉิน/สถานการณ์ภัยพิบัติ โดยทั่วไปจะแบ่งวัฏจักรการบริหารจัดการออกเป็น 4 ขั้นตอน คือ

1. การป้องกันและลดผลกระทบ
2. การเตรียมพร้อมรับภัย
3. การจัดการในภาวะฉุกเฉิน
4. การจัดการหลังเกิดภัย



รูปที่ 1 วัฏจักรการบริหารจัดการในสภาวะวิกฤติ

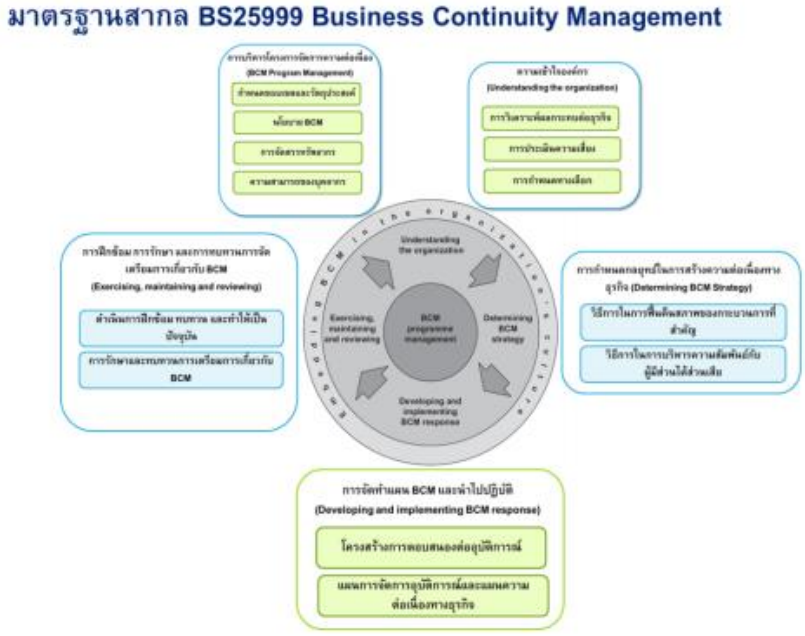
โดยแนวคิดการบริหารความต่อเนื่องของหน่วยงานภาครัฐ คือ การควบคุมดูแลและป้องกันทรัพยากรที่สำคัญต่อการดำเนินงานหรือให้บริการ เพื่อสร้างประโยชน์สูงสุดสำหรับผู้รับบริการและผู้มีส่วนได้เสียซึ่งภายในช่วงระยะเวลาแรกจะเป็นช่วงของการตอบสนองต่ออุบัติการณ์ (Incident/Emergency Management) และในกรณีที่เหตุการณ์และความเสียหายขยายตัวไปในวงกว้าง การตอบสนองอาจจำเป็นต้องยกระดับเป็นการบริหารจัดการวิกฤต (Crisis Management) ภายหลังจากนั้นจะเป็นช่วงของการทำให้เกิดความต่อเนื่องของกระบวนการทางธุรกิจ (Continuity Management) เพื่อให้หน่วยงานสามารถกลับมาดำเนินงานได้ จึงมีความจำเป็นที่หน่วยงานต้องทบทวนแผนความต่อเนื่อง Business Continuity Plans (BCP) โดยมีวัตถุประสงค์ คือ

1. เพื่อใช้เป็นแนวทางในการบริหารความต่อเนื่องของการปฏิบัติงานในสภาวะวิกฤต
2. เพื่อให้หน่วยงานมีการเตรียมความพร้อมล่วงหน้าในการรับมือกับสภาวะวิกฤต หรือเหตุการณ์ฉุกเฉินต่างๆ ที่อาจเกิดขึ้น
3. เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงาน เช่น ผลกระทบด้านเศรษฐกิจการเงิน

4. การให้บริการสังคม ชุมชน และสิ่งแวดล้อม ตลอดจนชีวิตและทรัพย์สินของประชาชน เป็นต้น

5. เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้

แผนบริหารความต่อเนื่อง หรือ Business Continuity Plans (BCP) เป็นชุดของเอกสารคำแนะนำและวิธีการที่ช่วยให้การดำเนินงาน/งานบริการขององค์กรสามารถตอบสนองต่อการเกิดอุบัติเหตุ ภัยพิบัติ ภาวะฉุกเฉินและหรือภัยคุกคามได้โดยไม่ต้องหยุดชะงัก/หรือมีอุปสรรคที่สำคัญต่อการดำเนินงาน ซึ่งจำเป็นจะต้องมีแผนการกู้คืนระบบหรือแผนการกู้คืนทรัพยากรบุคคลและกระบวนการทำงาน เพื่อให้สามารถปฏิบัติงาน หรือสามารถให้บริการแก่ประชาชนต่อไปได้ แผนดังกล่าวจัดทำขึ้นตามแนวทางของการบริหารความต่อเนื่องที่ได้รับการใช้อย่างแพร่หลาย คือ มาตรฐาน Business Continuity Standard (BS25999) ซึ่งกำหนดโดย British Standards Institution: BSI มีสำนักงานใหญ่ ตั้งอยู่ในประเทศอังกฤษ เป็นต้นแบบของการพัฒนาไปสู่มาตรฐาน ISO223011 ปัจจุบันพัฒนาเป็น ISO22301:2019 ซึ่งมาตรฐาน BS25999 มี 6 องค์ประกอบหลัก เป็นวงจรการบริหารความต่อเนื่อง (BCM Life Cycle) ซึ่งหน่วยงานสามารถนำไปประยุกต์ใช้ได้ ตามขอบเขตวิธีการบริหารจัดการ และทรัพยากรที่ต้องใช้ ใน BCM ของแต่ละองค์กรที่แตกต่างกันไปตามขนาด ภารกิจ และทรัพยากรที่ใช้งาน ดังนี้



รูปที่ 2 วงจรการบริหารความต่อเนื่อง (BCM Life Cycle)

1. การบริหารโครงการจัดการความต่อเนื่อง (BCM Program Management) ถือว่าเป็นองค์ประกอบหลักและเป็นขั้นตอนแรกของการบริหารความต่อเนื่อง มีขั้นตอนคือ

1.1. การจัดทำกรอบนโยบาย BCM

1.2. โครงสร้าง BCM หน้าที่และความรับผิดชอบของบุคลากรที่เกี่ยวข้อง ตั้งแต่ผู้บริหารระดับสูงลงมาถึงพนักงานระดับต่างๆ รวมถึงการจัดตั้งทีมงานด้าน BCM

1.3. การกำหนดตัวชี้วัดผลการดำเนินงาน

1.4. การปรับระดับของเหตุการณ์ (Incident Escalation Progress)

1.5. วิธีการบริหารโครงการบริหารความต่อเนื่อง

1.6. การติดตามความพร้อมทั้งรายงานความคืบหน้า

2. การศึกษาและทำความเข้าใจองค์กร (Understanding of Organization) เพื่อให้เข้าใจในสภาพและการดำเนินงานขององค์กรและหน่วยงานในการรับผลกระทบหรือความเสี่ยงผ่านวิธีการวิเคราะห์ผลกระทบทางธุรกิจ Business Impact Analysis (BIA) และการประเมินความเสี่ยง Risk Assessment (RA) และภัยคุกคามต่างๆ เช่น แผ่นดินไหว อุทกภัย อัคคีภัย การก่อประท้วง การก่อจลาจล การก่อวินาศกรรม และโรคระบาด ที่จะมีผลกระทบต่อทรัพยากร 5 ด้าน ได้แก่

2.1. ผลกระทบด้านอาคาร/สถานที่ทำงานหลักและสำนักงานสาขา

2.2. ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ และการจัดส่งวัสดุอุปกรณที่สำคัญ

2.3. ผลกระทบด้านเทคโนโลยีสารสนเทศ ข้อมูลที่สำคัญ

2.4. ผลกระทบด้านบุคลากรหลัก

2.5. ผลกระทบด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ

เพื่อระบุความเร่งด่วนของกิจกรรมต่างๆ และระดับความสามารถที่ต้องการ เพื่อนำไปเป็นข้อมูลในการจัดระดับความสำคัญของกระบวนงาน การกำหนดแนวทางและการกำหนดกลยุทธ์ในขั้นตอนต่อไป

3. การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง BCM (Determining BCM Strategy) เป็นการกำหนดแนวทางในการตอบสนองต่อการหยุดชะงักของการดำเนินงานขององค์กร ได้แก่ กลยุทธ์กู้คืนการดำเนินงาน (Recovery Strategy) และการกำหนดกลยุทธ์ด้านการจัดการทรัพยากรที่เหมาะสมตามข้อมูลที่ได้จาก BIA ซึ่งประกอบด้วยเรื่อง บุคลากร สถานที่ปฏิบัติงาน อุปกรณ์และเครื่องมือเทคโนโลยี ข้อมูลและผู้ผลิตสินค้าหรือผู้ให้บริการ

4. การพัฒนาและเตรียมการตอบสนองต่อเหตุการณ์ในภาวะฉุกเฉิน (Developing and Implementing BCM Response) ได้แก่

4.1. Incident Management Plans (IMP) เพื่อจัดการกับวิกฤตฉุกเฉินที่เกิดขึ้น

4.2. Emergency/Crisis Management Plan (CMP) เพื่อจัดการกับวิกฤตฉุกเฉินที่เกิดขึ้น และผลกระทบขยายไปในวงกว้าง

4.3. Business Continuity Plans (BCP) เพื่อบริหารการดำเนินภารกิจอย่างต่อเนื่อง โดยมุ่งทำขั้นตอนงานที่ฉุกเฉินต่อภารกิจและใช้ทรัพยากรหลักอย่างเหมาะสม พร้อมทั้งเตรียมแผนรับสถานการณ์ที่ส่งผลกระทบ โดยแบ่งเป็น 3 ขั้นตอน ตามระยะเวลา คือ การตอบสนองทันทีภายใน 24 ชั่วโมง การตอบสนองในระยะเวลาภายใน 7 วัน และตอบสนองเหตุการณ์และกู้สถานการณ์ในระยะเวลาเกิน 7 วัน

4.4. Recovery Plan (RP) หรือแผนกู้คืนภารกิจหลังภัยพิบัติผ่านพ้นไป

5. การทดสอบ ปรับปรุงและทบทวนแผน (Exercising Monitoring and Reviewing) เป็นขั้นตอนที่สำคัญ เพื่อให้แน่ใจว่า BCM ที่จัดทำขึ้นสามารถใช้ได้จริง รวมทั้งเพื่อเตรียมความพร้อมตลอดจนตรวจสอบความสามารถของบุคลากร และประสิทธิภาพของแผนในการตอบสนองต่อวิกฤตการณ์ โดยรูปแบบการทดสอบอาจมีตั้งแต่ระดับง่ายไปหายาก ดังนี้

5.1. Call Tree คือ การซ้อมการแจ้งเหตุฉุกเฉินให้กับสมาชิก ทีมงานที่เกี่ยวข้องตามผังรายชื่อโทรศัพท์

5.2. Tabletop Testing คือ การประชุมแลกเปลี่ยนความคิดเห็นกับทุกหน่วยงานที่เกี่ยวข้องโดยจำลองโจทย์ทุกสถานการณ์ขึ้นมา และลองนำแผน BCP มาพิจารณาว่าใช้ตอบโจทย์แต่ละขั้นตอนได้หรือไม่

5.3. Simulation คือ การทดสอบโดยจำลองสถานการณ์เสมือนจริง และลองนำแผน BCP มาประยุกต์ใช้

5.4. FULL BCP Exercise คือ การทดสอบเต็มรูปแบบและใกล้เคียงสถานการณ์จริงมากที่สุด

6. การปลูกฝัง BCM ให้เป็นส่วนหนึ่งของวัฒนธรรมองค์กร (Embedding BCM in The Organization's Culture) การทำให้ BCM ผสมกลมกลืนเข้าจนเป็นวัฒนธรรมองค์กร เป็นเรื่องที่ต้องใช้เวลา และจิตวิทยาที่จะทำให้บุคลากรทุกคนได้ซึมซาบและเข้าใจถึงความสำคัญของ BCM ตลอดจนบทบาทหน้าที่ที่ทุกคนพึงมีเพื่อให้ภารกิจสามารถดำเนินต่อไปได้ในยามที่เกิดเหตุวิกฤต

สมมติฐานของแผนการบริหารความต่อเนื่อง (BCP Assumptions)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

1. รองรับได้ถึงสถานการณ์ร้ายแรงที่สุด (Worst Case Scenario) แผนรองรับการดำเนินภารกิจอย่างต่อเนื่อง ต้องครอบคลุมถึงสถานการณ์หรือเหตุการณ์ที่จะทำให้เกิดความเสียหายอย่างร้ายแรงที่สุดต่อสถานที่ ระบบงาน อุปกรณ์ และเครื่องมือเครื่องใช้ในการทำงาน และเอกสารข้อมูลที่สำคัญที่เป็นไปได้ในแต่ละกรณี รวมถึงความเสียหายที่เกิดกับผู้ให้บริการและการสูญเสียบุคลากรสำคัญ การมีแผนรองรับในสถานการณ์ที่ร้ายแรงที่สุด จะช่วยให้ส่วนราชการสามารถกู้คืนในสถานการณ์ที่รุนแรงน้อยกว่าได้ ทั้งนี้ เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาต่างๆ มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่เตรียมไว้

2. ระยะเวลาในการกู้คืน (Recovery Time Frame) แผนจะระบุทรัพยากรที่จะต้องใช้ในการทำงานเป็นระยะเวลา 30 วัน หากยังไม่สามารถกู้คืนได้ภายใน 30 วัน หน่วยงานที่ได้รับผลกระทบจะต้องดำเนินการร่วมกับหน่วยงานสนับสนุน และหน่วยงานบริการที่เกี่ยวข้อง เพื่อเตรียมการให้หน่วยงานสามารถดำเนินการต่อไปได้

3. ศูนย์เทคโนโลยีสารสนเทศรับผิดชอบในการสำรองระบบสารสนเทศต่างๆ โดยระบบสารสนเทศสำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก

4. ศูนย์ปฏิบัติงานสำรอง (Alternate Site) ในการกู้คืนงานที่สำคัญ จำเป็นที่จะต้องมีศูนย์ปฏิบัติงานสำรองไว้อย่างน้อย 1 แห่ง หน่วยงานต้องพิจารณาปัจจัยสำคัญที่ส่งผลต่อการกำหนดศูนย์ปฏิบัติงานสำรอง

5. “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และบุคลากรทั้งหมดขององค์การจัดการน้ำเสีย

การศึกษาและทำความเข้าใจองค์กร (Understanding the Organization)

เป็นการระบุ ศึกษาความสำคัญ และอธิบายสถานการณ์วิกฤติทางธุรกิจที่สำคัญภายในองค์กร เพื่อค้นหาและระบุว่ามีธุรกรรม สายปฏิบัติงาน ภาระงาน บริการ/ผลิตภัณฑ์ใดบ้างที่วิกฤติ ที่กิจการควรจะต้องทำการส่งมอบตามพันธกิจที่มีต่อลูกค้า/ผู้รับบริการลูกค้า คู่ค้า ผู้ที่เกี่ยวข้องภายใน Value Chain การที่จะระบุและอธิบายสถานการณ์วิกฤติทางธุรกิจที่สำคัญได้ อาจจะต้องเริ่มต้นจากการทบทวน

1. พันธกิจหลักของกิจการ
2. ยุทธศาสตร์หรือแผนกลยุทธ์ของกิจการ
3. เงื่อนไข หรือพันธะสำคัญทางกฎหมายที่กิจการต้องการส่งมอบ ดำเนินการให้ครบถ้วนตามเงื่อนไข และให้ทันตามกรอบเวลาที่กำหนด

การอธิบายถึงลักษณะของการส่งมอบ การปฏิบัติให้เป็นไปตามเงื่อนไข รายละเอียดของการส่งมอบต้องระบุให้ชัดเจนที่สุดถือว่ามีความสำคัญต่อการได้มาซึ่งข้อมูลสถานการณ์วิกฤติ กระบวนงาน/สายงานวิกฤติ ภาระงานวิกฤติ บริการวิกฤติ ที่จะนำไปใช้ประโยชน์ต่อไปในขั้นตอนต่อไป โดยกล่าวถึงกระบวนการทำงานและกิจกรรมในการทำงานของทุกคนในภาวะปกติ ขนาดของการปฏิบัติงาน ข้อกำหนดสำคัญที่ต้องปฏิบัติตาม (เช่น กรอบเวลาที่กำหนด พันธะสัญญาตามกฎหมาย กฎระเบียบข้อบังคับของทางราชการ เป็นต้น) ตลอดจนหน่วยงานหรือองค์กรที่ส่งงาน/ให้บริการ และที่รับงาน/บริการจากหน่วยงาน (Upstream and downstream dependencies) ทำให้เข้าใจขอบเขตการกู้คืนเพื่อที่จะได้สามารถสั่งการและควบคุมการปฏิบัติงานอย่างมีประสิทธิผลเพื่อ

1. ลดโอกาสของการดำเนินงานที่ต้องหยุดชะงัก
2. ลดระยะเวลาในการตอบสนองและกอบกู้สถานการณ์ให้กลับสู่สภาวะปกติ
3. จำกัดผลกระทบต่อองค์กรจากการหยุดชะงักการดำเนินงาน

โดยมีขั้นตอนของการทำความเข้าใจกับองค์กร ดังนี้

1. การวิเคราะห์ผลกระทบทางธุรกิจ Business Impact Analysis (BIA)

การวิเคราะห์ผลกระทบทางธุรกิจ หรือ Business Impact Analysis (BIA) หมายถึงกระบวนการในการวิเคราะห์ถึงกิจกรรมทางธุรกิจ และผลกระทบที่จะเกิดขึ้นจากการหยุดชะงักของกิจกรรมนั้นๆ มีขั้นตอนการดำเนินการ ดังนี้

ขั้นตอนที่ 1 การระบุกิจกรรม กระบวนการ บริการและ/หรือผลิตภัณฑ์หลัก เป็นการพิจารณาการปฏิบัติราชการ/กระบวนงานตามโครงสร้างและอำนาจหน้าที่ของหน่วยงาน ต่างๆ ในองค์การจัดการน้ำเสีย โดยระบุกิจกรรม/กระบวนการ กรอบเวลา หรือรอบเวลาในการทำงาน ผู้ส่งมอบงาน หน่วยงานที่เกี่ยวข้องและผู้รับบริการเพื่อให้เห็นถึงผลกระทบที่จะเกิดขึ้นในแต่ละกระบวนการ/กิจกรรมการทำงาน

ขั้นตอนที่ 2 ระบุถึงผลกระทบที่จะเกิดขึ้นจากการหยุดชะงัก และพิจารณาถึงการเปลี่ยนแปลงของผลกระทบเมื่อเวลาผ่านไป การระบุผลกระทบในขั้นตอนนี้จะเริ่มต้นที่การประเมินความเสี่ยงและภัยคุกคาม ซึ่งแผนความต่อเนื่อง (BCP) ฉบับนี้ใช้รองรับสถานการณ์กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินในพื้นที่สำนักงานของหน่วยงาน หรือภายในหน่วยงาน ด้วยเหตุการณ์ต่อไปนี้

- เหตุการณ์อุทกภัย
- เหตุการณ์แผ่นดินไหว
- เหตุการณ์อัคคีภัย
- เหตุการณ์ชุมนุมประท้วง/จลาจล
- เหตุการณ์ก่อการร้าย
- เหตุการณ์โรคระบาด
- ภัยคุกคามและเหตุการณ์ผิดปกติทางไซเบอร์

ขั้นตอนที่ 3 การวิเคราะห์ผลกระทบทางธุรกิจที่ครอบคลุมระบบงานที่สำคัญทั้ง 8 ด้าน เพื่อป้องกันการหยุดชะงักขณะดำเนินงานที่สำคัญ ดังนี้

1. การกำกับดูแลที่ดีและการนำองค์กร
2. การวางแผนเชิงกลยุทธ์
3. การบริหารความเสี่ยงและการควบคุมภายใน
4. การมุ่งเน้นผู้มีส่วนได้ส่วนเสียและลูกค้า
5. การพัฒนาเทคโนโลยีดิจิทัล
6. การบริหารทุนมนุษย์
7. การจัดการความรู้และนวัตกรรม
8. การตรวจสอบภายใน

ตารางที่ 1 สรุปการวิเคราะห์ผลกระทบทางธุรกิจเบื้องต้น (Business Impact Analysis) ที่ครอบคลุมระบบงานที่สำคัญ

ลำดับ	การบริหารจัดการองค์กร	กระบวนงาน/ระบบงานที่สำคัญ	ประเมินผลกระทบหากหยุดชะงัก	ระยะเวลาในการกู้คืน		
				เป้าหมาย	หยุดชะงักที่รับได้	ระยะเวลาในการฟื้นฟู
1	การกำกับดูแลที่ดีและการนำองค์กร	คณะกรรมการมีการติดตามผลการดำเนินงานขององค์กร	การดำเนินงานภายในองค์กรไม่เป็นไปในทิศทางเดียวกัน	ไม่เกิน 1 สัปดาห์	ไม่เกิน 1 สัปดาห์	5 วัน
2	การวางแผนเชิงกลยุทธ์	การกำหนดทิศทางในการดำเนินงานขององค์กรทั้งในระยะสั้นและระยะยาว	การดำเนินงานภายในองค์กรไม่เป็นไปตามเป้าหมาย	ไม่เกิน 5 วัน	ไม่เกิน 5 วัน	3 วัน
3	การบริหารความเสี่ยงและการควบคุมภายใน	1) การกำหนดวัตถุประสงค์ 2) การระบุความเสี่ยง 3) การประเมินความเสี่ยง 4) การจัดการและแผนบริหารความเสี่ยง 5) การรายงานและติดตามผล 6) การประเมินผลการจัดการ	ยอมรับความเสี่ยงที่เกิดขึ้นจากการปฏิบัติงานภายใต้ระดับความเสี่ยงที่องค์กรสามารถยอมรับได้	ไม่เกิน 1 สัปดาห์	ไม่เกิน 1 สัปดาห์	5 วัน
4	การมุ่งเน้นผู้มีส่วนได้ส่วนเสียและลูกค้า	การประเมินผลที่ได้รับจากผู้มีส่วนได้ส่วนเสีย และลูกค้า	ขาดความน่าเชื่อถือต่อผู้ที่มีส่วนได้ส่วนเสียและลูกค้า	ไม่เกิน 5 วัน	ไม่เกิน 5 วัน	2 วัน
5	การพัฒนาเทคโนโลยีดิจิทัล	ระบบสารสนเทศภายในองค์กร	การดำเนินงานภายในองค์กรเกิดการล่าช้า	ไม่เกิน 2 วัน	ไม่เกิน 2 วัน	1 วัน
6	การบริหารทุนมนุษย์	1) การกำหนดมาตรฐานของแต่ละบุคคลภายในองค์กร 2) การสร้างกลยุทธ์ในการพัฒนาบุคคลากรภายในองค์กร	การพัฒนามาตรฐานของบุคคลากรขาดความต่อเนื่อง	ไม่เกิน 1 สัปดาห์	ไม่เกิน 1 สัปดาห์	5 วัน
7	การจัดการความรู้และนวัตกรรม	การเผยแพร่ความรู้ภายในและภายนอกองค์กร	พนักงานภายในองค์กรจะไม่เกิดความคิดสร้างสรรค์	ไม่เกิน 5 วัน	ไม่เกิน 5 วัน	3 วัน
8	การตรวจสอบภายใน	การประเมินและปรับปรุงกระบวนการทำงานต่างๆ ของภายในองค์กร	การประเมินประสิทธิภาพการดำเนินงานภายในน้อยลง	ไม่เกิน 5 วัน	ไม่เกิน 5 วัน	3วัน

การประเมินความเสี่ยง โดยการระบุความเสี่ยงและผลกระทบที่มาจากวัตถุประสงค์เชิงยุทธศาสตร์และ KPIs ขององค์กร ด้วยการวิเคราะห์จากสถานการณ์ไม่แน่นอนจากแหล่งที่มาของเหตุการณ์ที่ใช้ประกอบการระบุความเสี่ยง 6 แหล่ง คือ กลยุทธ์องค์กร และ SWOT Analysis เกณฑ์ประเมินผลการดำเนินงานรัฐวิสาหกิจประจำปีบัญชี (PA) ข้อเสนอแนะของคณะกรรมการ และคณะอนุกรรมการบริหารความเสี่ยงและควบคุมภายในและผู้บริหารระดับสูงขององค์กร

2. การวิเคราะห์ผลกระทบทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉิน มีหลากหลายรูปแบบ ดังนั้นเพื่อให้องค์การจัดการน้ำเสีย สามารถบริหารจัดการการดำเนินงานขององค์กรให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็น และต้องระบุไว้ในแผนบริหารความต่อเนื่อง ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบ 5 ด้าน ดังนี้

2.1 <u>ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก</u> หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักของหน่วยงาน ได้รับความเสียหาย หรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้ และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ในช่วงระยะแรก หรือระยะกลาง หรือระยะยาว ซึ่งรวมถึงการที่ผู้รับบริการไม่สามารถเข้าถึงสถานที่ให้บริการของหน่วยงานด้วย

2.2 <u>ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ</u> หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญเพื่อนำไปใช้ในการปฏิบัติงานได้

2.3 <u>ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ</u> หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้ระบบงานเทคโนโลยีหรือระบบสารสนเทศ หรือเข้าถึงข้อมูลที่สำคัญในการปฏิบัติงานได้

2.4 <u>ผลกระทบด้านบุคลากรหลัก</u> หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

2.5 <u>ผลกระทบด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย</u> หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการแก่หน่วยงาน/ผู้มีส่วนได้ส่วนเสียไม่สามารถที่จะให้บริการหรือส่งมอบงาน เพื่อให้หน่วยงานใช้งานในการปฏิบัติงาน

หลักเกณฑ์การประเมินผลกระทบต่อกระบวนการดำเนินงาน

ตารางที่ 2 ระดับผลกระทบและลักษณะของผลกระทบ

ระดับผลกระทบ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ
สูงมาก	■ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูงมาก ■ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่า ร้อยละ ๕๐ ■ เกิดการสูญเสียชีวิตและ/หรือภัยคุกคามต่อสาธารณชน ■ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศและนานาชาติ
สูง	■ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูง ■ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ ๒๕-๕๐ ■ เกิดการบาดเจ็บต่อผู้รับบริการ/บุคคล/กลุ่มคน ■ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศ
ปานกลาง	■ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับปานกลาง ■ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ ๑๐-๒๕ ■ ต้องมีการรักษาพยาบาล ■ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ต่ำ	■ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำ ■ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ ๕-๑๐ ■ ต้องมีการปฐมพยาบาล ■ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ไม่เป็นสาระสำคัญ	■ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงมากกว่าร้อยละ ๕

3. สรุปเหตุการณ์สภาวะวิกฤติและผลกระทบจากเหตุการณ์

ความเสี่ยงและภัยคุกคาม	ผลกระทบ				
	ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	ด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ
เหตุการณ์อุทกภัย	✓	✓	✓	✓	✓
เหตุการณ์ภัยพิบัติ	✓	✓	✓	✓	✓
เหตุการณ์อัคคีภัย	✓	✓	✓	✓	✓
เหตุการณ์ชุมนุมประท้วง/จลาจล	✓	-	-	✓	✓
เหตุการณ์ก่อการร้าย	✓	-	-	✓	✓
เหตุการณ์โรคระบาด	✓	-	-	✓	✓
ภัยคุกคามทางไซเบอร์	✓	✓	✓	✓	✓

4. การประเมินผลกระทบต่อกระบวนการ/กิจกรรม

โดยกำหนดช่วงเวลาหยุดชะงักที่ยอมรับได้สูงสุดของแต่ละกิจกรรม หรือกระบวนการ เพื่อจัดพิจารณากำหนดระดับผลกระทบ (สูงมาก สูง ปานกลาง ต่ำ ไม่เป็นสาระ) และจัดกลุ่มกิจกรรมตามลำดับของระดับผลกระทบ/ความสำคัญในการฟื้นคืนกลับสู่ภาวะปกติ

5. จัดทำแผนบริหารความต่อเนื่อง (BCP)

สำหรับกลุ่มกิจกรรมที่มีระดับผลกระทบสูงมาก สูง ปานกลาง

แผนบริหารความต่อเนื่อง (BCP) ฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องเกิดขึ้นจากการดำเนินงานปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของหน่วยงาน เนื่องจากหน่วยงานยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้บริหารหน่วยงานหรือผู้บริหารของแต่ละกลุ่มงานและฝ่ายงานสามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

บทที่ 2

การบริหารความต่อเนื่อง

กลยุทธ์การบริหารความต่อเนื่อง Business Continuity Strategy (BCS)

เมื่อเกิดกรณีการสูญเสีย/เสียหายของปัจจัยหลัก (Loss of Key Pillars) องค์การจะต้องเลือกวิธีการในการลดความเสี่ยงในแต่ละกิจกรรมที่สำคัญ (กิจกรรมที่มีระดับผลกระทบสูงมาก สูง ปานกลาง) เพื่อให้ความเสี่ยงอยู่ในระดับที่ยอมรับและสามารถนำไปปฏิบัติได้โดยกำหนดกลยุทธ์ความต่อเนื่อง Business Continuity Strategy (BCS) ดังนี้

1. กำหนดกลยุทธ์การกู้คืนของกิจกรรมที่สำคัญโดยระบุถึงปัจจัยหลักของการสูญเสียและเสียหายเพื่อการกู้คืนภายในระยะเวลาที่ยอมให้หยุดดำเนินการขั้นต่ำได้

2. กำหนดทรัพยากรที่สำคัญ/จำเป็นต่อการบริหารความต่อเนื่อง โดยระบุทรัพยากรสำคัญขั้นต่ำที่กระบวนงานต้องใช้ในการดำเนินงานทั้ง 5 อย่าง ได้แก่ อาคาร/สถานที่ปฏิบัติงาน เครื่องมือและอุปกรณ์ ระบบงานเทคโนโลยีหรือระบบสารสนเทศ บุคลากร และคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย

3. กำหนดบุคลากรสำคัญ/จำเป็นต่อการบริหารความต่อเนื่อง เพื่อให้แผนความต่อเนื่อง (BCP) สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล จึงมีการจัดตั้งคณะบริหารความต่อเนื่อง (BCP Team) ของหน่วยงาน

ทีมงานแผนบริหารความต่อเนื่อง (Business Continuity Plans Team)

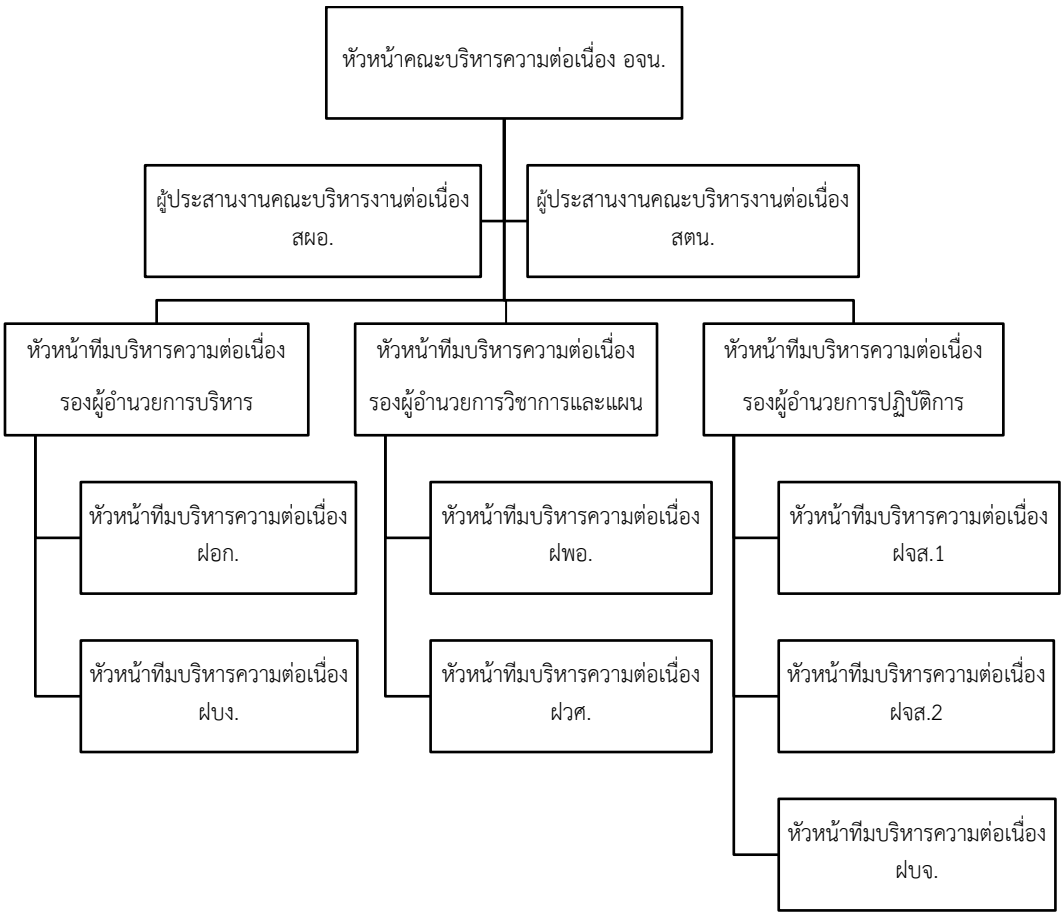
เพื่อให้แผนบริหารความต่อเนื่อง (BCP) ขององค์การจัดการน้ำเสีย สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผลจะต้องจัดตั้งทีมงานบริหารความต่อเนื่อง (BCP Team) องค์การจัดการน้ำเสีย มีโครงสร้างดังนี้

1. หัวหน้าคณะบริหารความต่อเนื่อง ได้แก่ ผู้บริหารสูงสุดของหน่วยงาน หรือผู้บริหารระดับรองลงมาที่ได้รับมอบหมาย มีหน้าที่ในการประเมินลักษณะ ขอบเขตและแนวโน้มของอุบัติการณ์ที่

เกิดขึ้น เพื่อตัดสินใจประกาศใช้แผนบริหารความต่อเนื่อง และดำเนินการตามขั้นตอนของแนวทางการบริหารความต่อเนื่อง ตลอดจนสรรหาทรัพยากรตามที่ได้กำหนดไว้ในแผนบริหารความต่อเนื่อง

2. หัวหน้าทีมบริหารความต่อเนื่อง ได้แก่ รองผู้อำนวยการ/ผู้อำนวยการฝ่าย มีหน้าที่ในการสนับสนุนการปฏิบัติงานของหัวหน้าคณะบริหารความต่อเนื่อง และดำเนินการตามขั้นตอนของแนวทางการบริหารความต่อเนื่อง ตลอดจนสรรหาทรัพยากรตามที่ได้กำหนดไว้ในแผนบริหารความต่อเนื่องของหน่วยงาน

3. ผู้ประสานงานคณะบริหารงาน มีหน้าที่ในการติดต่อและประสานงานภายในหน่วยงาน และให้การสนับสนุนในการติดต่อสื่อสารกับหัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่องดำเนินการตามขั้นตอนและแนวทางของแผนบริหารความต่อเนื่อง



อำนาจหน้าที่

1. จัดทำแผนบริหารความพร้อมต่อสภาวะวิกฤต โดยครอบคลุมการเตรียมความพร้อมด้านกระบวนการ ด้านบุคลากร ด้านข้อมูล ด้านสถานที่ และด้านงบประมาณ

2. จัดทำโครงการฝึกอบรมและการประชาสัมพันธ์แผนการบริหารความพร้อมต่อสภาวะวิกฤตแก่ผู้ที่เกี่ยวข้องทั้งภายในและภายนอกองค์การ พร้อมทั้งจัดให้มีการสื่อสารเพื่อป้องกันและลดความตระหนักของผู้ที่เกี่ยวข้องและสาธารณชน รวมทั้งสามารถแจ้งเหตุแก่หน่วยงานที่เกี่ยวข้องได้อย่างทันท่วงที

3. จัดหาพื้นที่เพื่อเตรียมตั้งเป็นสถานที่ปฏิบัติงานสำรอง เพื่อให้สามารถใช้เป็นที่ทำงานได้ทันที รวมทั้งการจัดหาอุปกณ์ที่จำเป็นเพื่อให้การบริการไม่หยุดชะงัก

4. ติดตามและประเมินผลการปฏิบัติตามระบบที่วางแผนไว้ มีการปรับปรุงและซักซ้อมแผนการบริหารความพร้อมต่อสภาวะวิกฤตอย่างสม่ำเสมอ

5. จัดทำรายงานผลการดำเนินงานในการบริหารความพร้อมต่อสภาวะวิกฤต ทุกสิ้นปีงบประมาณ

6. แต่งตั้งคณะทำงานย่อยเพื่อปฏิบัติหน้าที่ต่างๆ ตามที่มอบหมาย

7. รายงานความก้าวหน้าในการดำเนินการบริหารความพร้อมต่อสภาวะวิกฤตให้ผู้อำนวยการองค์การจัดการน้ำเสียทราบเป็นระยะๆ

โดยแต่ละตำแหน่งจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนเหตุการณ์ฉุกเฉินในฝ่ายงานของตนเอง ให้สามารถบริหารความต่อเนื่องและกลับสู่สภาวะปกติได้โดยเร็วตามบทบาท หน้าที่ที่กำหนดไว้ของทีมงานบริหารความต่อเนื่อง (BCP Team) และในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ให้บุคลากรสำรองรับผิดชอบทำหน้าที่ในบทบาทของบุคลากรหลักไปก่อน ปรากฏดังตารางที่ 3

ตารางที่ 3 รายชื่อและหมายเลขติดต่อบุคลากรและบทบาทของทีมงานบริหารความต่อเนื่อง (BCP Team)

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์มือถือ		ชื่อ	เบอร์มือถือ
นายชีระ วงศบูรณะ	081-8423802	หัวหน้าคณะบริหารความต่อเนื่อง ผอ.อจน.	นายสุชัย เจนพจนารถ	081-4504600
นางดวงแข ยงสุวรรณ	081-8087080	ผู้ประสานงานคณะบริหารความต่อเนื่อง สผอ.	นางสาวอรทัย อินประสิทธิ์	095-9632434
น.ส.สรรพางดี ล่ามกิจจา	085-6891616	ผู้ประสานงานคณะบริหารความต่อเนื่อง สตน.	นายอภินท์ ธนัพประภัศร์	086-8922298
นางสาววรนันท์ จันทร์ดนู	095-4596051	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.บร.	น.ส.อาภากร อมาตยกุล	081-1956661
นายสุชัย เจนพจนารถ	081-4504600	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.วผ.	นายปัณณพัฒน์ จันทร์เจริญสุข	096-1496364
นายอธิรักษ์ บุพจันโท	063-2035762	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.ปก.	นายรัฐวุฒิ ทับทอง	081-8349880
นายอนุกูล แหลมปัญญา	081-7121248	หัวหน้าทีมบริหารความต่อเนื่อง รก.ฝอก.	นายอนุกูล แหลมปัญญา	081-7121248
นางสาววรนันท์ จันทร์ดนู	095-4596051	หัวหน้าทีมบริหารความต่อเนื่อง ฝบง.	นายบรรพต ศุขวัฒนะกุล	089-6693769
นายปัณณพัฒน์ จันทร์เจริญสุข	096-1496364	หัวหน้าทีมบริหารความต่อเนื่อง ฝพอ.	นางบุณฑริกา สุดใจนาค	099-1599818
นายอนุพันธ์ เตียไพรัชกูลกิจ	081-4749090	หัวหน้าทีมบริหารความต่อเนื่อง ฝวศ.	น.ส.ศุทธวดี ศิริยานนท์	093-3241988
นายอธิรักษ์ บุพจันโท	063-2035762	หัวหน้าทีมบริหารความต่อเนื่อง ฝจส.1	นายรัฐวุฒิ ทับทอง	081-8349880
นายอนุพันธ์ เตียไพรัชกูลกิจ	081-4749090	หัวหน้าทีมบริหารความต่อเนื่อง รก.ฝจส.2	น.ส.ศิริวรรณ ลิมป์รุ่งรัตนา	081-3767696

กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารความต่อเนื่องและทีมงานบริหารความต่อเนื่องที่เกี่ยวข้องตามผังรายชื่อทางโทรศัพท์ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อพนักงานภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตขององค์การจัดการน้ำเสีย จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากหัวหน้าคณะบริหารความต่อเนื่องแจ้งให้ผู้ประสานงานคณะบริหารความต่อเนื่อง โดยผู้ประสานงานฯ จะแจ้งให้หัวหน้าทีมบริหารความต่อเนื่องรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่องตามสายงานการบังคับบัญชาของแต่ละสายงาน หัวหน้าทีมบริหารความต่อเนื่องแต่ละท่านจึงติดต่อและแจ้งไปยังบุคลากรภายใต้การบังคับบัญชาของตนรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่องขององค์การจัดการน้ำเสียที่ได้รับผลกระทบตามรายชื่อและช่องทางติดต่อสื่อสารที่ได้ระบุในตารางที่ 3

ในกรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา :

1. ถ้าเหตุการณ์เกิดขึ้นในเวลาทำการให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของหน่วยงานเป็นช่องทางแรก
2. ถ้าเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
3. ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบดังต่อไปนี้ :

3.1. สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง

3.2. เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนขององค์การจัดการน้ำเสียสำหรับผู้บริหารขององค์การจัดการน้ำเสียและทีมงานบริหารความต่อเนื่อง

3.3. ขั้นตอนการปฏิบัติงานเพื่อบริหารความต่อเนื่องต่อไป เช่น สถานที่รวมพลในกรณีที่มีการย้ายสถานที่ทำการ

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าหน่วยงาน มีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่อง เพื่อรวบรวมสรุปความพร้อมของหน่วยงานในการบริหารความต่อเนื่อง รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยงานและเจ้าหน้าที่ทั้งหมดในหน่วยงาน ทีมบริหารความต่อเนื่องมีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อพนักงานภายในหน่วยงาน

สามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนความต่อเนื่อง

กลยุทธ์ความต่อเนื่อง Business Continuity Strategy (BCS)

การกำหนดกลยุทธ์หรือแนวทางในการสร้างความต่อเนื่องของการปฏิบัติงานซึ่งเป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งทรัพยากรที่ต้องเตรียมพร้อมมี 5 ด้าน ไดแก่

1. ด้านอาคาร/สถานที่ปฏิบัติงานหลัก
2. ด้านวัสดุอุปกรณ์ที่สำคัญ
3. ด้านระบบสารสนเทศและเทคโนโลยีที่สำคัญ
4. ด้านบุคลากร
5. ด้านคู่ค้า ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย

โดยมีขั้นตอนในการกำหนดกลยุทธ์ ตามตารางที่ 4 ดังนี้

ตารางที่ 4 การกำหนดทรัพยากรสำคัญที่ใช้ในการดำเนินงานและการให้บริการ

กระบวนการ	การกำหนดทรัพยากรที่สำคัญ				
	อาคาร/สถานที่ปฏิบัติงานหลัก	เครื่องมือและอุปกรณ์	ระบบสารสนเทศและเทคโนโลยีที่สำคัญ	บุคลากร	คู่ค้า ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย
งานสารบรรณและธุรการทั่วไป	ใช้พื้นที่สำรอง 10 ตรม. (5 คน)	เครื่องคอมฯ พร้อมเครื่องพิมพ์ 1 ชุด	- ระบบจัดซื้อจัดจ้าง - ระบบเชื่อมโยงอินเทอร์เน็ต	บุคลากรหลัก 5 คน	ผู้ให้บริการเชื่อมโยงระบบเครือข่ายอินเทอร์เน็ต*
งานด้านการเงินบัญชี วัสดุครุภัณฑ์ การบริหารบุคคล	ใช้พื้นที่สำรอง 10 ตรม. (5 คน)	เครื่องคอมฯ พร้อมเครื่องพิมพ์ 1 ชุด	- ระบบบัญชีการเงิน ครุภัณฑ์และบริหารบุคคล - ระบบเชื่อมโยงอินเทอร์เน็ต	บุคลากรหลัก 5 คน	ผู้ให้บริการเชื่อมโยงระบบเครือข่ายอินเทอร์เน็ต*

กระบวนการ	การกำหนดทรัพยากรที่สำคัญ				
	อาคาร/ สถานที่ ปฏิบัติงาน หลัก	**เครื่องมือและ อุปกรณ์**	**ระบบสารสนเทศ และเทคโนโลยีที่ สำคัญ**	**บุคลากร**	**คู่ค้า ผู้ให้บริการที่ สำคัญ/ผู้มีส่วนได้ ส่วนเสีย**
งานจัดทำแผนงาน งบประมาณ ควบคุมและ ตรวจสอบภายใน และเร่งรัดติดตาม การประเมินผล ปฏิบัติงาน	ใช้พื้นที่สำรอง 10 ตรม. (5 คน)	เครื่องคอมฯ พร้อมเครื่อง พิมพ์ 1 ชุด	- ระบบตรวจสอบ ภายใน - ระบบเชื่อมโยง อินเทอร์เน็ต	บุคลากร หลัก 5 คน	ผู้ให้บริการเชื่อมโยง ระบบเครือข่าย อินเทอร์เน็ต*

ตารางที่ 5 กลยุทธ์ความต่อเนื่อง Business Continuity Strategy (BCS)

ทรัพยากร		กลยุทธ์ความต่อเนื่องทางธุรกิจ
	อาคาร/สถานที่ปฏิบัติงาน หลัก	- กำหนดให้ใช้พื้นที่ปฏิบัติงานสำรอง คือ สำนักงานจัดการน้ำเสียสาขา โดยมีการสำรวจความเหมาะสมของสถานที่ ประสานงาน และการเตรียมความพร้อม - กรณีที่เกิดความเสียหายกับพื้นที่ ปฏิบัติงานสำรองในขณะนั้น ให้เช่าสถานที่ของเอกชนเป็นสถานที่ ปฏิบัติงานสำรอง
	วัสดุอุปกรณ์ที่สำคัญ/การ จัดหาจัดส่งวัสดุอุปกรณ์ที่ สำคัญ	- กำหนดให้มีการจัดหาคอมพิวเตอร์ สำรองที่มีคุณลักษณะ เหมาะสมกับการ ใช้งาน พร้อมอุปกรณ์ที่สามารถ เชื่อมโยงต่อผ่านอินเทอร์เน็ตเข้าสู่ระบบ เทคโนโลยีของ อจน. ได้ - กำหนดให้ใช้คอมพิวเตอร์แบบพกพา (Laptop/Notebook) ของเจ้าหน้าที่

ทรัพยากร		กลยุทธ์ความต่อเนื่องทางธุรกิจ
		ของหน่วยงานได้เป็นการชั่วคราว หากมีความจำเป็นเร่งด่วนในช่วงระหว่างการจัดหาคอมพิวเตอร์สำรอง ทั้งนี้ ต้องได้รับอนุญาตจากหัวหน้าคณะบริหารความต่อเนื่อง ในการกอบกู้คืนก่อน
	เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	- เนื่องจากระบบการบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของ อจน. มีลักษณะแบบรวมศูนย์และเชื่อมโยงระบบเครือข่ายต่อผ่านระบบอินเทอร์เน็ต ดังนั้นหากเกิดภาวะฉุกเฉินต้องรอจนกว่าระบบการบริหารเทคโนโลยีสารสนเทศ สำรองของ อจน. จะกอบกู้ให้สามารถใช้งานได้ -ประสานงานกับสำนักงานรัฐบาลอิเล็กทรอนิกส์แห่งชาติ ขอติดตั้ง/ใช้บริการเครื่องแม่ข่ายสำหรับเก็บข้อมูลระบบสารสนเทศของ อจน. ในแต่ละระบบ ทั้งนี้เพื่อไม่ให้เกิดความเสียหายต่อข้อมูลที่มีความสำคัญของ อจน. - ดำเนินการบันทึกข้อมูลด้วยระบบมือไปก่อน แล้วจึงบันทึก ข้อมูลด้วยระบบการบริหารเทคโนโลยีสารสนเทศ
	บุคลากรหลัก	- กำหนดให้ใช้บุคลากรสำรอง / ทดแทนภายในหน่วยงาน ฝ่ายงานหรือกลุ่มงานเดียวกัน

ทรัพยากร		กลยุทธ์ความต่อเนื่องทางธุรกิจ
	คู่ค้า ผู้ให้บริการที่สำคัญ	- การไฟฟ้านครหลวงเป็นผู้ดูแลรับผิดชอบในการจำหน่ายไฟฟ้า และเจ้าหน้าที่ของ อจน. มีความพร้อมที่จะดำเนินการปรับปรุงระบบไฟฟ้าได้เอง หรือสามารถขอการสนับสนุนจาก การไฟฟ้านครหลวงได้ภายใน 24 ชั่วโมง - การประปานครหลวงเป็นผู้ดูแลรับผิดชอบในการจำหน่ายน้ำประปา และเจ้าหน้าที่ของ อจน. มีความพร้อมที่จะดำเนินการปรับปรุงระบบประปาได้เองภายในเวลา 1 ชั่วโมง - ระบบเทคโนโลยีสารสนเทศของ อจน. ใช้บริการเชื่อมโยงระบบเครือข่ายอินเทอร์เน็ตของบริษัทภายนอกซึ่งในกรณีที่เกิดภาวะวิกฤตกับตัวอาคารและส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศของ อจน. หรือต้องย้ายอาคารปฏิบัติงาน เมื่อประสานทางบริษัทจะสามารถเชื่อมโยงระบบเครือข่ายอินเทอร์เน็ตใหม่ได้ในเวลา 24 ชั่วโมง

ผลกระทบทางธุรกิจ Business Impact Analysis (BIA)

ในการวิเคราะห์ผลกระทบทางธุรกิจ Business Impact Analysis (BIA) ของ อจน. พบว่ากระบวนการหลักส่วนใหญ่มีความสำคัญและจำเป็นต้องดำเนินงานให้บริการได้ภายในระยะเวลาอันสั้น อันประกอบด้วย

ตารางที่ 6 ผลกระทบทางธุรกิจ Business Impact Analysis (BIA)

กระบวนการ	ระดับความเร่งด่วน	ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ					
		0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
ดำเนินการเกี่ยวกับงานสารบรรณและธุรการทั่วไป	สูง		✓	✓	✓	✓	✓
ดำเนินงานเกี่ยวกับงานด้านการเงิน บัญชี วัสดุ ครุภัณฑ์ การบริหารบุคคล	ปานกลาง			✓	✓	✓	✓
ดำเนินงานเกี่ยวกับการจัดทำแผนงาน งบประมาณ ควบคุมและตรวจสอบภายในและเร่งรัดติดตามการประเมินผลปฏิบัติงาน	ต่ำ						✓

สำหรับกระบวนการอื่นๆ ที่ประเมินแล้วอาจไม่ได้รับผลกระทบในระดับสูงถึงสูงมาก หรือมีความยืดหยุ่น ให้สามารถชะลอการดำเนินงานและให้บริการได้ ให้ผู้บริหารของฝ่ายงานหรือกลุ่มงานประเมินความจำเป็นและเหมาะสม ทั้งนี้หากมีความจำเป็นให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกันกับกระบวนการหลัก

การวิเคราะห์เพื่อกำหนดความต้องการทรัพยากรที่สำคัญ

1. ด้านสถานที่ปฏิบัติงานสำรอง (Working Space Requirement)

ตารางที่ 7 การระบุพื้นที่การปฏิบัติงานสำรอง

ประเภททรัพยากร	สถานที่/แหล่งที่มา	0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
พื้นที่สำหรับปฏิบัติงานสำรอง	สำนักงานจัดการน้ำเสียสาขาจังหวัดใกล้เคียง	60 ตร.ม. (30 คน)	60 ตร.ม. (30 คน)	100 ตร.ม. (50 คน)	200 ตร.ม. (100 คน)	200 ตร.ม. (100 คน)	200 ตร.ม. (100 คน)
	เช่าพื้นที่สำนักงานเอกชน				30 ตร.ม. (10 คน)	30 ตร.ม. (20 คน)	30 ตร.ม. (30 คน)
รวม		60 ตร.ม. (30 คน)	60 ตร.ม. (30 คน)	100 ตร.ม. (50 คน)	230 ตร.ม. (110 คน)	230 ตร.ม. (120 คน)	230 ตร.ม. (130 คน)

2. ด้านวัสดุอุปกรณ์ (Equipment & Supplies Requirement)

ตารางที่ 8 การระบุจำนวนวัสดุอุปกรณ์

ประเภททรัพยากร	สถานที่/แหล่งที่มา	0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
คอมพิวเตอร์สำรองที่มีคุณลักษณะเหมาะสม	ร้านค้าผ่านกระบวนการจัดซื้อพิเศษ		2 เครื่อง	2 เครื่อง	4 เครื่อง	8 เครื่อง	10 เครื่อง
ระบบจัดซื้อจัดจ้าง	เจ้าหน้าที่ฝ่ายฯ ที่เก็บรักษา		1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง
ระบบงานบัญชีการเงิน	เจ้าหน้าที่ฝ่ายฯที่เก็บรักษา		1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง
เครื่องพิมพ์รองรับการใช้งานกับเครื่องคอมพิวเตอร์	ร้านค้าผ่านกระบวนการจัดซื้อพิเศษ		1 เครื่อง	2 เครื่อง	2 เครื่อง	3 เครื่อง	3 เครื่อง
โทรศัพท์พร้อมหมายเลข	ร้านค้าผ่านกระบวนการจัดซื้อพิเศษ		1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง
โทรสารพร้อมหมายเลข	ร้านค้าผ่านกระบวนการจัดซื้อพิเศษ		1 เครื่อง	1 เครื่อง	2 เครื่อง	2 เครื่อง	3 เครื่อง
เครื่องถ่ายเอกสาร	ร้านค้าผ่านกระบวนการจัดซื้อพิเศษ		1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง
รวม			8 เครื่อง	9 เครื่อง	12 เครื่อง	17 เครื่อง	20 เครื่อง

3. ด้านเทคโนโลยีสารสนเทศและข้อมูล (IT & Information Requirement)

เนื่องจากระบบการบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยงานอยู่ในความดูแลของสำนักงานพัฒนารัฐบาลดิจิทัล (สพร.) ดังนั้นหน่วยงานจึงสามารถใช้ข้อมูลสารสนเทศสำรองได้ภายหลังการเชื่อมต่อระบบการบริหารเทคโนโลยีสารสนเทศสำรองแล้วเสร็จภายในเวลา 24 ชั่วโมง

ตารางที่ 9 การระบุความต้องการด้านเทคโนโลยี

ประเภททรัพยากร	สถานที่/แหล่งที่มา	0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
E-mail	หน่วยงาน IT ของ สรอ.	✓	✓	✓	✓	✓	✓
ระบบจัดซื้อจัดจ้าง	หน่วยงาน IT ของ สรอ.	✓	✓	✓	✓	✓	✓
ระบบงานบัญชี การเงิน และ บริหารงานบุคคล	หน่วยงาน IT ของ สรอ.	✓	✓	✓	✓	✓	✓
หนังสือสั่งการต่างๆ ออกโดยหน่วยงาน	หน่วยงานต้นสังกัด			✓	✓	✓	✓
เอกสารใบแจ้งหนี้	คู่ค้า				✓	✓	✓
ข้อมูลการจัดทำแผนงบประมาณ ประจำปีงบประมาณ	หน่วยงานต่างๆ ของ อจน. และสำนักงานสาขา						✓ (เร่งด่วนช่วงเดือน (ก.ค.)

4. ด้านบุคลากรสำหรับความต่อเนื่องเพื่อปฏิบัติงาน (Personnel Requirement)

ตารางที่ 10 การระบุจำนวนบุคลากรหลักที่จำเป็น

ประเภททรัพยากร	0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
จำนวนบุคลากรปฏิบัติงานที่สำนักงาน/สถานที่ปฏิบัติงานสำรอง	4 คน	6 คน	10 คน	30 คน	40 คน	50 คน
จำนวนบุคลากรปฏิบัติงานที่บ้าน	40 คน	25 คน	15 คน	5 คน	-	-
รวม	44 คน	31 คน	25 คน	35 คน	40 คน	50 คน

5. ด้านผู้ให้บริการที่สำคัญ (Service Requirement)

ตารางที่ 11 การระบุจำนวนผู้ให้บริการที่ต้องการติดต่อหรือขอรับบริการ

ประเภททรัพยากร	0-2 ชั่วโมง	2-4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
ผู้ให้บริการเชื่อมโยงระบบเครือข่ายอินเทอร์เน็ต*		2 คน	2 คน	2 คน	2 คน	2 คน
รวม		2 คน	2 คน	2 คน	2 คน	2 คน

หมายเหตุ ให้จัดหาอุปกรณ์เชื่อมโยงระบบเครือข่ายต่อผ่านอินเทอร์เน็ต แบบพกพา (Air Card) ของผู้ให้บริการโทรศัพท์มือถือ เชื่อมโยงการบริหารเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญของหน่วยงานกลางผ่านอินเทอร์เน็ต ในกรณีผู้ให้บริการหลักและสำรองไม่สามารถให้บริการได้ภายในระยะเวลาที่กำหนด

บทที่ 3

ขั้นตอนการดำเนินงานใช้แผนบริหารความต่อเนื่อง

แผนปฏิบัติการเพื่อบริหารความต่อเนื่องขององค์การจัดการน้ำเสีย

ลำดับที่	กิจกรรมหลัก	กลุ่มเป้าหมาย/รายละเอียด	ผู้รับผิดชอบหลัก
1	คัดเลือกสถานที่ที่เหมาะสม	กำหนดสถานที่ที่เหมาะสมในการเป็นศูนย์ปฏิบัติการใน มท. และสำนักงานจัดการน้ำเสียสาขา	กกล. / กปง.1 และ กปง.2
2	เตรียมความพร้อมด้านสถานที่	- จัดหาสถานที่ทำงานสำรอง - จัดหาที่พักสำหรับผู้บริหารและเจ้าหน้าที่ที่จะไปปฏิบัติงาน จำนวนไม่เกิน 100 คน - จัดเตรียมความพร้อมด้านสารสนเทศและการสื่อสาร - จัดเตรียมระบบส่งกำลังบำรุง เช่น อาหาร รถที่จะใช้ใน มท. และการอำนวยความสะดวกอื่นๆ	กกล. / กปง.1 และ กปง.2 กกล. กสป. รผอ.อจน.(บร.)/กพบ.
3	สำรวจความพร้อมของสถานที่	ดำเนินการสำรวจความพร้อมของสถานที่ปฏิบัติงานสำรอง	สผอ. / ฝจส.1 และ ฝจส.2
4	กำหนดและจัดทำรายชื่อผู้ที่จะต้องไปปฏิบัติงาน ณ สถานที่สำรอง และเตรียมงบประมาณสำหรับค่าใช้จ่ายต่างๆ	- กำหนดกลุ่มเป้าหมายที่จะต้องไปปฏิบัติงาน ณ สถานที่สำรอง - ประสานและรวบรวมรายชื่อเจ้าหน้าที่ - จัดทำแผนและเตรียมงบประมาณ	รผอ.อจน.(บร.) กทบ. กนผ. และ กงป.
5	แจ้งแผนการอพยพให้ผู้เกี่ยวข้องรับทราบและเตรียมตัว	แจ้งใน war room และช่องทางต่างๆ ให้เจ้าหน้าที่ที่เกี่ยวข้องรับทราบและเตรียมตัวให้พร้อม	รผอ. อจน.(วผ.)
6	เตรียมการรองรับผู้ติดตามและครอบครัวของเจ้าหน้าที่	- สำรวจและเตรียมอำนวยความสะดวกให้ผู้ติดตามและครอบครัวของเจ้าหน้าที่	กปส. และ กธค.
7	เตรียมความพร้อมด้านการเดินทางไป มท.	จัดรถ/เรือ/ประสานขอรับการสนับสนุนพาหนะตามความเหมาะสมกับสถานการณ์	กพบ.

ลำดับที่	กิจกรรมหลัก	กลุ่มเป้าหมาย/รายละเอียด	ผู้รับผิดชอบหลัก
8	ประกาศย้ายศูนย์และเริ่มอพยพเมื่อมีความจำเป็น	ประกาศให้เจ้าหน้าที่ทุกคนทราบและเริ่มอพยพตามแผน	กกล.
9	แจ้งแนวทางการปฏิบัติงานใน อจน. ให้เจ้าหน้าที่ทุกท่านทราบ	แจ้งให้เจ้าหน้าที่ของ อจน. ทุกท่าน ทั้งส่วนกลางและภูมิภาค รวมทั้งกระทรวง มท. และสถานที่ปฏิบัติงานสำรองของสาขาได้ทราบ เพื่อการปฏิบัติงานและประสานงานได้อย่างราบรื่น	กกล.

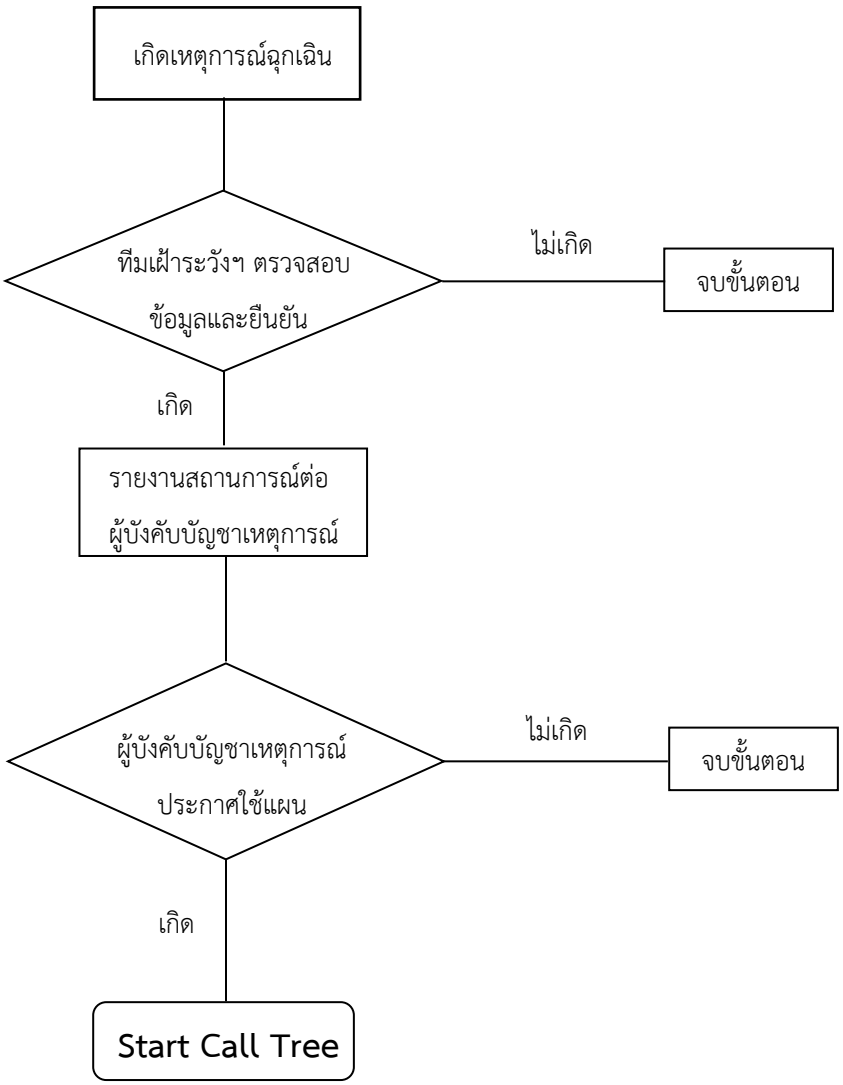
โดยที่ อจน. มอบผู้รับผิดชอบสำนักผู้อำนวยการ เป็นผู้แจ้งจุดนัดพบให้กับบุคลากรทราบ โดยโทรศัพท์ตามผังการสื่อสาร Call Tree และ SMS ให้บุคลากรทุกคนทราบ หรืออาจเปลี่ยนแปลงได้ตามความเหมาะสม

ข้อแนะนำสำหรับผู้ที่ต้องไปปฏิบัติงาน ณ สถานที่ปฏิบัติงานสำรองทั้งส่วนกลางและภูมิภาค

1. ฟังคำสั่งการแจ้งแผนอพยพจาก อจน. โดย ผอ.อจน. ว่าจะเคลื่อนย้ายเมื่อใดและนัดหมายการอพยพ
2. เตรียมเสื้อผ้า ของใช้ส่วนตัว พร้อมใช้ 7-14 วัน
3. วิธีการเดินทางสามารถใช้รถยนต์ส่วนตัว หากต้องการเดินทางพร้อมคณะ อจน. ได้จัดยานพาหนะไว้รองรับ และรอการนัดหมายการเดินทาง
4. ที่พัก อจน. ได้จัดที่พักไว้ตามที่กระทรวงมหาดไทยกำหนด
5. อจน. จัดเตรียมอาหารไว้ทั้ง 3 มื้อ ณ สถานปฏิบัติงาน
6. อจน. จัดทำคำสั่งให้ไปปฏิบัติราชการนอกพื้นที่ และสามารถเบิกค่าใช้จ่ายในการเดินทางไปราชการกับ อจน. ได้
7. เตรียมอุปกรณ์สื่อสาร/Notebook ส่วนตัวนำไปด้วย และทาง อจน.จะจัดเตรียมให้จำนวนหนึ่งสำหรับการใช้งาน
8. สำหรับผู้ที่มีความจำเป็นต้องนำครอบครัวไปด้วย อจน. จะจัดที่พักให้สำหรับครอบครัว (แต่อาจทำได้อย่างจำกัด)
9. คาดว่า อจน. จะปฏิบัติงานนอกสถานที่ประมาณ 1-2 อาทิตย์และจะกลับมาปฏิบัติงานที่ อจน. โดยเร็วที่สุด เมื่อสถานการณ์เข้าสู่ภาวะปกติ

ระบุขั้นตอนของเหตุการณ์หรือภัยเพื่อประกาศใช้แผน

วิธีประกาศใช้แผน



ขั้นตอนการดำเนินงานใช้แผน BCP (Plan Activation)

การเฝ้าระวังก่อนเกิดเหตุ : เพื่อลดความเสี่ยง/ผลกระทบ ในการเกิดเหตุการณ์ภัยพิบัติให้กับหน่วยงานต่างๆ ในองค์กร

ระยะเหตุการณ์	ประเด็นในแผน	ผู้รับผิดชอบหลักและรอง
ก่อนเกิดเหตุ	1. การเตรียมการป้องกัน • สถานที่ • ระบบงาน • ข้อมูลและเอกสารสำคัญต่างๆ • อุปกรณ์ เครื่องมือ	หน่วยงานต่างๆ
	2. สถานที่เก็บและตำแหน่งที่ตั้งของวัสดุอุปกรณ์ที่ใช้ในการป้องกันความเสียหาย	สผอ.
	3. การระบุสถานที่ที่เป็นอันตรายต่างๆ ในองค์กร	หน่วยงานต่างๆ
	4. การมอบหมายหน้าที่ให้แต่ละหน่วยงาน • หน่วยงานประเมินสถานการณ์ • หน่วยงานปฏิบัติหน้าที่ป้องกัน • หน่วยงานสื่อสารและประชาสัมพันธ์	รผอ.อจน.(ปก.) รผอ.อจน.(วผ.) รผอ.อจน.(บร.)
	5. หน่วยงานภายในและภายนอกองค์กร ที่ให้การช่วยเหลือและเตือนภัย • ภารกิจที่ช่วยเหลือ • หมายเลขโทรศัพท์ที่ติดต่อได้	กกล. และ กทบ.
	6. การทดสอบแผนป้องกัน • หน่วยงานที่รับผิดชอบ • ความถี่/ช่วงเวลาในการทดสอบ • วิธีปฏิบัติ	กกล./กพบ./กสป. และ กมว.

ระยะเหตุการณ์	ประเด็นในแผน	ผู้รับผิดชอบหลักและรอง
ก่อนเกิดเหตุ	7. การบำรุงรักษาแผน ● หน่วยงานที่รับผิดชอบ	กสป.
	8. การกำหนดสถานการณ์ที่ต้องดำเนินการทบทวนแผนป้องกัน ● การเปลี่ยนแปลงเกี่ยวกับสถานที่ทำงาน ● การเปลี่ยนแปลงเกี่ยวกับระบบงาน ● การเปลี่ยนแปลงเกี่ยวกับขั้นตอนการปฏิบัติงาน ● การเปลี่ยนแปลงเกี่ยวกับโครงสร้างองค์กร	ผอ.อจน. รผอ.อจน.(บร.) รผอ.อจน.(ปก.) รผอ.อจน.(วผ.)
	9. ทีมงานสำหรับการประสานงานกลาง ● ทีมประเมินความเสียหาย ● ทีมขนย้ายทรัพย์สิน ● ทีมสื่อสารประชาสัมพันธ์ข่าวสาร	กกล./กกม./กพบ./กสป./กปง. และ กสป.

ขณะเกิดเหตุ : เพื่อช่วยลดผลกระทบด้านภารกิจ ชื่อเสียง การเงินและมิใช่การเงิน เป็นต้น

ระยะเหตุการณ์	ประเด็นในแผน	ผู้รับผิดชอบหลักและรอง
ขณะเกิดเหตุ	1. การระบุแผนผังแสดงที่ตั้ง อุปกรณ์ และเส้นทางคมนาคมต่างๆ ● ทางคมนาคมที่เกี่ยวข้องกับการบรรเทาขณะเกิดภัย ได้แก่ ทางเข้า-ออก ที่ใช้ในการหนีภัย ● ที่ตั้งอุปกรณ์ในการบรรเทาขณะเกิดภัย	กกล./กพบ./กปง.1/ กปง.2 และ กสป.
	2. การสื่อสารและรหัสสัญญาณที่ใช้ในการเตือนภัย	กปส. / กปง.1 และ กปง.2
	3. รายละเอียดเกี่ยวกับสถานที่และที่ตั้งของศูนย์อพยพ	กกล. และ กปส.
	4. การมอบหมายหน้าที่ให้แต่ละหน่วยงาน ● หน่วยงานส่งกำลังบำรุง ● หน่วยงานสื่อสารและประชาสัมพันธ์	รผอ.อจน.(บร.) รผอ.อจน.(ปก.)
	5. หน่วยงานภายในและภายนอกองค์กร ที่ให้การช่วยเหลือและเตือนภัย ● ภารกิจที่ช่วยเหลือ ● หมายเลขโทรศัพท์ที่ติดต่อได้	กกล. และ กทบ.
	6. การทดสอบและบรรเทาขณะเกิดภัย	กกล./กพบ./กสป. และ กมว.
	7. การบำรุงรักษาแผน	กสป.

ฟื้นฟูหลังเกิดภัย : เพื่อช่วยให้องค์กรสามารถกอบกู้กระบวนการภารกิจสำคัญให้กลับมาดำเนินการได้

ระยะเหตุการณ์	ประเด็นในแผน	ผู้รับผิดชอบหลักและรอง
หลังเกิดเหตุ	1. เครื่องมือที่จำเป็นต่อการปฏิบัติงาน • สถานที่ปฏิบัติงานสำรอง • อุปกรณ์ที่จำเป็นต่อการปฏิบัติงาน • ข้อมูล • เอกสารต่างๆ • เครื่องใช้งานที่จำเป็น • งบประมาณ	หน่วยงานต่างๆ
	2. กระบวนการปฏิบัติงาน	หน่วยงานต่างๆ
	3. การมอบหมายหน้าที่ให้แต่ละหน่วยงาน • หน่วยงานประเมินความเสียหาย • หน่วยงานปฏิบัติการฟื้นฟู • หน่วยงานสื่อสาร และประชาสัมพันธ์	รผอ.อจน.(บร.) รผอ.อจน.(วผ.) รผอ.อจน.(ปก.)
	4. หน่วยงานภายในและภายนอกองค์กร ที่ให้การช่วยเหลือและเตือนภัย • ภารกิจที่ช่วยเหลือ • หมายเลขโทรศัพท์ที่ติดต่อได้	กกล. และ กทบ.
	5. การทดสอบและฟื้นฟูหลังเกิดภัย	หน่วยงานต่างๆ
	6. การบำรุงรักษาแผน	กสป.

ขั้นตอนการปฏิบัติ	แนวทางปฏิบัติ	ผู้รับผิดชอบ
1. ก่อนเกิดเหตุ	1.1 ติดตามข้อมูลข่าวสารจากเหตุการณ์ที่เกิดขึ้น 1.2 หน่วยงานที่รับผิดชอบและเตรียมการแก้ไขปัญหา 1.3 จัดเตรียมกำลังเจ้าหน้าที่ บุคลากร อุปกรณ์ เครื่องมือ เครื่องใช้ ระบบการสื่อสาร ยานพาหนะ 1.4 สื่อสารประชาสัมพันธ์อย่างต่อเนื่อง 1.5 รวบรวมรายชื่อ ที่อยู่ หมายเลขโทรศัพท์ของผู้ที่รับผิดชอบและประสานงาน เมื่อเกิดเหตุฉุกเฉิน และรายชื่อหน่วยราชการที่เกี่ยวข้อง หมายเลขโทรศัพท์ที่สามารถใช้ในกรณีฉุกเฉิน	
2. ขณะเกิดเหตุ	2.1 ติดต่อประสานงานกับผู้ที่เกี่ยวข้อง ตามหมายเลขโทรศัพท์ฉุกเฉิน รายงานเหตุการณ์ต่อผู้บังคับบัญชาตามลำดับขั้น 2.2 ดำเนินการตามคำสั่งในแผน 2.3 สื่อสารให้เจ้าหน้าที่ บุคลากรได้ทราบและเข้าใจเกี่ยวกับการปฏิบัติตน 2.4 ควบคุม ดูแล ประสานงาน จัดเตรียมพื้นที่สำรองหรือจุดรวมพลที่สามารถตรวจนับบุคลากรของหน่วยงาน เพื่อปฏิบัติงานหากเกิดเหตุฉุกเฉินและประสานงานเพื่อแก้ไขปัญหาที่เกิดขึ้น 2.5 ติดตามผลการแก้ไขปัญหา 2.6 บันทึกเหตุการณ์ การบันทึกข้อมูลที่เกี่ยวข้องกับภาวะฉุกเฉินทั้งหมด ตั้งแต่รายงานเหตุการณ์ การเกิดเหตุ และระหว่างเกิดเหตุ 2.7 การให้ข้อมูลขณะเกิดเหตุภาวะฉุกเฉิน การตอบคำถามขณะเกิดเหตุภาวะฉุกเฉินให้กับสื่อ ผู้ให้ข้อมูล ได้แก่ ผู้บริหารระดับสูง หรือผู้ที่ได้รับมอบหมาย	
3. หลังเกิดเหตุ	3.1 รายงานเหตุการณ์ฉุกเฉินที่เกิดขึ้นขององค์กร ต่อหัวหน้าคณะบริหารความต่อเนื่อง 3.2 หัวหน้าคณะบริหารความต่อเนื่องประกาศยุติแผนฉุกเฉิน	

ผังการติดต่อหน่วยงานฉุกเฉิน

แจ้งเหตุร้าย	หมายเลขโทรศัพท์ฉุกเฉิน
กองปราบปราม	1195
ตำรวจทางหลวง	1193
ไฟฟ้าขัดข้อง	1130
มูลนิธิร่วมกตัญญู	0-2751-0951-3
ศูนย์จราจรอุบัติเหตุ จส.100	1137
สวพ. 91	1644
ศูนย์เตือนภัยพิบัติแห่งชาติ	1860
ศูนย์นเรนทร	1669
สายด่วนกรมทางหลวง	1586
สายด่วนกรมป้องกันและบรรเทาสาธารณภัย	1784
หน่วยแพทย์กู้ชีพ กทม.	1554
เหตุด่วนเหตุร้าย	191
การไฟฟ้าส่วนภูมิภาค	1129
การไฟฟ้านครหลวง	1555, 1130
การประปานครหลวง	1125
การประปาส่วนภูมิภาค	1662
สถานีดับเพลิงและกู้ภัย	199

กระบวนการที่ใช้เพื่อถอนตัวออกเมื่อเหตุการณ์ยุติ

หัวหน้าคณะบริหารความต่อเนื่องและทีมบริหารความต่อเนื่อง เป็นผู้พิจารณาการยุติเหตุการณ์และแจ้งผู้ประสานงานคณะบริหารความต่อเนื่อง เพื่อสั่งการให้คณะทำงานถอนตัวออกจากสถานที่สำรองและบริหารจัดการกับวัสดุอุปกรณ์ต่างๆ ที่ใช้ในสถานที่สำรองตามที่ได้ตกลงกันก่อนที่จะมาปฏิบัติงานยังสถานที่สำรอง โดยครอบคลุมประเด็นดังต่อไปนี้

- การสำรวจความเสียหาย
- การกู้คืน
- การกลับสู่สถานที่ปฏิบัติงานหลัก

คณะบริหารความต่อเนื่องในการเตรียมแผนบริหารความต่อเนื่องในสถานการณ์อุทกภัย พิจารณาความพร้อมกลับสู่สถานปฏิบัติงานหลัก โดยกำหนดบทบาทหน้าที่รับผิดชอบของทีมงานที่เกี่ยวข้อง ดังนี้

1. ทีมยุทธศาสตร์
   - ออกคำสั่งปิดสถานที่ปฏิบัติงานสำรอง และเปิดสถานปฏิบัติงานหลัก
   - ออกคำสั่งให้เจ้าหน้าที่ บุคลากรกลับมาปฏิบัติงานยังสถานที่ปฏิบัติงานหลัก
   - ดำเนินการช่วยเหลือและสงเคราะห์เจ้าหน้าที่ บุคลากร ที่ประสบอุทกภัย
2. ทีมบริหารจัดการ
   - ตรวจสอบความเสียหายและสิ่งอำนวยความสะดวก
   - ดำเนินการซ่อมแซม
   - ทำความสะอาดพื้นที่ทำการ
3. ทีมเทคโนโลยีสารสนเทศ และส่งกำลังบำรุง
   - ดำเนินการกู้คืนระบบงานเทคโนโลยีสารสนเทศทั้งหมด
   - ดำเนินการย้ายการปฏิบัติงานของระบบเทคโนโลยีสารสนเทศมายังสถานที่ปฏิบัติงานหลัก
   - สนับสนุนการกลับมาปฏิบัติงานยังระบบงานหลัก
4. ทีมสื่อสาร
   - จัดเตรียมการสื่อสารประชาสัมพันธ์การกลับมาสู่ภาวะปกติ
   - สื่อสารไปยังบุคลากรและหน่วยงาน/บุคลากรภายนอกเพื่อกลับมาปฏิบัติงานในภาวะปกติ

เจ้าหน้าที่ บุคลากร เมื่อได้รับแจ้งการเหตุการณ์ยุติ ต้องจัดเก็บข้อมูลเพื่อเตรียมการย้ายมาปฏิบัติงานยังสถานที่ปฏิบัติงานหลัก และตรวจสอบความครบถ้วนของระบบ/ข้อมูล/เอกสาร ที่ใช้ปฏิบัติงานจริงกลับมายังสถานที่ปฏิบัติงานหลัก

บทที่ 4

แผนปฏิบัติการในการตอบโต้เหตุการณ์ฉุกเฉิน และการกู้คืนระบบ

ในการตอบโต้เหตุการณ์ฉุกเฉิน และการกู้คืนระบบได้กำหนดแนวทางการปฏิบัติไว้ ดังนี้

หมวด ก : สำหรับทุกสถานการณ์ - การประกาศใช้แผน BCP (Plan Activation)

หมวด ข : ความสูญเสีย/เสียหายต่อสถานที่ทำงาน (รวมถึงการสูญเสีย/เสียหายของเอกสารข้อมูล) (Loss of Workplace covering Loss of Vital Records)

หมวด ค : การสูญเสียบุคลากรสำคัญ (Loss of Key Personnel)

หมวด ง : ความล้มเหลวของระบบไอที (Loss of IT System)

หมวด จ : ผู้ให้บริการที่สำคัญไม่สามารถให้บริการได้ (Failure of Key Dependency)

หมวด ก : สำหรับทุกสถานการณ์ - การประกาศใช้แผน BCP (Plan Activation)

	การดำเนินการ		ขั้นตอนการปฏิบัติการ
	สิ่งที่ต้องทำ	ผู้รับผิดชอบ	
ก่อนเกิดวิกฤติ			
1	ปรับปรุงแผนผังการแจ้งเหตุ (Recall Tree) ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	1. ปรับปรุงแผนผังการแจ้งเหตุให้เป็นปัจจุบัน 2. ส่งสำเนาให้กับหัวหน้าคณะและทีมบริหารความต่อเนื่องทุกครั้งที่มีการปรับปรุงแผนผังการแจ้งเหตุ
2	ปรับปรุงแผนผังการแจ้งเหตุสำหรับบุคคลสนับสนุนการกู้คืนการปฏิบัติงาน (External Support Recall List) ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	ปรับปรุงแผนผังให้เป็นปัจจุบัน และจัดเก็บแผนผังการแจ้งเหตุสำหรับบุคคลภายนอกที่สนับสนุนการกู้คืนการปฏิบัติงาน
เมื่อประกาศใช้แผน BCP			
1	แจ้งบุคลากรที่สำคัญ	ผู้ประสานงาน BCP	โทรศัพท์หาบุคลากรสำคัญตามรายชื่อแจ้งเหตุเพื่อแจ้งการประกาศใช้แผน BCP
2	แจ้งเหตุให้บุคลากรหลักในกระบวนการ/กิจกรรมที่สำคัญเข้าปฏิบัติงานที่ศูนย์ปฏิบัติงานสำรอง	ติดต่อเจ้าหน้าที่ให้ไปปฏิบัติงานที่ศูนย์ปฏิบัติงานสำรอง	แจ้งเหตุให้บุคลากรสำรองทราบเพื่อรองรับในบทบาทที่บุคลากรหลักไม่สามารถทำได้
3	แจ้งผู้จัดเตรียมศูนย์ปฏิบัติงานสำรอง	ผู้ประสานงาน BCP	แจ้งให้ผู้จัดเตรียมศูนย์ปฏิบัติงานสำรองทราบเพื่อให้จัดเตรียมความพร้อมสำหรับใช้ศูนย์ปฏิบัติงานสำรอง
4	แจ้งบุคลากรอื่นๆ ทั่วไปที่ไม่ได้อยู่ในทีมเฉพาะ	ผู้ประสานงาน BCP	แจ้งให้บุคลากรอื่นๆ ที่ไม่ได้อยู่ในทีมเฉพาะทราบเกี่ยวกับสถานการณ์และการตัดสินใจสำหรับการจัดการของหน่วยงาน (เช่น ให้อยู่บ้าน, การจัดสรรพนักงานให้มาทำงาน เป็นต้น)
5	แจ้งบุคลากรสนับสนุนอื่นๆ ที่สำคัญ	ผู้ประสานงาน BCP และหัวหน้าทีมบริหารความต่อเนื่อง	แจ้งบุคลากรสนับสนุนอื่นๆ ที่สำคัญ เพื่อให้ความช่วยเหลือในการกู้คืนธุรกิจ เช่น คู่ค้า ผู้ให้เช่าระบบ suppliers หรือผู้ให้บริการอื่นๆ และผู้รับบริการหลักเป็นต้น

หมวด ข : ความสูญเสีย/เสียหายต่อสถานที่ทำงาน (รวมถึงการสูญเสีย/เสียหายของเอกสารข้อมูล) (Loss of Workplace covering Loss of Vital Records)

	การดำเนินการ		ขั้นตอนการปฏิบัติการ
	สิ่งที่ต้องทำ	ผู้รับผิดชอบ	
ก่อนเกิดวิกฤติ			
1	ปรับปรุงแผน BCP ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	ทบทวนแผน BCP อย่างน้อยเป็นประจำทุกปีเพื่อให้แน่ใจว่าแผนเป็นปัจจุบันอยู่ตลอดเวลา
2	จัดเตรียมศูนย์ปฏิบัติงานสำรอง/ศูนย์สั่งการ	ผู้ประสานงาน BCP	ตรวจสอบการจัดเตรียมศูนย์ปฏิบัติงานสำรองให้มีความพร้อม และอุปกรณ์ที่จำเป็นสำหรับใช้ในการปฏิบัติงานที่สำคัญเป็นเวลาอย่างน้อย 1 สัปดาห์ ขึ้นไปโดยมีหัวหน้าคณะบริหารความต่อเนื่องเป็นผู้สั่งการหรืออาจมีการแต่งตั้งผู้สั่งการแทนก็ได้
3	ดูแลและจัดเก็บเอกสารข้อมูลสำคัญ	หัวหน้าทีมบริหารความต่อเนื่อง	ตรวจสอบว่าได้มีการเก็บเอกสารข้อมูลสำคัญไว้ในที่ปลอดภัยตามระยะเวลาที่กำหนดโดยสม่ำเสมอหรือไม่ เพื่อให้สามารถกู้คืนหรือสร้างเอกสารข้อมูลสำคัญขึ้นมาใหม่ได้
4	มาตรฐานกระบวนการทำงานในช่วงเหตุการณ์ฉุกเฉิน	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่อง	กำหนดมาตรฐานของกระบวนการทำงานในภาวะของเหตุการณ์ฉุกเฉิน คือ • ลดขั้นตอนความซับซ้อนในการปฏิบัติงานลงแต่ต้องแม่นยำและถี่ถ้วนในการปฏิบัติงานมากขึ้น เนื่องจากปริมาณงานในสภาวะเช่นนี้ จะมีข้อราชการไม่มากอาจใช้เวลาต่อหนึ่งเรื่องมากกว่าปกติเพื่อความถูกต้องในการทำงาน • หัวหน้างานหรือผู้ปฏิบัติงานควรเขียนบันทึกการปฏิบัติงาน รายงานผลสรุปที่เกิดขึ้น เช่น ระยะเวลาในการฟื้นคืนระบบ ความขัดข้องระหว่างการปฏิบัติงาน ความไม่เพียงพอในการใช้ทรัพยากรต่างๆ ผลสำเร็จของการปฏิบัติงาน • ติดต่อผู้รับบริการทางโทรศัพท์ตามเบอร์ติดต่อที่ได้จัดทำไว้เพื่อแจ้งสถานที่ปฏิบัติงานใหม่ และเบอร์โทรศัพท์ เบอร์โทรสาร และแจ้งความล่าช้าที่อาจเกิดขึ้นจากระยะเวลาของการฟื้นคืนระบบ

ภายในเวลา 6 ชม. - 2 วัน			
1	แจ้งบุคลากรที่สำคัญ	ผู้ประสานงาน BCP	จัดเตรียมเคลื่อนย้ายไปศูนย์ปฏิบัติการสำรอง
2	เคลื่อนย้ายไปศูนย์ปฏิบัติการสำรอง/ศูนย์สั่งการ	ผู้ประสานงาน BCP/ หัวหน้าทีมบริหารความต่อเนื่อง	เคลื่อนย้ายไปยังศูนย์ปฏิบัติงานสำรอง/ศูนย์สั่งการ อย่างรวดเร็ว (จัดทำแผนที่ตั้งศูนย์ปฏิบัติงานสำรองและเส้นทางการเดินทางเพื่อแจกบุคลากร)
3	จัดตั้งศูนย์ปฏิบัติการสำรอง/ศูนย์สั่งการ	ผู้ประสานงาน BCP/ หัวหน้าทีมบริหารความต่อเนื่อง	● จัดเตรียมสถานที่ อุปกรณ์ ระบบงานที่ต้องใช้ ● ตรวจสอบ ทดสอบอุปกรณ์และระบบงาน IT ที่ต้องใช้ ● ทดสอบการส่งสัญญาณโทรศัพท์และแฟกซ์ที่จำเป็น ● จัดหาบริการสนับสนุนจากหน่วยงานภายในและภายนอก ● จัดทำแผนจัดซื้อจัดจ้างเร่งด่วนตามความสำคัญ ความจำเป็นในการจัดตั้งศูนย์ปฏิบัติงานสำรองและดำเนินการตามแผนฯ
4	การกู้คืนเอกสารข้อมูลสำคัญ	หัวหน้าทีมบริหารความต่อเนื่อง	● เรียกเอกสารข้อมูลสำคัญซึ่งเก็บ หรือจัดทำสำรองไว้ ● สร้างเอกสารข้อมูลสำคัญที่เสียหายขึ้นมาใหม่ ● เปลี่ยนเส้นทางการจัดส่งเอกสารข้อมูลที่สำคัญ ● ตรวจสอบความครบถ้วนสมบูรณ์ของเอกสารข้อมูลสำคัญสำหรับงานที่ทำค้างอยู่ในเวลาที่เกิดเหตุการณ์
5	แจ้งให้ทราบว่ามีบริการใดได้รับผลกระทบ	หัวหน้าคณะบริหารความต่อเนื่องหรือผู้ได้รับแต่งตั้งเป็นหัวหน้าศูนย์สั่งการ	● ประกาศใช้แผนการสื่อสารของหน่วยงาน ● ดำเนินการเพื่อให้แน่ใจว่าผู้ให้บริการ/ผู้ใช้บริการที่สำคัญได้รับแจ้งเรื่องการเปลี่ยนแปลงรายละเอียดการติดต่อบริการที่ยังคงมีอยู่ บริการที่ได้รับผลกระทบ ข้อชี้แจงเพิ่มเติม และทางเลือกที่เป็นไปได้สำหรับบริการที่ได้รับผลกระทบ
6	รายงานต่อผู้บริหาร/ศูนย์สั่งการ	หัวหน้าทีมบริหารความต่อเนื่อง	รวบรวมข้อมูลความเสียหายและสถานการณ์ กู้คืนการปฏิบัติงานล่าสุด เพื่อรายงานต่อศูนย์สั่งการ
ภายในเวลา 1 - 7 วัน			
7	จัดหาอุปกรณ์เครื่องใช้ในการทำงาน	ผู้ประสานงาน BCP	● ประเมินความเพียงพอของอุปกรณ์เครื่องใช้ในการทำงานสำหรับระยะเวลาทำงาน 30 วัน ● ส่งแบบฟอร์มการจัดซื้อให้กับฝ่ายพัสดุและบริการ **หมายเหตุ :** ในการประเมินความเพียงพอดังกล่าว ให้พิจารณารายการที่ต้องจัดเตรียมการสั่งซื้อไว้แล้วในแบบฟอร์มจัดซื้อเพื่อให้สามารถขออนุมัติได้ทันที

หมวด ค : การสูญเสียบุคลากรสำคัญ (Loss of Key Personnel)

	การดำเนินการ		ขั้นตอนการปฏิบัติการ
	สิ่งที่ต้องทำ	ผู้รับผิดชอบ	
ก่อนเกิดวิกฤติ			
1	ปรับปรุงแผน BCP ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	ทบทวนแผน BCP อย่างน้อยเป็นประจำทุกปีเพื่อให้แน่ใจว่าแผนเป็นปัจจุบันอยู่ตลอดเวลา
2	เตรียมบุคลากรสำรอง/มีการสับเปลี่ยนหน้าที่กันเพื่อให้สามารถทำงานแทนกันได้	หัวหน้าทีมบริหารความต่อเนื่อง	จัดให้มีการหมุนเวียนการทำงานของบุคลากรเพื่อการทดแทนกัน มีการสอนงาน/ฝึกอบรมที่จำเป็นเพื่อให้คุ้นเคยกับภารกิจที่สำคัญ กรณีสูญเสียบุคลากรหลัก
ภายในเวลา 1 - 7 วัน			
1	รายงานต่อศูนย์สั่งการ	หัวหน้าคณะบริหารความต่อเนื่องหรือผู้ได้รับแต่งตั้งเป็นหัวหน้าศูนย์สั่งการ	รายงานความเคลื่อนไหวให้ศูนย์สั่งการทราบอย่างต่อเนื่อง
2	สื่อสารให้ทราบถึงบริการที่ได้รับผลกระทบ		● ประกาศใช้แผนการสื่อสารของหน่วยงาน ● ดำเนินการเพื่อให้แน่ใจว่าผู้ให้บริการ/ผู้ใช้บริการที่สำคัญได้รับแจ้งเรื่องการเปลี่ยนแปลงรายละเอียดการติดต่อ บริการที่ยังคงมีอยู่ บริการที่ได้รับผลกระทบ ข้อชี้แจงเพิ่มเติม และทางเลือกที่เป็นไปได้สำหรับบริการที่ได้รับผลกระทบ
3	สั่งการให้บุคลากรสำรองเข้าปฏิบัติงาน		ดำเนินการเพื่อให้บุคลากรสำรองสามารถปฏิบัติงานแทนได้ เช่น สิทธิเข้าถึงอาคารสถานที่ เอกสาร ข้อมูล ระบบ
4	ให้อำนาจอนุมัติและอำนาจการลงนามที่จำเป็นแก่บุคลากรสำรอง		ปรับปรุงเอกสารอำนาจอนุมัติ และอำนาจในการลงนามที่จำเป็นเพื่อให้บุคลากรสำรองมีอำนาจในการดำเนินการ
5	เปลี่ยนสถานที่/ที่อยู่ในการจัดส่งเอกสารข้อมูล	ผู้ประสานงาน BCP และหัวหน้าทีมงานบริหารความต่อเนื่อง	หากบุคลากรสำรองไม่ได้ปฏิบัติงานในสถานที่เดิมของบุคลากรหลัก ให้เปลี่ยนเส้นทางของเอกสาร จดหมายหมายเลขโทรศัพท์ และอื่นๆ ส่งไปยังสถานที่ที่บุคลากรสำรองทำงานอยู่
6	ทำรายการที่หยุดชะงักขณะเกิดเหตุ	หัวหน้าทีมบริหารความต่อเนื่อง	● ตรวจสอบสถานะของรายการที่เพิ่งทำเสร็จ ก่อนที่จะเกิดเหตุการณ์หยุดชะงักและทำรายการที่ยังคงค้างอยู่ให้เสร็จสิ้น
7	พิจารณาจัดสรร/เกลี่ยบุคลากรตามความเหมาะสม	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมงานบริหารความต่อเนื่อง	● ประเมินจำนวนบุคลากรที่เหลืออยู่ ● ประสานงานกับกองการเจ้าหน้าที่จัดสรรบุคลากรที่มีอยู่ให้กับหน่วยที่ขาดแคลนมากตามความเหมาะสมและแต่งตั้งรักษาการแทนกรณีจำเป็น ● แจ้งหัวหน้าหน่วยงานและตัวบุคลากรขอความร่วมมือไปช่วยงานในบทบาทที่ต้องการหรือขาดแคลนมาก

หมวด ง : ความล้มเหลวของระบบไอที (Loss of IT System)

	การดำเนินการ		ขั้นตอนการปฏิบัติการ
	สิ่งที่ต้องทำ	ผู้รับผิดชอบ	
ก่อนเกิดวิกฤติ			
1	ปรับปรุงแผน BCP ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	ทบทวนแผน BCP อย่างน้อยเป็นประจำทุกปีเพื่อให้แน่ใจว่าแผนเป็นปัจจุบันอยู่ตลอดเวลา
2	จัดทำแผนฟื้นฟูจากความเสียหาย (Disaster Recovery Plan : DRP)	หัวหน้าทีมบริหารความต่อเนื่อง	จัดทำแผนฟื้นฟูจากความเสียหายโดยมีหัวข้อ ดังต่อไปนี้ - วัตถุประสงค์ บอกถึงวัตถุประสงค์ของแผนฯ เพื่อเป็นแนวทางในการปฏิบัติเมื่อเกิดขึ้นจริง - ขอบเขต ระบุหน่วยงานหรือหน้าที่ทางธุรกิจและกลุ่มบุคคลที่ต้องนำแผนฯ ไปใช้ได้จริง - บทบาทและความรับผิดชอบ ระบุบทบาทและความรับผิดชอบของบุคลากรในการฟื้นฟูจากความเสียหาย - ระบุทรัพยากรที่ต้องใช้ในการฟื้นฟูการดำเนินงาน - การฝึกอบรม ระบุโปรแกรมการฝึกอบรมที่จำเป็นต่อทุกฝ่ายและจำเป็นต่อผู้ใช้ทุกกลุ่ม - ตารางการทดสอบและฝึกซ้อม จัดตารางการทดสอบแผนฟื้นฟูและการฝึกซ้อมฟื้นฟูการดำเนินงาน - ตารางบำรุงรักษา จัดตารางทบทวนและปรับปรุงข้อมูลในแผนฟื้นฟูเป็นระยะ - ข้อควรระวัง ระบุเรื่องที่ผู้เกี่ยวข้องควรระวังหรือควรให้ความสนใจ เป็นต้น
3	ทบทวนการจัดเตรียมระบบคอมพิวเตอร์ตามแผนฟื้นฟูจากความเสียหาย (DRP)	หัวหน้าทีมบริหารความต่อเนื่อง	ตรวจสอบว่าได้มีการระบุระบบงานที่ต้องใช้สำหรับการปฏิบัติงานสำคัญอย่างครบถ้วน และพิจารณาว่า ● มี DRP พร้อมและเพียงพอ ● มีวิธีการทำงานอื่นที่ไม่ต้องพึ่งพาระบบคอมพิวเตอร์ (workaround procedure) เมื่อเกิดความล้มเหลวของระบบงาน
4	พิจารณาระบบงานที่ DRP ไม่รองรับ	ผู้ประสานงาน BCP	หากระบบงานคอมพิวเตอร์ใดไม่มีแผน DRP รองรับ ให้พิจารณาความจำเป็นและแจ้งเจ้าของระบบงานเพื่อดำเนินการในลำดับต่อไป

ภายในเวลา 4 ชม. - 2 วัน			
1	รายงานต่อศูนย์สั่งการ	ผู้ประสานงาน BCP และหัวหน้าทีมบริหารความต่อเนื่อง	รายงานสถานการณ์ให้ศูนย์สั่งการทราบอย่างต่อเนื่อง
2	สื่อสารให้ทราบถึงบริการที่ได้รับผลกระทบ	หัวหน้าคณะบริหารความต่อเนื่องและหัวหน้าทีมบริหารความต่อเนื่อง	• ประกาศใช้แผนการสื่อสารของหน่วยงาน • ดำเนินการเพื่อให้แน่ใจว่าผู้ให้บริการ/ผู้ใช้บริการที่สำคัญ ได้รับแจ้งเรื่องการเปลี่ยนแปลงรายละเอียดการติดต่อ บริการที่ยังคงมีอยู่ บริการที่ได้รับผลกระทบ ข้อชี้แจงเพิ่มเติม และทางเลือกที่เป็นไปได้สำหรับบริการที่ได้รับผลกระทบ
3	ใช้ขั้นตอนวิธีการทำงานด้วยตัวเองที่ไม่ต้องพึ่งพาระบบ (Manual Work around)	หัวหน้าทีมบริหารความต่อเนื่อง	ใช้ขั้นตอนการทำงานด้วยตัวเองโดยที่ไม่ต้องพึ่งพาระบบ
เมื่อมีการกู้คืนระบบงาน			
1	กู้คืนข้อมูลเมื่อสถานการณกลับสู่ภาวะปกติ	หัวหน้าทีมงานบริหารความต่อเนื่อง	• ตรวจสอบสถานะของข้อมูลที่กู้คืนได้ • สร้างข้อมูลที่เสียหายไปขึ้นมาใหม่ • บันทึกรายการที่เกิดขึ้นระหว่างที่ระบบล้มเหลว และระมัดระวังไม่ให้มีการบันทึกรายการซ้ำหรือขาดไป
2	สื่อสารให้ทราบถึงการบริการที่ได้รับผลกระทบ	หัวหน้าทีมงานบริหารความต่อเนื่อง	• ประกาศใช้แผนการสื่อสารภายของหน่วยงานถ้ามีบริการที่ยังได้รับผลกระทบหลังจากกู้คืนระบบงาน • ดำเนินการเพื่อให้แน่ใจว่าผู้ให้บริการ/ผู้ใช้บริการที่สำคัญได้รับแจ้งเรื่องการเปลี่ยนแปลงรายละเอียดการติดต่อ บริการที่ยังคงมีอยู่ บริการที่ได้รับผลกระทบ ข้อชี้แจงเพิ่มเติม และทางเลือกที่เป็นไปได้สำหรับบริการที่ได้รับผลกระทบ

หมวด จ : ผู้ให้บริการที่สำคัญไม่สามารถให้บริการได้ (Failure of Key Dependency)

	การดำเนินการ		ขั้นตอนการปฏิบัติการ
	สิ่งที่ต้องทำ	ผู้รับผิดชอบ	
ก่อนเกิดวิกฤติ			
1	ปรับปรุงแผน BCP ให้เป็นปัจจุบัน	ผู้ประสานงาน BCP	ทบทวนแผน BCP อย่างน้อยเป็นประจำทุกปีเพื่อให้แน่ใจว่าแผนเป็นปัจจุบันอยู่ตลอดเวลา
2	ทบทวนความพร้อมของการบริหารความต่อเนื่อง (BCM) ของผู้ให้บริการสำคัญ	ผู้รับผิดชอบกระบวนงาน	ทบทวนรายชื่อหน่วยงาน บุคคลของผู้ให้บริการสำคัญ เพื่อให้แน่ใจว่าเป็นปัจจุบัน และสามารถติดต่อ ประสานหรือให้บริการในระดับที่ยอมรับได้ เมื่อเกิดเหตุการณ์หยุดวิกฤต
ภายในเวลา 1 - 3 วัน			
1	สื่อสารให้ทราบถึงการบริการที่ได้รับผลกระทบ	หัวหน้าคณะบริหารความต่อเนื่อง และผู้ประสานงาน BCP	ประกาศใช้แผนการสื่อสารของหน่วยงานเพื่อแจ้งข้อมูลเกี่ยวกับบริการที่ยังคงมีอยู่ บริการที่ได้รับผลกระทบ ข้อชี้แจงหรือเงื่อนไขพิเศษ และทางเลือกที่เป็นไปได้สำหรับบริการที่ได้รับผลกระทบ
2	ใช้ขั้นตอนวิธีการทำงานด้วยตัวเองที่ไม่ต้องพึ่งพาระบบ	หัวหน้าทีมบริหารความต่อเนื่อง	ใช้ขั้นตอนวิธีการทำงานด้วยตัวเองที่ไม่ต้องพึ่งพาระบบ
ภายในเวลา 7 วัน			
3	พิจารณาแนวทาง/ช่องทางต่างๆ ในการติดต่อสื่อสาร/ประสานงาน เพื่อให้การดำเนินการเป็นไปอย่างต่อเนื่อง	หัวหน้าทีมงานบริหารความต่อเนื่อง	• รวบรวมข้อมูลสำคัญ/จำเป็นต่อการใช้ดำเนินการต่อไป • ประสานขอสำเนาข้อมูลกรณีข้อมูลขาดหายไป หรือมีไม่ครบ กรณีระบบยังใช้การไม่ได้ต้องประสานผู้ดูแลระบบนั้น และทำงานตรวจสอบข้อมูล สำรองข้อมูลเพื่อยืนยันความถูกต้อง • ดำเนินการประสานงาน ระบบต่างๆ เพื่อให้ขั้นตอนการปฏิบัติการเข้าสู่ภาวะปกติ

รายงานความคืบหน้าของขั้นตอนการกู้คืนการปฏิบัติงาน

รายงานต่อ	ความถี่/สัญญาณแจ้งเหตุ	หัวข้อรายงาน	ผู้รายงาน
หัวหน้าคณะทำงานบริหารความต่อเนื่องและผู้บริหารสูงสุด	แจงเหตุการณ์ฉุกเฉิน	การติดต่อในสายงานตาม Call Tree เรียบร้อย แจ้งการประกาศใช้แผนฉุกเฉิน	ผู้ประสานงาน BCP
ผู้ประสานงาน BCP	พบกันที่จุดนัดพบ	เจ้าหน้าที่ที่ต้องเข้าปฏิบัติงานระหว่างเหตุการณ์ฉุกเฉินมาถึงจุดนัดพบครบถ้วน	หัวหน้าทีมบริหารความต่อเนื่อง
หัวหน้าทีมบริหารความต่อเนื่อง	การย้ายสถานที่ปฏิบัติงาน	การโยกย้ายสถานที่ปฏิบัติงาน	ทีมกู้คืนการปฏิบัติงานของหน่วยงาน
ผู้ประสานงาน BCP	สถานที่ปฏิบัติงานใหม่	สามารถเข้าสถานที่ปฏิบัติงาน ณ ศูนย์สำรองได้ เจ้าหน้าที่เข้าประจำการครบถ้วน ตรวจสอบเอกสารสำรองและอุปกรณ์ต่างๆ ว่าใช้งานได้ อยู่ระหว่างการรอติดตั้งระบบ	หัวหน้าทีมบริหารความต่อเนื่อง
หัวหน้าทีมบริหารความต่อเนื่อง	ความสัมฤทธิ์ผลของการเชื่อมต่อระบบงานต่างๆ ณ ศูนย์ฏิบัติงานสำรอง	ทุกระบบสามารถ Log-in เข้าระบบใช้งานได้หรือมีข้อขัดข้องประการใด	ทีมกู้คืนการปฏิบัติงานของหน่วยงาน
หัวหน้าทีมบริหารความต่อเนื่อง	Processing รายการ	การเริ่มปฏิบัติงานตามปกติได้	กลุ่ม/ฝ่ายสังกัด สำนัก
หัวหน้าทีมบริหารความต่อเนื่อง	ปัญหาคงค้าง	สรุปการแก้ไขปัญหา หรือปัญหาคงค้างแก่หัวหน้าฝ่ายเป็นระยะๆ	กลุ่ม/ฝ่ายสังกัด สำนัก
หัวหน้าทีมบริหารความต่อเนื่อง	การปิดงานทุกสิ้นวัน	กระบวนการปิดงานทุกสิ้นวัน สรุปงานที่เสร็จสิ้น ปัญหาที่ยังไม่ได้รับการแก้ไข	กลุ่ม/ฝ่ายสังกัด สำนัก
หัวหน้าคณะทำงานบริหารความต่อเนื่องและผู้บริหารสูงสุด	การปฏิบัติงาน ณ ศูนย์สำรอง	สรุปการปฏิบัติงาน ณ ศูนย์สำรองประจำวัน	- ผู้ประสานงาน BCP - หัวหน้าคณะทำงานบริหารความต่อเนื่อง

ขั้นตอนการปฏิบัติงานเพื่อกลับสู่ภาวะปกติ

	ผู้รับผิดชอบ	ขั้นตอนการปฏิบัติการ
ก่อนเกิดวิกฤติ		
1	ผู้ประสานงาน BCP	ปรับปรุงเอกสารเหล่านี้ให้เป็นปัจจุบันและจัดเก็บ : ● ข้อมูลที่จำเป็นสำหรับการฟื้นฟูสถานที่ที่ได้รับความเสียหาย เช่น แผนผัง สถานที่ทำงานของหน่วยงาน (ซึ่งมีรายละเอียดของการวางเฟอร์นิเจอร์และอุปกรณ์ต่างๆ), แผนผังการเดินสายเคเบิ้ล, สายโทรศัพท์ต่างๆ และเงื่อนไขพิเศษ (เช่น ภาพถ่ายสถานที่ทำงานปัจจุบัน แผนผังสถานที่ทำงานปัจจุบัน) เป็นต้น ● รายละเอียดการติดตั้งฮาร์ดแวร์และซอฟแวร์ การสำรองข้อมูลโดยเฉพาะอย่างยิ่งสำหรับระบบที่ไม่มี DRP Server ● เอกสาร/ข้อมูลข่าวสารอื่นๆ ที่จำเป็นสำหรับการฟื้นฟูสถานที่ทำงานที่ได้รับความเสียหายขึ้นมาใหม่ **หมายเหตุ:** ควรมีการเก็บสำเนาข้อมูลปัจจุบันไว้ในระบบกลาง หรือนอกสถานที่หากเกิดเหตุจำเป็นสามารถเรียกมาใช้งานได้
2	ผู้ประสานงาน BCP	ส่งสำเนาข้อมูลไปเก็บไว้นอกสถานที่ทำงานทุกครั้งที่มีการเปลี่ยนแปลง
ภายในเวลา 1 - 7 วัน		
3	หัวหน้าคณะทำงานบริหารความต่อเนื่อง	เรียกข้อมูลที่ต้องใช้ในการนำกลับสู่สภาพเดิม ซึ่งเก็บไว้นอกสถานที่ทำงาน (เช่น แผนผังสถานที่ทำงานหลัก system configuration เอกสารสำคัญต่างๆ)
4	หัวหน้าคณะบริหารความต่อเนื่อง และผู้ประสานงาน BCP	ประชุมคณะทำงานเพื่อวางแผนร่วมกันในเรื่อง : ● การซ่อมแซมและฟื้นฟูสถานที่ทำงานหลักที่เสียหายขึ้นมาใหม่ หรือการเสาะหาและการจัดตั้งสถานที่ทำงานหลักแห่งใหม่ ● จัดซื้อและติดตั้งระบบที่ได้รับความเสียหาย ● กำหนดตารางเวลา/บุคลากรการทำงาน ● เกลี่ยหรือจัดสรรบุคลากรให้เหมาะสมเพื่อทดแทนจำนวนบุคลากรในจุดที่ขาดอยู่
ภายในเวลา 14 วัน		
5	หัวหน้าคณะทำงานบริหารความต่อเนื่อง	ตัดสินใจกลยุทธ์การกลับสู่ภาวะปกติ และระยะเวลา ซึ่งควรประกอบด้วย ● สถานที่ทำงานหลักจะต้องซ่อมแซมหรือย้ายไปยังที่อื่นหรือไม่ ● ควรซื้อระบบ (ฮาร์ดแวร์และซอฟท์แวร์) หรือไม่ ● การจัดสรรบุคลากร/การแต่งตั้งรักษาการ (ตำแหน่ง จำนวนคน อื่นๆ) ● ต้นทุนที่จะเกิดขึ้น

		● กรอบระยะเวลาที่ใช้ในการฟื้นฟูให้กลับสู่ภาวะปกติ
	ผู้รับผิดชอบ	**ขั้นตอนการปฏิบัติการ**
ภายในเวลา 21 วัน		
6	หัวหน้าคณะทำงานบริหารความต่อเนื่อง	● ประชุมคณะทำงานมาวางแผนร่วมกันเพื่อฟื้นฟูให้กลับสู่ภาวะปกติ ● สร้างแบบฟอร์มตรวจสอบ เพื่อช่วยในการระบุงาน หน้าที่ที่จะทำ ระยะเวลาที่ต้องดำเนินการ และผู้รับผิดชอบงาน หน้าที่นี้ควรประกอบด้วย ● การเปลี่ยนเส้นทางของสายโทรศัพท์ ● การจัดตั้งและทดสอบอุปกรณ์ ● ตรวจสอบการกู้คืนข้อมูลขึ้นมาใหม่เพื่อเก็บรักษาข้อมูลให้ถูกต้องและเป็นระเบียบ ● การเตรียมบุคลากรในตำแหน่งสำคัญที่ขาดไป ● การติดต่อสื่อสารกับผู้ให้บริการ/ผู้รับบริการ
7	หัวหน้าคณะทำงานบริหารความต่อเนื่อง	เมื่อจัดทำแผนเรียบร้อยแล้ว สื่อสารให้บุคลากรทราบเกี่ยวกับแผนการกลับสู่ภาวะปกติและตารางเวลาการดำเนินการ
ภายในเวลา 30 วัน		
8	หัวหน้าคณะบริหารความต่อเนื่อง และผู้ประสานงาน BCP	ก่อนที่จะยกเลิกการใช้ศูนย์ปฏิบัติงานสำรอง/ศูนย์สั่งการต้องทดสอบว่ากระบวนการปฏิบัติงานสามารถดำเนินไปได้อย่างดีในสถานที่ทำงานใหม่
9	ผู้ประสานงาน BCP/ หัวหน้าทีม บริหารความต่อเนื่อง	ดำเนินการเปลี่ยนศูนย์ปฏิบัติงานสำรองให้กลับไปอยู่ในสภาพเดิม (Original Condition) ดังนี้ : ● เอาซอฟต์แวร์ที่ได้ติดตั้งไว้ที่ศูนย์สำรองออก ● ตรวจสอบว่าข้อมูลที่มีความอ่อนไหว ได้เอาออกจากฮาร์ดดิสก์และที่เก็บชั่วคราวอื่นๆ เรียบร้อยแล้ว ● ทำลายหรือกำจัดเอกสารต่างๆ และรายงานข้อมูลอื่นๆ ที่ไม่ใช้แล้วออกไป ● ตรวจสอบว่าทรัพยากรทุกอย่างที่ให้ผู้อื่นไปใช้ได้คืนกลับมาในสภาพที่ดี ● ส่งคืนสถานที่
10	หัวหน้าคณะทำงานบริหารความต่อเนื่อง	ดำเนินการยกเลิกสิทธิการเขาถึงอาคารสถานที่ ข้อมูล และอำนาจต่างๆ ที่เคยอนุญาตให้กับบุคลากรชุดสำรอง

ภาคผนวก 1

การปฏิบัติตนกรณีเกิดเหตุภัยพิบัติ

การปฏิบัติตนกรณีเกิดเหตุภัยพิบัติ

ปัจจุบันปัญหาเรื่องภัยพิบัติเป็นสาธารณภัยในประเทศไทยมีแนวโน้มที่จะเกิดขึ้นอย่างต่อเนื่องและรุนแรงมากขึ้น เนื่องจากสภาพแวดล้อมที่เปลี่ยนแปลงไป เช่น ความแปรปรวนของภูมิอากาศความไม่สมดุลของระบบนิเวศน์ ความแปรปรวนของระบบการเมือง เศรษฐกิจ และสังคม จนมีผลกระทบอย่างหลีกเลี่ยงไม่ได้

ดังนั้น เพื่อเป็นการลดความเสี่ยงจากภัยพิบัติของผู้ปฏิบัติงาน อจน. จึงได้จัดทำคู่มือป้องกันกรณีหากเกิดภัยพิบัติ ซึ่งประกอบด้วย วิธีการปฏิบัติตน แผนป้องกันและบรรเทากรณีหากเกิดภัยพิบัติไว้รองรับสถานการณ์และเพื่อเป็นเครื่องมือที่จะช่วยให้การปฏิบัติงานในภาวะฉุกเฉินสามารถดำเนินไปได้อย่างเป็นระบบ มีประสิทธิภาพและเกิดประสิทธิผลสูงสุด

<u>แผนการบรรเทาภัยพิบัติที่เกิดจากวาตภัย</u>

วาตภัย หมายถึง ภัยธรรมชาติซึ่งเกิดจากพายุลมแรงจนทำให้เกิดความเสียหายแก่อาคารบ้านเรือน ต้นไม้ และสิ่งก่อสร้างต่างๆ ที่เกิดขึ้นเป็นบริเวณกว้างจากความแรงของลมที่พัดเวียนเข้าหาจุดศูนย์กลางของพายุ โดยความเสียหายจะมีมากที่สุดบริเวณใกล้แนวศูนย์กลางที่พายุเคลื่อนผ่าน

1. อันตรายที่เกิดจากวาตภัย

เกิดบนบก ต้นไม้ถอนรากถอนโคน ต้นไม้ทับบ้านเรือนพัง ผู้คนได้รับบาดเจ็บถึงตาย เรือกสวนไร่นาเสียหาย บ้านเรือนที่ไม่แข็งแรงไม่สามารถต้านทานความรุนแรงของลมได้พังระเนระนาด หลังคาบ้านที่ทำด้วยสังกะสีจะถูกพัดเปิด กระเบื้องหลังคาปลิวว่อน เสาไฟฟ้า เสาโทรเลข เสาโทรศัพท์ล้ม สายไฟฟ้าขาด ไฟฟ้าลัดวงจร เกิดเพลิงไหม้ ผู้คนที่พักอยู่ริมทะเลจะถูกคลื่นซัดท่วมบ้านเรือนและกวาดลงทะเล ฝนตกหนักมากทั้งวันและทั้งคืน อุทกภัยจะตามมา น้ำป่าจากภูเขาไหลหลากลงมาอย่างรวดเร็วและรุนแรงเกิดน้ำท่วมฉับพลันในบริเวณที่ราบลุ่มเชิงเขา เส้นทางคมนาคม ทางรถไฟ สะพาน และถนนถูกตัดขาด

ในทะเล มีลมพัดแรงจัดมากเกิดคลื่นใหญ่ เรือขนาดใหญ่อาจถูกพัดพาไปเกยฝั่งหรือชนหินโสโครกทำให้จมได้ เรือขนาดเล็กอาจพลิกคว่ำและจมลงเกิดคลื่นใหญ่ซัดฝั่งทำให้ระดับน้ำสูงท่วมอาคารบ้านเรือนบริเวณริมทะเล และอาจกวาดสิ่งก่อสร้างที่ไม่แข็งแรงลงทะเลได้ เรือประมงบริเวณชายฝั่งจะถูกทำลาย

2. ขั้นตอนการปฏิบัติการบรรเทาภัยที่เกิดจากวาตภัย

เป็นการกำหนดหน้าที่ความรับผิดชอบของหน่วยงานในองค์กรที่เกี่ยวข้องเพื่อให้สามารถดำเนินการป้องกันและแก้ไขปัญหาที่เกิดจากวาตภัยได้อย่างรวดเร็วและมีประสิทธิภาพในระยะก่อนเกิดภัย ขณะเกิดภัย และภายหลังที่ภัยได้ผ่านพ้นไปแล้ว

2.1 ขั้นตอนการปฏิบัติก่อนการเกิดวาตภัย

เป็นการดำเนินการเพื่อจัดเตรียมและลดผลกระทบ หรือแก้ไขปัญหาอุปสรรคไว้ล่วงหน้าก่อนที่วาตภัยจะเกิดขึ้น

1. จัดทำแผนป้องกันและบรรเทาวาตภัยรวมทั้งประสานและฝึกซ้อมแผนการบรรเทาวาตภัยกับพนักงานภายในหน่วยงานและสำนักงานสาขาที่เกี่ยวข้อง

2. เฝ้าระวังและเตือนภัย เผยแพร่ให้ความรู้ ประชาสัมพันธ์ เพื่อเป็นการรู้เท่าทันและหลีกเลี่ยงให้พ้นจากภัยธรรมชาติทั้งรูปแบบที่เป็นทางการและไม่เป็นทางการ

3. ตรวจสภาพความปลอดภัยของอาคาร สำนักงาน ประตู หน้าต่าง ช่องทางลม เสาไฟฟ้าและสายไฟฟ้า ทั้งในและนอกบริเวณสำนักงาน โดยปรับปรุงยึดเหนี่ยวให้มั่นคงแข็งแรง

4. ตัดกิ่งไม้หรือริดกิ่งไม้บริเวณสำนักงานที่อาจหักโค่นลงได้จากวาตภัย

5. ติดตั้งสายล่อฟ้าสำหรับอาคารสูง

6. สำรวจอาคาร สถานที่ที่มีความมั่นคงแข็งแรงเพื่อกำหนดเป็นเขตพื้นที่ปลอดภัย รองรับการอพยพของพนักงานในกรณีฉุกเฉิน พร้อมจัดทำแผนที่แสดงบริเวณสถานที่ที่กำหนดเป็นเขตพื้นที่ที่ปลอดภัย

7. ประชาสัมพันธ์และแจ้งข้อมูลหน่วยงานด้านข่าวสาร การแจ้งเตือนและการให้ความช่วยเหลือให้พนักงานรับทราบและเตรียมความพร้อมอพยพเมื่อมีเหตุ เช่น การเตรียมเสบียงอาหาร น้ำดื่ม ยารักษาโรค ไฟฉายและอุปกรณ์ กรณีที่จำเป็นในการเผชิญวาตภัยที่อาจเกิดขึ้น

8. สำรวจจัดทำทะเบียนอุปกรณ์ เครื่องมือ เครื่องใช้ และยานพาหนะที่จำเป็นใช้ในขณะเกิดเหตุ ถ้ามีไม่ครบควรจัดหาเพิ่มเติม

9. สนับสนุนให้มีการปลูกป่าเพื่อบรรเทาความรุนแรงของลมพายุ

2.2 ขั้นตอนการปฏิบัติขณะเกิดวาตภัย

เป็นการดำเนินการในสถานการณ์ฉุกเฉินโดยการระดมทรัพยากรต่างๆ เข้าช่วยเหลือเพื่อรักษาชีวิต ทรัพย์สินและบรรเทาทุกข์แก่พนักงานผู้ประสบภัยตลอดจนลดความรุนแรงของวาตภัยที่เกิดขึ้น

1. ไม่ตื่นตกใจ พยายามควบคุมสติอย่างสงบ และอยู่ในอาคารที่มั่นคงแข็งแรงตลอดเวลาที่เกิดเหตุ ไม่ออกมาในที่โล่งแจ้ง

2. ปิดประตู หน้าต่างทุกบาน รวมทั้งปรับปรุงและปิดกั้นช่องทางลมและช่องทางต่างๆ ที่ลมจะเข้าไปทำให้เกิดความเสียหายได้

3. ตัดสะพานไฟ ปิดวาล์วน้ำและแก๊สหุงต้มให้เรียบร้อย

4. ออกห่างจากวัตถุที่เป็นสื่อไฟฟ้าทุกชนิด เช่น ลวด โลหะ ท่อน้ำ แนวรั้วบ้าน เป็นต้น ไม่ใช้อุปกรณ์ไฟฟ้าทุกชนิด รวมทั้งไม่สวมใส่เครื่องประดับที่เป็นโลหะ

5. ไม่ควรอยู่ในพื้นที่ต่ำ เนื่องจากอาจเกิดน้ำป่าไหลหลากหรือน้ำท่วมฉับพลันหรือแผ่นดินถล่มได้

6. ไม่ใช้เทียน ไม้ขีดไฟ หรือสิ่งที่จะทำให้เกิดเปลวไฟหรือประกายไฟเพราะอาจมีแก๊สรั่วอยู่

7. ติดตามเหตุการณ์และคำเตือนลักษณะอากาศของทางราชการอย่างใกล้ชิด

8. เตรียมพร้อมที่จะอพยพไปในที่ปลอดภัย จัดตั้งศูนย์อำนวยการเฉพาะกิจตามแผนที่กำหนดไว้ เพื่อช่วยเหลือพนักงานผู้ประสบภัยในพื้นที่ที่เกิดภัยและเป็นหน่วยงานในการสั่งการอำนวยการ วางแผน และประสานการปฏิบัติ

9. ประเมินระดับความรุนแรงของวาตภัยที่เกิดขึ้นและรายงานให้หน่วยงานที่เกี่ยวข้อง

10. จัดชุดปฏิบัติการพยาบาลในลักษณะของหน่วยเคลื่อนที่เพื่อให้การช่วยเหลือเบื้องต้นและค้นหาพนักงานผู้ประสบภัยเพื่อทำการปฐมพยาบาลผู้ได้รับบาดเจ็บ ณ จุดที่เกิดเหตุและนำส่งโรงพยาบาล

11. จัดระบบรักษาความปลอดภัยบริเวณที่ได้รับความเสียหายโดยเฉพาะบริเวณอาคารประกาศเป็นเขตควบคุมเพื่อสะดวกต่อการปฏิบัติงานของเจ้าหน้าที่

12. ดำเนินการอพยพเคลื่อนย้ายผู้ประสบภัย รวมทั้งเคลื่อนย้ายทรัพย์สินไปไว้ในพื้นที่ปลอดภัย และจัดให้มีระบบรักษาความปลอดภัยในบริเวณพื้นที่อพยพ

13. ประกาศแนะนำ แจ้งเตือนเกี่ยวกับสถานการณ์ที่เกิดขึ้นและเป็นปัจจุบัน

14. รวบรวมรายงานข้อมูลความเสียหายและการช่วยเหลือ พร้อมทั้งสรุปเหตุการณ์และสถานการณ์เสนอต่อผู้บริหารสูงสุด เพื่อให้ได้รับทราบข้อมูลที่ถูกต้องและเป็นปัจจุบันจนกว่าเหตุการณ์จะยุติ

15. ประสานขอความช่วยเหลือไปยังสำนักงานเขต หรือจังหวัดที่รับผิดชอบพื้นที่จังหวัดนั้นๆ หรือศูนย์ป้องกันและบรรเทาสาธารณภัย เมื่อเกินขีดความสามารถของหน่วยงาน

16. เมื่อจวนตัวให้คำนึงถึงความปลอดภัยของชีวิตมากกว่าทรัพย์สิน

2.3 ขั้นตอนการปฏิบัติหลังเกิดวาตภัย

เป็นการดำเนินการช่วยเหลือพนักงานผู้ประสบภัยจากวาตภัยให้กลับคืนสู่สภาพคงเดิมในช่วงก่อนเหตุการณ์หรือดีกว่าเดิม เพื่อเป็นการสร้างขวัญกำลังใจของพนักงานผู้ประสบภัยให้กลับคืนสู่สภาพปกติ

1. การฟื้นฟูสภาพแวดล้อมชีวิตความเป็นอยู่

- สำรวจความเสียหายและความต้องการด้านต่างๆ ของพนักงานผู้ประสบภัย
- จัดส่งเครื่องอุปโภค บริโภค เวชภัณฑ์ วัสดุอุปกรณ์ที่จำเป็นเข้าไปยังพื้นที่ที่เกิดวาตภัยโดยเร่งด่วนเพื่อสงเคราะห์พนักงานผู้ประสบภัยและรายงานขอรับการสนับสนุนเพิ่มเติมหากสิ่งของที่จัดเตรียมไม่เพียงพอจากหน่วยงานของรัฐและเอกชนทั้งในและนอกพื้นที่ เพื่อให้การสงเคราะห์พนักงานผู้ประสบภัย
- ให้การสงเคราะห์พนักงานผู้ประสบภัย เช่น ด้านที่พัก น้ำอุปโภคบริโภค เพื่อบรรเทาความเดือดร้อนในเบื้องต้น
- ความสะอาด รื้อสิ่งปรักหักพัง ซ่อมแซมสิ่งชำรุดเสียหายให้กลับคืนสู่สภาพปกติโดยเร็ว
- ซ่อมแซมหรือปรับปรุงสิ่งสาธารณประโยชน์และระบบสาธารณูปโภค เช่น การไฟฟ้า ประปา ถนนที่ชำรุดเสียหายให้กลับคืนสู่สภาพเดิมโดยเร็ว
- เฝ้าระวังโรคติดต่อที่อาจเกิดขึ้นได้ เช่น โรคระบบทางเดินหายใจ โรคติดเชื้อและปรสิต โรคฉี่หนู โรคผิวหนัง โรคระบบทางเดินอาหาร รวมทั้งดำเนินการกำจัดของเสียต่างๆ และพาหะนำโรค

2. การฟื้นฟูทางด้านร่างกายและจิตใจของผู้ประสบภัย

○ จัดให้มีบริการรักษาพยาบาลผู้บาดเจ็บ ผู้ป่วย เพื่อรักษาชีวิตผู้ได้รับอันตรายในระยะแรก

○ จัดการประชาสัมพันธ์ เพื่อฟื้นฟูสภาพจิตใจและสร้างความเชื่อมั่นในการให้ความช่วยเหลือของหน่วยงานต่อพนักงานผู้ประสบภัยอย่างเต็มที่และเท่าเทียมกัน

<u>แผนการบรรเทาภัยพิบัติที่เกิดจากอุทกภัย ดินถล่มหรือโคลนถล่ม</u>

อุทกภัย หมายถึง เหตุการณ์ที่มีน้ำท่วมพื้นดินสูงกว่าระดับปกติ ซึ่งมีสาเหตุจากมีปริมาณน้ำฝนมากจนทำให้มีปริมาณน้ำส่วนเกินมาเติมปริมาณน้ำผิวดินที่มีอยู่ตามสภาพปกติจนเกินขีดความสามารถการระบายน้ำของแม่น้ำ ลำคลอง และยังมีสาเหตุมาจากการกระทำของมนุษย์ โดยการปิดกั้นการไหลของน้ำตามธรรมชาติ ทั้งเจตนาและไม่เจตนา จนเป็นอันตรายต่อชีวิต ทรัพย์สินของประชาชนและสิ่งแวดล้อม

ดินถล่มหรือโคลนถล่ม หมายถึง ปรากฏการณ์ที่มวลดินหรือหินไถลเลื่อนลงจากพื้นที่ต่ำกว่าภายใต้อิทธิพลแรงโน้มถ่วงของโลก และการมีน้ำเป็นตัวกลางทำให้มวลวัสดุเกิดความไม่เสถียรภาพ อัตราการไถลเลื่อนดังกล่างข้างต้นอาจช้าหรือเร็วขึ้นอยู่กับประเภทของวัสดุ ความลาดชัน สภาพสิ่งแวดล้อม และปริมาณน้ำฝน

1. อันตรายที่เกิดจากอุทกภัย

1) ความเสียหายโดยตรง

○ น้ำท่วมอาคารบ้านเรือน สิ่งก่อสร้างและสาธารณสถาน ซึ่งจะทำให้เกิดความเสียหายทางเศรษฐกิจอย่างมาก บ้านเรือนหรืออาคารสิ่งก่อสร้างที่ไม่แข็งแรงจะถูกกระแสน้ำที่ไหลเชี่ยวพังทลายได้ คนและสัตว์พาหนะและสัตว์เลี้ยงอาจได้รับอันตรายถึงชีวิตจากการจมน้ำตาย

○ เส้นทางคมนาคมและการขนส่งอาจจะถูกตัดเป็นช่วงๆ โดยความแรงของกระแสน้ำ ถนนและสะพานอาจจะถูกกระแสน้ำพัดให้พังทลายได้ สินค้า พัสดุอยู่ระหว่างการขนส่งจะได้รับความเสียหาย

○ ระบบสาธารณูปโภค จะได้รับความเสียหาย เช่น โทรศัพท์ โทรเลข ไฟฟ้า และประปา

2) ทางอ้อม

○ จะส่งผลกระทบต่อเศรษฐกิจโดยทั่วไป เกิดโรคระบาด สุขภาพจิตเสื่อม และสูญเสียความปลอดภัย

2. ขั้นตอนการปฏิบัติในการบรรเทาภัยที่เกิดจากอุทกภัย ดินถล่มหรือโคลนถล่ม

เป็นการกำหนดหน้าที่ความรับผิดชอบของหน่วยงาน เพื่อให้สามารถดำเนินการป้องกันและแก้ไขปัญหาที่เกิดจากอุทกภัยได้อย่างรวดเร็วและมีประสิทธิภาพในระยะก่อนเกิดภัย ขณะเกิดภัยและภายหลังที่ภัยได้ผ่านพ้นไปแล้ว

2.1 ขั้นตอนการปฏิบัติก่อนการเกิดอุทกภัย ดินถล่มหรือโคลนถล่ม

เป็นการดำเนินการเพื่อจัดเตรียมและลดผลกระทบหรือแก้ไขปัญหาอุปสรรคไว้ล่วงหน้าก่อนที่อุทกภัยจะเกิดขึ้น

○ จัดทำแผนป้องกันและบรรเทาอุทกภัย รวมทั้งประสานและฝึกซ้อมแผนการบรรเทาอุทกภัยกับพนักงานหรือหน่วยงานภายนอกที่เกี่ยวข้อง

○ การติดตามข้อมูลข่าวสารอย่างต่อเนื่องของกรมอุตุนิยมวิทยาหรือทางราชการจากวิทยุโทรทัศน์

○ เชื่อฟังคำเตือนอย่างเคร่งครัด

○ เคลื่อนย้ายพนักงาน และอุปกรณ์สำนักงาน พาหนะและสิ่งของต่างๆ ไปอยู่ในที่สูงซึ่งเป็นพื้นที่พ้นระดับน้ำที่เคยท่วมมาก่อน

○ เตรียมแพ เรือไม้ หรือเรือยาง ไว้ใช้เป็นพาหนะเมื่อน้ำท่วมเป็นเวลานาน เพื่อช่วยอพยพเมื่อเกิดอุทกภัยร้ายแรง

○ เตรียมสำรองอาหาร น้ำดื่มสะอาด เครื่องเวชภัณฑ์ ไว้ให้พอจะมีอาหารรับประทานเมื่อน้ำท่วมเป็นเวลาหลายวัน

○ เคลื่อนย้ายพาหนะเช่น รถยนต์หรือล้อเลื่อนไปอยู่ที่สูง หรือทำแพสำหรับที่พักรถยนต์อาจจะใช้ถังน้ำขนาด 200 ลิตร ผูกติดกันแล้วใช้กระดานปูก็ได้

○ เตรียมกระสอบใส่ดินหรือทราย เพื่อเสริมคันดินที่กั้นน้ำให้สูงขึ้นเมื่อน้ำขึ้นสูงท่วมคันดินที่สร้างอยู่

o สำรวจ รวบรวมข้อมูลพื้นที่เสี่ยงภัยในพื้นที่รับผิดชอบ ตลอดจนปรับปรุงข้อมูลให้เป็นปัจจุบัน รวมทั้งสำรวจพื้นที่ปลอดภัยเพื่อรองรับการอพยพ

o ประชาสัมพันธ์และเผยแพร่ความรู้ในการป้องกันภัย เพื่อเตรียมรับสถานการณ์

o กำหนดบทบาทและความรับผิดชอบของหน่วยงานต่างๆ ให้ชัดเจน ไม่ซ้ำซ้อน สามารถปฏิบัติงานได้อย่างรวดเร็วเมื่อเกิดเหตุการณ์ในพื้นที่รับผิดชอบ

2.2 ขั้นตอนการปฏิบัติขณะเกิดอุทกภัย ดินถล่มหรือโคลนถล่ม

เป็นการดำเนินการในสถานการณ์ฉุกเฉินโดยการระดมทรัพยากรต่างๆ เข้าช่วยเหลือเพื่อรักษาชีวิตทรัพย์สินตลอดจนลดความรุนแรงของอุทกภัยที่เกิดขึ้น

o ตัดสะพานไฟและปิดแก๊สหุงต้มให้เรียบร้อย

o อยู่ในอาคารที่แข็งแรงหรืออยู่ในที่สูงพ้นระดับน้ำที่เคยท่วมมาก่อน

o ไม่ควรขับขี่ยานพาหนะฝ่าไปในขณะเกิดน้ำหลากหรือขณะเกิดน้ำท่วม

o ติดตามเหตุการณ์และคำเตือนเกี่ยวกับลักษณะอากาศจากทางราชการอย่างใกล้ชิด

o แจ้งเตือนภัยให้พนักงานอพยพหรือขนย้ายทรัพย์สินไปไว้ที่ปลอดภัย

o ตั้งศูนย์อำนวยการป้องกันและบรรเทาภัยตามแผนที่กำหนดไว้ เช่น ด้านเครื่องอุปโภคบริโภค น้ำดื่มที่จำเป็นต่อการดำรงชีพโดยเร่งด่วน

o อพยพพนักงานออกจากพื้นที่ประสบภัย ดูแลที่พักชั่วคราว อาหาร น้ำอุปโภคบริโภค เครื่องนุ่งห่ม ที่เห็นว่าเหมาะสมกับสถานการณ์ รวมทั้งจัดระบบรักษาความปลอดภัยในบริเวณพื้นที่อพยพ

o จัดหน่วยบรรเทาทุกข์ การรักษาพยาบาล รวมทั้งจัดหาเวชภัณฑ์ยารักษาโรคที่จำเป็นเพื่อดูแลสุขภาพอนามัยผู้ประสบภัย

o รายงานสถานการณ์ความเสียหายให้ ผอ.ศูนย์ฯ

o เมื่อจวนตัวให้คำนึงถึงความปลอดภัยของชีวิตมากกว่าทรัพย์สิน

2.3 ขั้นตอนการปฏิบัติหลังเกิดอุทกภัย ดินถล่มหรือโคลนถล่ม

เป็นการดำเนินการช่วยเหลือผู้ประสบภัยจากอุทกภัย ให้กลับคืนสู่สภาพคงเดิมในช่วงก่อนเหตุการณ์ เพื่อเป็นการสร้างขวัญกำลังใจของผู้ประสบภัยให้กลับคืนสู่สภาพปกติ

1. การฟื้นฟูสภาพแวดล้อมชีวิตความเป็นอยู่

- ให้การช่วยเหลือแก่พนักงานผู้ประสบภัย เพื่อบรรเทาความเดือดร้อน
- สำรวจความเสียหายและความต้องการด้านต่างๆ ของพนักงานผู้ประสบอุทกภัย
- ทำความสะอาดโคลนตม รื้อสิ่งปรักหักพัง ซ่อมแซมสิ่งชำรุดเสียหายให้กลับคืนสู่สภาพปกติ
- ซ่อมแซมสิ่งสาธารณประโยชน์และระบบสาธารณูปโภค ให้กลับคืนสู่สภาพปกติโดยเร็วที่สุด
- ทำความสะอาด ทำลายซากสัตว์ที่ล้มตาย พร้อมทั้งจัดการเก็บฝังเพื่อป้องกันโรคระบาด

2. การฟื้นฟูทางด้านร่างกายและจิตใจของพนักงานผู้ประสบภัย

- จัดให้มีบริการรักษาพยาบาลพนักงานผู้บาดเจ็บ ผู้ป่วย เพื่อรักษาชีวิตผู้ได้รับอันตรายในระยะแรก
- จัดการประชาสัมพันธ์ เพื่อฟื้นฟูสภาพจิตใจและสร้างความเชื่อมั่นในการให้ความช่วยเหลือขององค์การจัดการน้ำเสียต่อพนักงานผู้ประสบภัย

<u>แผนการบรรเทาภัยพิบัติที่เกิดจากแผ่นดินไหวและอาคารถล่ม</u>

แผ่นดินไหว (Earthquake) หมายถึง การสั่นสะเทือนของพื้นดิน อันมีสาเหตุหลักมาจากการขยับเคลื่อนตัวของเปลือกโลก การสั่นสะเทือนนี้อาจมีระดับความรุนแรงขั้นต่ำที่ไม่ก่อให้เกิดความเสียหายใดๆ แต่บางครั้งก็อาจมีระดับความรุนแรงในขั้นที่เป็นอันตรายจนก่อให้เกิดความเสียหายอย่างใหญ่หลวงได้

อาคารถล่ม หมายถึง อาคารและสิ่งปลูกสร้าง ได้แก่ ตึก บ้าน โรง เรือน แพ คลังสินค้า สำนักงาน ที่ได้รับความเสียหายจากการโยกไหวตัวรุนแรง ซึ่งเป็นผลมาจากแผ่นดินไหวและอาจทำให้เกิดความเสียหายหรือพังทลายลงมาได้

พื้นที่เสี่ยงภัยแผ่นดินไหวในประเทศไทย

○ แผ่นดินไหวขนาดใหญ่ที่มีแหล่งกำเนิดจากภายนอกประเทศ โดยมีแหล่งกำเนิดจากตอนใต้ของประเทศจีน พม่า ลาว ทะเลอันดามัน ตอนเหนือของ เกาะสุมาตรา ซึ่งจะทำให้เกิดแรงสั่นไหวในบริเวณภาคเหนือ ภาคใต้ ภาคตะวันตก ภาคตะวันออกเฉียงเหนือ และกรุงเทพมหานคร

○ แผ่นดินไหวเกิดจากแนวรอยเลื่อนที่ยังสามารถเคลื่อนตัว ซึ่งอยู่บริเวณภาคเหนือและภาคตะวันตกของประเทศ เช่น รอยเลื่อนเชียงแสน รอยเลื่อนแม่ทา รอยเลื่อนแพร่ รอยเลื่อนเถิน รอยเลื่อนเมยอุทัยธานี รอยเลื่อนศรีสวัสดิ์ รอยเลื่อนเจดีย์สามองค์ รอยเลื่อนคลองมะรุย

1. อันตรายที่เกิดจากแผ่นดินไหวและอาคารถล่ม ภัยที่เกิดจากแผ่นดินไหวสามารถแบ่งออกได้ดังนี้

○ ภัยจากการสั่นไหวของพื้นดิน ก่อให้เกิดการปรับตัวของดินที่ต่างกัน การพังทลายของดินและโคลน และการที่ดินมีสภาพกลายเป็นของเหลวอาจเกิดอาคารถล่มได้

○ ภัยจากการยกตัวของพื้นดินบริเวณรอยเลื่อน

○ ภัยที่เกิดจากคลื่นใต้น้ำที่เรียกว่า “Tsunami” คลื่นนี้เกิดขึ้นจากแผ่นดินไหวขนาดใหญ่ในทะเลและมหาสมุทร ทำให้เกิดคลื่นทะเลซัดฝั่ง

○ ภัยจากอัคคีภัยหลังการเกิดแผ่นดินไหว

2. ขั้นตอนการปฏิบัติในการบรรเทาภัยที่เกิดจากแผ่นดินไหวและอาคารถล่ม

เพื่อให้สามารถดำเนินการป้องกันและแก้ไขปัญหาที่เกิดจากแผ่นดินไหวและอาคารถล่มได้อย่างรวดเร็วและมีประสิทธิภาพในระยะก่อนเกิดภัย ขณะเกิดภัย และภายหลังที่ภัยได้ผ่านพ้นไปแล้ว

2.1 ขั้นตอนการปฏิบัติก่อนการเกิดแผ่นดินไหวและอาคารถล่ม

เป็นการดำเนินการเพื่อจัดเตรียมและลดผลกระทบความเสียหายหรือแก้ไขปัญหาอุปสรรคไว้ล่วงหน้าก่อนที่แผ่นดินไหวและอาคารถล่มจะเกิดขึ้น

○ จัดทำแผนป้องกันและบรรเทาภัยแผ่นดินไหวและอาคารถล่มรวมทั้งประสานและฝึกซ้อมแผนการบรรเทาภัยกับพนักงานหรือหน่วยงานภายนอกที่เกี่ยวข้อง

○ การติดตามข้อมูลข่าวสารของกรมอุตุนิยมวิทยาหรือทางราชการจากวิทยุโทรทัศน์และเชื่อฟังคำเตือนอย่างเคร่งครัด

o ตรวจสภาพความปลอดภัยของอาคารและเครื่องใช้ภายในอาคาร ทำการยึดอุปกรณ์ที่อาจก่อให้เกิดอันตราย เช่น ตู้และชั้นหนังสือยึดติดกับฝาหรือเสา ไม่วางของหนักบนที่สูง

o สอนพนักงานให้รู้จักตัดไฟ ปิดวาล์วน้ำและแก๊ส

o สำรองเสบียงอาหาร น้ำดื่ม ยารักษาโรค เครื่องนุ่งห่ม วัสดุอุปกรณ์ต่างๆ อาทิ ไฟฉาย เครื่องมือช่าง อุปกรณ์ดับเพลิง เพื่อเตรียมรับแผ่นดินไหวและอาคารถล่มที่จะเกิดขึ้น

o ซักซ้อมความพร้อมของพนักงาน โดยกำหนดวิธีปฏิบัติตนเมื่อเกิดแผ่นดินไหวและกำหนดจุดนัดพบที่ปลอดภัย เมื่อมีการพลัดพรากหรือเตรียมการเพื่อการอพยพเคลื่อนย้ายไปอยู่ที่ปลอดภัย

o องค์การจัดการน้ำเสียต้องจัดเตรียมเจ้าหน้าที่รวมทั้งฝึกซ้อมการช่วยเหลือพนักงานเมื่อเกิดแผ่นดินไหวหรืออาคารถล่มอันเนื่องมาจากแผ่นดินไหว

o สำรวจพื้นที่เสี่ยงภัยในพื้นที่รับผิดชอบ ตลอดจนปรับปรุงข้อมูลให้เป็นปัจจุบัน รวมทั้งสำรวจพื้นที่ปลอดภัยเพื่อรองรับการอพยพโดยหน่วยงานที่เกี่ยวข้อง

o ให้มีการตรวจสภาพของอาคารหากไม่แข็งแรงให้ประสานแจ้งผู้รับผิดชอบเพื่อให้มีการเสริมความแข็งแรง รวมทั้งควบคุมการก่อสร้างอาคารให้สามารถต้านทานแรงแผ่นดินไหว

o ประชาสัมพันธ์และเผยแพร่ความรู้ในการป้องกันภัยให้ เพื่อเตรียมรับสถานการณ์

2.2 ขั้นตอนการปฏิบัติขณะเกิดแผ่นดินไหวและอาคารถล่ม

เป็นการดำเนินการในสถานการณ์ฉุกเฉิน โดยการระดมทรัพยากรต่างๆ เข้าช่วยเหลือเพื่อรักษาชีวิต ทรัพย์สินและบรรเทาทุกข์แก่พนักงานผู้ประสบภัย ตลอดจนลดความรุนแรงของแผ่นดินไหวและอาคารถล่มที่เกิดขึ้น

o ไม่ตื่นตกใจ พยายามควบคุมสติอย่างสงบ อยู่ในที่แข็งแรงปลอดภัย ถ้าอยู่ในอาคารให้ยืนหรือหมอบอยู่ในส่วนของอาคารที่มีโครงสร้างแข็งแรงที่สามารถรับน้ำหนักได้มาก หรืออยู่ใต้โต๊ะที่แข็งแรง เพื่อป้องกันอันตรายจากสิ่งปรักหักพังร่วงหล่นลงมา อยู่ให้ห่างจากประตู หน้าต่าง สายไฟ อุปกรณ์ไฟฟ้า และสิ่งห้อยแขวน

o ตัดสะพานไฟ ปิดวาล์วน้ำ และแก๊สหุงต้มให้เรียบร้อย

o หากอยู่ในรถ ให้หยุดรถจนกว่าความสั่นสะเทือนจะหยุด

o หากอยู่ชายหาดให้อยู่ห่างจากชายฝั่งให้มากที่สุดเพราะอาจเกิดคลื่นสึนามิ (Tsunami)

o อย่าใช้เทียน ไม้ขีดไฟหรือสิ่งที่จะทำให้เกิดเปลวไฟหรือประกายไฟ เพราะอาจมีแก๊สรั่วอยู่

o ติดตามเหตุการณ์และคำเตือนของทางราชการอย่างใกล้ชิดและปฏิบัติตามอย่างเคร่งครัด ไม่ตื่นตกใจ

o เตรียมความพร้อมที่จะอพยพไปในที่ปลอดภัย

o จัดตั้งศูนย์อำนวยการเฉพาะกิจตามแผนที่กำหนดไว้ เพื่อช่วยเหลือผู้ประสบภัยในพื้นที่ที่เกิดภัยและเป็นศูนย์กลางในการประสานการช่วยเหลือผู้ประสบภัย

o จัดระบบรักษาความปลอดภัยบริเวณที่ได้รับความเสียหาย

o ดำเนินการอพยพเคลื่อนย้ายผู้ประสบภัยรวมทั้งเคลื่อนย้ายทรัพย์สินขององค์กรไปไว้ในพื้นที่ปลอดภัย

o เมื่อจวนตัวให้คำนึงถึงความปลอดภัยของชีวิตมากกว่าทรัพย์สิน

2.3 ขั้นตอนการปฏิบัติหลังเกิดแผ่นดินไหวและอาคารถล่ม

เป็นการดำเนินการช่วยเหลือพนักงานผู้ประสบภัยจากแผ่นดินไหวและอาคารถล่มให้กลับคืนสู่สภาพคงเดิมในช่วงก่อนเหตุการณ์ เพื่อเป็นการสร้างขวัญกำลังใจของพนักงานผู้ประสบภัย

1) การฟื้นฟูสภาพแวดล้อมชีวิตความเป็นอยู่

o สำรวจความเสียหายและความต้องการด้านต่างๆ ของพนักงานผู้ประสบภัย

o ให้การช่วยเหลือพนักงานผู้ประสบภัย เช่น ที่พักอาศัยชั่วคราว น้ำอุปโภคบริโภค เพื่อบรรเทาความเดือดร้อน

o ทำความสะอาดรื้อสิ่งปรักหักพัง สิ่งชำรุดเสียหายให้กลับคืนสู่สภาพปกติโดยเร็ว

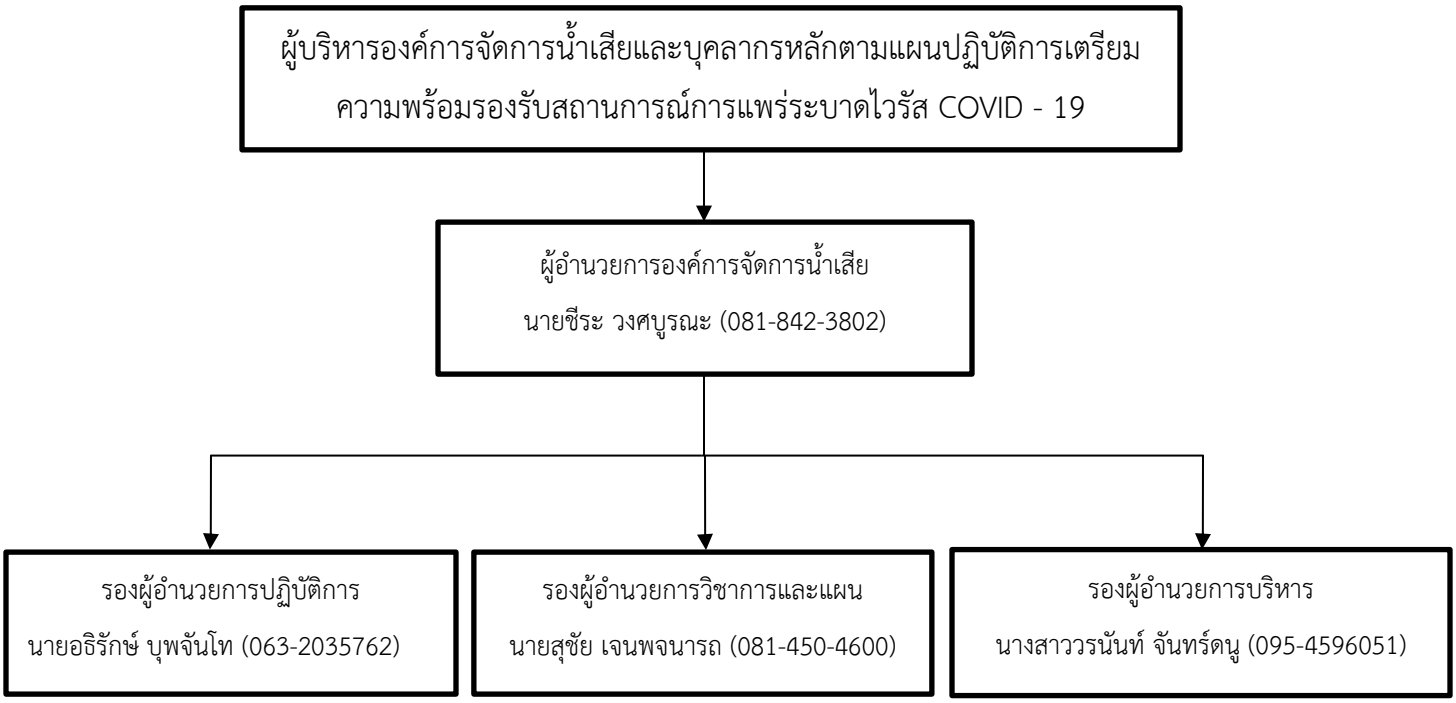
2) การฟื้นฟูทางด้านร่างกายและจิตใจของผู้ประสบภัย

o จัดให้มีบริการรักษาพยาบาลผู้บาดเจ็บ ผู้ป่วย เพื่อรักษาชีวิตผู้ได้รับอันตรายในระยะแรก

o จัดการประชาสัมพันธ์ เพื่อฟื้นฟูสภาพจิตใจและสร้างความเชื่อมั่นในการให้ความช่วยเหลือขององค์การจัดการน้ำเสียต่อพนักงานผู้ประสบภัยอย่างเต็มที่และเท่าเทียมกัน

<u>แผนปฏิบัติการเตรียมความพร้อมรับสถานการณ์แพร่ระบาดไวรัส COVID-19</u>

จากสถานการณ์แพร่ระบาดของเชื้อไวรัส COVID-19 กำลังขยายวงกว้างอย่างรวดเร็วทั่วโลกในขณะนี้ (ในช่วงปลายปี พ.ศ. 2562) องค์การจัดการน้ำเสีย (อจน.) โดยนายชีระ วงศบูรณะ ผู้อำนวยการองค์การจัดการน้ำเสีย ได้ออกประกาศมาตรการป้องกันการแพร่ระบาดของเชื้อไวรัสตามมาตรการและการเฝ้าระวังของกรมควบคุมโรคและกระทรวงสาธารณสุขให้แก่พนักงาน ผู้มาประชุม ผู้มาติดต่อที่สำนักงานใหญ่หรือผู้มาติดต่อสำนักงานจัดการน้ำเสียสาขา ให้ได้รับความปลอดภัยด้านสุขภาพสูงสุด โดยมีมาตรการความปลอดภัยด้านสุขภาพ และการป้องกันการแพร่ระบาดของเชื้อ COVID-19 ตามแนวปฏิบัติ ดังนี้



ศูนย์ปฏิบัติการสำรอง

ศูนย์บริหารจัดการคุณภาพน้ำ องค์การบริหารส่วนตำบลบางบัวทอง

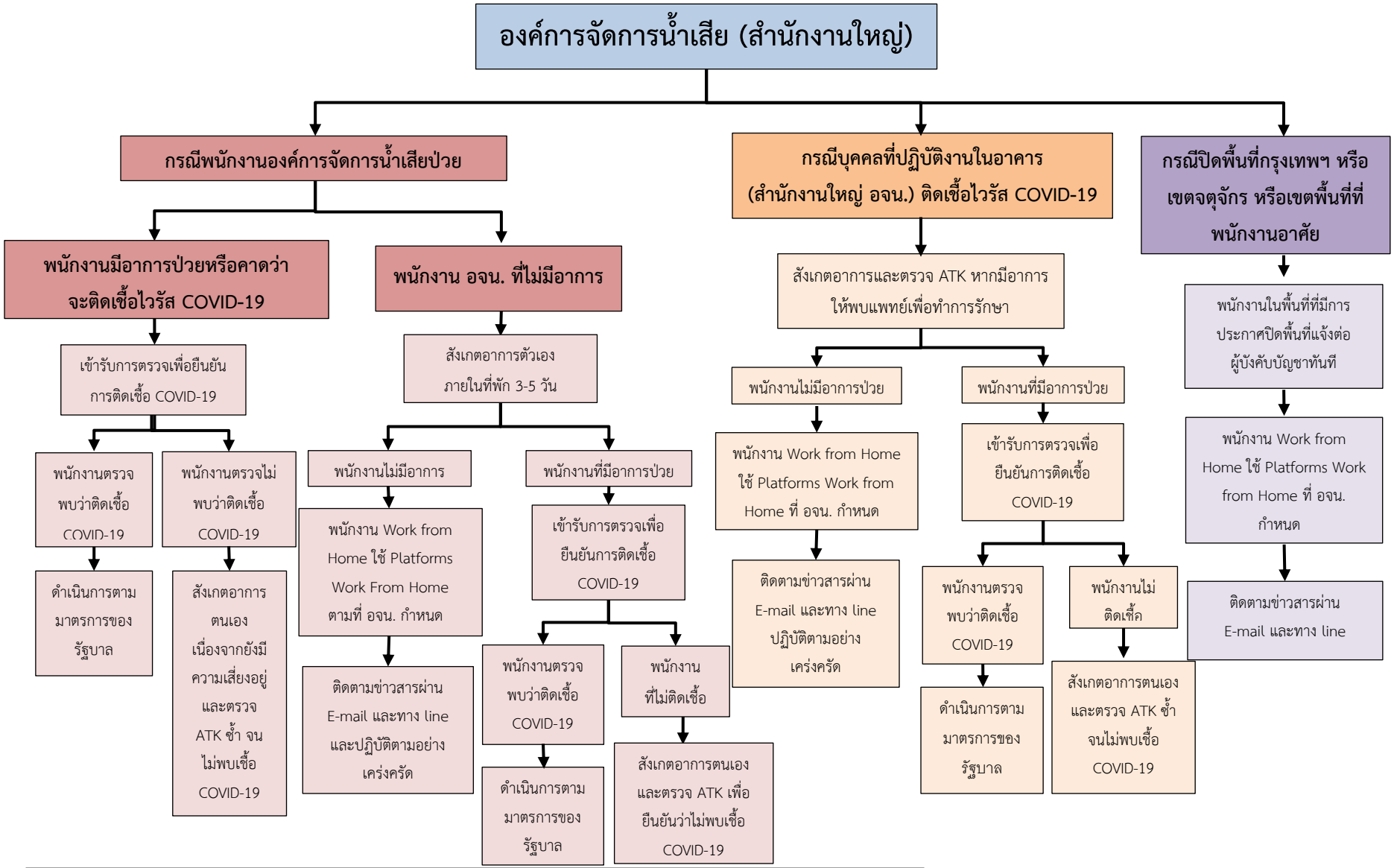
ที่อยู่ : หมู่ 11 ถ.บางกรวย-ไทรน้อย ตำบลบางบัวทอง อำเภอบางบัวทอง จังหวัดนนทบุรี 11110

โทรศัพท์ : 063-2035763

ผู้ประสานงาน : นางสาวพจมาลย์ ต้นทิพย์

Location : https://www.google.com/maps?q=13.958091,100.37481099999999

ขั้นตอนปฏิบัติรองรับแผนรองรับสถานการณ์ฉุกเฉิน COVID-19



1. กรณีพนักงานสำนักงานใหญ่

1.1 พนักงานที่ต้องให้บริการลูกค้า ผู้มาติดต่อ ให้สวมใส่หน้ากากอนามัยตลอดเวลาที่ปฏิบัติงาน หากมีพนักงานเดินทางกลับจากประเทศกลุ่มเสี่ยงตามที่รัฐบาลกำหนด หรือสัมผัสใกล้ชิดกับกลุ่มเสี่ยง พนักงานจะต้องหยุดพักและแยกตัวเอง (Self-Quarantine) หรือแยกกักตัวที่บ้าน (Self-Isolation) จำนวน 3-5 วัน และไม่ใช้สิ่งของร่วมกับผู้อื่น ไม่ออกไปสถานที่ชุมชนหรือที่สาธารณะและเฝ้าระวังอาการอย่างต่อเนื่องจนครบระยะเวลา 5 วัน เพื่อเฝ้าระวังการติดเชื้อไวรัส COVID-19

1.2 จัดเตรียมอุปกรณ์หรือเจลล้างมือแอลกอฮอล์ที่ได้มาตรฐาน สำหรับให้ผู้มาติดต่อหรือลูกค้าได้ใช้ฆ่าเชื้อ ณ จุดติดต่อประชาสัมพันธ์หรือจุดรับบริการ รวมถึงเพิ่มความถี่ในการทำความสะอาดทุกจุดสัมผัสสาธารณะทุกๆ 1 ชั่วโมง

1.3 พนักงานเข้า-ออกประตูเพื่อปฏิบัติงานในสำนักงานใหญ่ ให้ใช้การทาบบัตรแข็งแทนการสแกนลายนิ้วมือ และใช้มาตรการ Social Distancing เช่น ให้ยืนห่างกันประมาณ 1 เมตร ขณะสแกนบัตรหรือยืนรอลิฟต์โดยสาร และนั่งเว้นเก้าอี้ตัวเว้นตัวในขณะประชุม เป็นต้น

1.4 พนักงานที่มีอาการป่วย หรือแสดงอาการที่เข้าข่ายติดเชื้อไวรัส COVID-19 เช่น อุณหภูมิร่างกายสูงตั้งแต่ 37.5 องศาเซลเซียสขึ้นไป และมีอาการ ไอ มีน้ำมูก เจ็บคอ หายใจเหนื่อย หอบ ให้เข้ารับการรักษาในโรงพยาบาลจนกว่าจะมีผลตรวจยืนยันว่าไม่มีการติดเชื้อและอาการป่วยหายเป็นปกติ รวมทั้งเตรียมความพร้อม ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง อาทิ กรมควบคุมโรค กระทรวงสาธารณสุข ฯลฯ

<u>ข้อปฏิบัติกรณีพนักงานป่วย</u>

1. พนักงานที่มีอาการป่วยหรือคาดว่าจะติดเชื้อไวรัส COVID-19

1.1 เข้ารับการตรวจเพื่อยืนยันการติดเชื้อ หากตรวจพบว่าพนักงานติดเชื้อไวรัส COVID-19 จริง ให้ปฏิบัติดังนี้

- รายงานต่อผู้บังคับบัญชา เจ้าของอาคาร กระทรวงมหาดไทย กรมควบคุมโรค
- ปิดทำการอาคารสำนักงานเป็นเวลา 1-2 วัน เพื่อฉีดพ่นสารเคมีในการทำความสะอาดและฆ่าเชื้อตามมาตรฐานสาธารณสุขทั่วพื้นที่อาคารสำนักงาน
- พนักงานที่ติดเชื้อไวรัส COVID-19 เข้ารับการรักษาตัวในโรงพยาบาลหรือแยกกักตัวที่บ้าน (Self-Isolation) และรักษาจนไม่พบการติดเชื้อ

1.2 หากตรวจพบว่าไม่มีการติดเชื้อไวรัส COVID-19 ให้ดำเนินการกักตัวตามมาตรการของรัฐและต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ

1.3 พนักงานที่ไม่มีอาการป่วย ให้สังเกตอาการตัวเองโดยการไม่ออกไปที่ชุมชนสาธารณะ งดการใช้สิ่งของร่วมกับผู้อื่น เป็นเวลา 10 วัน และปฏิบัติดังนี้

1.3.1 พนักงานปฏิบัติงานที่บ้าน Work from Home โดยให้พนักงานใช้ Platforms Work from Home ที่ อจน. ได้นำมาใช้ ดังนี้

ที่	ชื่อระบบ	รายละเอียด
1	WMA Attendance	ให้ยืนยันเข้า-ออกตัวตนเข้าออกเวลาทำงาน (ดำเนินการตามคู่มือ)
2	Zoom Meeting	การประชุมออนไลน์
3	WMA Storage (on PC/Mobile)	การรวบรวมข้อมูลผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (ดำเนินงานตามคู่มือ)
4	E-Saraban	ระบบติดตามหนังสือภายในและภายนอก
5	Mail Go Thai (on PC/Mobile)	การส่งข้อมูล – เอกสาร ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (ดำเนินงานตามคู่มือ)
6	SCADA Control and Monitoring	ศูนย์ติดตามและรายงานสถานการณ์น้ำเสียประเทศไทย

1.3.2 ให้พนักงานนำข้อมูลสำคัญที่ใช้ประกอบการทำงานขึ้นบน WMA Storage (สามารถเปิดได้บนเครื่อง PC หรือผ่านมือถือ) หรือนำใส่ External Hard Disk เพื่อนำกลับไปทำงานที่บ้านในช่วงระยะเวลาที่สังเกตอาการ ในกรณีที่พนักงานไม่มีเครื่อง PC ทำงานที่บ้านให้ทำเรื่องขออนุมัติสายงานเพื่อทำการยืม Laptop ชั่วคราว หรือนำเครื่อง PC นำเครื่องกลับไปทำงานที่บ้าน

1.3.3 ให้พนักงาน Download Application/Software ชื่อ “Zoom” สำหรับใช้ในการประชุมออนไลน์ และให้ดำเนินการตามคู่มือการใช้งาน WMA Attendance คู่มือการใช้งาน Mail Go Thai (on PC/Mobile) และคู่มือการใช้งาน WMA Storage (on PC/Mobile) โดยหากจำเป็นต้องส่งหนังสือ/เอกสารให้พนักงานส่งทางตู้ไปรษณีย์ของ อจน.(ตู้ ป.ณ.1 ปณฝ คูคต 12131)

1.3.4 พนักงานติดตามข่าวสารและประกาศสถานการณ์การแพร่ระบาดของไวรัส COVID-19 อย่างต่อเนื่องจากหน่วยงานผ่านทางเว็บไซต์ (www.wma.or.th) จดหมายอิเล็กทรอนิกส์ Mail go.th หรือ Line และปฏิบัติตามอย่างเคร่งครัด

1.3.5 หากครบกำหนดแล้วไม่พบอาการป่วย ให้พนักงานเข้าพบแพทย์แผนปัจจุบันในโรงพยาบาลที่ได้มาตรฐานหลังจากแพทย์ลงความเห็นว่าไม่มีอาการป่วยแล้ว ต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ หรือยืนยันผลการตรวจ ATK ที่ตรวจไม่เกิน 24 ชั่วโมง

1.4 กรณีที่มีความจำเป็นต้องจัดการประชุม หรือจัดตั้งสำนักงานใหญ่ชั่วคราวให้ใช้สถานที่ที่พิจารณาแล้วว่าเหมาะสม หรือพื้นที่สำนักงานจัดการน้ำเสียสาขาจังหวัดใกล้กรุงเทพฯ ให้กำหนดจำนวนผู้เข้าร่วมไม่เกิน 50 คน ในต่างจังหวัดให้จำกัดจำนวน ผู้เข้าร่วมไม่เกิน 100 คน จัดห้องให้ผู้เข้าร่วมนั่งหรือยืนห่างกัน ระยะ 2 เมตร ไม่สัมผัสตัวและมีสิ่งอำนวยความสะดวกในการล้างมือ เช่น เจลแอลกอฮอล์ โดยให้จัดทำแผนการประชุม สัมมนาเสนอเพื่อพิจารณาความเห็นชอบก่อนทุกครั้ง

1.5 กรณีที่มีความจำเป็นต้องจัดการประชุม หรือจัดตั้งสำนักงานใหญ่ชั่วคราว ให้ใช้สถานที่ที่พิจารณาแล้วว่าเหมาะสม หรือพื้นที่สำนักงานจัดการน้ำเสียสาขาจังหวัดใกล้กรุงเทพฯ

<u>ข้อปฏิบัติในกรณีผู้ทำงานในอาคาร (สำนักงานใหญ่) ติดเชื้อไวรัส COVID-19</u>

1. พนักงานที่มีอาการป่วยหรือคาดว่าจะติดเชื้อไวรัส COVID-19

1.1 เข้ารับการตรวจเพื่อยืนยันการติดเชื้อ หากตรวจพบว่าพนักงานติดเชื้อไวรัส COVID-19 จริง ให้ปฏิบัติดังนี้

- รายงานต่อผู้บังคับบัญชา เจ้าของอาคาร กระทรวงมหาดไทย กรมควบคุมโรค
- ฆ่าเชื้อและปิดสำนักงานใหญ่ 1 วัน
- พนักงานที่ติดเชื้อไวรัส COVID-19 เข้ารับการรักษาตัวในโรงพยาบาลหรือแยกรักษาตัวอยู่ที่พักอาศัย (Home Isolation)

1.2 หากตรวจพบว่าไม่มีการติดเชื้อ COVID-19 ให้ดำเนินการกักตัวตามมาตรการของรัฐและต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ

2. พนักงานที่ไม่มีอาการป่วย ให้สังเกตอาการตัวเองโดยการไม่ออกไปที่ชุมชนสาธารณะ งดการใช้สิ่งของร่วมกับผู้อื่น เป็นเวลา 10 วันและปฏิบัติดังนี้

2.1 พนักงานปฏิบัติงานที่บ้าน Work from Home โดยให้พนักงานใช้ Platforms Work from Home ที่ อจน. ได้นำมาใช้ ดังนี้

ที่	ชื่อระบบ	รายละเอียด
1	WMA Attendance	ให้ยืนยันเข้า-ออกตัวตนเข้าออกเวลาทำงาน (ดำเนินการตามคู่มือ)
2	Zoom Meeting	การประชุมออนไลน์
3	WMA Storage (on PC/Mobile)	การรวบรวมข้อมูล ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (ดำเนินงานตามคู่มือ)
4	E-Saraban	ระบบติดตามหนังสือภายในและภายนอก
5	Mail Go Thai (on PC/Mobile)	การส่งข้อมูล – เอกสาร ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่(ดำเนินงานตามคู่มือ)
6	SCADA Control and Monitoring	ศูนย์ติดตาม และรายงานสถานการณ์น้ำเสียประเทศไทย

2.2 ให้พนักงานนำข้อมูลสำคัญที่ใช้ประกอบการทำงานขึ้นบน WMA Storage (สามารถเปิดได้บนเครื่อง PC หรือผ่านมือถือ) หรือนำใส่ External Hard Disk เพื่อนำกลับไปทำงานที่บ้านในช่วงระยะเวลาที่สังเกตอาการในกรณีที่พนักงานไม่มีเครื่อง PC ทำงานที่บ้าน ให้ทำเรื่องขออนุมัติภายในสายงานเพื่อยืม Laptop ชั่วคราว หรือเครื่อง PC เพื่อนำเครื่องกลับไปทำงานที่บ้าน

2.3 ให้พนักงาน Download Application/Software ชื่อ “Zoom” สำหรับใช้ในการประชุมออนไลน์ และให้ดำเนินการตามคู่มือการใช้งาน WMA Attendance คู่มือการใช้งาน Mail Go Thai (on PC/Mobile) และคู่มือการใช้งาน WMA Storage (on PC/Mobile) โดยหากจำเป็นต้องส่งหนังสือ/เอกสารให้พนักงานส่งทางตู้ไปรษณีย์ของ อจน. (ตู้ ป.ณ.1 ปณฝ คูคต 12131)

2.4 พนักงานติดตามข่าวสารและประกาศสถานการณ์ไวรัส COVID-19 จากหน่วยงานผ่านทางเว็บไซต์ (www.wma.or.th) จดหมายอิเล็กทรอนิกส์ Mail go.th หรือ Line และปฏิบัติตามอย่างเคร่งครัด

2.5 หากครบกำหนดแล้วไม่พบอาการป่วย ให้พนักงานเข้าพบแพทย์แผนปัจจุบันในโรงพยาบาลที่ได้มาตรฐานหลังจากแพทย์ลงความเห็นว่าไม่มีอาการป่วยแล้ว ต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ หรือแสดงผลการตรวจ ATK ที่ตรวจไม่เกิน 24 ชั่วโมง

ข้อปฏิบัติกรณีมีการประกาศปิดพื้นที่กรุงเทพฯ หรือเขตจตุจักร หรือเขตพื้นที่ที่พนักงานอาศัย เพื่อควบคุมการแพร่ไวรัส COVID-19 ให้ปฏิบัติ ดังนี้

1. พนักงานที่อาศัยในพื้นที่ที่มีการประกาศปิดพื้นที่แจ้งต่อผู้บังคับบัญชาให้ทราบโดยทันที

2. พนักงานปฏิบัติงานที่บ้าน Work from Home โดยให้พนักงานใช้ Platforms Work from Home ที่ อจน. ได้นำมาใช้ ดังนี้

ที่	ชื่อระบบ	รายละเอียด
1	WMA Attendance	ให้ยืนยันเข้า-ออกตัวตนเข้าออกเวลาทำงาน (ดำเนินการตามคู่มือ)
2	Zoom	การประชุมออนไลน์
3	WMA Storage (on PC/Mobile)	การรวบรวมข้อมูล ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (ดำเนินงานตามคู่มือ)
4	E-Saraban	ระบบติดตามหนังสือภายในและภายนอก
5	Mail Go Thai (on PC/Mobile)	การส่งข้อมูล – เอกสาร ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่(ดำเนินงานตามคู่มือ)
6	SCADA Control and Monitoring	ศูนย์ติดตาม และรายงานสถานการณ์น้ำเสียประเทศไทย

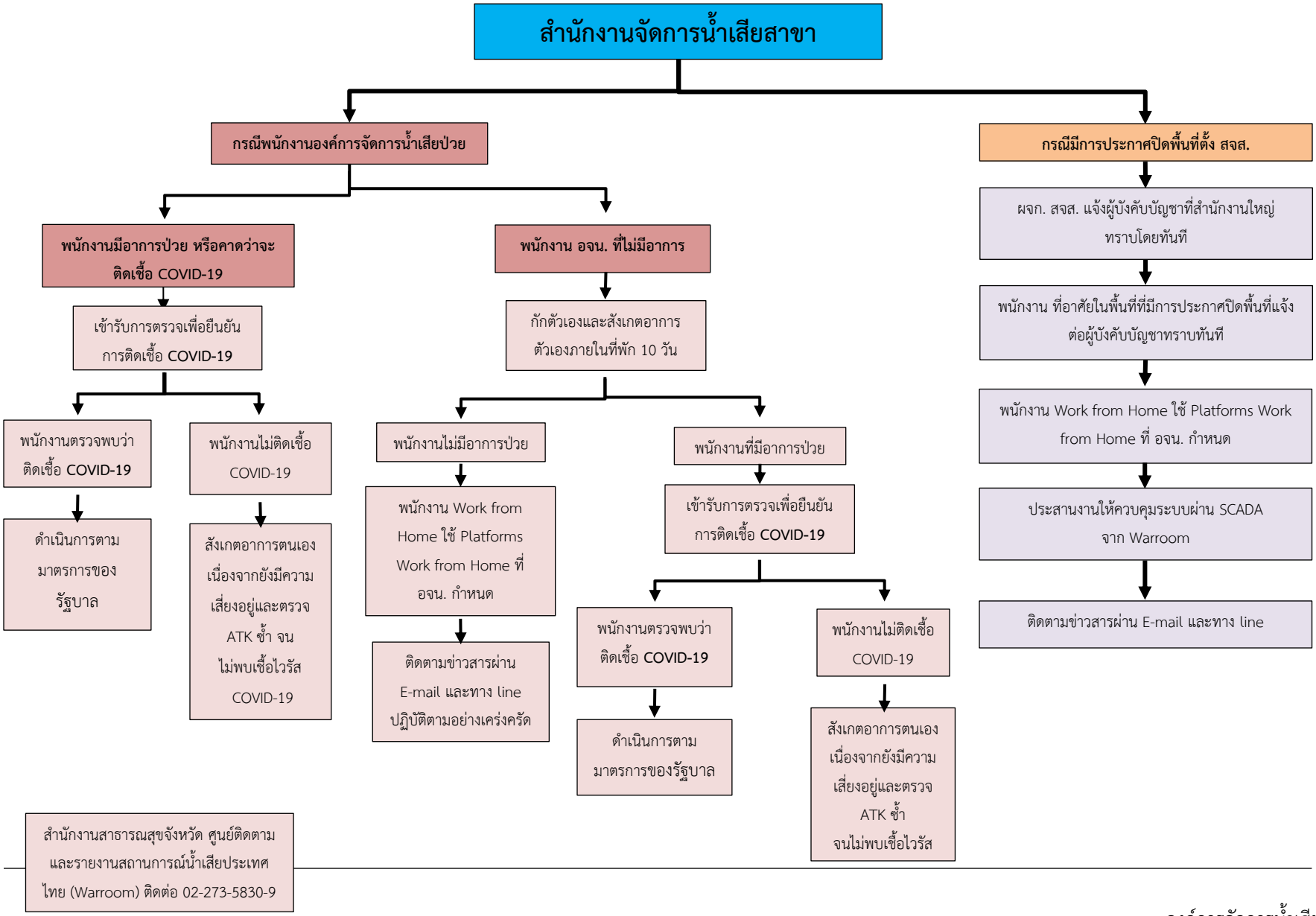
3. ให้พนักงานนำข้อมูลสำคัญที่ใช้ประกอบการทำงานขึ้นบน WMA Storage (สามารถเปิดได้บนเครื่อง PC หรือผ่านมือถือ) หรือนำใส่ External Hard disk เพื่อนำกลับไปทำงานที่บ้านในช่วงระยะเวลาที่สังเกตอาการ ในกรณีที่พนักงานไม่มีเครื่อง PC ทำงานที่บ้าน ให้ทำเรื่องขออนุมัติสายงานเพื่อยืม Laptop ชั่วคราว หรือเครื่อง PC นำเครื่องกลับไปทำงานที่บ้าน

4. ให้พนักงาน Download Application/Software ชื่อ “Zoom” สำหรับใช้ในการประชุมออนไลน์ และให้ดำเนินการตามคู่มือการใช้งาน Mail Go Thai (on PC/Mobile) คู่มือการใช้งาน WMA Attendance และคู่มือการใช้งาน WMA Storage (on PC/Mobile) โดยหากจำเป็นต้องส่งหนังสือ/เอกสารให้พนักงานส่งทางตู้ไปรษณีย์ของ อจน. (ตู้ ป.ณ. 1 ปณฝ คูคต 12131)

5. กรณีที่มีความจำเป็นต้องจัดการประชุม หรือจัดตั้งสำนักงานใหญ่/สำนักงานย่อย (เฉพาะสายงาน/ฝ่าย) ให้ใช้สถานที่ที่พิจารณาแล้วว่าเหมาะสม หรือพื้นที่สำนักงานจัดการน้ำเสียสาขาใกล้เคียงกับพื้นที่

6. พนักงานติดตามข่าวสารและประกาศสถานการณ์การแพร่ระบาดของไวรัส COVID-19 อย่างต่อเนื่องจากหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์Mail go.th หรือ Line และปฏิบัติตามอย่างเคร่งครัด พร้อมทั้งรายงานให้ผู้บังคับบัญชาทราบเป็นระยะๆ

ขั้นตอนปฏิบัติรองรับแผนรองรับสถานการณ์ฉุกเฉิน COVID-19



<u>กรณีพนักงานสำนักงานจัดการน้ำเสียสาขา</u>

1. พนักงานที่ต้องให้บริการลูกค้า ผู้มาติดต่อ ให้สวมใส่หน้ากากอนามัยตลอดเวลาที่ปฏิบัติงาน หากมีพนักงานเดินทางกลับจากประเทศกลุ่มเสี่ยงตามที่รัฐบาลกำหนด หรือสัมผัสใกล้ชิดกับกลุ่มเสี่ยง พนักงานจะต้องหยุดพักและแยกตัวเอง (Self-Quarantine) หรือแยกกักตัวที่บ้าน (Self-Isolation) จำนวน 10 วัน และไม่ใช้สิ่งของร่วมกับผู้อื่น ไม่ออกไปสถานที่ชุมชนหรือที่สาธารณะและเฝ้าระวังอาการอย่างต่อเนื่องจนครบระยะเวลา 10 วัน เพื่อเฝ้าระวังการติดเชื้อไวรัส COVID-19

2. จัดเตรียมอุปกรณ์หรือเจลล้างมือแอลกอฮอล์ที่ได้มาตรฐาน สำหรับให้ผู้มาติดต่อหรือลูกค้าได้ใช้ฆ่าเชื้อ ณ จุดติดต่อประชาสัมพันธ์ หรือจุดรับบริการ รวมถึงเพิ่มความถี่ในการทำความสะอาดทุกจุดสัมผัสสาธารณะทุกๆ 1 ชั่วโมง

3. พนักงานที่มีอาการป่วย หรือแสดงอาการที่เข้าข่ายติดเชื้อไวรัส COVID-19 เช่น อุณหภูมิร่างกายสูงตั้งแต่ 37.5 องศาเซลเซียสขึ้นไป และมีอาการ ไอ มีน้ำมูก เจ็บคอ หายใจเหนื่อย หอบ ให้เข้ารับการรักษาในโรงพยาบาลจนกว่าจะมีผลตรวจยืนยันว่าไม่มีการติดเชื้อและอาการป่วยหายเป็นปกติ รวมทั้งเตรียมความพร้อม ประสานความร่วมมือกับหน่วยงานที่เกี่ยวข้อง อาทิ กรมควบคุมโรค กระทรวงสาธารณสุข ฯลฯ

4. พนักงานที่มีอาการป่วยหรือคาดว่าจะติดเชื้อไวรัส COVID-19

4.1 เข้ารับการตรวจเพื่อยืนยันการติดเชื้อ หากตรวจพบว่าพนักงานติดเชื้อไวรัส COVID-19 จริง ให้ปฏิบัติดังนี้

- รายงานต่อผู้บังคับบัญชา กระทรวงมหาดไทย กรมควบคุมโรค
- ฆ่าเชื้อและปิด สจส. 1-2 วัน พร้อมปิดประกาศหน้า สจส. ไม่ให้หน่วยงานหรือบุคคลภายนอกเข้ามาติดต่อและแจ้งช่องทางติดต่อสื่อสาร เช่น โทรศัพท์ โทรสาร จดหมายอิเล็กทรอนิกส์ ไลน์ เป็นต้น
- พนักงานที่ติดเชื้อ COVID-19 เข้ารับการรักษาตัวในโรงพยาบาล

4.2 หากตรวจพบว่าไม่มีการติดเชื้อ COVID-19 ให้ดำเนินการรักษาจนหายเป็นปกติและต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ

5. พนักงานที่ไม่มีอาการป่วย ให้สังเกตอาการตัวเองโดยการไม่ออกไปที่ชุมชนสาธารณะ งดการใช้สิ่งของร่วมกับผู้อื่น เป็นเวลา 10 วันและปฏิบัติดังนี้

5.1 พนักงานปฏิบัติงานที่บ้าน Work from Home โดยให้พนักงานใช้ Platforms Work from Home ที่ อจน. ได้นำมาใช้ ดังนี้

ที่	ชื่อระบบ	รายละเอียด
1	WMA Attendance	ให้ยืนยันเข้า-ออกตัวตนเข้าออกเวลาทำงาน (ดำเนินการตามคู่มือ)
2	Zoom Meeting	การประชุมออนไลน์
3	WMA Storage (on PC/Mobile)	การรวบรวมข้อมูล ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่ (ดำเนินงานตามคู่มือ)
4	E-Saraban	ระบบติดตามหนังสือภายในและภายนอก
5	Mail Go Thai (on PC/Mobile)	การส่งข้อมูล – เอกสาร ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์เคลื่อนที่(ดำเนินงานตามคู่มือ)
6	SCADA Control and Monitoring	ศูนย์ติดตาม และรายงานสถานการณ์น้ำเสียประเทศไทย

5.2 ให้พนักงานนำข้อมูลสำคัญที่ใช้ประกอบการทำงานขึ้นบน WMA Storage (สามารถเปิดได้บนเครื่อง PC หรือผ่านมือถือ) หรือนำใส่ External Hard disk เพื่อนำกลับไปทำงานที่บ้านในช่วงระยะเวลาที่สังเกตอาการ ในกรณีที่พนักงานไม่มีเครื่อง PC ทำงานที่บ้าน ให้ทำเรื่องขออนุมัติสายงานเพื่อเบิก Laptop ชั่วคราว หรือเครื่อง PC นำเครื่องกลับไปทำงานที่บ้าน

5.3 ให้พนักงาน Download Application/Software ชื่อ “Zoom” สำหรับใช้ในการประชุมออนไลน์ และให้ดำเนินการตามคู่มือการใช้งาน WMA Attendance คู่มือการใช้งาน Mail Go Thai (on PC/Mobile) และคู่มือการใช้งาน WMA Storage (on PC/Mobile) โดยหากจำเป็นต้องส่งหนังสือ/เอกสารให้พนักงานส่งทางตู้ไปรษณีย์ของ อจน. (ตู้ ป.ณ.1 ปณฝ คูคต 12131)

5.4 ให้ควบคุมผ่านระบบ Online Monitoring หรือระบบ SCADA ผ่านศูนย์ติดตามและรายงานสถานการณ์น้ำเสียประเทศไทย (War Room) จนกว่าสำนักงานจัดการน้ำเสียสาขานั้นจะสามารถกลับเข้าไปดำเนินการได้ตามปกติ

5.5 พนักงานติดตามข่าวสารและประกาศสถานการณ์การแพร่ระบาดของไวรัส COVID-19 อย่างต่อเนื่องจากหน่วยงานผ่านเว็บไซต์ (www.wma.or.th) จดหมายอิเล็กทรอนิกส์ Mail go.th หรือ Line และปฏิบัติตามอย่างเคร่งครัด

5.6 หากครบกำหนดแล้วไม่พบอาการป่วย ให้พนักงานเข้าพบแพทย์แผนปัจจุบันในโรงพยาบาลที่ได้มาตรฐานหลังจากแพทย์ลงความเห็นว่าไม่มีอาการป่วยแล้ว ต้องนำใบรับรองแพทย์มาแสดงก่อนเข้ามาปฏิบัติงานตามปกติ

6. กรณีที่มีความจำเป็นต้องจัดการประชุมหรือจัดตั้งสำนักงานใหญ่ชั่วคราว ให้ใช้สถานที่ที่พิจารณาแล้วว่าเหมาะสมหรือพื้นที่สำนักงานจัดการน้ำเสียสาขาจังหวัดใกล้กรุงเทพฯ

<u>ข้อปฏิบัติกรณีมีการประกาศปิดพื้นที่รอบๆ สำนักงานจัดการน้ำเสียสาขา เพื่อควบคุมการแพร่ไวรัส COVID-19</u>

1. ให้ ผจก. สจส. แจ้งให้ผู้บังคับบัญชาในสำนักงานใหญ่ ทราบโดยทันที

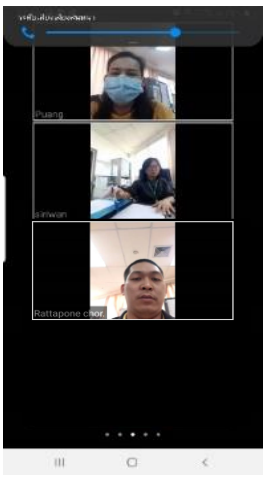
2. ให้พนักงานที่อาศัยในพื้นที่ที่มีการประกาศปิดพื้นที่แจ้งต่อผู้บังคับบัญชาให้ทราบโดยทันที

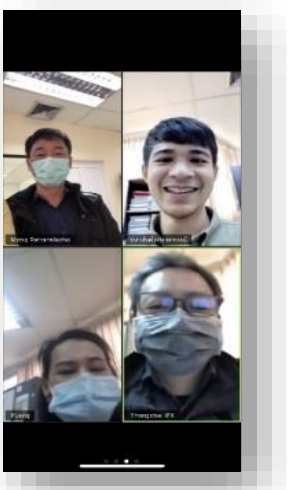
3. ในกรณีที่ไม่มีผู้ใดสามารถเดินทางมาปฏิบัติงาน ณ สจส. ได้ ให้ควบคุมระบบบำบัดน้ำเสียผ่านศูนย์ติดตามและรายงานสถานการณ์น้ำเสียประเทศไทย (War Room) จนกว่า สจส. สาขานั้นจะสามารถกลับเข้าไปดำเนินการได้ตามปกติ

4. ให้พนักงานที่อยู่ในพื้นที่ที่ได้รับการประกาศปิดพื้นที่ติดตามข่าวสารและประกาศสถานการณ์การแพร่ระบาดของไวรัส COVID-19 อย่างต่อเนื่องจากหน่วยงานผ่านทางเว็บไซต์ (www.wma.or.th) จดหมายอิเล็กทรอนิกส์ Mail go.th หรือ Line และปฏิบัติตามอย่างเคร่งครัด พร้อมทั้งรายงานให้ผู้บังคับบัญชาทราบเป็นระยะๆ

<u>ผลการซักซ้อมการป้องกันและควบคุมการแพร่ระบาดของเชื้อไวรัส COVID-19</u>

1. การทดสอบการประชุมทางไกล ภายในหน่วยงานโดยผ่านระบบ Zoom ระหว่างพนักงานและผู้บริหาร

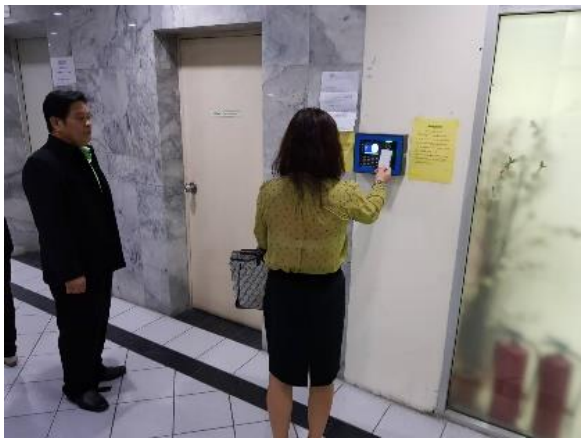




2. การจัดการประชุมโดยการเว่นระยะห่างซึ่งกันและกัน (Social Distancing) อย่างน้อย 1 เมตร



3. การใช้บัตรแทนการการสแกนลายนิ้วมือ



ภาคผนวก 2

การบริหารบำรุงรักษาระบบบำบัดน้ำเสีย

จากเหตุภาวะฉุกเฉิน

การบริหารบำรุงรักษาระบบบำบัดน้ำเสียจากเหตุภาวะฉุกเฉิน

ในกรณีเหตุภาวะฉุกเฉินที่อาจจะเกิดขึ้นบริเวณพื้นที่จัดการน้ำเสียหรือระบบบำบัดน้ำเสียของสำนักงานจัดการน้ำเสียสาขาต่างๆ ไม่ว่าจะเป็นเหตุที่เกิดจากภัยพิบัติ อุทกภัย อัคคีภัย ชุมนุม การก่อการร้าย และโรคระบาด เป็นต้น หรือเหตุการณ์ที่เกิดจากระบบบำบัดน้ำเสีย องค์การจัดการน้ำเสียมีแนวทางการป้องกันและแก้ไขปัญหาต่างๆ ที่เกิดขึ้น ดังนี้

ปัญหาที่เกิดกับระบบรวบรวมน้ำเสีย

1. ปัญหาขยะมูลฝอยและตะกอนสะสมในเส้นท่อ

สาเหตุ

- มีขยะมูลฝอย ดิน และทรายไหลจากพื้นผิวดินเข้าในเส้นท่อ

ผลกระทบ

- ทำให้เกิดกลิ่นเหม็น
- ทำให้เกิดการสึกหรอแก่เครื่องสูบน้ำหรือเกิดการอุดตันในเส้นท่อ และเป็นสาเหตุให้เครื่องจักรในระบบเสียหายได้

วิธีการป้องกัน/แก้ไข

- ตรวจสอบและทำความสะอาดท่อรวบรวมน้ำเสีย เช่น ใช้เครื่องมือล้างท่อที่ติดตั้งกับรถบรรทุก เรียกว่า รถดูดสิ่งโสโครกและฉีดล้างท่อ

2. ปัญหาท่อชำรุด แตก รั่ว

สาเหตุ

- ท่อรวบรวมน้ำเสียมีอายุการใช้งานมานาน หรือมีน้ำหนักมากดหรือกระแทกจนแตกหรือทรุดตัวจนเสียรูปทรงไป

ผลกระทบ

- ทำให้น้ำเสียไม่สามารถไหลผ่านไปได้ตามปกติ

- น้ำเสียไหลลงสู่แหล่งน้ำสาธารณะหรือแหล่งน้ำธรรมชาติ

วิธีการป้องกัน/แก้ไข

- ตรวจสอบตำแหน่งของส่วนที่ชำรุดแล้วจึงขุดดินลงไปจนถึงระดับของท่อที่ฝังอยู่ใช้กระสอบทรายกั้นน้ำชั่วคราวและกระเทาะปูนทรายที่ยึดรอยต่อของท่อ แล้วจึงปรับระดับท้องท่อโดยใช้ทรายรองพื้น จากนั้นก็นำท่อใหม่มาเปลี่ยนแทนท่อเดิมที่ชำรุด โดยการจัดวางท่อทั้ง 3 ท่อน ให้ได้แนวเดียวกัน แล้วจึงโบกปูนทรายโดยรอบรอยต่อของแต่ละท่อนดังเดิม แล้วรอให้ปูนทรายแข็งตัวก่อนที่จะกลบดินต่อไป
- ใช้ EM ช่วยลดความสกปรกของน้ำเสียระหว่างรอการแก้ไขซ่อมแซมท่อรวบรวมน้ำเสีย

3. ระบบควบคุมไฟฟ้าของเครื่องจักรขัดข้อง/เสียหาย

สาเหตุ

- มีการใช้งานของเครื่องจักรอย่างต่อเนื่องและเป็นระยะเวลานาน

ผลกระทบ

- เครื่องจักรกลไฟฟ้าตัวนั้นจะหยุดการทำงานในทันที จนกว่าจะมีการแก้ไขแล้วเปิดเดินเครื่องใหม่ ทำให้ระบบทำงานไม่สมบูรณ์

วิธีการป้องกัน/แก้ไข

- ตรวจสอบเบื้องต้นถึงสาเหตุความผิดปกติ เพื่อซ่อมแซมแก้ไข
- เปลี่ยนอุปกรณ์ทันทีในกรณีที่อุปกรณ์หลักเกิดการเสียหายใช้ไม่ได้

4. ระบบไฟฟ้ากำลังขัดข้อง

สาเหตุ

- ไฟฟ้าดับ หรืออุปกรณ์ชำรุดเสียหาย

ผลกระทบ

- หากขัดข้องเกินกว่า 6 ชั่วโมง เป็นผลให้เกิดความเสียหายต่อการทำงานของระบบ รวมทั้งการที่ไฟฟ้ากำลังขัดข้องบ่อยครั้ง จะลดอายุการทำงานของเครื่องจักรและอุปกรณ์ไฟฟ้าในระบบ

วิธีการป้องกัน/แก้ไข

- ปิด Main Control Breaker เพื่อตัดไฟในระบบพร้อมปิดสวิทช์ควบคุมวงจรอุปกรณ์ขนาดใหญ่ทั้งหมด
- ในกรณีที่ระบบไฟฟ้าปกติให้ทำการเปิด Main Control Breaker ก่อนแล้วจึงค่อยๆ เปิดสวิทช์เครื่องจักรแต่ละตัวเพื่อป้องกันการกระชากของกระแสไฟฟ้า
- ตรวจสอบการทำงานของเครื่องจักรกลที่อาจได้รับผลกระทบจากการขัดข้องของระบบไฟฟ้า เช่น เครื่องสูบน้ำ

5. ปัญหาที่เกิดกับประตูน้ำและวาล์ว

สาเหตุ

- ปัญหาจากการรั่วซึมหรือปิดไม่สนิท
- ปัญหาจากประตูน้ำฝืด

ผลกระทบ

- ทำให้ประตูน้ำไม่สามารถปิดให้สนิทและเกิดการรั่วซึมของน้ำ

วิธีการป้องกัน/แก้ไข

- ตรวจสอบหัวเปิด-ปิดวาล์วสัปดาห์ละครั้ง

6. อุปกรณ์เครื่องจักรกลเกิดการขัดข้อง

สาเหตุ

- มีอายุการใช้งานนานและมีการใช้งานอย่างต่อเนื่อง

ผลกระทบ

- ทำให้กระบวนการทำงานของระบบบำบัดน้ำเสียดำเนินไปอย่างไม่ต่อเนื่องและต้องหยุดสูบน้ำเสียเข้าระบบ
- น้ำที่ผ่านการบำบัดไม่มีคุณภาพตามความต้องการ

วิธีการป้องกัน/แก้ไข

- ตรวจสอบหัวเปิด-ปิดวาล์วสัปดาห์ละครั้ง

7. ตู้ควบคุมระบบไฟฟ้าเกิดการชำรุด

สาเหตุ

- สัตว์เข้าไปแทะทำลายสายไฟภายในตู้
- มีอายุการใช้งานนาน

ผลกระทบ

- ทำให้ระบบควบคุมไฟฟ้าเสียหายเสื่อมสภาพ

วิธีการป้องกัน/แก้ไข

- อุดช่องโหว่ของตู้ควบคุมระบบไฟ
- ฉีดพ่นยาฆ่าแมลงบริเวณโดยรอบตู้ควบคุมระบบไฟ
- เปลี่ยนตู้หากเกิดการชำรุดเสียหายมาก

ปัญหาที่เกิดกับบ่อบำบัดน้ำเสีย

1. ปริมาณน้ำเสียที่เข้าระบบบำบัดมีปริมาณน้อยกว่าปกติ

สาเหตุ

- มีขยะมูลฝอย ดิน และทรายไหลจากพื้นผิวดินเข้าในเส้นท่อ

ผลกระทบ

- ทำให้เกิดกลิ่นเหม็น
- ทำให้เกิดการสึกหรอแก่เครื่องสูบน้ำหรือเกิดการอุดตันในเส้นท่อ และเป็นสาเหตุให้เครื่องจักรในระบบเสียหายได้

วิธีการป้องกัน/แก้ไข

- ตรวจสอบและทำความสะอาดท่อรวบรวมน้ำเสีย เช่น ใช้เครื่องมือล้างท่อที่ติดตั้งกับรถบรรทุก เรียกว่า รถดูดสิ่งโสโครกและฉีดล้างท่อ

2. ปัญหาการรั่วซึมของบ่อ

สาเหตุ

- บ่อบำบัดมีลักษณะเป็นบ่อดิน ทำให้สัตว์เลื้อยคลานขุดรูเพื่อเป็นที่อาศัยได้ง่าย

ผลกระทบ

- ทำให้น้ำเสียในระบบบำบัดเกิดการรั่วซึมออกสู่ภายนอก
- เกิดการพังทลายของคันดิน

วิธีการป้องกัน/แก้ไข

- การก่อสร้างจะต้องบดอัดคันดินให้แข็งแรง และมีความลาดชันของคันดินเพียงพอ
- ปลูกหญ้าบริเวณคันดิน เพื่อจะช่วยยึดดินไม่ให้พังทลายได้
- ตรวจสอบรอบๆ บ่อ ขจัดเศษอาหารรอบบ่อ
- คอยซ่อมแซมส่วนที่พังทลายของบ่อ

3. น้ำในบ่อบำบัดเกิดกลิ่นเหม็นที่รุนแรง

สาเหตุ

- การหมักหมมของตะกอนที่ก้นบ่อและเกิดภาวะไร้ออกซิเจน

ผลกระทบ

- ตะกอนจะลอยขึ้นเป็นฝ้าไขทำให้ปิดกั้นการถ่ายเทออกซิเจนจากอากาศลงสู่น้ำในบ่อ เครื่องจักรในระบบเสียหายได้

วิธีการป้องกัน/แก้ไข

- ต้องคอยกวาดหรือตักฝ้าตะกอนทิ้งแล้วทำลายอยู่เสมอจะลดปัญหาเรื่องกลิ่นลงได้

4. ระยะเวลาเก็บกักน้ำในบ่อลดลง

สาเหตุ

- สารแขวนลอยในน้ำเสียจะเกิดการตกตะกอนและสะสมอยู่ที่ก้นบ่อมากเกินไป

ผลกระทบ

- บ่อบำบัดตื้นขึ้นทำให้น้ำที่ออกจากระบบยจึงไม่ดีพอ

วิธีการป้องกัน/แก้ไข

- ควรมีการตรวจวัดความลึกของบ่อเป็นระยะๆ เพื่อประเมินการสะสมของตะกอนที่ก้นบ่อ
- วัดความลึกที่กลางบ่ออย่างน้อยปีละ 1 ครั้ง ถ้ามีการสะสมหนามากกว่า 50 ซม. ให้ทำการขุดลอกตะกอนออกจากบ่อ

5. สาหร่ายเติบโตเร็วมากเกินไป

สาเหตุ

- มีสภาพปัจจัยต่างๆ ที่เหมาะสมในการเจริญเติบโตของสาหร่าย

ผลกระทบ

- น้ำทิ้งที่ผ่านการบำบัดมีปริมาณของแข็งแขวนลอย (SS) และค่า BOD เกินมาตรฐานที่กำหนดไว้
- แหล่งรับน้ำทิ้งมีปริมาณสาหร่ายเพิ่มมากขึ้นอาจก่อให้เกิดปัญหา Algae Bloom ตามมาเมื่อสภาวะเหมาะสม

วิธีการป้องกัน/แก้ไข

- ปล่อยน้ำออกที่ระดับใต้ผิวน้ำที่มีสาหร่ายน้อย
- ปลูกผักตบชวาในบ่อบ่มบ่อสุดท้าย
- ก่อสร้างบึงประดิษฐ์ก่อนปล่อยลงสู่แหล่งน้ำธรรมชาติ

6. มีสารพิษเข้าสู่ระบบ

สาเหตุ

- น้ำในบ่อบำบัดมีอุณภูมิสูงทำให้เกิดความเป็นกรด เป็นด่างสูง

ผลกระทบ

- มีผลกระทบต่อจุลินทรีย์ภายในระบบบำบัดน้ำเสีย ทำให้น้ำทิ้งไม่ผ่านเกณฑ์มาตรฐาน

วิธีการป้องกัน/แก้ไข

- ตรวจสอบระดับสารพิษ เช่น ค่า pH อุณหภูมิ ทุกวัน
- หากพบว่าน้ำเสียมีค่า pH ต่ำหรือสูงเกินไป หรืออุณหภูมิสูงเกินไป ให้สูบน้ำเสียเข้าบ่อเก็บน้ำฝนจนกว่าจะเข้าสู่สภาวะปกติ

ภาคผนวก ๓

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

(Cyber Incident Response Plan: CIRP)

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Plan: CIRP)

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ เป็นแผนงานที่กำหนดเป็นลายลักษณ์อักษร แสดงถึงวิธีปฏิบัติเพื่อตอบสนองเมื่อเกิดเหตุภัยคุกคามทางไซเบอร์ที่ปัจจุบันมีแนวโน้มเพิ่มสูงขึ้นเป็นอย่างมาก โดยครอบคลุมระบบงานด้านเทคโนโลยีสารสนเทศที่สำคัญขององค์กร และได้รับอนุมัติจากคณะกรรมการขององค์กรหรือคณะกรรมการชุดย่อยที่ได้รับมอบหมาย อีกทั้งควรมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ นอกจากนี้แผน CIRP ควรครอบคลุมตั้งแต่กระบวนการจัดการ การเตรียมความพร้อมในการรับมือ การตอบสนองต่อเหตุการณ์ และการรายงานเหตุการณ์ภัยคุกคามทางไซเบอร์ที่อาจก่อให้เกิดความเสียหายหรือส่งผลกระทบต่อระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรือข้อมูลอื่นที่เกี่ยวข้อง

ทั้งนี้ องค์การจัดการน้ำเสีย (อจน.) ควรพิจารณาจัดให้มีบุคลากรหรือทีมงานที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Team) โดยอย่างน้อยทีมรับมือและตอบสนองฯ ควรประกอบด้วยบุคลากร ดังต่อไปนี้

๑) บุคลากรที่ทำหน้าที่รับแจ้งเหตุหรือรับรายงานด้านความมั่นคงปลอดภัยทางเทคโนโลยีสารสนเทศจากผู้ที่พบหรือสงสัยว่ามีเหตุภัยคุกคามเกิดขึ้นภายในองค์กร โดยควรจัดให้มีช่องทางในการรายงาน เช่น ช่องทางอีเมล โทรศัพท์ โทรสาร แอปพลิเคชัน Line Social Media แบบฟอร์มบนเว็บไซต์ หรือระบบที่รวบรวมข้อมูลอัตโนมัติ และการสื่อสารทางตรง เป็นต้น

๒) บุคลากรที่ทำหน้าที่รับผิดชอบในการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ ทั้งนี้หน่วยงานอาจพิจารณาเพิ่มจำนวนบุคลากรที่มีความเชี่ยวชาญตามความเหมาะสมของความเสี่ยงและระดับความรุนแรงของภัยคุกคามที่อาจเกิดขึ้น โดยอาจจัดหาบุคลากรที่มีทักษะทางเทคนิคที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ เช่น การตรวจจับภัยคุกคามการวิเคราะห์โปรแกรมไม่ประสงค์ดี (Malware) การบริหารจัดการระบบและเครือข่าย การสนับสนุนทางเทคนิค เป็นต้น

ทั้งนี้ หน่วยงานสามารถดำเนินการใช้บริการ Security Operation Center (SOC) จากผู้ให้บริการภายนอกได้ในการปฏิบัติงานดังกล่าว โดยหน่วยงานควรกำหนดเงื่อนไขให้ผู้บริการภายนอกปฏิบัติตามนโยบายด้านการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเตอร์เน็ตของ อจน. พร้อมทั้งมีการประเมินความความเสี่ยงจากการใช้ผู้ให้บริการภายนอก รวมถึงตรวจสอบและติดตามการให้บริการอย่างสม่ำเสมอ

แผนรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ควรระบุขั้นตอนการรับมือและตอบสนองเหตุการณ์ที่ชัดเจน เพื่อให้สามารถดำเนินการได้อย่างรวดเร็วและง่ายต่อการปฏิบัติ โดยอย่างน้อยควรครอบคลุม

- ชื่อแผน วัตถุประสงค์ และขอบเขต

- โครงสร้างของการบังคับบัญชาในการดำเนินการตามแผน ผู้ปฏิบัติหน้าที่และความรับผิดชอบและผู้ปฏิบัติหน้าที่แทนในกรณีผู้ปฏิบัติหน้าที่หลักที่ได้รับมอบหมายไม่สามารถปฏิบัติงานได้ รวมถึงบันทึกการบันทึกการเปลี่ยนแปลงของแผน

- รายละเอียดของระบบเทคโนโลยีสารสนเทศ เช่น โครงสร้างสถาปัตยกรรมเครือข่าย เป็นต้น

- ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์และแผนการสื่อสารให้หน่วยงานที่เกี่ยวข้องรับทราบ

- ขั้นตอนการกู้คืนระบบ โดยจัดทำเป็นเอกสาร หรือคู่มือ หรือ Checklist เพื่อควบคุมกระบวนการให้เป็นไปตามขั้นตอนที่กำหนดไว้

การรับมือภัยคุกคามทางไซเบอร์ (Incident Response) เพื่อใช้ในการบริหารจัดการความเสี่ยง รวมถึงตอบสนองต่อเหตุการณ์ที่เกิดขึ้นเพื่อให้หน่วยงานสามารถดำเนินการด้านเทคโนโลยีสารสนเทศได้อย่างต่อเนื่อง พร้อมทั้งลดผลกระทบที่มีต่อข้อมูลสารสนเทศ และเครือข่ายทางสารสนเทศให้น้อยที่สุด เพื่อให้ธุรกิจยังสามารถดำเนินงานได้อย่างต่อเนื่องและสร้างความเชื่อมั่นให้กับลูกค้าหรือผู้มีส่วนได้เสียตลอดเวลา

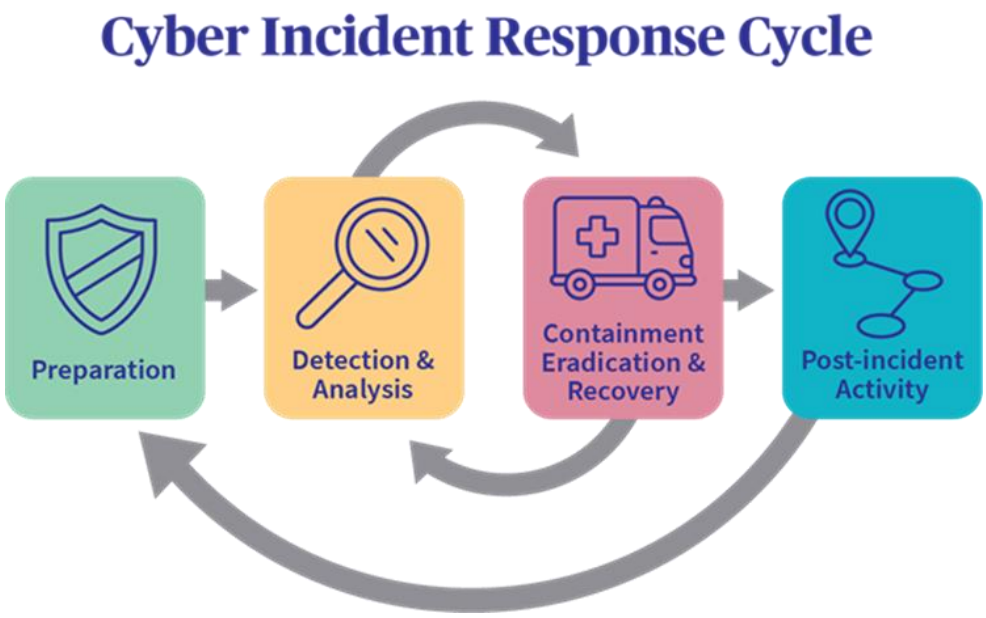
แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Cycle) จะกำหนดขั้นตอนการดำเนินงาน รวมทั้งการดำเนินงานด้านเทคนิคอย่างละเอียดเพื่อให้สามารถดำเนินงานตามแผนและได้ผลลัพธ์ตามที่กำหนดโดยต้องครอบคลุมในเรื่องดังต่อไปนี้

๑. การเตรียมความพร้อม (Preparation)

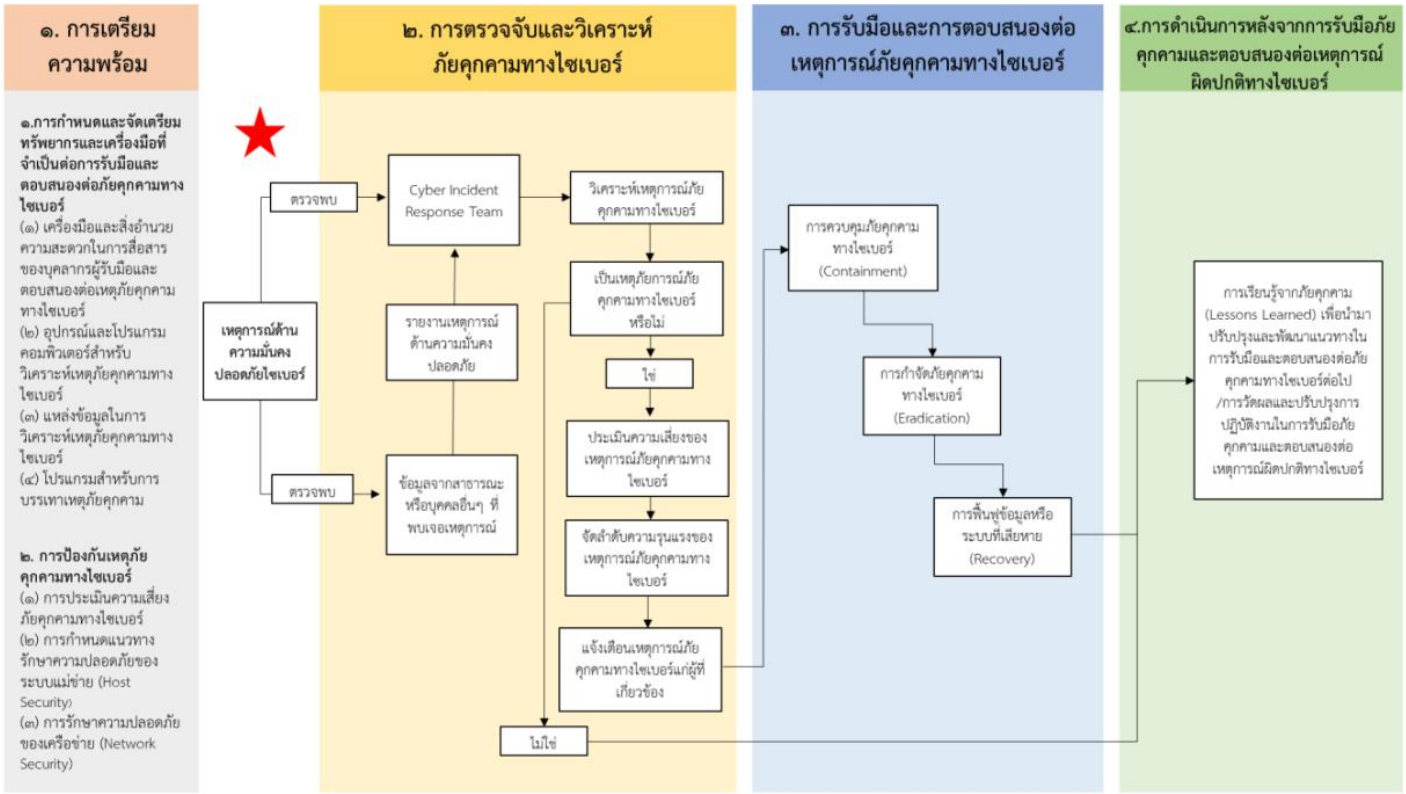
๒. การตรวจจับและวิเคราะห์ (Detection & Analysis)

๓. การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน (Containment, Eradication & Recovery)

๔. การดำเนินการหลังจากการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์เสร็จสิ้น (Post-Incident Activity)



รูปที่ ๑ แนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Cyber Incident Response Cycle)



รูปที่ ๒ แผนภาพสรุปแนวทางการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

ขั้นตอนการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

หน่วยงานควรกำหนดขั้นตอนการรับมือและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ โดยสามารถแบ่งได้เป็น ๔ ขั้นตอน ดังนี้

<u>ขั้นตอนที่ ๑</u> : การเตรียมความพร้อม (Preparation)

๑.๑ การกำหนดและจัดเตรียมทรัพยากรและเครื่องมือที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมถึงการกำหนดแนวทางการติดต่อสื่อสารอย่างเป็นระบบ หน่วยงานควรมีเครื่องมือสำหรับทำการวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์และมีการกำหนดแนวทางรักษาความปลอดภัยของระบบแม่ข่าย (Host Security) ควรติดตั้งโปรแกรม (Software) เพื่อตรวจจับและยับยั้งโปรแกรมไม่ประสงค์ดี (Malware) ภายในระบบเทคโนโลยีสารสนเทศขององค์กร ระบบปฏิบัติการ ระบบโปรแกรมที่ใช้งาน (Application) และระบบโปรแกรมงานสำหรับลูกค้า (Application Clients) รวมถึงมีกระบวนการประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและระบบงานที่สำคัญของหน่วยงาน โดยอย่างน้อยเครื่องมือและทรัพยากรที่จำเป็นต่อการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ควรครอบคลุม ดังนี้

(๑) เครื่องมือและสิ่งอำนวยความสะดวกในการสื่อสารของบุคลากรผู้ทำหน้าที่รับมือและตอบสนองต่อเหตุภัยคุกคามทางไซเบอร์

(๑.๑) รายชื่อและช่องทางการติดต่อสำหรับสมาชิกภายในทีมรับมือภัยคุกคามทางไซเบอร์ รวมถึงหน่วยงานอื่นๆ ที่จำเป็นต่อการรับมือเหตุทั้งภายในและภายนอกองค์กร (รายชื่อผู้รับผิดชอบหลัก และรายชื่อสำรอง) เช่น ฝ่ายรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ฝ่ายบริหารความเสี่ยง ฝ่ายสื่อสารองค์กร ฝ่ายทรัพยากรบุคคล คู่ค้าและผู้มีส่วนได้ส่วนเสียขององค์กร เป็นต้น

(๑.๒) รายชื่อและช่องทางการติดต่อสำหรับทีมหรือหน่วยงานภายในองค์กรในกรณีที่มีการยกระดับความรุนแรงของเหตุการณ์โดยสามารถให้ความช่วยเหลือหรือรับช่วงต่อในการรับมือได้ทันท่วงทีหลังได้รับการแจ้ง

(๑.๓) ช่องทางการรายงานเหตุการณ์ เช่น หมายเลขโทรศัพท์ อีเมล แบบรายงานออนไลน์ และระบบการส่งข้อความทันทีที่มีเหตุการณ์กระทบต่อความมั่นคงปลอดภัย เพื่อให้ผู้ใช้งานทั่วไปสามารถใช้ในการรายงานเหตุการณ์ที่เข้าข่ายจะเป็นภัยคุกคามทางไซเบอร์

(๑.๔) ระบบในการรายงานและติดตามข้อมูล สถานะการดำเนินการของเหตุการณ์ที่ได้รับแจ้ง

(๑.๕) โปรแกรมเข้ารหัส (Encryption Software) เพื่อเพิ่มความปลอดภัยในการสื่อสารทั้งระหว่างภายในและภายนอกองค์กร

(๑.๖) ห้องประชุม (War Room) สำหรับการสื่อสารและประสานงานระหว่างส่วนกลางและหน่วยงานที่เกี่ยวข้อง ซึ่งอาจเป็นห้องประชุมที่ใช้งานชั่วคราวเพื่อการรับมือภัยคุกคามทางไซเบอร์ก็ได้

(๑.๗) สถานที่จัดเก็บที่มีความมั่นคงปลอดภัยเพื่อใช้ในการจัดเก็บหลักฐานข้อมูลและพยานวัตถุอื่นๆ ที่สำคัญ

(๒) อุปกรณ์และซอฟต์แวร์สำหรับวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๒.๑) เครื่องคอมพิวเตอร์หรืออุปกรณ์สำรองข้อมูล (Backup Device) ที่ใช้งานเพื่อการจัดเก็บข้อมูลบันทึกเหตุการณ์ (Log Files) หรือสร้าง Disk Image หรือบันทึกข้อมูลเหตุการณ์ที่เกี่ยวข้องอื่นๆ โดยเฉพาะ

(๒.๒) เครื่องมือสำหรับตรวจจับและวิเคราะห์ข้อมูลในเครือข่ายคอมพิวเตอร์ (Packet Sniffers and Protocol Analyzers) เพื่อใช้ศึกษาพฤติกรรมของ Malware หรือความผิดปกติของเครือข่ายเครื่องคอมพิวเตอร์สำรอง และอุปกรณ์ที่ใช้ในการรวบรวมหลักฐาน เป็นต้น

(๒.๓) เครื่องคอมพิวเตอร์สำรอง เซิร์ฟเวอร์ และอุปกรณ์เครือข่ายที่สามารถใช้ทดแทนเครื่องคอมพิวเตอร์หรืออุปกรณ์หลักได้ ซึ่งสามารถใช้เพื่อสำหรับสนับสนุนการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์

(๒.๔) อุปกรณ์ที่ใช้ในการรวบรวมหลักฐาน เช่น โน้ตบุ๊ค กล้องดิจิทัล เครื่องบันทึกเสียงแบบบันทึกข้อมูลผู้ครอบครองพยานหลักฐาน เป็นต้น เพื่อเก็บหลักฐานสำหรับการดำเนินการทางกฎหมาย

๓) แหล่งข้อมูลในการวิเคราะห์เหตุภัยคุกคามทางไซเบอร์ (Cyber Incident Analysis Resources)

(๓.๑) รายการพอร์ตช่องทางการแลกเปลี่ยนข้อมูลผ่านอินเตอร์เน็ตหรือระบบเครือข่ายคอมพิวเตอร์ (Port Lists) ตั้งแต่พอร์ตที่ใช้งานทั่วไปจนถึงพอร์ตที่เสี่ยงต่อการถูกโจมตี

(๓.๒) เอกสารหรือคู่มือการใช้งานของระบบปฏิบัติการแอปพลิเคชันโปรโตคอลที่ใช้ในการสื่อสาร ระหว่างเครื่องคอมพิวเตอร์ซอฟต์แวร์สำหรับตรวจจับการบุกรุกและซอฟต์แวร์ป้องกันไวรัส

(๓.๓) แผนผังเครือข่ายและรายการทรัพย์สินทางสารสนเทศที่สำคัญ เช่น ฐานข้อมูลเป็นต้น

(๓.๔) ค่าปกติ (Current Baseline) ของระบบเครือข่าย และแอปพลิเคชัน

(๓.๕) ค่า hash ของไฟล์ที่มีความสำคัญ เพื่อเพิ่มความเร็วในการวิเคราะห์การตรวจสอบ และกำจัดภัยคุกคามที่เกิดขึ้น

(๔) ซอฟต์แวร์สำหรับการบรรเทาเหตุภัยคุกคาม

ไฟล์ disk image ของระบบปฏิบัติการ (OS) และแอปพลิเคชัน (Application) เพื่อใช้ในการกู้คืนและฟื้นฟูระบบ เป็นต้น

ทั้งนี้ หน่วยงานสามารถพิจารณาเพิ่มเติมได้ในเรื่องดังต่อไปนี้

- คอมพิวเตอร์ที่ใช้สำหรับการวิเคราะห์หลักฐานทางดิจิทัล (Digital Forensic Workstation) ที่ต้องแยกจากการใช้งานอื่นๆ รวมถึงการเชื่อมต่อทางเครือข่าย และต้องได้รับการตั้งค่าเพื่อความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงข้อมูล หลักฐาน และการวิเคราะห์โดยมิชอบ และการปนเปื้อนของหลักฐาน (Cross-Contamination)

- Backup Device สำหรับใช้ในการเก็บข้อมูลต่างๆ ที่จำเป็นและเกี่ยวข้องกับ Incident เช่น log file, Screen Capture, บันทึกการสัมภาษณ์ผู้ใช้งาน เป็นต้น

- เครื่องคอมพิวเตอร์สำหรับใช้ในการวิเคราะห์ (Analyst Laptop) เพื่อใช้ในการวิเคราะห์ Malware, ดักจับ Live Packet

- เครื่องพิมพ์เคลื่อนที่ (Portable Printer) สำหรับกรณีที่มีความจำเป็นต้องพิมพ์ข้อมูลออกจากระบบปลายทางเป็นกระดาษ

- โปรแกรมสำหรับวิเคราะห์และกู้คืนข้อมูลหลักฐานทางดิจิทัล (Digital forensic software) เช่น Hard Disk Image เป็นต้น เพื่อใช้ในการหาข้อสรุปหรือสาเหตุของ Incident

- อุปกรณ์ในการเชื่อมต่อและเก็บข้อมูลหลักฐานจากแหล่งข้อมูลทางดิจิทัลต่างๆ (Evidence Gathering Accessories) เช่น Computer, Network Storage, Removable Media, Mobile Device เป็นต้น

- Threat Intelligence Information ที่ให้ข้อมูลภัยคุกคามที่เป็นที่รู้จักเพื่อเพิ่มความรวดเร็วของกระบวนการตอบสนอง ให้ทราบถึงการมีอยู่ของภัยคุกคามภายในระบบได้อย่างรวดเร็ว ประกอบด้วย

  - เครื่องมือและวิธีการที่ภัยคุกคามใช้ (Threat Agent's Tools, Tactics, Procedure) เช่น Protocol ที่เป็นเป้าหมายของการโจมตี, Malware ที่ใช้ในการโจมตี เป็นต้น
  - ช่องโหว่ที่เกี่ยวข้องกับระบบในความดูแล (Vulnerability Databases) เพื่อใช้ประกอบการวิเคราะห์ความน่าจะเป็น รวมถึงร่องรอยที่เป็นไปได้หากเกิดการโจมตีขึ้น
  - Malware Indicator of Compromise (IoC) ข้อมูลที่บ่งชี้ว่าการถูกโจมตีสำเร็จ เช่น Cryptographic Hash, commonly used port lists: Network port ต่างๆ ที่ถูกใช้โดย Malware และ Channel ปลายทางที่ระบบที่ถูกโจมตีสำเร็จจะต้องติดต่อด้วยเพื่อรับคำสั่งจากผู้โจมตีหรือส่งข้อมูลที่จารกรรมได้ออกไป เป็นต้น

- รายการทรัพย์สินสารสนเทศที่สำคัญ โดยอย่างน้อยควรประกอบด้วย Hardware, Software, Data, Network Diagram, Data Flow Diagram

- การศึกษาและเข้าใจพฤติกรรมการทำงานปกติของระบบ เครือข่าย และแอปพลิเคชั่น (Baseline) เพื่อช่วยในการสังเกตพฤติกรรมที่ผิดปกติและสามารถตรวจจับได้เร็วขึ้น โดยการตรวจสอบบันทึกเหตุการณ์ และการแจ้งเตือนด้านความมั่นคงปลอดภัย เพื่อให้มีความคุ้นเคยและจะช่วยให้การสังเกตเหตุการณ์และการแจ้งเตือนที่ผิดปกติได้เร็วและแม่นยำมากยิ่งขึ้น เช่น Network, Operating System Software Whitelist, Application เป็นต้น

- ตัวอย่างช่องทางการสื่อสาร

- สื่อหลักประเภทโทรทัศน์ วิทยุ Social Media และ Website สำหรับใช้กรณีสถานการณ์ที่ประชาชนส่วนใหญ่ได้รับผลกระทบ โดยสามารถเลือกใช้ช่องทางใดช่องทางหนึ่งหรือหลายๆ ช่องทางร่วมกัน
- อีเมล (Email) สำหรับใช้ในการติดต่อประสานงานภายในหน่วยงานหรือกับหน่วยงานภายนอกที่เป็นทางการ เช่น การสรุปข้อมูลการโจมตีทางไซเบอร์ที่เกิดขึ้น การนัดประชุม หรือการปฏิบัติการร่วม เป็นต้น
- Instant Messaging สำหรับใช้ในการติดต่อสื่อสารประสานงานภายในหน่วยงานหรือกับหน่วยงานภายนอกกรณีเร่งด่วน และสามารถมีบันทึกการสื่อสารไว้อ้างอิงภายหลัง
- โทรศัพท์มือถือ สำหรับใช้ในการติดต่อสื่อสารประสานงานภายในหน่วยงานหรือกับภายนอกหน่วยงานกรณีเร่งด่วน หรือใช้ในการยืนยันเมื่อมีการส่งข้อมูลเอกสารที่เป็นทางการไปแล้วอีกครั้งหนึ่ง

๑.๒ การดำเนินการป้องกันเหตุภัยคุกคามทางไซเบอร์ก่อนเกิดเหตุ (Preventing Incidents)

สิ่งสำคัญที่สุดในการป้องกันเหตุภัยคุกคามทางไซเบอร์ คือ การลดจำนวนเหตุภัยคุกคามให้เหลือน้อยที่สุด เพื่อลดผลกระทบต่อการดำเนินงานของหน่วยงาน หากหน่วยงานมีมาตรการการรักษาความมั่นคงปลอดภัยที่ไม่เพียงพอ อาจทำให้เกิดเหตุภัยคุกคามมากจนเกินขีดความสามารถในการจัดการของหน่วยงาน ซึ่งส่งผลให้การรับมือและตอบสนองกับเหตุภัยคุกคามที่เกิดขึ้นล่าช้าและไม่มีประสิทธิภาพ อาจส่งผลกระทบทางธุรกิจที่รุนแรงต่อหน่วยงานได้

การป้องกันเหตุภัยคุกคามทางไซเบอร์ ควรครอบคลุมอย่างน้อยในเรื่องดังต่อไปนี้

๑) การประเมินความเสี่ยงภัยคุกคามทางไซเบอร์

หน่วยงานควรทำการประเมินความเสี่ยง เพื่อพิจารณาว่ามีความเสี่ยงใดบ้างที่เกี่ยวข้องกับภัยคุกคามทางไซเบอร์หรือช่องโหว่ด้านความมั่นคงปลอดภัย โดยควรระบุเหตุการณ์

ภัยคุกคามที่อาจเกิดขึ้นและส่งผลกระทบหรือสร้างความเสียหายต่อระบบงาน ข้อมูลสำคัญ และการดำเนินงานขององค์กร

ทั้งนี้ ควรประเมินความเสี่ยงรวมทั้งผลกระทบที่เกิดขึ้นจริงในระหว่างการเกิดเหตุอย่างน้อยปีละ ๑ ครั้ง เพื่อประเมินผลกระทบและมูลค่าความเสียหายที่แท้จริงและเป็นข้อมูลประกอบการพิจารณาทบทวนหรือปรับปรุงแนวทางในการรับมือและการตอบสนองต่อภัยคุกคามทางไซเบอร์ต่อไป

(๒) การกำหนดแนวทางรักษาความมั่นคงปลอดภัยของระบบแม่ข่าย (Host Security)

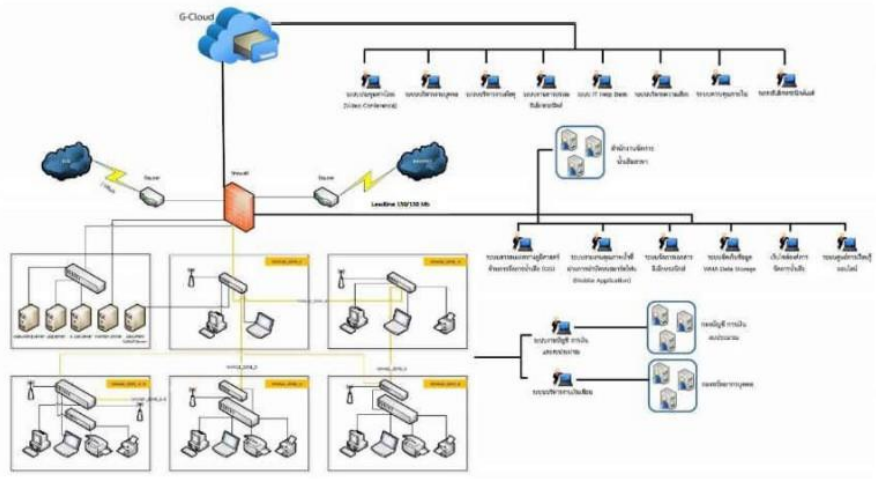
ระบบแม่ข่าย (Host) ควรกำหนดให้มีการรักษาความมั่นคงปลอดภัยที่เหมาะสมและมีมาตรฐาน รวมทั้งการปิดช่องโหว่และทำการแพตช์ระบบอย่างเหมาะสม นอกจากนี้ ควรมีการกำหนดสิทธิ์ของผู้ใช้งาน โดยให้สิทธิเท่าที่จำเป็นต่อการปฏิบัติงานที่ได้รับอนุญาตเท่านั้น รวมทั้งระบบแม่ข่ายควรบันทึกเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่สำคัญของหน่วยงาน และได้รับการติดตามตรวจสอบอย่างสม่ำเสมอ

(๓) การรักษาความปลอดภัยของเครือข่าย (Network Security)

ระบบการรักษาความมั่นคงปลอดภัยของเครือข่าย ควรตั้งค่าให้ปฏิเสธการเข้าถึงของกิจกรรมทั้งหมดที่ไม่ได้รับอนุญาต รวมทั้งอุปกรณ์เครือข่ายทั้งหมดของหน่วยงานที่เชื่อมต่อกับเครือข่ายภายนอก

(๔) การจัดให้มี User Awareness training

เพื่อให้ทุกคนในองค์กรมีความรู้ความเข้าใจ มีความตระหนัก มีความระมัดระวังและเข้าใจถึงความผิดปกติที่เกิดขึ้นจากการโจมตีทางไซเบอร์รวมทั้งเข้าใจวิธีการตอบสนองในเบื้องต้นและดำเนินการแจ้งให้หน่วยงานที่ทำหน้าที่ในการรับมือและตอบสนองรับทราบเมื่อมีเหตุการณ์ผิดปกติเกิดขึ้น



รูปที่ ๓ ตัวอย่าง Network Diagram

ตัวอย่างตารางทะเบียนทรัพย์สินสารสนเทศของ อจน.

1. รายการทะเบียนทรัพย์สินสารสนเทศประเภทอุปกรณ์ (Hardware)								
เลขทะเบียนทรัพย์สินสารสนเทศ	**ประเภท Hardware**	**ลักษณะการใช้งาน**	**ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)**	**ผู้เป็นเจ้าของ Hardware**	**ผู้ใช้งาน**	**ที่ตั้ง**	**วันที่เริ่มบำรุงรักษา**	**หมายเหตุ**
A-3130-54-3509-008	เครื่องคอมพิวเตอร์แม่ข่าย	GIS Server	สูง	กสป.	กสป.	ห้อง Server	2011-05-12	

2. รายการทะเบียนทรัพย์สินสารสนเทศประเภทระบบ (Software)								
เลขทะเบียนทรัพย์สินสารสนเทศ	**ประเภท Software**	**ลักษณะการใช้งาน**	**ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)**	**ผู้เป็นเจ้าของ Software**	**ผู้ใช้งาน**	**ที่ตั้ง**	**วันที่เริ่มบำรุงรักษา**	**หมายเหตุ**
A-3130-54-3516-011	โปรแกรมระบบงานบัญชีและการเงิน	Oracle Standard Edition	สูง	กสป.	กบช. กงป. กกง.	ห้อง Server	2011-05-12	

3. รายการทะเบียนทรัพย์สินสารสนเทศประเภทข้อมูล (Data)								
เลขทะเบียน	**ประเภท Data**	**ลักษณะการใช้งาน**	**ระดับความมั่นคงปลอดภัย (สูง/ปานกลาง/ต่ำ)**	**ผู้เป็นเจ้าของ Data**	**ผู้ใช้งาน**	**ที่ตั้ง**	**วันที่เริ่มบำรุงรักษา**	**หมายเหตุ**
A-3130-60-3550-001	log file	จัดเก็บ	สูง	กสป.	กสป.	ห้อง Server	2016-12-01	

<u>ขั้นตอนที่ ๒</u> : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)

การรวบรวมข้อมูลและตรวจวิเคราะห์จากระบบงานที่มีช่องโหว่จากการโจมตีทางไซเบอร์ภายในองค์กร ควรมีเครื่องมือในการชี้วัดและเฝ้าระวังภัยคุกคามทางไซเบอร์จากหลายแหล่งที่มา โดยอย่างน้อยต้องมีการจัดเก็บและสอบทานบันทึกการเข้าถึงระบบ (Access Log) และบันทึกการดำเนินงาน (Activity Log) และทำการแจ้งเตือนแก่ผู้เกี่ยวข้องเมื่อพบเหตุการณ์ภัยคุกคามทางไซเบอร์

(๑) รูปแบบของการโจมตีหรือภัยคุกคามที่มีโอกาสเกิดขึ้นหรือพบเห็นบ่อยครั้ง

(๑.๑) การโจมตีหรือภัยคุกคามที่เกิดจากสื่อบันทึกข้อมูลที่สามารถถอดหรือเคลื่อนย้ายได้ หรืออุปกรณ์ต่อพ่วง เช่น มัลแวร์ที่แพร่กระจายเข้าระบบงานจากแฟลชไดรฟ์ USB ที่ติดมัลแวร์

(๑.๒) การโจมตีเพื่อทำให้ระบบประสิทธิภาพลดลง เช่น การโจมตีแบบ DDoS เพื่อทำให้ไม่สามารถให้บริการได้ เป็นต้น

(๑.๓) การโจมตีผ่านเว็บไซต์หรือระบบงานบนเว็บไซต์ เช่น การโจมตีด้วยวิธี Cross Site Scripting เพื่อขโมยข้อมูล หรือการเปลี่ยนเส้นทางไปยังเว็บไซต์ที่มีการโจมตีผ่านช่องโหว่ของ Web Browser และติดตั้งมัลแวร์ไว้ และการโจมตีผ่านทางข้อความหรือเอกสารแนบในอีเมล เป็นต้น

(๑.๔) การโจมตีที่เข้าข่ายการปลอมแปลงตัวตน เช่น การปลอมตัว (Spoofing) เพื่อหลอกลวงและควบคุมระบบการโจมตีโดยการปลอมตัวเป็นบุคคลอื่นเพื่อแทรกสัญญาณการรับส่งข้อมูลระหว่างผู้ใช้งานระบบ (Man in the Middle Attack) และการโจมตีโดยส่งคำสั่ง SQL ผ่านทางระบบงานบนเว็บไซต์เพื่อไปโจมตีระบบฐานข้อมูล (SQL Injection) เป็นต้น

(๑.๕) ภัยคุกคามที่เกิดจากผู้ใช้งานละเมิดนโยบายการใช้งานระบบเทคโนโลยีสารสนเทศขององค์กร เช่น การติดตั้งโปรแกรมที่นำไปสู่การรั่วไหลข้อมูลสำคัญของหน่วยงานหรือผู้ใช้งานทำกิจกรรมที่ผิดกฎหมายผ่านระบบงานเทคโนโลยีสารสนเทศของหน่วยงาน เป็นต้น

(๑.๖) อุปกรณ์คอมพิวเตอร์หรือสื่อต่างๆ สูญหาย เช่น เครื่องโน๊ตบุ๊ค แท็บเล็ต โทรศัพท์มือถือ หรือสิ่งที่ใช้ยืนยันตัวตนซึ่งเป็นทรัพย์สินของบริษัทที่สูญหายหรือถูกขโมย

(๒) สัญญาณการเกิดเหตุภัยคุกคาม สามารถติดตามได้จากช่องทางอย่างน้อยดังต่อไปนี้

(๒.๑) สัญญาณแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์สามารถตรวจสอบได้จากระบบดังต่อไปนี้

- ระบบตรวจจับและป้องกันการบุกรุก (Intrusion Detection and Prevention Systems: IDPS) ใช้ในการระบุเหตุการณ์ที่น่าสงสัยว่าอาจเป็นภัยคุกคามและบันทึกข้อมูลที่เกี่ยวข้อง รวมถึงวันที่และเวลาที่ตรวจพบการโจมตี ประเภทของการโจมตี ที่อยู่ IP ต้นทางและ

ปลายทาง และชื่อผู้ใช้งาน โดยส่วนใหญ่ระบบ IDPS จะระบุกิจกรรมที่เป็นอันตรายโดยใช้ลักษณะเฉพาะของการโจมตี (Attack Signature) ดังนั้น ข้อมูลลักษณะเฉพาะของการโจมตีจะต้องได้รับการอัปเดตอย่างสม่ำเสมอ เพื่อให้สามารถตรวจพบการโจมตีรูปแบบใหม่ได้ ทั้งนี้ ระบบ IDPS สามารถเกิดการแจ้งเตือนที่ผิดพลาดได้ (False Positive) โดยแจ้งว่ามีกิจกรรมที่เป็นอันตรายกำลังเกิดขึ้น แต่ในความจริงยังไม่เกิด ดังนั้น นักวิเคราะห์ระบบจึงควรตรวจสอบข้อมูล แจ้งเตือนจาก IDPS ด้วยตนเองและทบทวนรายละเอียดหรือรวมรวมข้อมูลที่เกี่ยวข้องจากแหล่งข้อมูลอื่นๆ ประกอบการวิเคราะห์

- ระบบบริหารจัดการข้อมูลและวิเคราะห์เหตุการณ์ด้านความมั่นคงปลอดภัย (SIEM) ช่วยในการตรวจจับและทำการแจ้งเตือนจากการวิเคราะห์ที่ได้จากข้อมูลบันทึกเหตุการณ์ (Log data)

- ซอฟแวร์ป้องกันไวรัส (Antivirus Software) เพื่อป้องกันและตรวจจับไวรัส หรือมัลแวร์ในรูปแบบต่างๆ แล้วแจ้งเตือนและป้องกันไม่ให้เกิดการแพร่กระจายที่ระบบแม่ข่าย รวมทั้ง เพื่อให้ระบบทำงานได้อย่างมีประสิทธิภาพในการป้องกัน ควรมีการอัปเดตลักษณะเฉพาะของการโจมตีอยู่เสมอ

- ซอฟแวร์ตรวจสอบความถูกต้องของไฟล์เพื่อตรวจสอบการเปลี่ยนแปลงหรือการแก้ไขที่เกิดขึ้นกับไฟล์ที่มีความสำคัญในระหว่างเกิดเหตุภัยคุกคาม (File Integrity Checking Software)

- การใช้บริการเฝ้าระวังภัยคุกคามจากผู้ให้บริการภายนอก (Third-Party Monitoring Services)

(๒.๒) ข้อมูลบันทึกเหตุการณ์ควรจัดเก็บข้อมูล ดังต่อไปนี้เป็นอย่างน้อย

- ข้อมูลบันทึกเหตุการณ์ของระบบปฏิบัติการการบริการและแอปพลิเคชัน (Operating System, Service and Application Logs)

- ข้อมูลบันทึกเหตุการณ์ของอุปกรณ์เครือข่าย (Network Device Logs)

- ข้อมูลบันทึกการเคลื่อนไหวของข้อมูลในเครือข่าย (Network Flow Logs)

(๒.๓) ข้อมูลสาธารณะ (Publicly Available Information)

- ข้อมูลของช่องโหว่หรือจุดอ่อนใหม่จากหน่วยงานด้านการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ เช่น สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA หรือช่องทางอื่นๆ ที่มีการอัปเดตและเผยแพร่ข้อมูลภัยคุกคามสู่สาธารณะ เป็นต้น

(๒.๔) บุคคล (People)

- บุคลากรภายในหน่วยงาน เช่น ผู้ใช้งานระบบ ผู้ดูแลระบบ ผู้ดูแลระบบเครือข่าย เจ้าหน้าที่ด้านความมั่นคงปลอดภัย เป็นต้น ซึ่งเมื่อได้รับรายงานแล้วจะต้องมีการตรวจสอบ

ข้อเท็จจริงหรือยืนยันข้อมูลทุกครั้ง

- บุคคลภายนอกหน่วยงาน เช่น รายงานจากผู้ใช้งานภายนอกถึงหน้าเว็บไซต์ที่ไม่สามารถใช้งานได้ เป็นต้น โดยหน่วยงานควรมีขั้นตอนในการรับรายงานและตรวจสอบข้อมูลอย่างละเอียดถี่ถ้วน

(๓) การวิเคราะห์เหตุการณ์ภัยคุกคามทางไซเบอร์ ควรครอบคลุมอย่างน้อยดังต่อไปนี้

(๓.๑) การจัดทำข้อมูลเครือข่ายและระบบ (Profile Network and System) เพื่อให้สามารถระบุการเปลี่ยนแปลงที่เกิดขึ้นจากการเข้าถึงหรือใช้งานเครือข่ายและระบบงานจากปกติได้ เช่น การวัดปริมาณการใช้งาน bandwidth ของเครือข่ายและบันทึกข้อมูลระดับการใช้งานเฉลี่ยและระดับสูงสุด ในแต่ละช่วงเวลาเพื่อตรวจสอบพฤติกรรมการใช้งานที่ผิดปกติของเครือข่าย

(๓.๒) การศึกษาและเข้าใจพฤติกรรมตามปกติของระบบ เครือข่าย และแอปพลิเคชัน เพื่อช่วยในการสังเกตพฤติกรรมที่ผิดปกติโดยการตรวจสอบบันทึกเหตุการณ์ และการแจ้งเตือนด้านความมั่นคงปลอดภัย เพื่อให้มีความคุ้นเคยและจะช่วยให้การสังเกตเหตุการณ์และการแจ้งเตือนที่ผิดปกติได้เร็วและแม่นยำมากยิ่งขึ้น

(๓.๓) การจัดทำนโยบายการเก็บรักษาบันทึกเหตุการณ์ (Log Retention Policy)

(๓.๔) การตรวจสอบความสัมพันธ์ของเหตุการณ์ภัยคุกคาม (Event Correlation) โดยการตรวจสอบข้อมูลบันทึกเหตุการณ์ของเครื่องแม่ข่ายเพื่อหาความเชื่อมโยง เพื่อนำประกอบการพิจารณาว่ามีเหตุภัยคุกคามเกิดขึ้นจริงหรือไม่

(๓.๕) การตั้งเวลาเครื่องแม่ข่ายให้เป็นมาตรฐานเดียวกัน

(๓.๖) การจัดทำเอกสารหรือฐานข้อมูล ที่ใช้เพื่ออ้างอิงสำหรับการดำเนินการวิเคราะห์ข้อมูลภัยคุกคาม

(๓.๗) การเปิดใช้งานโปรแกรมสำหรับดักจับภัยคุกคาม (Packet Sniffer) เพื่อบันทึกหรือเก็บข้อมูลการจราจรภายในเครือข่ายของหน่วยงานเพิ่มเติม

(๔) การลงบันทึกข้อมูลเหตุการณ์ภัยคุกคามทางไซเบอร์ (Cyber Incident Documentation) การบันทึกข้อมูลเหตุการณ์ภัยคุกคาม จะช่วยให้การรับมือและตอบสนองภัยคุกคามมีประสิทธิภาพและเป็นระบบมากขึ้น หน่วยงานควรบันทึกข้อมูลเกี่ยวกับเหตุการณ์ที่เกิดขึ้นตั้งแต่การตรวจพบจนถึงการสิ้นสุดของเหตุการณ์ภัยคุกคาม โดยการบันทึกข้อมูลเกี่ยวกับสถานะของเหตุการณ์ภัยคุกคามและข้อมูลที่เกี่ยวข้อง อาจจัดเก็บในโปรแกรมประยุกต์หรือฐานข้อมูล เช่น ระบบติดตามปัญหา (Issues Tracking System) เพื่อประโยชน์ในการติดตามเหตุการณ์ ขั้นตอนการจัดการและแก้ไขเหตุภัยคุกคาม เพื่อให้มั่นใจได้ว่าเหตุการณ์ภัยคุกคามที่เกิดขึ้นได้รับการจัดการแก้ไขภายในระยะเวลาที่เหมาะสม

ในการบันทึกข้อมูลเหตุการณ์ภัยคุกคาม ควรประกอบด้วยข้อมูลอย่างน้อย ดังนี้

- ชื่อเหตุการณ์ภัยคุกคาม
- วันที่บันทึกเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคาม
- หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้
- ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม
- ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม
- ข้อมูลติดต่อสำหรับผู้ที่เกี่ยวข้องอื่นๆ เช่น เจ้าของระบบงาน ผู้ดูแลระบบงาน
- ประเภทของเหตุการณ์ภัยคุกคาม
- วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม
- วันที่และเวลาพบเหตุภัยการณ์คุกคาม
- วันที่และเวลารายงานเหตุภัยคุกคาม
- รายละเอียดเหตุการณ์ภัยคุกคาม
  - สิ่งที่เกิดขึ้น
  - เกิดขึ้นอย่างไร
  - ทำไมจึงเกิดขึ้น
  - การประเมินทรัพย์สินสารสนเทศที่เสียหาย
  - ผลกระทบทางธุรกิจ
  - ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม
- การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้
- ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ
- รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม
- สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม

ตัวอย่างแบบฟอร์มการบันทึกข้อมูลเหตุการณ์ภัยคุกคามขององค์การจัดการน้ำเสีย

<table>
<tr><th colspan="6">แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="2">ชื่อเหตุการณ์ภัยคุกคาม</td><td colspan="2"></td><td>หมายเลขของเหตุการณ์ภัยคุกคาม</td><td></td></tr>
<tr><td colspan="2">วันที่บันทึกเหตุการณ์ภัยคุกคาม</td><td colspan="2"></td><td>หมายเลขของเหตุการณ์ภัยคุกคามอื่นๆ ที่เกี่ยวข้องกับเหตุการณ์นี้</td><td></td></tr>
<tr><th colspan="3">ข้อมูลของผู้แจ้งเหตุการณ์ภัยคุกคาม</th><th colspan="3">ข้อมูลของเจ้าหน้าที่ผู้รับมือเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="2">ชื่อ – นามสกุล</td><td colspan="2"></td><td>ชื่อ – นามสกุล</td><td></td></tr>
<tr><td colspan="2">หน่วยงาน</td><td colspan="2"></td><td>โทรศัพท์</td><td></td></tr>
<tr><td>โทรศัพท์</td><td></td><td>อีเมล</td><td></td><td>อีเมล</td><td></td></tr>
<tr><td colspan="3">วันที่และเวลาเกิดเหตุการณ์ภัยคุกคาม</td><td colspan="3"></td></tr>
<tr><td colspan="3">วันที่และเวลาพบเหตุภัยการณ์คุกคาม</td><td colspan="3"></td></tr>
<tr><td colspan="3">วันที่และเวลารายงานเหตุภัยคุกคาม</td><td colspan="3"></td></tr>
<tr><th colspan="6">รายละเอียดเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="6">- สิ่งที่เกิดขึ้น
- เกิดขึ้นอย่างไร
- ทำไมจึงเกิดขึ้น
- การประเมินทรัพย์สินสารสนเทศที่เสียหาย
- ผลกระทบทางธุรกิจ
- ช่องโหว่ที่พบ/ตัวบ่งชี้ของเหตุการณ์ภัยคุกคาม</td></tr>
<tr><th colspan="3">การดำเนินการทั้งหมดของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้</th><th colspan="3">การดำเนินการในขั้นถัดไปของทีมรับมือและตอบสนองภัยคุกคามในเหตุการณ์นี้</th></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><th colspan="3">ค่าใช้จ่ายในการฟื้นคืนสู่สภาพปกติ</th><th colspan="3">รายการหลักฐานที่รวบรวมระหว่างการสืบสวนเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="3"></td><td colspan="3"></td></tr>
<tr><th colspan="6">สรุปสาระสำคัญของเหตุการณ์ภัยคุกคาม</th></tr>
<tr><td colspan="6"></td></tr>
</table>

(๕) การจัดลำดับความรุนแรงของเหตุการณ์ภัยคุกคามทางไซเบอร์ ควรคำนึงปัจจัยดังต่อไปนี้

- ผลกระทบต่อการให้บริการ และการดำเนินงานของหน่วยงานที่เกิดภัยคุกคาม โดยควรพิจารณาผลกระทบที่เกิดขึ้นทั้งในปัจจุบัน และผลกระทบที่มีโอกาสเกิดขึ้นหากเหตุการณ์ภัยคุกคามยังไม่ถูกควบคุมโดยทันที

- ผลกระทบต่อข้อมูล ควรพิจารณา ๓ ด้าน ได้แก่ ด้านการรักษาความลับ (Confidentiality) ด้านการรักษาความครบถ้วน (Integrity) และด้านการรักษาสภาพพร้อมใช้ (Availability) รวมทั้งควรพิจารณาว่าเหตุการณ์ภัยคุกคามส่งผลต่อการดำเนินงานโดยรวมของหน่วยงานอย่างไร และส่งผลต่อข้อมูลสำคัญของหน่วยงาน (Sensitive Information) อย่างไร

- ความสามารถในการฟื้นฟูระบบ ควรพิจารณาจากระยะเวลาและทรัพยากรที่ต้องใช้ในการฟื้นฟูระบบจากเหตุภัยคุกคาม ซึ่งความรุนแรงของเหตุภัยคุกคามและประเภทของทรัพย์สินสารสนเทศที่ได้รับผลกระทบจะเป็นส่วนสำคัญในการพิจารณาความสามารถในการฟื้นฟูระบบ

(๖) การแจ้งเตือนเหตุภัยคุกคามทางไซเบอร์แก่ผู้ที่เกี่ยวข้อง

ทีมรับมือและตอบสนองฯ ควรดำเนินการแจ้งข้อมูลเกี่ยวกับเหตุภัยคุกคามกับผู้ที่เกี่ยวข้อง เพื่อให้ทุกคนสามารถดำเนินการตามหน้าที่ความรับผิดชอบที่ได้กำหนดไว้ ทั้งนี้ หน่วยงานควรมีข้อกำหนดเกี่ยวกับการแจ้งข้อมูลเหตุภัยคุกคาม ข้อมูลอะไรบ้างที่ต้องรายงาน รายงานต่อใคร และเมื่อใด โดยอย่างน้อยควรกำหนดบุคคลผู้รับรายงาน ข้อมูลที่ต้องรายงาน และเวลาที่ต้องรายงาน รวมถึงหน่วยงานต่างๆ ทั้งภายในและภายนอกที่ต้องได้รับแจ้ง บุคลากรหรือหน่วยงานที่ควรได้รับการแจ้งเหตุภัยคุกคาม มีดังต่อไปนี้

- ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) หรือเทียบเท่า (กรณีไม่มีตำแหน่ง CIO)
- ผู้บริหารความมั่นคงปลอดภัยสารสนเทศ (CISO) หรือเทียบเท่า (กรณีไม่มีตำแหน่ง CISO)
- ทีมรับมือและตอบสนองต่อเหตุการณ์อื่นๆ ของหน่วยงาน
- ทีมรับมือและตอบสนองต่อเหตุการณ์ภายนอกหน่วยงาน (ตามความเหมาะสม)
- เจ้าของระบบงาน
- ฝ่ายทรัพยากรบุคคล (สำหรับกรณีที่เกี่ยวข้องกับพนักงาน เช่น การล่วงละเมิดทางอีเมล)
- ฝ่ายสื่อสารองค์กร (สำหรับเหตุการณ์ที่จำเป็นต้องให้การประชาสัมพันธ์)
- ฝ่ายกฎหมาย (สำหรับเหตุการณ์ที่อาจมีข้อเกี่ยวข้องทางกฎหมาย)

- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) สพร. หรือ DGA
- ทีมบริหารความต่อเนื่องในการดำเนินธุรกิจ (Business Continuity Team)
- หน่วยงานกำกับ (Regulators)
- หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง (Law Enforcer)

ขั้นตอนที่ ๓ : การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน

ประกอบด้วย ๓ ขั้นตอน ได้แก่ การควบคุมภัยคุกคามและจำกัดความเสียหาย (Containment) การกำจัดภัยคุกคาม (Eradication) และการฟื้นฟูระบบ (Recovery) โดยมีรายละเอียดดังนี้

(๑) กำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหายที่เกิดขึ้นจากเหตุการณ์ภัยคุกคามทางไซเบอร์ ซึ่งจะมีความแตกต่างกันไปขึ้นกับลักษณะ ประเภทของภัยคุกคาม ระบบงานหรือบริการที่ได้รับผลกระทบ ระยะเวลาและทรัพยากรที่จำเป็นต่อการควบคุมความเสียหาย

เกณฑ์ประกอบการพิจารณากำหนดแนวทางการควบคุมภัยคุกคามและจำกัดความเสียหาย ควรพิจารณาอย่างน้อยในเรื่องดังต่อไปนี้

- ความเสียหายที่อาจเกิดขึ้นและการโจรกรรมข้อมูล
- ความจำเป็นในการเก็บรักษาหลักฐาน
- ความพร้อมให้บริการ เช่น การเชื่อมต่อเครือข่าย การให้บริการกับบุคคลภายนอก เป็นต้น
- เวลาและทรัพยากรที่จำเป็นในการดำเนินการ
- ประสิทธิผลของแนวทางในการควบคุมและจำกัดความเสียหาย เช่น การควบคุมบางส่วนหรือการควบคุมทั้งหมด
- ระยะเวลาในการแก้ปัญหา เช่น การแก้ไขปัญหาแบบฉุกเฉินภายใน ๔ ชั่วโมง การแก้ไขปัญหาแบบชั่วคราวภายใน ๒ สัปดาห์ และการแก้ไขปัญหาแบบถาวร เป็นต้น

นอกจากนี้ หน่วยงานควรเก็บรวบรวมหลักฐานที่เกิดขึ้นระหว่างเกิดเหตุการณ์ภัยคุกคาม เพื่อใช้ในการแก้ไขปัญหาและจัดการเหตุภัยคุกคาม รวมทั้งเพื่อใช้ในกระบวนการทางกฎหมาย หากจำเป็นหน่วยงานควรจัดทำเอกสารรวบรวมหลักฐานทั้งหมดที่ได้ถูกบุกรุกโจมตี รวมถึงระบุขั้นตอนการเก็บรักษาหลักฐานที่เป็นไปตามกฎหมายและระเบียบข้อบังคับ เพื่อให้สามารถใช้เป็นพยานหลักฐานได้ในชั้นศาล นอกจากนี้ควรมีการบันทึกหลักฐานทุกครั้งหากมีการถ่ายโอนหลักฐานจากบุคคลหนึ่งสู่อีกคน และลงลายมือชื่อกำกับของแต่ละฝ่าย

การจัดทำเอกสารรายละเอียดหลักฐานควรครอบคลุมอย่างน้อยดังนี้

- ข้อมูลระบุพยานหลักฐาน เช่น สถานที่ตั้ง หมายเลขซีเรียล (Serial Number)

หมายเลขรุ่น (Model Number) ชื่อเครื่องแม่ข่ายที่อยู่สำหรับควบคุมการเข้าใช้งานสื่อกลาง (Media Access Control Addresses) และที่อยู่ IP ของคอมพิวเตอร์ เป็นต้น

- ชื่อ-สกุล และหมายเลขโทรศัพท์ของบุคคลที่เก็บรวบรวมหรือดูแลพยานหลักฐานในระหว่างการสอบสวน
- วันที่และเวลาที่มีการดำเนินการกับพยานหลักฐานในแต่ละครั้ง
- สถานที่เก็บหลักฐาน

(๒) การกำจัดภัยคุกคามทางไซเบอร์ (Eradication)

หน่วยงานควรกำจัดต้นเหตุของเหตุการณ์ที่เป็นอันตรายต่อเครือข่าย ระบบหรือแอปพลิเคชัน รวมถึงการกำจัดไฟล์ที่เกี่ยวข้องกับการโจมตีและการปิดช่องโหว่ที่ถูกใช้ในการโจมตี ทั้งนี้ การกำจัดภัยคุกคามมีวิธีที่แตกต่างกันโดยขึ้นกับประเภทของเหตุภัยคุกคาม

ตัวอย่างของวิธีการกำจัดภัยคุกคาม ดังนี้

(๒.๑) การลบมัลแวร์ (Malware) คือ การกักกัน ลบ แทนที่ หรือกู้คืนไฟล์ที่ติดมัลแวร์ ซึ่งโดยส่วนใหญ่ หน่วยงานจะต้องกู้คืนระบบสารสนเทศใหม่โดยการติดตั้งระบบปฏิบัติการ ระบบงาน และข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้ และอาจรวมถึงการอัพเดตข้อมูลคุณลักษณะเฉพาะของโปรแกรมป้องกันไวรัส (Antivirus Signature) ให้เป็นปัจจุบัน

(๒.๒) การแก้ไขหรือลดผลกระทบจากช่องโหว่ การแก้ไขช่องโหว่สามารถทำได้ด้วยการติดตั้งแพตช์ (Patch) รุ่นล่าสุดของระบบปฏิบัติการและระบบงาน เพื่อป้องกันการใช้งานช่องโหว่ที่เป็นช่องทางการโจมตี ทั้งนี้ หากระบบสารสนเทศไม่สามารถติดตั้งแพตช์ได้ด้วยเหตุผลทางเทคนิคหรือเหตุผลในการปฏิบัติงาน ให้ลดผลกระทบจากช่องโหว่โดยปรับปรุงการตั้งค่า (Configuration) ของระบบสารสนเทศให้สามารถป้องกันหรือจำกัดความเสียหายจากเครื่องแม่ข่ายที่ติดมัลแวร์ หากกรณียังไม่มี patch ให้ใช้วิธีแก้ไขปัญหาหรือลดผลกระทบชั่วคราว

(๒.๓) การปรับปรุงการควบคุมการเข้าถึงผู้ใช้งานและเครือข่าย เช่น การลบบัญชีผู้ใช้งาน หรือผู้ดูแลระบบที่ถูกบุกรุก การปรับปรุงการควบคุมการเข้าถึงเครือข่าย เช่น การตั้งค่าของระบบตรวจจับและป้องกันการบุกรุก (IDPS) ไฟร์วอลล์ (firewall) เป็นต้น การปรับปรุงการกำหนดค่าพื้นฐาน (Baseline Configuration) และการลบกลไกการเข้าถึงอื่นๆ ที่ถูกใช้โดยผู้โจมตี

(๓) การฟื้นฟูระบบ (Recovery)

การฟื้นฟูระบบ เป็นการกู้คืนข้อมูลหรือระบบ เพื่อทำให้ระบบสารสนเทศ ข้อมูล ความมั่นคงปลอดภัยของระบบและเครือข่ายกลับสู่สถานะปกติ ด้วยการติดตั้งระบบปฏิบัติการ ระบบงาน และข้อมูลจากสื่อบันทึกข้อมูลที่เชื่อถือได้ พร้อมทั้งมีกลไกติดตามการดำเนินการเพื่อป้องกันการเกิดเหตุภัยคุกคามที่มีความคล้ายคลึงกันขึ้นอีกในอนาคต การฟื้นฟูระบบมีวิธีการที่แตกต่างกัน

ขึ้นอยู่กับประเภทของเหตุภัยคุกคาม เช่น การ ติดตั้งระบบใหม่จากต้นฉบับหรือติดตั้งจากข้อมูลที่สำรองที่เชื่อถือได้ การเปลี่ยนรหัสผ่านของระบบการติดตั้งแพตช์ (Patch) ให้เป็นเวอร์ชั่นปัจจุบัน และการปรับปรุงความมั่นคงปลอดภัยของเครือข่าย เป็นต้น ทั้งนี้ ในกรณีที่การกู้คืนข้อมูลและระบบที่เสียหายเสร็จสิ้น ผู้ดูแลระบบควรทำการยืนยันว่าระบบสามารถกลับมาทำงานได้ตามปกติให้ผู้ที่เกี่ยวข้องทราบ

<u>ขั้นตอนที่ ๔</u> : การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Post Cyber Incident Activity)

๔.๑ การเรียนรู้จากภัยคุกคาม (Lessons Learned)

หน่วยงานควรมีการเรียนรู้จากเหตุภัยคุกคามที่เกิดขึ้น เพื่อนำมาปรับปรุงและพัฒนาแนวทางในการรับมือและตอบสนองต่อภัยคุกคามทางไซเบอร์ รวมทั้งจัดสรรทรัพยากรและเทคโนโลยีให้มีความพร้อมต่อการรับมือเหตุภัยคุกคามต่อไปในอนาคต นอกจากนี้ หน่วยงานควรจัดให้มีการประชุมของฝ่ายหรือหน่วยงานย่อยที่มีความเกี่ยวข้องกับเหตุการณ์ภัยคุกคามทางไซเบอร์ที่เกิดขึ้น โดยวัตถุประสงค์ของการประชุมเพื่อให้ทุกหน่วยงานย่อยที่เกี่ยวข้องได้มีการแลกเปลี่ยนข้อมูล รวมทั้งทบทวนเหตุภัยคุกคามและวิธีการรับมือและตอบสนองต่อภัยคุกคามที่เกิดขึ้น

ตัวอย่างประเด็นคำถามที่หน่วยงานสามารถพิจารณาปรับใช้ประกอบการประชุมแลกเปลี่ยนข้อมูลหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ เช่น

- เหตุภัยคุกคามที่เกิดขึ้นคืออะไร เกิดขึ้นเมื่อเวลาใดบ้าง
- เจ้าหน้าที่และฝ่ายบริหารสามารถรับมือภัยคุกคามได้ดีเพียงใด การดำเนินการเป็นไปตามขั้นตอนการปฏิบัติงานที่กำหนดไว้หรือไม่
- ข้อมูลอะไรบ้างที่จำเป็นต้องได้รับรายงานภายในระยะเวลาอันสั้น เพื่อเพิ่มประสิทธิภาพในการรับมือและตอบสนองต่อเหตุการณ์
- มีขั้นตอนหรือการดำเนินการใดๆ ที่อาจเป็นอุปสรรคหรือไม่สอดคล้องกับขั้นตอนของการฟื้นฟูระบบหรือไม่
- เจ้าหน้าที่และฝ่ายบริหารมีแนวทางดำเนินการเพิ่มเติมหรือแตกต่างไปจากเดิม หากเกิดภัยคุกคามที่มีรูปแบบคล้ายคลึงกันเกิดขึ้นในครั้งต่อไป
- การแลกเปลี่ยนข้อมูลกับหน่วยงานอื่นๆ สามารถปรับปรุงให้ดีขึ้นได้อย่างไร
- แนวทางการดำเนินการแก้ไข (Corrective Action) ที่สามารถเพิ่มเติมเพื่อป้องกันภัยคุกคามที่คล้ายคลึงกันในอนาคตได้
- สัญญาณอะไรบ้างที่สามารถนำมาใช้เพื่อตรวจจับภัยคุกคามที่มีลักษณะคล้ายคลึงกันซึ่งอาจเกิดขึ้นในอนาคต

- เครื่องมือหรือทรัพยากรที่มีความจำเป็นต้องได้รับการจัดสรรเพิ่มเติม เพื่อใช้ดำเนินการในการตรวจจับ วิเคราะห์ และบรรเทาเหตุภัยคุกคามที่อาจเกิดขึ้นในอนาคต

๔.๒ การวัดผลและปรับปรุงการปฏิบัติงานในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์

(๑) จำนวนเหตุการณ์ภัยคุกคามทางไซเบอร์ที่รับมือต่อเดือน/ไตรมาส/ปี

(๒) ระยะเวลาในการรับมือและตอบสนองต่อเหตุการณ์ สามารถวัดได้หลายวิธี เช่น

๑) ระยะเวลาทั้งหมดที่ใช้ในการรับมือและตอบสนอง

๒) ระยะเวลาที่ใช้ในการดำเนินการในแต่ละช่วงของกระบวนการรับมือและตอบสนองในแต่ละขั้นตอน

๓) ระยะเวลาที่ทีมรับมือฯ ใช้ในการตอบสนองหลังจากที่ได้รับรายงานภัยคุกคาม

๔) ระยะเวลาที่ทีมรับมือฯ ใช้ในการรายงานภัยคุกคามต่อผู้บริหารหรือหน่วยงานภายนอกที่เกี่ยวข้อง

(๓) การประเมินกระบวนการรับมือในแต่ละเหตุการณ์ (Objective Assessment) ตัวอย่างของการประเมิน เช่น

- การตรวจทานบันทึกเหตุการณ์ (log) แบบฟอร์มรายงาน และเอกสารอื่นๆ ที่เกี่ยวข้องกับภัยคุกคาม เพื่อให้การปฏิบัติงานเป็นไปตามขั้นตอนการรับมือภัยคุกคามทางไซเบอร์ที่กำหนดไว้

- การระบุว่าสัญญาณการเกิดเหตุภัยคุกคามอะไรบ้างที่บันทึกไว้ เพื่อพิจารณาว่าการบันทึกเหตุการณ์และระบุเหตุภัยคุกคามมีประสิทธิภาพเพียงใด

- การพิจารณาว่าภัยคุกคามที่เกิดขึ้นก่อให้เกิดความเสียหายก่อนที่จะตรวจพบหรือไม่

- การพิจารณาว่ามีการระบุสาเหตุที่แท้จริงของภัยคุกคามไว้หรือไม่ และการระบุช่องทางการโจมตี ช่องโหว่ที่เปิดเผย และลักษณะของระบบ เครือข่าย และแอปพลิเคชันที่ถูกโจมตี

- การพิจารณาว่าภัยคุกคามเป็นการเกิดขึ้นอีกครั้งของภัยคุกคามก่อนหน้าหรือไม่

- การประเมินความเสียหายทางการเงินจากภัยคุกคามที่เกิดขึ้น เช่น ข้อมูลและกระบวนการทางธุรกิจที่สำคัญที่ได้รับผลกระทบจากภัยคุกคาม

(๔) การประเมินประสิทธิภาพของทีมรับมือและตอบสนองฯ (Subjective Assessment) หน่วยงานอาจกำหนดให้มีการประเมินผลการปฏิบัติงานของทีมรับมือและตอบสนองฯ

ทั้งในรูปแบบรายบุคคลหรือทั้งทีม รวมทั้งอาจให้เจ้าของระบบงานที่ระบบถูกโจมตีเป็นผู้ทำการประเมินการปฏิบัติหน้าที่ของทีมรับมือและตอบสนองฯ ก็ได้ เพื่อประกอบการพิจารณาว่าประสิทธิภาพของการรับมือให้ผลลัพธ์เป็นที่น่าพอใจหรือไม่

ขั้นตอนเพิ่มเติม : การดูแลรักษาหลักฐานทางดิจิทัล (Digital Evidence Handling Guide)

หลักฐานทางดิจิทัลจะมีความอ่อนไหวต่อความเปลี่ยนแปลงสูง ดังนั้น จึงจำเป็นต้องระมัดระวังตั้งแต่ขั้นตอนการจัดเก็บจนถึงการวิเคราะห์และนำเสนอผลการวิเคราะห์ เพื่อให้มั่นใจได้ว่าข้อเท็จจริงที่ได้จากการวิเคราะห์มีความถูกต้องแม่นยำ รวมถึงการที่หลักฐานจะสามารถถูกนำไปใช้ได้ในชั้นศาลหากมีความจำเป็น ทั้งนี้ หลักการดูแลรักษาหลักฐานทางดิจิทัลที่สำคัญมี ๕ ข้อ ดังนี้

๑. Assessment การประเมินเพื่อหาจุดที่ต้องมีดำเนินการจัดเก็บหลักฐานของ Incident ที่เรากำลังรับมือและตอบสนอง เช่น Hard Disk, RAM, External Hard Disk, Mobile Device เป็นต้น เพื่อดำเนินการจัดเตรียมเครื่องมือและวิธีการที่เหมาะสมในการเก็บข้อมูลหลักฐาน

๒. Acquisition ดำเนินการทำเก็บหลักฐานด้วยการทำสำเนา (Duplication/Bit-for-bit Acquisition) ด้วยเครื่องมือที่เหมาะสม โดยมีข้อควรระวังในเรื่องดังต่อไปนี้

(๑) ต้องป้องกันการเปลี่ยนแปลงของหลักฐาน ด้วยการใช้งาน Hardware Write Blocker

(๒) ต้องคำนึงถึง Volatility หรือความอ่อนไหวต่อการสูญเสียกระแสไฟฟ้าของหลักฐาน เช่น ข้อมูลที่เสี่ยงต่อการสูญหายหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM ต้องได้รับการเก็บรักษาเป็นอันดับแรก เป็นต้น

(๓) ต้องบันทึกรายละเอียดการดำเนินงานทุกขั้นตอนที่ลงมือปฏิบัติอย่างละเอียด

(๔) ต้องทำการบันทึกหลักฐาน (Chain of Custody)

๓. Authentication ทำการตรวจสอบความถูกต้องของหลักฐานที่ Duplicate และเปรียบเทียบกับต้นฉบับด้วยวิธี Cryptographic Hash เช่น MD๕, SHA๑, SHA๒๕๖

๔. Analysis & Report วิเคราะห์หาข้อมูลจากชุดหลักฐานที่ดำเนินการจัดเก็บเพื่อพิสูจน์ข้อเท็จจริง หรือเพื่อค้นหาสาเหตุของการเกิด Incident

๕. Archive จัดเก็บหลักฐานไว้ในที่เหมาะสม ปลอดภัย และบันทึก Chain of Custody Form ทุกครั้งที่มีการเคลื่อนย้ายหลักฐาน พร้อมทั้งระบุเหตุผลของการเคลื่อนย้าย

Cybersecurity ยังคงเป็นเรื่องที่ทุกคนต้องให้ความสำคัญ โดยเฉพาะในปัจจุบันก็มีข่าวเกี่ยวกับเรื่องการหลอกลวงมากมาย โดยเฉพาะการหลอกให้คลิกลิงก์ปลอม หรือหลอกให้ลง Application ที่อยู่นอก Store จากนั้นมิจฉาชีพก็จะขโมยเงินจากบัญชีธนาคารของเราผ่านโทรศัพท์ของเราเองออกไปได้ แต่หากเปลี่ยนจากตัวบุคคลเป็นองค์กร ที่มีทรัพย์สินที่มีความสำคัญมากกว่าหลายเท่า เช่น ข้อมูลภายในองค์กร หรือข้อมูลลูกค้าองค์กร จึงจำเป็นต้องปกป้องไม่ให้ทรัพย์สินพวกนี้หลุดออกไปถึงมืออาชญากร

เพราะฉะนั้นสิ่งสำคัญที่ทุกองค์กรควรจะมีก็คือ การเตรียมความพร้อมรับมือกับภัยคุกคามทางไซเบอร์ หรือเรียกว่า BCP ด้าน Cybersecurity ที่แบ่งความสำคัญออกเป็น ๓ ด้านด้วยกัน ตั้งแต่

๑. การสร้างระบบรักษาความปลอดภัยให้แข็งแกร่ง

องค์กรจะต้องมีความแข็งแกร่งในการป้องกันตั้งแต่การตรวจจับไปจนถึงความรวดเร็วในการหาช่องโหว่ เพื่อให้สามารถดำเนินการแก้ไขได้ทันท่วงที สำหรับการใช้งานซอฟต์แวร์ต่างๆ ก็จะต้องอัปเดตเป็นเวอร์ชันล่าสุดอยู่เสมอเพื่อป้องกันช่องโหว่ด้านการรักษาข้อมูลให้ใช้กฎ ๓-๒-๑ คือ ทำ Backup ข้อมูลทั้งหมด ๓ ชุด ทำรูปแบบไฟล์ (Format) ให้แตกต่างกัน ๒ รูปแบบ และนำข้อมูล ๑ ชุด ไปเก็บไว้ในตำแหน่งที่ยากต่อการค้นหา

๒. ตรวจสอบการเข้าถึงระบบของทุกคนในองค์กร

เพราะการโจมตีในปัจจุบัน บางครั้งจะเข้ามาในรูปแบบของการปลอมตัวตน องค์กรจึงควรแบ่งสิทธิ์การเข้าถึงข้อมูลอย่างชัดเจน รวมถึงการตรวจสอบสถานะผู้ใช้ก่อนเข้าระบบเพื่อยืนยันตัวตน นอกจากนี้ องค์กรควรมีระบบช่วยตรวจจับการโจมตี และนำข้อมูลการถูกโจมตีมาวิเคราะห์เพื่อคาดการณ์การโจมตีครั้งต่อไปด้วย

๓. สร้างวัฒนธรรมองค์กรด้าน Cybersecurity

บางครั้งองค์กรมีเครื่องมือที่ดี แต่กลับถูกโจมตีเพราะความผิดพลาดของมนุษย์ เพราะฉะนั้นการวางรากฐานวัฒนธรรมองค์กร ให้มีความรู้ความเข้าใจ เกี่ยวกับการรักษาความปลอดภัยทางไซเบอร์นั้นเป็นอีกหนึ่งปัจจัยสำคัญ นอกจากนี้ องค์กรยังควรตั้งมาตรฐานด้านความปลอดภัยขององค์กร เช่น การกำหนดให้พนักงานต้องเปลี่ยน Password ทุก ๓ เดือน พร้อมสร้างความเข้าใจกับพนักงานถึงความสำคัญว่าการเปลี่ยน Password จะช่วยรักษาความปลอดภัยให้องค์กรได้อย่างไร และนอกเหนือจากการเตรียมความพร้อมทั้ง ๓ ข้อข้างต้น องค์กรควรจะมีพนักงานในระดับหัวหน้า ที่เข้าใจภาพรวมของระบบงานด้านการรักษาความปลอดภัยเข้ามาช่วยวางแผน ก็จะช่วยให้องค์กรอยู่รอดปลอดภัย ไร้กังวลจากการโจมตีได้ในระยะยาว

ตัวอย่างการประยุกต์ใช้ขั้นตอนการรับมือภัยคุกคามทางไซเบอร์

กรณีตัวอย่างที่ ๑ : Ransomware และ Data Leakage จากภายในองค์กร

ขั้นตอนที่ ๑ : การเตรียมความพร้อม (Preparation)		
วัตถุประสงค์ **(Objectives)**	๑. มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ ๒. มีกระบวนการ และกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นหน้าที่ในการตรวจจับความพยายามในการบุกรุกได้อีกด้วย	
Activity	Description	Stakeholders
จัดเตรียมทรัพยากร	อ้างอิงข้อ ๑.๑ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)”	ผู้บริหารเทคโนโลยีสารสนเทศ อจน. (CIO)
ดำเนินการป้องกันก่อนเกิดเหตุ	อ้างอิงข้อ ๒.๑ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)”สำหรับการรับมือ Ransomware ในปัจจุบันให้มุ่งเน้นไปที่เรื่องของการ Backup ระบบและข้อมูลการจัดการเรื่องของข้อมูลที่รั่วไหลโดยเฉพาะเรื่องของการ Take Down แหล่งที่รั่วไหลของข้อมูล การมีมาตรการในการเยียวยาผู้ที่ได้รับผลกระทบจากการรั่วไหลของข้อมูล รวมทั้งควรมีความพร้อมในการดำเนินการ Personal Information Usage Monitoring สำหรับบุคคลที่ข้อมูลรั่วไหล ว่าจะมีการถูกนำไปใช้ที่ใดได้บ้าง และกิจกรรมใดบ้าง	CIO / ผู้ดูแลระบบสารสนเทศ อจน.
ขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)		
วัตถุประสงค์ **(Objectives)**	๑. รับแจ้งเหตุการณ์การโจมตี ๒. การระบุความเสียหายเบื้องต้น ๓. การระบุสาเหตุที่การโจมตีสำเร็จ ๔. การระบุความสามารถของผู้บุกรุกและเครื่องมือที่ใช้ รวมถึง Malware	
Activity	Description	Stakeholders
รับแจ้งเหตุ	ส่วนใหญ่เมื่อการโจมตีประเภท Ransomware เกิดขึ้นจะรับทราบได้จากการที่ผู้ใช้งานระบบเป็นผู้แจ้ง	ผู้ใช้งาน (Users) / ทีมดูแลระบบฯ
วิเคราะห์การโจมตีและ ขอบเขตเสียหาย	ผลกระทบเบื้องต้นสามารถสอบถามได้จากผู้ใช้งานระบบ รวมถึงกิจกรรมก่อนหน้าที่กระทำไป และเป็นผลให้การโจมตีสำเร็จ รวมทั้งใช้ข้อมูลจากการสอบถามเป็นข้อมูลเบื้องต้นในการจัดการภัยคุกคามและค้นหาระบบอื่นๆ ที่อาจจะได้รับผลกระทบในลักษณะเดียวกัน	ทีมดูแลระบบสารสนเทศ อจน.

จัดเก็บหลักฐานทางดิจิทัลที่จำเป็น รวมถึงตัวอย่าง (Specimen) Malware **จัดเก็บหลักฐานทางดิจิทัลที่จำเป็น รวมถึงตัวอย่าง (Specimen) Malware**	การโจมตีที่สำเร็จ หมายถึง การโจมตีที่สามารถผ่านกลไกการป้องกันมาได้ ซึ่งเป็นการโจมตีที่มีความซับซ้อน การจะทราบถึงเทคนิควิธีการโจมตีลักษณะที่ใช้และผลกระทบที่เป็นไปได้ทั้งหมดต้องอาศัยการเก็บข้อมูลและการวิเคราะห์ชั้นสูง - RAM - Network Connection - Running Processes - Opened Files - Swap Memory - Hard Disk Image - System Log - Network Log - External Media ข้อมูลที่อ่อนไหวต่อการสูญเสียกระแสไฟฟ้า คือ ข้อมูลที่จะหายไปหากไม่มีกระแสไฟคอยเลี้ยง เช่น RAM เป็นต้น ดังนั้นเพื่อให้หลักฐานที่กล่าวมาคงอยู่ครบถ้วน ในบางกรณี การเก็บข้อมูลจึงต้องกระทำอย่างรวดเร็วโดยผู้เชี่ยวชาญ และก่อนที่จะมีการปิดเครื่องคอมพิวเตอร์และหากการตอบสนองเกิดขึ้นเร็วพอ โอกาสที่จะได้ตัวอย่างของ Malware ที่เป็น Ransomware มาวิเคราะห์จะมีโอกาสสูงขึ้น การดำเนินการทั้งหมดจะต้องถูกบันทึกอย่างละเอียดเพื่อการอ้างอิงถึงในภายหลังโดยเฉพาะการขึ้นสู่ชั้นศาล (หากจำเป็น)	ผู้ใช้งาน (Users) / ผู้ดูแลระบบฯ / System Admins
วิเคราะห์ข้อมูล หลักฐานทางดิจิทัลเพื่อ หาข้อสรุปจากการโจมตีและความเสียหายที่เกิดจาก Malware	ข้อมูลจากขั้นตอนก่อนหน้า จะต้องถูกนำมาหาข้อสรุปให้ได้ ๓ เรื่อง ดังต่อไปนี้ ๑. สาเหตุที่การโจมตีประสบผลสำเร็จ เพื่อการแก้ไขที่ตรงจุด ซึ่งต้องวิเคราะห์จากข้อมูลการสัมภาษณ์ และข้อมูลที่จัดเก็บได้ในขั้นตอนก่อนหน้า โดยเฉพาะการทำ Data Correlation และ Timeline Analysis ๒. โอกาสและรูปแบบของผลกระทบที่อาจจะขยายวงกว้างออกไปได้ โดยเฉพาะความสามารถของภัยคุกคามและ Malware ที่ใช้งาน เพื่อที่จะได้ค้นหาและหยุดการแพร่กระจายของภัยคุกคาม ซึ่งต้องพิจารณาจากข้อมูลที่จัดเก็บได้ในขั้นตอนก่อนหน้าเช่นเดียวกัน ที่ได้จากการทำ Malware Analysis ๓. การจัดทำ Indicator of Compromise (IoC) จากผลการวิเคราะห์ที่ได้ เพื่อใช้ในการ Scan ระบบอื่นๆ ในเครือข่ายเดียวกัน และ/หรือ เครือข่ายใกล้เคียง เพื่อระบุขอบเขตของการแพร่กระจายของ Malware และภัยคุกคาม *** ขั้นตอนการวิเคราะห์อาจจะต้องมีการทำซ้ำ ในกรณีพบข้อมูลใหม่ เช่น พบ Malware อีกประเภทหนึ่งในระบบอื่นที่ไม่เหมือนกับระบบที่โดนโจมตีในครั้งแรก	ทีมดูแลระบบสารสนเทศ อจน.
ขยายผลการวิเคราะห์ ความเสียหายที่เกิดจาก ข้อมูลรั่วไหล	เมื่อทราบว่ามีข้อมูลรั่วไหล ต้องทำการเตรียมความพร้อมและตรวจสอบความเป็นไปได้ของข้อมูลที่รั่วไหลว่าสามารถไปปรากฏอยู่ในแหล่งใดบ้าง โดยสามารถพิจารณาจากระบบที่ได้รับผลกระทบ	ทีมดูแลระบบสารสนเทศ อจน.

		/ System Admins
ติดต่อประสานงานกับ หน่วยงานภายในและ ภายนอก	ข้อมูลที่ได้จากการวิเคราะห์จำเป็นที่จะต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้อง โดยขึ้นอยู่กับเหตุการณ์และความจำเป็น โดยในกรณีของ Ransomware และ Data Leakage จากภายในองค์กร ควรมีหน่วยงานที่ต้องติดต่อสื่อสารอย่างน้อยดังต่อไปนี้ ๑. การแจ้งผลการวิเคราะห์ให้กับทีมผู้ดูแลระบบ เพื่อทำการแก้ไขจุดอ่อนและความเสียหายที่เกิดขึ้นกับระบบ ๒. กรณีระบบไม่สามารถให้บริการตามปกติได้ ต้องติดต่อประสานงานกับทีม BCP ซึ่งอาจเป็นการติดต่อโดยตรง หรือผ่าน Crisis Management Team ได้ ทั้งนี้จะขึ้นอยู่กับโครงสร้างขององค์กร ๓. การแจ้งหน่วยงานกำกับดูแลตามเกณฑ์ที่กำหนด ๔. การแจ้งเจ้าของข้อมูลที่รั่วไหล ตามเงื่อนไขของกฎหมายที่เกี่ยวข้องหรือตามความเหมาะสมและความจำเป็น	ทีมดูแลระบบสารสนเทศ อจน. / ผู้ควบคุมกฎ (Regulators) / พนักงาน (Employees
ขั้นตอนที่ ๓ : การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Containment, Eradication & Recovery)		
วัตถุประสงค์ (Objectives)	๑. การค้นหา กำจัด และควบคุมการแพร่กระจายของ Malware ๒. การค้นหาและควบคุมการรั่วไหลของข้อมูล ๓. การกู้คืนระบบให้กลับมาทำงานปกติ	
Activity	**Description**	**Stakeholders**
นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัด ภัยคุกคามออกจากระบบ	ขั้นตอนที่สามารถดำเนินการควบคู่กับการวิเคราะห์ข้อมูล คือ การจำกัดความเสียหายเบื้องต้น ซึ่งปกติจะดำเนินการตัดการเชื่อมต่อเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่โดนโจมตีออกจากเครือข่าย และ/หรือ ทำการปิดการทำงานของอุปกรณ์ลงโดยวิธี Shutdown หรือถอดสายไฟโดยทันที ทั้งนี้ วิธีที่เลือกใช้ควรคำนึงถึงความเสียหายที่จะเกิดกับข้อมูลหลักฐานทางดิจิทัลเสมอ และควรมีการเก็บข้อมูลออกจากอุปกรณ์นั้นๆ ด้วยวิธีที่ถูกต้องก่อนที่จะมีการปิดการทำงาน ผลการวิเคราะห์ข้อมูลหลักฐานทางดิจิทัลจะทำให้ได้ข้อสรุปของการโจมตีตั้งแต่ช่องโหว่ที่ใช้ความเสียหายที่เกิดขึ้น และร่องรอยที่เกี่ยวข้อง (เช่น การเข้าถึง/เปลี่ยนแปลง File, Registry, Networking Resource, Network Storage เป็นต้น ซึ่งทั้งหมดนี้สามารถใช้ในการแก้ไข Incident ได้ นอกจากนี้ การ Scan เพื่อค้นหา Indicator of Compromise (IoC) เป็นหนึ่งวิธีที่ช่วยให้การค้นหาและกำจัดภัยคุกคามสามารถดำเนินการได้เร็วขึ้น	ทีมดูแลระบบสารสนเทศ อจน. / System Admins
เรียกใช้งาน BCP หากมีความจำเป็น	ในระหว่างการรับมือและตอบสนองภัยคุกคาม หากความเสียหายที่เกิดขึ้นอยู่ในระดับที่ทำให้ระบบหลักไม่สามารถให้บริการได้ หน่วยงานต้องดำเนินการ Activate Disaster Recovery Site/System ตามที่กำหนดใน Business Continuity Plan (BCP)	ทีมดูแลระบบสารสนเทศ อจน. / System

		Admins / BCP-IT อจน.
ควบคุมและเยียวยาความเสียหายจากการ รั่วไหลของข้อมูล	การรั่วไหลของข้อมูลถึงแม้จะไม่สามารถถูกแก้ไขได้อย่างสิ้นเชิง แต่ควรมีการตอบสนองที่สำคัญเพื่อช่วยบรรเทาความเสียหาย และลดหรือกำจัดผลกระทบจากการรั่วไหลนั้นได้ คือ การระบุจุดที่ข้อมูลรั่วไหลถูกเปิดเผย เช่น Website, Bit Torrent เป็นต้น และควรมีขั้นตอนหรือแนวทางในการดำเนินการ Take Down แหล่งข้อมูลเหล่านั้นเท่าที่ทำได้ และควรมีมาตรการเยียวยาเจ้าของข้อมูลและผู้ที่ได้รับผลกระทบตามที่กฎหมายกำหนด นอกจากนี้ ควรร่วมมือกับหน่วยงานที่เกี่ยวข้อง เพื่อจัดทำ Information Marking และ Personal Information Usage Monitoring เพื่อให้รู้ได้ทันทีเมื่อข้อมูลชุดที่รั่วไหลถูกนำไปใช้งาน	ทีมดูแลระบบสารสนเทศ อจน. / ผู้ควบคุมกฎ (Regulators)
กู้คืนระบบ และข้อมูลหากมีความเสียหาย	เมื่อแก้ไขและกำจัดภัยคุกคามออกจากระบบได้แล้ว หากจำเป็นต้องมีการกู้คืนระบบ และ/หรือข้อมูลที่ได้รับความเสียหายกลับมาจาก Backup System Image และ Backup Dataและควรระมัดระวังช่องโหว่หรือจุดอ่อนใดที่ปรากฏอยู่ใน Backup System Image ซึ่งหากตรวจพบ ควรดำเนินการแก้ไขก่อนนำมาใช้งาน	ทีมดูแลระบบสารสนเทศ อจน. / System Admins
สอดส่องดูแลความ ผิดปกติอย่างต่อเนื่อง	การสอดส่องดูแลความผิดปกติ ต้องเริ่มตั้งแต่เมื่อมีการนำอุปกรณ์ที่โดนโจมตีออกจากเครือข่าย จนถึงการกู้คืนระบบเรียบร้อยแล้ว รวมทั้งหลังจากกลับมาปฏิบัติงานตามปกติอีกสักระยะหนึ่ง โดยการกำหนดระยะเวลาจะขึ้นอยู่กับแต่ละองค์กรซึ่งอย่างน้อยไม่ควรต่ำกว่า ๔๘ ชั่วโมง ทั้งนี้ หากพบเจอความผิดปกติให้กลับไปดำเนินการในขั้นตอน Detection & Analysis อีกครั้ง	ทีมดูแลระบบสารสนเทศ อจน.
ขั้นตอนที่ ๔ : การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Post Cyber Incident Activity)		
วัตถุประสงค์ (Objectives	การประเมินประสิทธิผล การปรับปรุง พัฒนาแผนการรับมือหรือความพร้อมด้านอื่นๆ จากข้อมูลที่ได้จากการรับมือ	
Activity	Description	Stakeholders
การเรียนรู้เพื่อปรับปรุง	อ้างอิงข้อ ๔.๑ และข้อ ๔.๒ ใน “ขั้นตอนที่ ๔: การเรียนรู้จากภัยคุกคาม (Lessons Learned) และการวัดผลและปรับปรุงการปฏิบัติงานในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์”	ทุกคนที่มีส่วนร่วมในขั้นตอนการตอบสนองทั้งภายในและภายนอก

<u>กรณีตัวอย่างที่ ๒</u> : การรั่วไหลของข้อมูล (Data Leakage) จากบุคคลภายนอก (Third Party) ที่ให้บริการ

ขั้นตอนที่ ๑ : การเตรียมความพร้อม (Preparation)		
วัตถุประสงค์ **(Objectives)**	๑. มีทรัพยากรที่สำคัญต่อการตอบสนองต่อภัยคุกคามทางไซเบอร์ ๒. มีกระบวนการ และกลไกในการป้องกันระบบที่ดี เพื่อช่วยลดโอกาสที่การโจมตีจะสำเร็จ หรือลดผลกระทบจากการโจมตี อีกทั้งยังเป็นทำหน้าที่ในการตรวจจับความพยายามในการบุกรุกได้อีกด้วย	
Activity	Description	Stakeholders
การจัดเตรียมทรัพยากร	อ้างอิงข้อ ๑.๑ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)”	ผู้บริหารเทคโนโลยีสารสนเทศ อจน. (CIO)
ดำเนินการป้องกันก่อนเกิดเหตุ	อ้างอิงข้อ ๑.๒ ใน “ขั้นตอนที่ ๑: การเตรียมความพร้อม (Preparation)” ๑. สำหรับการเตรียมพร้อมรับมือ Data Leakage จาก Third-Party ให้มุ่งเน้นไปที่เรื่องของ - กระบวนการคัดเลือก Third-Party (Selection) - ความสามารถในการให้บริการตามกำหนด - ความสามารถในการดำเนินการตาม Security Policy ขององค์กร ๒. การดำเนินงานระหว่างผู้ให้บริการกับบริษัท (Orientation & Integration) ควรแบ่งหน้าที่ความรับผิดชอบในการดำเนินการตามนโยบาย Security Policy ให้ชัดเจน อย่างน้อยในเรื่องดังต่อไปนี้ - กำหนดขั้นตอนการดำเนินงานในแต่ละเรื่อง - มีการอบรมและฝึกฝนร่วมกันอย่างสม่ำเสมอ - มีกระบวนการตรวจสอบ และต้องกำหนดสิทธิในการตรวจสอบสัญญาการให้บริการ มีการตรวจสอบด้วยมาตรฐานระดับเดียวกับองค์กร - มีการติดตามและปรับปรุงอย่างสม่ำเสมอ - มีกระบวนการยกเลิกการใช้บริการ - สามารถอำนวยความสะดวกเมื่อต้องมีการเปลี่ยนแปลงผู้ให้บริการ - ข้อกำหนดในการทำลายข้อมูลสำคัญออกจากระบบ	ผู้ดูแลระบบ อจน. / Outsource ด้าน IT / บุคคลภายนอก (Third-Party)
ขั้นตอนที่ ๒ : การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)		
วัตถุประสงค์ **(Objectives)**	๑. รับแจ้งเหตุการณ์การโจมตี ๒. การระบุความเสียหายเบื้องต้น ๓. การระบุสาเหตุที่การโจมตีสำเร็จ ๔. การระบุความสามารถของผู้บุกรุกและเครื่องมือที่ใช้รวมถึง Malware	

Activity	Description	Stakeholders
รับแจ้งเหตุ	เมื่อมีการรั่วไหลของข้อมูลเกิดขึ้น Third-Party จะต้องแจ้งให้กับองค์กรทราบ ตามเงื่อนไขและวิธีการที่ได้ชี้แจงและฝึกฝนไว้ และต้องสอดคล้องกับ Security Policy ขององค์กรทั้งหมด	Outsource ด้าน IT / บุคคลภายนอก (Third-Party) / ผู้ดูแลระบบสารสนเทศ อจน.
วิเคราะห์การโจมตีและขอบเขตความเสียหาย	๑. ทีมผู้ดูแลระบบฯ ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ข้อมูลความเสียหายเบื้องต้นสำหรับการพิจารณามาตรการในส่วนที่องค์กรเองจะต้องดำเนินการ ๒. การรายงานความคืบหน้าและผลลัพธ์ควรกระทำเป็นระยะ และมีข้อมูลชัดเจน ๓. ทีมผู้ดูแลระบบฯ อาจจะพิจารณาให้ความช่วยเหลือได้ ตามที่กำหนดไว้ตอนเริ่มสัญญาหรือตามสถานการณ์	ผู้ดูแลระบบสารสนเทศ อจน. / Outsource ด้าน IT / บุคคลภายนอก (Third-Party)
จัดเก็บหลักฐานทางดิจิทัลที่จำเป็นรวมถึง ตัวอย่าง (Specimen) Malware	ทีมผู้ดูแลระบบฯ ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ผลลัพธ์ เช่นเดียวกับ ขั้นตอนที่ ๒ การตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis) ส่วน Activity “จัดเก็บหลักฐานทางดิจิทัลที่จำเป็น รวมถึงตัวอย่าง (Specimen) Malware”	ผู้ดูแลระบบสารสนเทศ อจน. / Outsource ด้าน IT / บุคคลภายนอก (Third-Party)
ขยายผลการวิเคราะห์ความเสียหายที่เกิดจากข้อมูลรั่วไหล	ต้องได้ข้อมูลการรั่วไหลที่ชัดเจนจากผู้ให้บริการ เพื่อให้มีความพร้อมในการสอดส่องเสาะหาข้อมูลที่รั่วไหลว่าไปปรากฏอยู่ในที่ใดบ้าง	ผู้ดูแลระบบสารสนเทศ อจน. / บุคคลภายนอก (Third-Party)
ติดต่อประสานงานกับหน่วยงานภายในและ ภายนอก	ข้อมูลที่ได้จากการวิเคราะห์จำเป็นที่จะต้องถูกสื่อสารไปยังผู้ที่เกี่ยวข้องต่างๆ ขึ้นอยู่กับเหตุการณ์และความจำเป็น ในกรณี Data Leakage ขององค์กร มีหน่วยงานที่ต้องติดต่อสื่อสาร ดังนี้ ๑. การแจ้งผลการวิเคราะห์ให้กับทีมผู้ดูแลระบบ เพื่อทำการแก้ไขจุดอ่อนและความเสียหายที่เกิดขึ้นกับระบบ ๒. การแจ้งหน่วยงานกำกับดูแลตามเกณฑ์ที่กำหนด ๓. การแจ้งเจ้าของข้อมูลที่รั่วไหล ตามเงื่อนไขของกฎหมายที่เกี่ยวข้องหรือตามความเหมาะสมและความจำเป็น	ผู้ดูแลระบบสารสนเทศ อจน. / ผู้ควบคุมกฎ (Regulators) / พนักงาน อจน.
ขั้นตอนที่ ๓ : การรับมือและการตอบสนองต่อเหตุการณ์ภัยคุกคามทางไซเบอร์ (Containment, Eradication & Recovery)		
วัตถุประสงค์ (Objectives)	๑. การค้นหา กำจัด และควบคุมการแพร่กระจายของ Malware ๒. การค้นหาและควบคุมการรั่วไหลของข้อมูล ๓. การกู้คืนระบบให้กลับมาทำงานปกติ	

Activity	Description	Stakeholders
นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัดภัยคุกคามออกจากระบบ	ทีมผู้ดูแลระบบฯ ควบคุมดูแลและประสานงานกับผู้ให้บริการเพื่อให้ได้ผลลัพธ์เช่นเดียวกับ “ขั้นตอนที่ ๓ : การควบคุมความเสียหาย การกำจัดสาเหตุของภัยคุกคาม และการกู้คืน Containment, Eradication & Recovery” ส่วน Activity “นำผลการวิเคราะห์ที่ได้มาทำการตรวจสอบกับเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้รับผลกระทบ เพื่อกำจัดภัยคุกคามออกจากระบบ”	ทีมผู้ดูแลระบบ อจน. / Third-Party
ควบคุมและเยียวยาความเสียหายจากการรั่วไหลของข้อมูล	การรั่วไหลของข้อมูลถึงแม้จะไม่สามารถถูกแก้ไขได้อย่างสิ้นเชิง แต่ควรมีการตอบสนองที่สำคัญเพื่อช่วยบรรเทาความเสียหาย และลดหรือกำจัดผลกระทบจากการรั่วไหลนั้นได้ คือ การระบุจุดที่ข้อมูลรั่วไหลถูกเปิดเผย เช่น Website, Bit Torrent เป็นต้น และควรมีขั้นตอนหรือแนวทางในการดำเนินการ Take Down แหล่งข้อมูลเหล่านั้นเท่าที่ทำได้ และควรมีมาตรการเยียวยาเจ้าของข้อมูลและผู้ที่ได้รับผลกระทบตามที่กฎหมายกำหนด นอกจากนี้ ควรร่วมมือกับหน่วยงานที่เกี่ยวข้องเพื่อจัดทำ Information Marking และ Personal Information Usage Monitoring เพื่อให้รู้ได้ทันทีเมื่อข้อมูลชุดที่รั่วไหลถูกนำไปใช้งาน	ทีมผู้ดูแลระบบ อจน. / Third-Party
สอดส่องดูแลความผิดปกติอย่างต่อเนื่อง	การสอดส่องดูแลความผิดปกติ ต้องเริ่มตั้งแต่เมื่อมีการนำอุปกรณ์ที่โดนโจมตีออกจากเครือข่าย จนถึงการกู้คืนระบบเรียบร้อยแล้ว รวมทั้งหลังจากกลับมาปฏิบัติงานตามปกติอีกสักระยะหนึ่ง โดยการกำหนดระยะเวลาจะขึ้นอยู่กับแต่ละองค์กรซึ่งอย่างน้อยไม่ควรต่ำกว่า ๔๘ ชั่วโมง ทั้งนี้ หากพบเจอความผิดปกติให้กลับไปดำเนินการในขั้นตอน Detection & Analysis อีกครั้ง	ทีมผู้ดูแลระบบ อจน. / Third-Party
ขั้นตอนที่ ๔ : การดำเนินการหลังจากการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์ (Post Cyber Incident Activity)		
วัตถุประสงค์ (Objectives)	การประเมินประสิทธิผล การปรับปรุง พัฒนาแผนการรับมือหรือความพร้อมด้านอื่นๆ จากข้อมูลที่ได้จากการรับมือ	
Activity	Description	Stakeholders
การเรียนรู้เพื่อปรับปรุง	อ้างอิงข้อ ๔.๑ และข้อ ๔.๒ ใน “ขั้นตอนที่ ๔: การเรียนรู้จากภัยคุกคาม (Lessons Learned) และการวัดผลและปรับปรุงการปฏิบัติงานในการรับมือภัยคุกคามและตอบสนองต่อเหตุการณ์ผิดปกติทางไซเบอร์”	ทุกคนที่มีส่วนร่วมในขั้นตอน การตอบสนองทั้งภายในและภายนอก

ภาคผนวก 4

แบบประเมินผลกระทบทางธุรกิจ

แบบประเมินผลกระทบทางธุรกิจ

หน่วยงาน.....

ลักษณะงาน	กิจกรรม/กระบวนการ	กรอบเวลา/รอบเวลาปฏิบัติงาน	ผู้ส่งมอบงาน	หน่วยงานภายในที่เกี่ยวข้อง	ผู้รับบริการ

ระดับผลกระทบ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ
สูงมาก	▪ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูงมาก ▪ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงมากกว่า ร้อยละ ๕๐ ▪ เกิดการสูญเสียชีวิตและ/หรือภัยคุกคามต่อสาธารณชน ▪ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศและนานาชาติ
สูง	▪ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับสูง ▪ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการลดลงร้อยละ ๒๕-๕๐ ▪ เกิดการบาดเจ็บต่อผู้รับบริการ/บุคคล/กลุ่มคน ▪ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับประเทศ
ปานกลาง	▪ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับปานกลาง ▪ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ ๑๐-๒๕ ▪ ต้องมีการรักษาพยาบาล ▪ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ต่ำ	▪ เกิดความเสียหายต่อองค์กรเป็นจำนวนเงินในระดับต่ำ ▪ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงร้อยละ ๕-๑๐ ▪ ต้องมีการปฐมพยาบาล ▪ ส่งผลกระทบต่อชื่อเสียงและความมั่นใจต่อองค์กรในระดับท้องถิ่น
ไม่เป็นสาระสำคัญ	▪ ส่งผลให้ขีดความสามารถในการดำเนินงานหรือให้บริการ ลดลงมากกว่าร้อยละ ๕

หลักเกณฑ์การประเมินผลกระทบต่อกระบวนการดำเนินงาน

สรุปเหตุการณ์และผลกระทบจากเหตุการณ์

ความเสี่ยงและภัยคุกคาม	ผลกระทบ				
	ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	ด้านคู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียที่สำคัญ
เหตุการณ์อุทกภัย	✓	✓	✓	✓	✓
เหตุการณ์ภัยพิบัติ	✓	✓	✓	✓	✓
เหตุการณ์อัคคีภัย	✓	✓	✓	✓	✓
เหตุการณ์ชุมนุมประท้วง/จลาจล	✓			✓	
เหตุการณ์ก่อการร้าย	✓			✓	
เหตุการณ์โรคระบาด	✓			✓	
เหตุการณ์ภัยคุกคามทางไซเบอร์	✓	✓	✓	✓	✓

วิเคราะห์ระดับผลกระทบต่อกระบวนการ

หน่วยงาน.....กิจกรรม/กระบวนงาน.....

ผลกระทบต่อ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ				
	ไม่เป็นสาระสำคัญ 1	ต่ำ 2	ปานกลาง 3	สูง 4	สูงมาก 5
1.ผู้รับบริการภายนอก (คุณภาพของงาน ความครบถ้วนของงาน การส่งต่องาน เป็นต้น)					
2. ผู้รับบริการภายใน (คุณภาพของงาน ความครบถ้วนของงาน การส่งต่องาน เป็นต้น)					
3.บุคลากรในหน่วยงาน (จำนวนลดลง ขวัญกำลังใจ ความเครียด)					
4. กรอบเวลาการดำเนินงานตาม ข้อบังคับ กฎระเบียบต่างๆข้อตกลงการ ดำเนินการ/สัญญาต่างๆ/TOR					
5. กระบวนการทำงาน/ระบบเทคโนโลยี ที่ใช้งาน (กระบวนการหยุดชะงัก/การเข้า ไมถึง server, application/ผู้ไหบริการระบบ)					
A = สรุปภาพรวมระดับผลกระทบ (ใช้ฐานนิยม หมายถึง ค่าที่ซ้ำกันมากที่สุด)					

ผลกระทบต่อ	หลักเกณฑ์ในการพิจารณาระดับผลกระทบ				
	มากกว่า 2 สัปดาห์ 1	2 สัปดาห์ 2	1 สัปดาห์ 3	1 - 2 วัน 4	ภายใน 1 วัน 5
B = ระยะเวลาที่ยอมให้หยุดได้นานที่สุด					

สรุประดับผลกระทบ เท่ากับ .... (A x B)

(ไม่เป็นสาระ = 1-5, ต่ำ = 6-8, ปานกลาง = 8-11, สูง = 12-15, สูงมาก = 16-25)

แบบประเมินผลกระทบต่อกระบวนการ/กิจกรรม

หน่วยงาน.....

หน่วยงานย่อย	กระบวนการ/กระบวนงาน/กิจกรรม	ผลกระทบต่อ			ระยะเวลานานที่สุดที่ยอมให้หยุดได้	เหตุผล	คะแนน/ระดับผลกระทบ
		ผู้ส่งมอบงาน	หน่วยงานภายในที่เกี่ยวข้อง	ผู้รับบริการ			

ภาคผนวก 5

กลยุทธ์การกู้คืนธุรกิจ

กลยุทธ์การกู้คืนธุรกิจ (Business Recovery Strategy)

หน่วยงาน.....กิจกรรม/กระบวนงาน.....

ความสูญเสีย/เสียหาย	บริการขั้นต่ำที่ให้ได้	ระยะเวลาหยุดดำเนินการขั้นต่ำที่ให้ได้	ระดับบริการที่คาดว่าจะกู้ได้ (วันที่ 1 ถึงสัปดาห์ที่ 4)	กลยุทธ์การกู้คืนที่นำมาปฏิบัติ Business Recovery Strategy Adopted
1. สถานที่ปฏิบัติงาน 2. วัสดุอุปกรณ์ที่สำคัญ/การจัดหาอุปกรณ์ที่สำคัญ 3. เอกสารสำคัญ	1. รับเอกสาร 2. พิจารณาเอกสารเร่งด่วนเพื่อดำเนินการ	4 ชม.	Day 1-3: 20% Week 1: 30% Week 2: 50% Week 3: 60% Week 4: 80%	(1) รายงานหัวหน้าทีมของตนเอง (2) แจ้งเจ้าหน้าที่ที่กำหนดตามผังใน Call Tree ให้อยู่ปฏิบัติงานตามแผนที่กำหนด (3) แจ้งหน่วยงานที่ติดต่อทั้งภายในและภายนอกถึงสถานการณ์และบริการขั้นต่ำที่ยังให้ได้รวมถึงระยะเวลาที่จะให้บริการอื่นๆ ต่อไปได้ (4) เตรียมการให้บริการด้วยระบบธรรมดาและสำรองข้อมูลสำหรับจัดเก็บเข้าระบบ (5) เตรียมการย้ายไปศูนย์ปฏิบัติการสำรองตามคำสั่งศูนย์สั่งการ (6) จัดเตรียมทรัพยากรตามที่กำหนด และ IT ติดตั้งระบบงานที่ศูนย์ปฏิบัติการสำรอง (7) ตรวจสอบการทำงานของระบบ (8) สอบทานเอกสารสำคัญที่จะใช้งาน (9) ลำดับงานเร่งด่วนให้สอดคล้องกับความพร้อมของระบบและอุปกรณ์ที่รองรับ (10) แจ้งทุกฝ่ายที่เกี่ยวข้องถึงสถานที่ปฏิบัติงานใหม่ให้เข้าทำงาน ณ สถานที่ใหม่ ตามลำดับความสำคัญของงานสำหรับลักษณะงานที่ทำที่บ้านได้ ให้ทำที่บ้านไปก่อน 1 สัปดาห์แล้วค่อยพิจารณาปรับตามขนาดของสถานที่สำรอง (11) เริ่มปฏิบัติงานต่อตามกระบวนการปกติ (12) เข้าฟื้นฟูและปรับปรุงสถานที่ทำงาน (13) รายงานหัวหน้าคณะทำงานบริหารความพร้อมต่อสภาวะวิกฤต

กลยุทธ์การกู้คืนธุรกิจ (Business Recovery Strategy)

หน่วยงาน.....กิจกรรม/กระบวนงาน.....

ความสูญเสีย/เสียหาย	บริการขั้นต่ำที่ให้ได้	ระยะเวลาหยุดดำเนินการขั้นต่ำที่ให้ได้	ระดับบริการที่คาดว่าจะกู้ได้ (วันที่ 1 ถึง สัปดาห์ที่ 4)	กลยุทธ์การกู้คืนที่นำมาปฏิบัติ Business Recovery Strategy Adopted
ระบบเทคโนโลยีสารสนเทศ/ข้อมูลสำคัญ			Day 1-3 : 20% Week 1 : 30% Week 2 : 50% Week 3 : 60% Week 4 : 80%	
บุคลากรหลัก/สำคัญ				
ผู้ให้บริการที่สำคัญ				

กำหนดทรัพยากรที่สำคัญ

หน่วยงาน.....กิจกรรม/กระบวนงาน.....

การกำหนดทรัพยากรที่สำคัญ						
อาคาร/สถานที่ปฏิบัติงาน	เครื่องมือและอุปกรณ์		ระบบงาน เทคโนโลยี หรือ ระบบสารสนเทศ	บุคลากร		คู่ค้าผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย
	ประเภท/ชนิด	จำนวน (หน่วย)		ตำแหน่ง	จำนวน (คน)	

ภาคผนวก 6

คณะผู้บริหารความต่อเนื่อง

องค์การจัดการน้ำเสีย

คณะผู้บริหารความต่อเนื่ององค์การจัดการน้ำเสีย

บุคลากรหลัก		บทบาท	บุคลากรสำรอง	
ชื่อ	เบอร์มือถือ		ชื่อ	เบอร์มือถือ
นายชีระ วงศบูรณะ	081-8423802	หัวหน้าคณะบริหารความต่อเนื่อง ผอ.อจน.	นายสุชัย เจนพจนารถ	081-4504600
นางดวงแข ยงสุวรรณ	081-4228990	ผู้ประสานงานคณะบริหารความต่อเนื่อง สผอ.	นางสาวอรทัย อินประสิทธิ์	081-4228990
น.ส.สรรพางดี ล่ามกิจจา	085-6891616	ผู้ประสานงานคณะบริหารความต่อเนื่อง สตน.	นายอภินท์ ธนัพประภัศร์	086-8922298
นางสาววรนันท์ จันทร์ดนู	095-4596051	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.บร.	น.ส.อาภากร อมาตยกุล	081-1956661
นายสุชัย เจนพจนารถ	081-4504600	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.วผ.	นายปัณณพัฒน์ จันทร์เจริญสุข	096-1496364
นายอธิรักษ์ บุพจันโท	063-2035762	หัวหน้าทีมบริหารความต่อเนื่อง รผอ.อจน.ปก.	น.ส.ศิริวรรณ ลิมป์รุ่งรัตนา	081-3767696
นายอนุกูล แหลมปัญญา	081-7121248	หัวหน้าทีมบริหารความต่อเนื่อง รก.ฝอก.	นายอนุกูล แหลมปัญญา	081-7121248
นางสาววรนันท์ จันทร์ดนู	095-4596051	หัวหน้าทีมบริหารความต่อเนื่อง ฝบง.	นายบรรพต ศุขวัฒนะกุล	089-6693769
นายปัณณพัฒน์ จันทร์เจริญสุข	096-1496364	หัวหน้าทีมบริหารความต่อเนื่อง ฝพอ.	นางบุณฑริกา สุดใจนาค	099-1599818
นายอนุพันธ์ เตียไพรัชกูลกิจ	081-4749090	หัวหน้าทีมบริหารความต่อเนื่อง ฝวศ.	น.ส.ศุทธวดี ศิริยานนท์	093-3241988
นายอธิรักษ์ บุพจันโท	063-2035762	หัวหน้าทีมบริหารความต่อเนื่อง รก.ฝจส.1	นายรัฐวุฒิ ทับทอง	081-8349880
นายอนุพันธ์ เตียไพรัชกูลกิจ	081-4749090	หัวหน้าทีมบริหารความต่อเนื่อง รก.ฝจส.2	น.ส.ศิริวรรณ ลิมป์รุ่งรัตนา	081-3767696

1. เมื่อเกิดเหตุวิกฤตหัวหน้าคณะบริหารความต่อเนื่อง โดยผู้อำนวยการองค์การจัดการน้ำเสียประกาศภาวะวิกฤต และโทรแจ้งผู้ประสานงานคณะบริหารความต่อเนื่องให้ดำเนินการตามแผน BCP และให้โทรแจ้งหัวหน้าทีมบริหารความต่อเนื่อง

2. ผู้ประสานงาน BCP โทรศัพท์แจ้งหัวหน้าทีมบริหารความต่อเนื่องและดำเนินการตามแผน BCP รวมถึงรายงานสถานะการดำเนินการตามแผนให้หัวหน้าคณะบริหารความต่อเนื่องทราบ

3. หัวหน้าทีมคณะบริหารความต่อเนื่องดำเนินการตามแผน BCP ในส่วนที่เกี่ยวข้อง

4. ผู้รับผิดชอบด้านอัคคีภัย (Fire warden) รับผิดชอบการเคลื่อนย้ายบุคลากรออกจากสถานที่เกิดเหตุตามขั้นตอนปฏิบัติการและต้องรายงานผลการเคลื่อนย้ายบุคลากรให้ผู้ดูแลความปลอดภัยอาคารสถานที่ (Building Safety Manager) และให้ความช่วยเหลือในการติดตามบุคลากรที่หายไปหรือไม่ได้รายงานตัว

5. หัวหน้าผู้ดูแลอาคาร (Building manager) ประสานงานกับผู้ดูแลประจำชั้นอาคาร (Floor manager) ในการช่วยเคลื่อนย้ายบุคลากร ณ สถานที่เกิดเหตุทันทีที่เกิดเหตุการณ์ฉุกเฉินที่คุกคามชีวิตและความปลอดภัยของบุคลากรรวมถึงทรัพย์สินสำคัญขององค์การจัดการน้ำเสีย

ทีมบริหารความต่อเนื่อง

กลุ่ม/ฝ่าย..... หน่วยงาน.....

ทีมบริหารความต่อเนื่อง	ตำแหน่ง	โทรศัพท์ที่ทำงาน	โทรศัพท์ที่บ้าน	โทรศัพท์มือถือ	อีมล์
	หัวหน้าทีมบริหารความต่อเนื่อง				
	หัวหน้ากลุ่ม/ฝ่าย				
	เจ้าหน้าที่ที่เกี่ยวข้อง				
	เจ้าหน้าที่สำรอง				
	เจ้าหน้าที่สำรอง				

ภาคผนวก 7

แผนการสื่อสารของหน่วยงาน

แผนการสื่อสารของหน่วยงาน

ในช่วงเวลาที่เกิดเหตุการณ์ความเสียหายขึ้น สิ่งสำคัญสำหรับหน่วยงานคือการสื่อสารข้อความสำคัญ (key messages) ให้ผู้ให้บริการ/ผู้ใช้บริการของตนทราบอย่างรวดเร็วและมีประสิทธิผล เพื่อให้ผู้ให้บริการเหล่านั้นได้รับทราบถึงสถานการณ์และข้อชี้แนะพิเศษในการดำเนินการจึงจำเป็นต้องมีแผนการสื่อสารของหน่วยงาน เตรียมการไว้ล่วงหน้า แผนการสื่อสารของหน่วยงานควร ประกอบด้วยแผนการสื่อสารที่จะดำเนินการ และข้อความที่มีการร่างไว้ล่วงหน้า รวมถึงคำถามที่พบบ่อย ภายใต้สถานการณ์เหตุการณ์ความเสียหายที่แตกต่างกันดังนั้น เมื่อมีการประกาศใช้ แผน BCP ให้ปฏิบัติดังนี้

1. เจ้าหน้าที่ที่ประจำอยู่ที่สถานที่ทำงานหลัก (Primary Site) จะต้องนำป้ายประกาศติดไว้ใกล้สถานที่ ทำการเดิม เพื่อให้ผู้มาติดต่อรับทราบถึงที่ทำการชั่วคราว **ตัวอย่างเนื้อความของป้ายประกาศ**

2. จากวันที่ .....องค์การจัดการน้ำเสีย ได้ย้ายที่ทำการเป็นการชั่วคราวไปที่ เลขที่..... อาคาร..... ถนน..... หมายเลขโทรศัพท์..... หมายเลขโทรสาร.....

3. ผู้ประสานงาน BCP นำแบบฟอร์มหนังสือขออนุญาตเข้าปฏิบัติงาน ณ อาคารศูนย์สำรอง (ที่ได้จัดทำและเก็บไว้) มากรอกข้อความด้วยลายมือ และลงลายมือชื่อเจ้าหน้าที่บริหารฯ เพื่อนำไปยังศูนย์สำรอง (เนื่องจากเวลาเกิดเหตุอาจไมมีระบบจัดพิมพ์หนังสือ หนังสือขออนุญาตเข้าปฏิบัติงานจึงควรจัดทำไว้ล่วงหน้า และจัดเก็บ 1 ชุดในสถานที่ปฏิบัติงานรวมไว้กับชุดวัสดุ/อุปกรณ์ที่ต้องเตรียมไว้ และอีก 1 ชุดที่บ้านของผู้ประสานงาน BCP กรณีเหตุการณ์เกิดหลังเวลาทำการ)

4. เมื่อไปถึงยังศูนย์สำรอง นำแบบฟอร์มจดหมายและแจ้งศูนย์สั่งการถึงการย้ายสถานที่ปฏิบัติงาน จัดส่งโทรสารหรือส่งผ่าน Line ในเบื้องต้นให้กับศูนย์สั่งการเพื่อแจ้งแก่ส่วนงานภายใน

5. ผู้ประสานงาน BCP จัดทำหนังสือติดต่อคู่ค้าหรือลูกค้าให้ทราบการเปลี่ยนแปลงสถานที่ปฏิบัติงาน หาก PC และเครื่องโทรสารยังไม่สามารถใช้การได้ระหว่างนั้นอาจจะแจ้งทางโทรศัพท์ก่อน

6. ณ ศูนย์สำรองการปฏิบัติงานผู้ประสานงาน BCP จัดทำประกาศแจ้งให้ทราบว่า มีบริการใดบ้างที่ยังให้บริการอยู่และระบบใดใช้การได้ระบบใดยังใช้การไม่ได้อาจมีความล่าช้าหรือต้องรอคอยเป็นเวลาเท่าไร

7. จัดให้มีการตอบรับโทรศัพท์แจ้งการย้ายสถานที่และบริการที่ยังให้บริการอยู่หรือบริการใดสามารถใช้ได้ ณ สถานที่ใดทดแทนได้

ภาคผนวก 8

แบบทดสอบแผนบริหารความต่อเนื่องทางธุรกิจ

☞ เหตุการณ์อัคคีภัย ☜

สถานการณ์จำลอง มีดังนี้

1. ไฟไหม้ตึกอาคารเล่าเป้งง่วน ชั้น 24 เหตุการณ์เกิดขึ้นในวันจันทร์เวลา 14.00 น. ซึ่งเป็นวันทำงาน

2. ครุภัณฑ์ เครื่องใช้ไฟฟ้า วัสดุ อุปกรณ์ เสียหายเป็นส่วนมาก

3. มีบุคลากรบาดเจ็บรวม 20 คน เนื่องจากเป็นวันทำงานตามปกติ

ภารกิจที่ต้องดำเนินการได้อย่างต่อเนื่อง

1. การวิเคราะห์สถานการณ์ของอัคคีภัย

2. การประชาสัมพันธ์ เผยแพร่ เตือนภัย และ call center

3. การดำเนินการด้านเทคโนโลยีสารสนเทศ

แผนการบริหารความต่อเนื่องและกอบกู้กระบวนการ ทีมงาน.....

วันที่ 1 (เหตุการณ์เกิดที่อาคารเล่าเป้งง้วน ชั้น 24)

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

วันที่ 2 – 7 การตอบสนองในระยะเวลาสั้น

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

วันที่ 8 การตอบสนองระยะกลาง (1 สัปดาห์)

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

☞ เหตุการณ์อุทกภัย ☜

สถานการณ์จำลอง มีดังนี้

1. น้ำท่วมบริเวณโดยรอบของอาคารเล่าเป้งง้วน ถ.วิภาวดีรังสิต ความลึกเฉลี่ย 1 เมตร การเดินทางเข้ามาในบริเวณองค์การจัดการน้ำเสีย อาคารเล่าเป้งง้วน ได้โดยทางเรือ

2. ไม่มีบุคลากรบาดเจ็บหรือเสียชีวิต

ภารกิจที่ต้องดำเนินการได้อย่างต่อเนื่อง

1. การวิเคราะห์สถานการณ์อุทกภัย

2. การประชาสัมพันธ์ เผยแพร่ เตือนภัย และ Call Center

3. การดำเนินการด้านเทคโนโลยีสารสนเทศ

แผนการบริหารความต่อเนื่องและกอบกู้กระบวนการ ทีมงาน.....

วันที่ 1 (เหตุการณ์เกิดที่บริเวณโดยรอบอาคารเล่าเป้งง้วน)

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

วันที่ 2 – 7 การตอบสนองในระยะเวลาสั้น

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

วันที่ 8 การตอบสนองระยะกลาง (1 สัปดาห์)

ขั้นตอนกิจกรรม

1. .....
2. .....
3. .....
4. .....
5. .....

องค์การจัดการน้ำเสีย
เลขที่ 333 อาคารเค้าเป้งง้วน 1 ชั้น 23
ถนนวิภาวดีรังสิต แขวงจอมพล เขตจตุจักร
กรุงเทพฯ 10900
โทรศัพท์ 0-2273-8530-39 โทรสาร 0-2273-8577
E-Mail: wastewtr@wma.or.th
www.wma.or.th.