กรมควบคุมโรค
Department of Disease Control

แผนประคองกิจการ
(Business Continuity Plan)

จัดทำโดย
คณะทำงานระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

รายละเอียดเอกสาร

รหัสเอกสาร	PLA-DDDC-001
ชื่อเอกสาร	แผนประคองกิจการ (Business Continuity Plan)
วันที่มีผลบังคับใช้	1 เม.ย. 2567
รอบการทบทวนเอกสาร	20 ส.ค. 2568 (ปีละ 1 ครั้ง)

ประวัติการปรับปรุงเอกสาร

เวอร์ชัน	ผู้จัดทำ	วันที่มีผลบังคับใช้	รายละเอียด
1	คณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	26 ส.ค. 2564	เอกสารอนุมัติใช้ครั้งแรก
2	คณะทำงานระบบบริหารการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	18 ก.ค. 2565	1.แก้ไขชื่อหน่วยงานและกลุ่มงาน 2.แก้ไขรหัสเอกสาร
3	คณะทำงานระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	1 เม.ย. 2567	1.แก้ไขภาคผนวก ก ความต้องการด้านบุคลากรต่อการปฏิบัติงาน 2.แก้ไขข้อมูลติดต่อสื่อสาร ผู้บริหาร 3. แก้ไขข้อมูลบุคลากร 4. แก้ไขแผนประคองกิจการ 5. เพื่อแผนประคองกิจการด้านสถานที่ปฏิบัติงาน 6. แก้ไขรายชื่อเจ้าหน้าที่รับผิดชอบและสิทธิ์
4	คณะทำงานระบบการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	20 ส.ค. 68	เพิ่งองค์ประกอบตามข้อเสนอแนะของกองควบคุมโรคในภาวะฉุกเฉิน เช่น เกณฑ์การใช้แผน กลยุทธการประเมินความเสี่ยง

สารบัญ

สารบัญ (ต่อ)

1. ข้อมูลเบื้องต้น

เนื่องด้วยในปัจจุบัน เหตุการณ์และปัจจัยภายนอกที่อาจส่งผลกระทบต่อการดำเนินงานของ DDC Data Center กรมควบคุมโรค มีจำนวนและความรุนแรงเพิ่มมากขึ้น ซึ่งจะมีความเสี่ยงบางประเภทที่ไม่สามารถคาดเดาได้ล่วงหน้า เช่น ภัยทางธรรมชาติ การก่อวินาศกรรม การเกิดโรคระบาด เป็นต้น หากเหตุการณ์ดังกล่าวเกิดขึ้นอาจส่งผลให้ DDC Data Center กรมควบคุมโรคไม่สามารถดำเนินงานได้อย่างต่อเนื่อง ดังนั้นแผนประคองกิจการ (Business Continuity Plan) จึงมีความสำคัญอย่างยิ่งที่จะช่วยบรรเทาความรุนแรงเมื่อเกิดเหตุการณ์ดังกล่าวขึ้น และทำให้ DDC Data Center กรมควบคุมโรค สามารถดำเนินงานต่อไปได้ในช่วงที่เกิดเหตุการณ์ความเสียหาย และสามารถกอบกู้การดำเนินการให้กลับคืนสู่สภาวะปกติได้ในระยะเวลาที่เหมาะสม

1.1 วัตถุประสงค์

เพื่อกำหนดบทบาทหน้าที่ ความรับผิดชอบ และแนวทางในการเตรียมความพร้อมและปฏิบัติในกรณีเกิดเหตุฉุกเฉินหรือภัยพิบัติ ซึ่งจะช่วยให้การให้บริการของ DDC Data Center กรมควบคุมโรค สามารถดำเนินงานได้อย่างต่อเนื่อง

1.2 ขอบเขตของแผนประคองกิจการ (Scope of BCP)

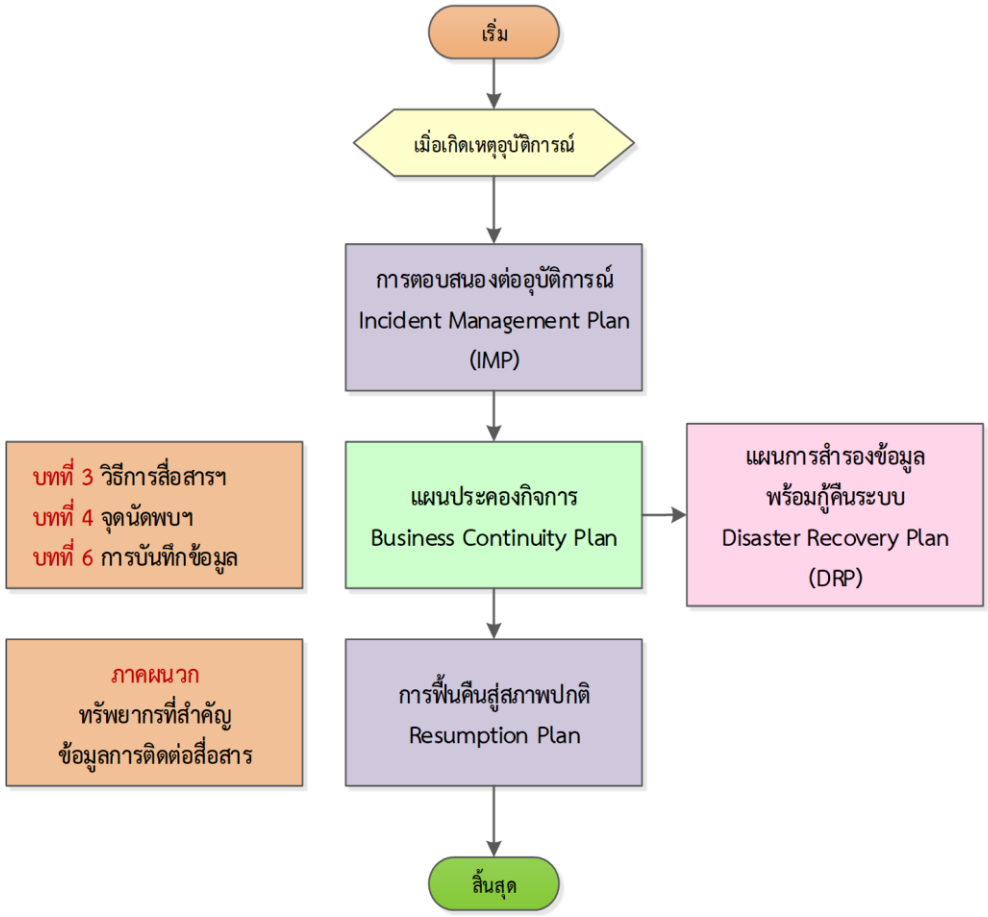
ขอบเขตของแผนประคองกิจการ Business Continuity Plan จะครอบคลุมโครงสร้างพื้นฐาน (Infrastructure) ของระบบเทคโนโลยีสารสนเทศ โดยมีรายละเอียดดังนี้

1) อุปกรณ์ภายในศูนย์คอมพิวเตอร์ทางกายภาพ
2) เครื่องคอมพิวเตอร์แม่ข่าย (Servers) อุปกรณ์เครือข่าย (Network Devices) และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

1.3 หลักเกณฑ์และวิธีการประกาศใช้แผน

กำหนดให้ รองอธิบดีกรมควบคุมโรค/ประธานคณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Committee) เป็นผู้มีอำนาจในการพิจารณาการประกาศใช้และยุติการใช้แผนประคองกิจการ (Business Continuity Plan) ฉบับนี้ โดยหลักเกณฑ์ในการพิจารณาประกาศใช้แผนอาจพิจารณาจากระดับความรุนแรงของผลกระทบ ความเสียหาย และโอกาสที่การดำเนินงานของ DDC Data Center จะเกิดการหยุดชะงักภายหลังจากการดำเนินการแก้ไขสถานการณ์เบื้องต้นตามขั้นตอนการปฏิบัติที่อยู่ในแผนการจัดการอุบัติการณ์ (Incident Management Plan: IMP) แล้วเสร็จ โดยมีการสื่อสารให้ผู้บริหารของผู้ที่ได้รับผลกระทบรับทราบ จากนั้นผู้บริหารจะแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ

1.4 โครงสร้างแผนความต่อเนื่องทางธุรกิจ



ภาพที่ 1 แผนผังแสดงโครงสร้างแผนประคองกิจการ Business Continuity Plan

1.5 สมมติฐานของแผน

บุคลากรกรมควบคุมโร ไม่สามารถเข้าถึงสำนักงานได้ และจำนวนพนักงานที่ปฏิบัติงานได้มีปริมาณไม่เพียงพอ ดังนั้นแผนการประคองกิจการจึงต้องมุ่งเน้นที่การรับรองความต่อเนื่องทางธุรกิจผ่านการทำงานจากระยะไกล โดยให้ความสำคัญกับความปลอดภัยทางไซเบอร์ ที่เพิ่มสูงขึ้นเมื่อเจ้าหน้าที่ใช้เครือข่ายภายนอกองค์กร นอกจากนี้ยังต้องมีระบบการสื่อสาร และโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศรองรับการทำงาน 24 ชั่วโมง 7 วัน เพื่อรองรับการเข้าใช้งานจากภายนอกจำนวนมาก รวมถึงการวางแผนรับมือกับ ปัญหาห่วงโซ่อุปทาน ของอุปกรณ์ที่เกี่ยวข้องด้านเทคโนโลยีสารสนเทศที่อาจหยุดชะงัก เพื่อให้ธุรกิจสามารถดำเนินต่อไปได้แม้จะอยู่ในภาวะวิกฤต ที่สอดคล้องกับมาตรการจำกัดการเดินทางและกักตัวของบุคลากร (Human Resources) ข้อจำกัดในด้านแหล่งเงินทุน (Capital) และข้อจำกัดด้านทรัพสิน (Assets)

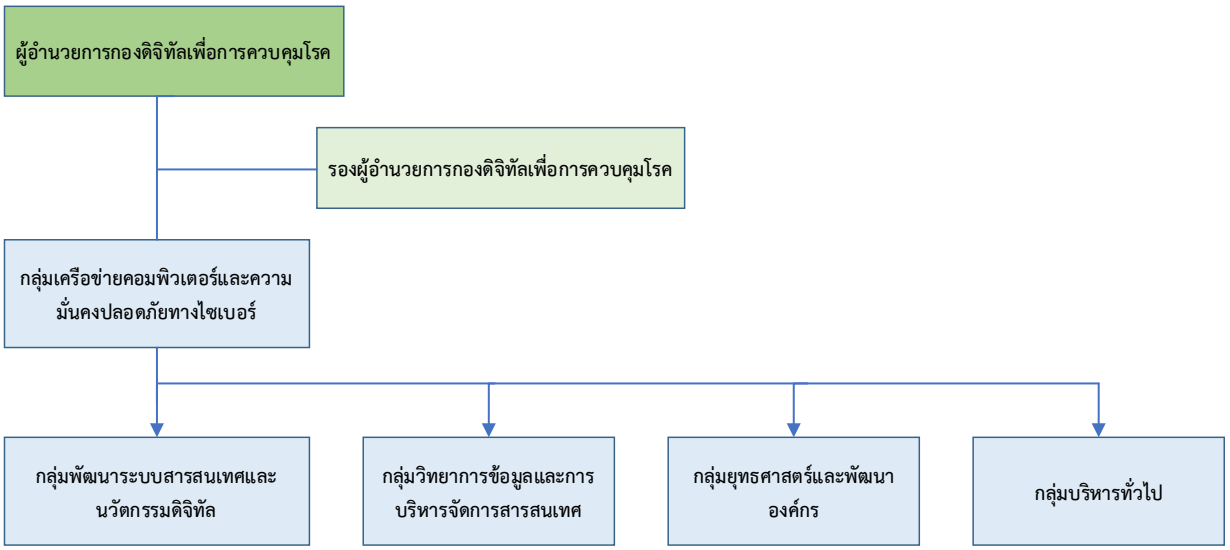
2. วิธีการสื่อสารในสถานการณ์วิกฤต

ลำดับขั้นตอนการสื่อสารในสถานการณ์ฉุกเฉินมีความสำคัญอย่างยิ่ง โดยเริ่มจากการสื่อสารภายในองค์กรอย่างรวดเร็วและเป็นระบบ เพื่อให้บุคลากรทุกคนรับทราบสถานการณ์ที่ถูกต้องและแนวทางการปฏิบัติที่ชัดเจน โดยเฉพาะทีมงานที่เกี่ยวข้องกับการกู้คืนระบบของ DDC Data Center จากนั้นจึงกำหนด โฆษก (Spokesperson)

เพียงคนเดียวในการสื่อสารกับสื่อมวลชนและบุคคลภายนอกอย่างเป็นทางการ เพื่อป้องกันความสับสนและข้อมูลที่ผิดพลาด โดยเน้นการให้ข้อมูลที่ถูกต้อง ครบถ้วน และเป็นปัจจุบันเกี่ยวกับผลกระทบของเหตุการณ์และมาตรการที่องค์กรกำลังดำเนินการเพื่อแก้ไขปัญหา ซึ่งจะช่วยสร้างความเชื่อมั่นและรักษาชื่อเสียงขององค์กรในระยะยาว

2.1 การสื่อสารกับผู้มีส่วนได้ส่วนเสีย

ในกรณีที่เกิดอุบัติการณ์หรือเหตุการณ์ที่อาจส่งผลให้การดำเนินงานของ DDC Data Center เกิดการหยุดชะงัก เป็นเหตุให้รองอธิบดีกรมควบคุมโรค ประกาศใช้แผนประคองกิจการ (Business Continuity Plan) ให้ผู้รับผิดชอบที่เกี่ยวข้องทั้งหมดติดต่อสื่อสาร เพื่อประสานงานและแลกเปลี่ยนข้อมูลระหว่างกันโดยโครงสร้างการติดต่อสื่อสาร (Call tree) เพื่อให้สามารถติดต่อสื่อสารกันได้อย่างรวดเร็วและทั่วถึง ดังนี้



กองดิจิทัลเพื่อการควบคุมโรค เบอร์โทรศัพท์ 02-590-3260
หัวหน้ากลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์ นายชัยรัตน์ ปรีชากร (086-520-6276)
รองหัวหน้ากลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์ นายอัษฎางค์ โชติมัย (089-498-5167)
*ข้อมูลการติดต่อเจ้าหน้าที่ท่านอื่น อ้างอิงตามข้อมูลติดต่อรายชื่อบุคลากรของกองดิจิทัลเพื่อการควบคุมโรค

ภาพที่ 2 ภาพโครงสร้างติดต่อสื่อสาร (Call Tree)

2.2 โครงสร้างและทีมงานแผนความต่อเนื่อง

การทำงานแบบบูรณาการในสถานการณ์วิกฤต โดยมี รองอธิบดี และ ผู้ช่วยอธิบดี เป็นผู้กำหนดนโยบายและตัดสินใจเชิงกลยุทธ์ ขณะที่ ผู้อำนวยการกองดิจิทัล และ หัวหน้ากลุ่ม ทำหน้าที่เป็นผู้รับผิดชอบหลักในการขับเคลื่อนและควบคุมการปฏิบัติงานในแต่ละด้าน เพื่อให้มั่นใจว่าการดำเนินงานที่สำคัญขององค์กรสามารถดำเนินต่อไปได้อย่างมีประสิทธิภาพและต่อเนื่อง

ลำดับ	บทบาท	ความรับผิดชอบ
1.	รองอธิบดีกรมควบคุมโรค	▪ มีอำนาจตัดสินใจอนุมัติใช้แผน
2.	ผู้ช่วยอธิบดีกรมควบคุมโรค	▪ กำกับดูแล
3.	ผู้อำนวยการ กองดิจิทัลเพื่อการควบคุมโรค	▪ ระดมทีมงานและทรัพยากรที่จำเป็น ▪ สั่งการและควบคุม ▪ พิจารณาขออนุมัติการใช้งบประมาณชั่วคราวสำหรับการแก้ไขปัญหาเฉพาะหน้า ▪ วิเคราะห์ ประเมิน เปลี่ยนแปลงระดับความสำคัญของสถานการณ์ ▪ เป็นผู้สื่อสารและปฏิสัมพันธ์กับสื่อและผู้มีส่วนได้ส่วนเสีย
4.	หัวหน้ากลุ่ม	▪ สนับสนุนและให้ข้อมูลแก่ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค ▪ ดำเนินการตามที่ได้รับมอบหมาย ▪ สั่งการและควบคุมผู้ใต้บังคับบัญชา ▪ ประสานงานกับหน่วยงานต่างๆ

2.3 ข้อจำกัดของแผน

การจัดทำแผน BCP (Business Continuity Plan) ด้านเทคโนโลยีสารสนเทศเพื่อรับมือกับภาวะโรคระบาด มีข้อจำกัดหลายประการที่ต้องนำมาพิจารณาเพื่อให้แผนมีความสมจริงและสามารถนำไปปฏิบัติได้จริง ดังนี้

2.3.1 ข้อจำกัดด้านบุคลากร

1) ความพร้อมของบุคลากร แผนการทำงานจากระยะไกล แต่บุคลากรหลักด้านเทคโนโลยีสารสนเทศ บางส่วนอาจไม่สามารถปฏิบัติงานได้เต็มที่

2) ทักษะที่จำกัด การทำงานจากระยะไกลอาจทำให้การแก้ปัญหาที่ต้องอาศัยการเข้าถึงอุปกรณ์ทางกายภาพทำได้ยากบุคลากรที่รับผิดชอบอาจขาดทักษะหรือเครื่องมือที่จำเป็นในการซ่อมบำรุงจากระยะไกล

2.3.2 ข้อจำกัดด้านเทคโนโลยีและโครงสร้างพื้นฐาน

1) ความปลอดภัยทางไซเบอร์ การที่เจ้าหน้าที่ทำงานจากระยะไกลผ่านบนเครือข่ายส่วนตัวที่ไม่ปลอดภัยทำให้ความเสี่ยงต่อการโจมตีทางไซเบอร์เพิ่มสูงขึ้น

2) อุปกรณ์ที่ไม่พร้อมใช้งาน พนักงานบางคนอาจไม่มีอุปกรณ์ที่เหมาะสมสำหรับการทำงานจากระยะไกลหรืออุปกรณ์ที่จัดหาให้มีจำนวนจำกัด ไม่เพียงพอต่อความต้องการใช้งานของทุกคน

2.3.3 ข้อจำกัดด้านการจัดการและการดำเนินงาน

1) การประสานงาน การทำงานที่อยู่คนละแห่งอาจทำให้การสื่อสาร และการประสานงานภายในทีมทำได้ยากกว่าปกติ โดยเฉพาะเมื่อต้องตัดสินใจในสถานการณ์ฉุกเฉิน

2) ห่วงโซ่อุปทาน: การขาดแคลนหรือความล่าช้าในการจัดส่งอุปกรณ์หรือชิ้นส่วนที่จำเป็นต่อการซ่อมบำรุงระบบ อาจเป็นอุปสรรคสำคัญที่ทำให้ไม่สามารถแก้ไขปัญหาได้อย่างทันท่วงที

2.4 การปฏิสัมพันธ์กับสื่อ

ในกรณีที่เกิดอุบัติการณ์หรือเหตุการณ์ที่อาจส่งผลให้การดำเนินงานของ DDC Data Center เกิดการหยุดชะงักเป็นเหตุให้รองอธิบดีกรมควบคุมโรค ประกาศใช้แผนประคองกิจการ (Business Continuity Plan) ให้คณะทำงานการบริหารความต่อเนื่องทางธุรกิจกำหนดผู้รับผิดชอบในการสื่อสารกับสื่อมวลชนและบุคคลภายนอก โดยใช้ช่องทางและตัวอย่างข้อความในการสื่อสาร ดังนี้

1. ติดประกาศที่ กรมควบคุมโรค
2. การประกาศลงเว็บไซต์ของกรมควบคุมโรค
3. การประกาศลง Facebook ของกรมควบคุมโรค

เรียน ผู้ใช้บริการ DDC Data Center ของกรมควบคุมโรค
เรื่อง ประกาศสถานการณ์ภาวะฉุกเฉิน

เนื่องจากสถานการณ์ไม่ปกติ ..... ที่เกิดขึ้น เมื่อวันที่ ..... เดือน ..... พ.ศ. ..... ส่งผลให้ DDC Data Center ของกรมควบคุมโรค ไม่สามารถให้บริการแก่ผู้ใช้บริการได้ตามปกติ อย่างไรก็ตาม กรมควบคุมโรค อยู่ระหว่างการเร่งแก้ไขสถานการณ์ที่เกิดขึ้น เพื่อให้สามารถกลับมาให้บริการแก่ผู้ใช้บริการได้ตามปกติ

จึงเรียนมาเพื่อทราบ และขออภัยในความไม่สะดวกมา ณ ที่นี้ด้วย

กรมควบคุมโรค สายด่วน : 1422 หรือโทร. 02-5903000 ตลอด 24 ชั่วโมง

ตัวอย่างข้อความในการสื่อสาร

3. จุดรวมพล

จุดนัดพบ คือบริเวณสนามหญ้าหน้าอาคาร 1 กรมควบคุมโรค

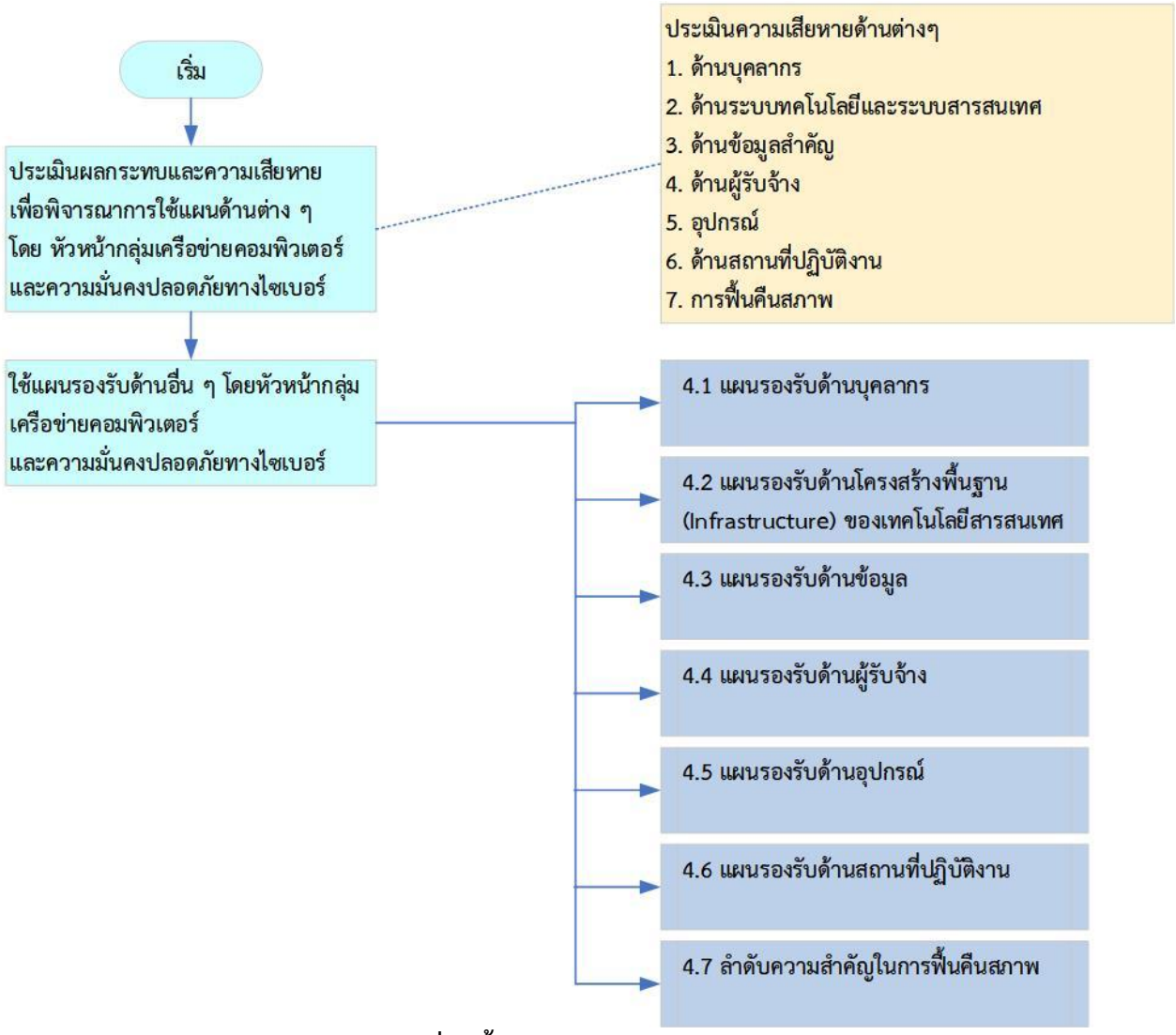
ภาพที่ 3 ภาพจุดรวมพล

ในกรณีที่เกิดเหตุการณ์ที่สร้างความเสียหายต่อสถานที่ปฏิบัติงาน จนเป็นเหตุให้ต้องอพยพออกจากอาคาร ให้บุคลากรทั้งหมดไปรวมตัวที่จุดนัดพบที่กำหนดไว้ หากจุดนัดพบดังกล่าวมีความไม่ปลอดภัยหรือไม่สามารถเข้าถึงได้ ให้กำหนดจุดนัดพบเป็นสถานที่อื่นตามแต่จะตกลงกัน

หน่วยงาน	เบอร์โทรศัพท์
ดับเพลิง นนทบุรี	0 2589 0489
การไฟฟ้า นนทบุรี	1130
สถานีตำรวจ นนทบุรี	0 2525 0900
ศูนย์นเรนทร	1669
เบอร์ฉุกเฉิน	191 หรือ 199
โรงพยาบาล	0 2590 3427

4. ขั้นตอนการปฏิบัติ และการวิเคราะห์ผลกระทบทางภารกิจ (Business Impact Analysis)

แผนประคองกิจการ (Business Continuity Plan) ฉบับนี้ ใช้วิธีการอธิบายภาพรวมและขั้นตอนการปฏิบัติ โดยการประเมินผลกระทบและความเสียหายภายในภาพรวมและตัดสินใจดำเนินการตามแผนรองรับต่าง ๆ โดยจำแนกตามผลกระทบที่เกิดขึ้นต่อทรัพยากรที่จำเป็นต้องใช้ในการดำเนินงานในแต่ละประเภท เพื่อให้กระบวนการที่สำคัญสามารถดำเนินการได้อย่างต่อเนื่อง ดังแผนภาพต่อไปนี้



ภาพที่ 4 ขั้นตอนการปฏิบัติในภาพรวม

4.1 กลยุทธ์ และมาตรการการจัดการความเสี่ยง (Business Continuity Strategy)

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ ในภาวะโรคระบาดต้องมีกลยุทธ์ที่มุ่งเน้นความต่อเนื่องของการดำเนินงานโดยให้ความสำคัญกับบุคลากรและระบบเป็นหลัก โดยสามารถแบ่งมาตรการออกได้เป็น 3 ส่วน ได้แก่ กลยุทธ์ด้านบุคลากร กลยุทธ์ด้านการดำเนินงาน และกลยุทธ์ด้านการรักษาความปลอดภัย

4.1.1 กลยุทธ์ด้านบุคลากร (Personnel Strategy)

กลยุทธ์นี้เน้นการลดความเสี่ยงจากการขาดแคลนบุคลากรและการสื่อสารที่หยุดชะงัก

1) การทำงานจากระยะไกล (Remote Work) จัดเตรียมและทดสอบระบบการทำงานจากที่บ้านอย่างเต็มรูปแบบ เพื่อให้มั่นใจว่าพนักงานทุกคนสามารถเข้าถึงระบบและข้อมูลที่จำเป็นได้จากทุกที่อย่างปลอดภัย

2) การมอบหมายงานแบบยืดหยุ่น (Flexible Staffing) จัดทำแผนมอบหมายงานสำรอง (Cross-training) ให้กับบุคลากรในทีม IT เพื่อให้สามารถปฏิบัติหน้าที่แทนกันได้ในกรณีที่เจ้าหน้าที่หลักไม่สามารถมาทำงานได้

3) ช่องทางการสื่อสาร โดยจะต้องกำหนดช่องทางการสื่อสารหลักที่เชื่อถือได้ และสามารถใช้งานได้ตลอดเวลา เช่น ระบบวิดีโอคอนเฟอเรนซ์ หรือแพลตฟอร์มการทำงานร่วมกันในองค์กร เพื่อให้การประสานงานภายในทีมเป็นไปอย่างราบรื่น

4.1.2 กลยุทธ์ด้านการดำเนินงาน (Operational Strategy)

กลยุทธ์นี้มุ่งเน้นการรักษาความพร้อมใช้งานของระบบและโครงสร้างพื้นฐาน

1) การเพิ่มความจุของระบบ (System Scalability) วางแผนและประเมินความจุของ Bandwidth สำหรับ VPN หรือขยายขนาด เพื่อรองรับปริมาณการเข้าใช้งานจากภายนอกที่เพิ่มขึ้นอย่างกะทันหัน

2) การสำรองระบบและข้อมูล (System and Data Backup) มีการสำรองข้อมูลอย่างสม่ำเสมอ และสอดคล้องกับค่า RPO (Recovery Point Objective) ที่กำหนดไว้ เพื่อลดการสูญเสียข้อมูลให้น้อยที่สุด และมีระบบสำรอง (Disaster Recovery) ที่สามารถกู้คืนได้จากระยะไกล

3) การจัดการห่วงโซ่อุปทาน (Supply Chain Management) จัดหาและสำรองอุปกรณ์ที่จำเป็น เพื่อรับมือกับปัญหาด้านการผลิตและการจัดส่งที่อาจหยุดชะงัก

4.1.3 กลยุทธ์ด้านการรักษาความปลอดภัย (Security Strategy)

กลยุทธ์นี้เน้นการป้องกันความเสี่ยงจากภัยคุกคามทางไซเบอร์ที่เพิ่มขึ้น

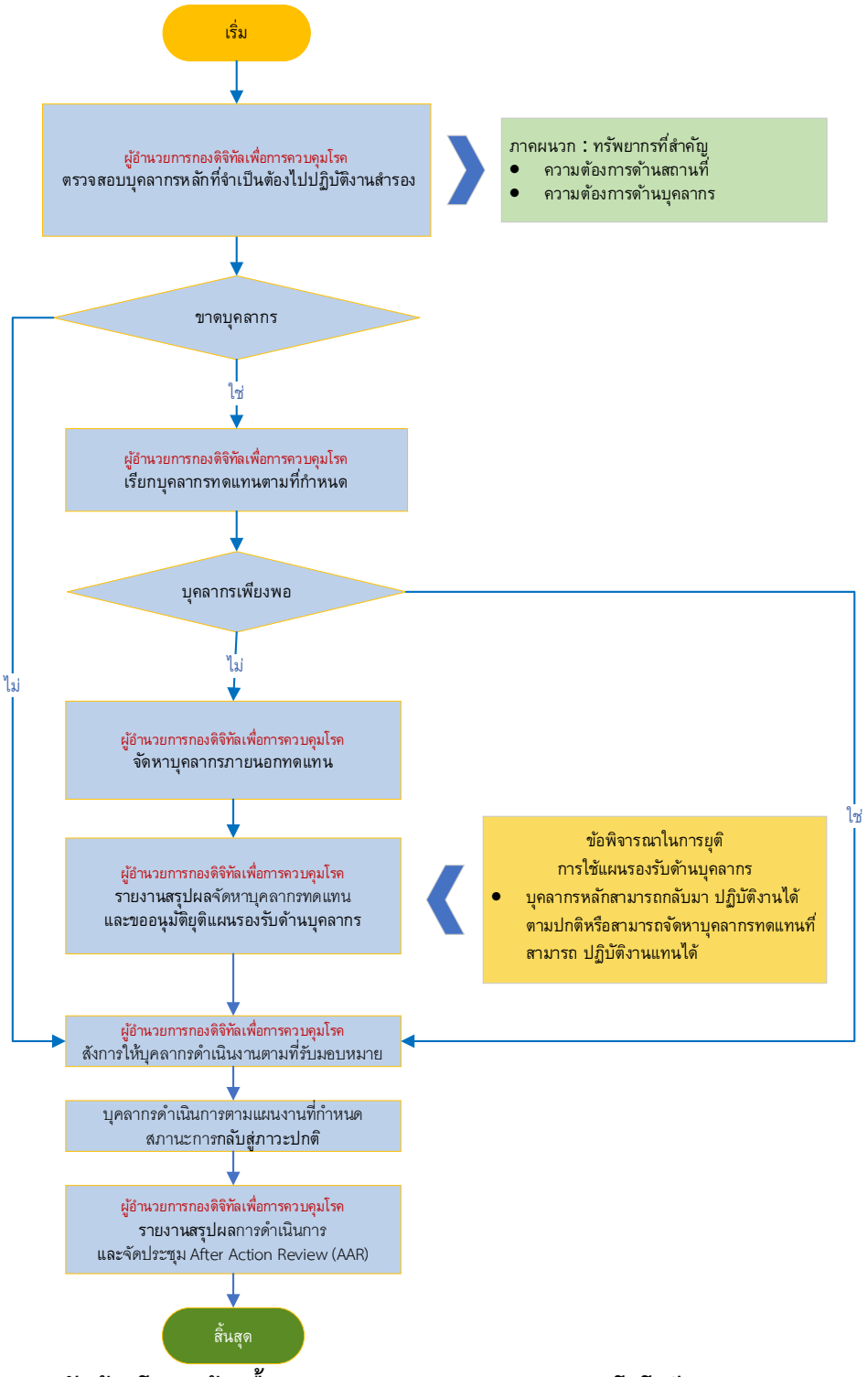
1) การตรวจสอบและควบคุมอุปกรณ์ที่เกี่ยวข้อง โดยพิจารณาติดตั้ง และอัปเดตซอฟต์แวร์รักษาความปลอดภัยบนอุปกรณ์ของพนักงานที่ทำงานจากบ้าน และกำหนดนโยบายที่ชัดเจนสำหรับการใช้อุปกรณ์ส่วนตัว

2) การฝึกอบรมและสร้างความตระหนักรู้ โดยจัดอบรมให้พนักงานทราบถึงภัยคุกคามทางไซเบอร์รูปแบบใหม่ ๆ เช่น Phishing ที่มุ่งเป้ามาที่ผู้ทำงานจากระยะไกล เพื่อลดโอกาสในการถูกโจมตี

4.2 รายละเอียดการเรียกใช้แผน และขั้นตอนการเรียกใช้แผน (Activation process)

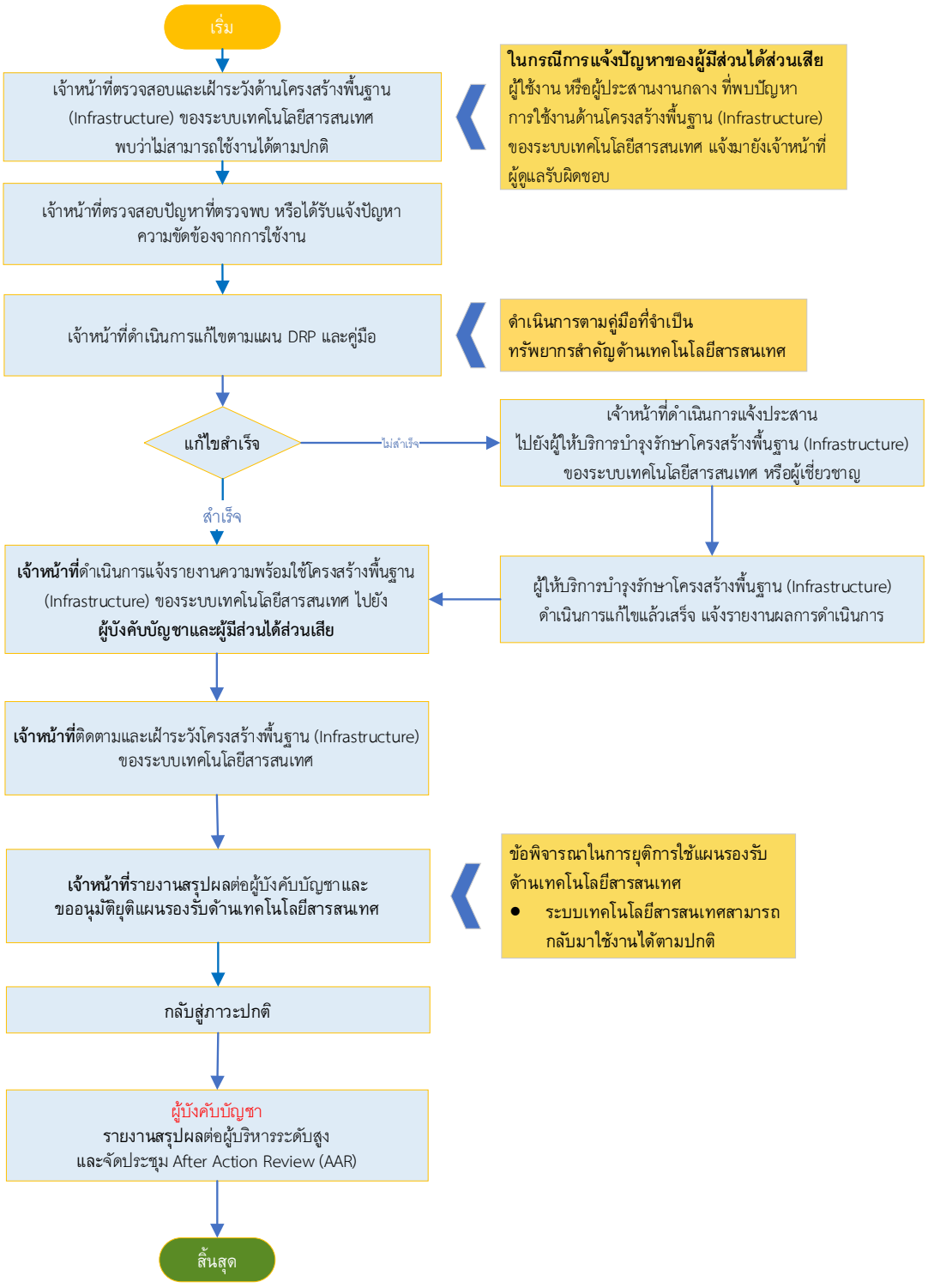
4.2.1 แผนรองรับด้านบุคลากร

หากการประเมินผลกระทบและความเสียภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อปริมาณความเพียงพอของบุคลากรในการตอบสนองต่อการดำเนินการตามแผนประคองกิจการ ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



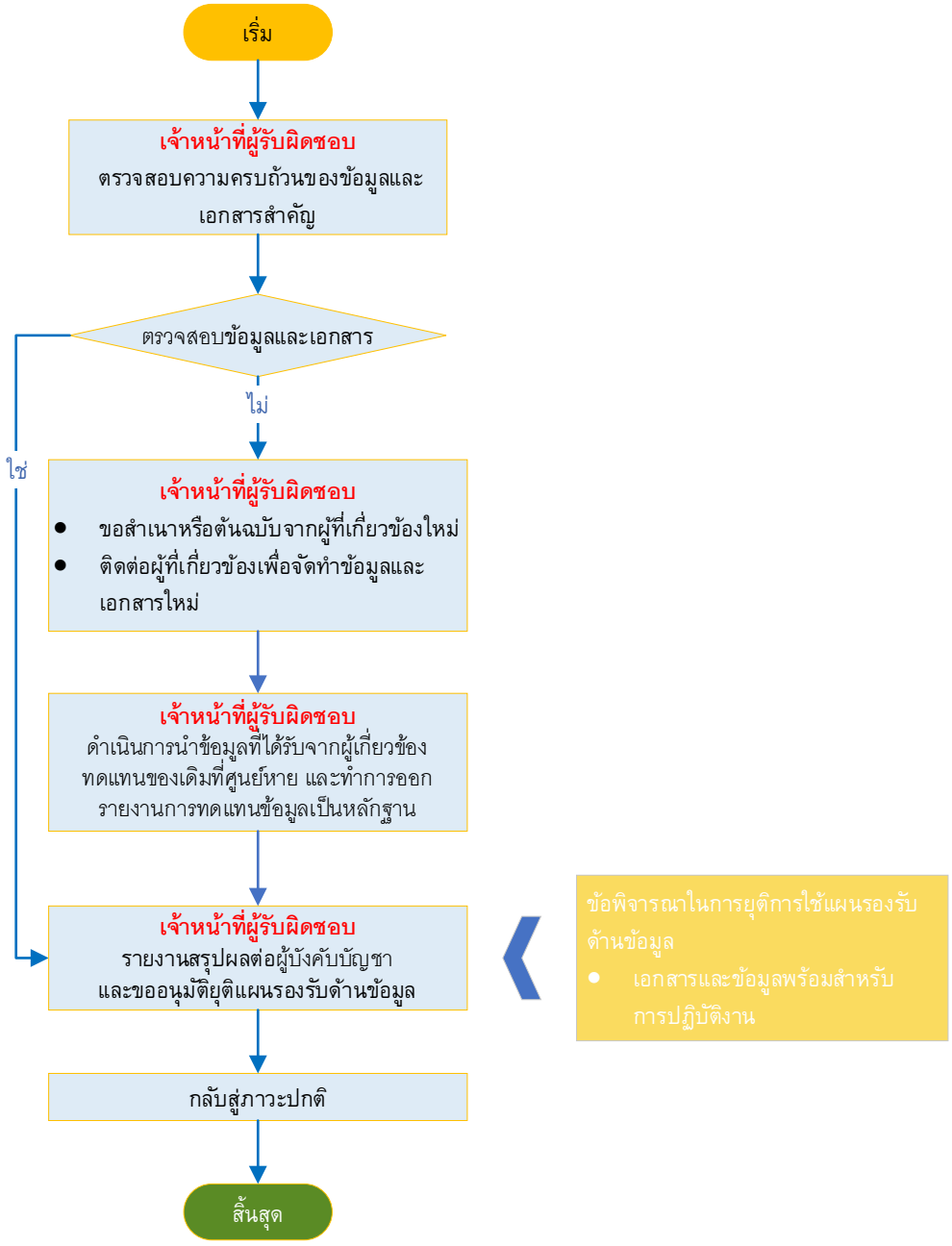
4.2.2 แผนรองรับด้านโครงสร้างพื้นฐาน (Infrastructure) ของเทคโนโลยีสารสนเทศ

หากการประเมินผลกระทบและความเสียหายภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



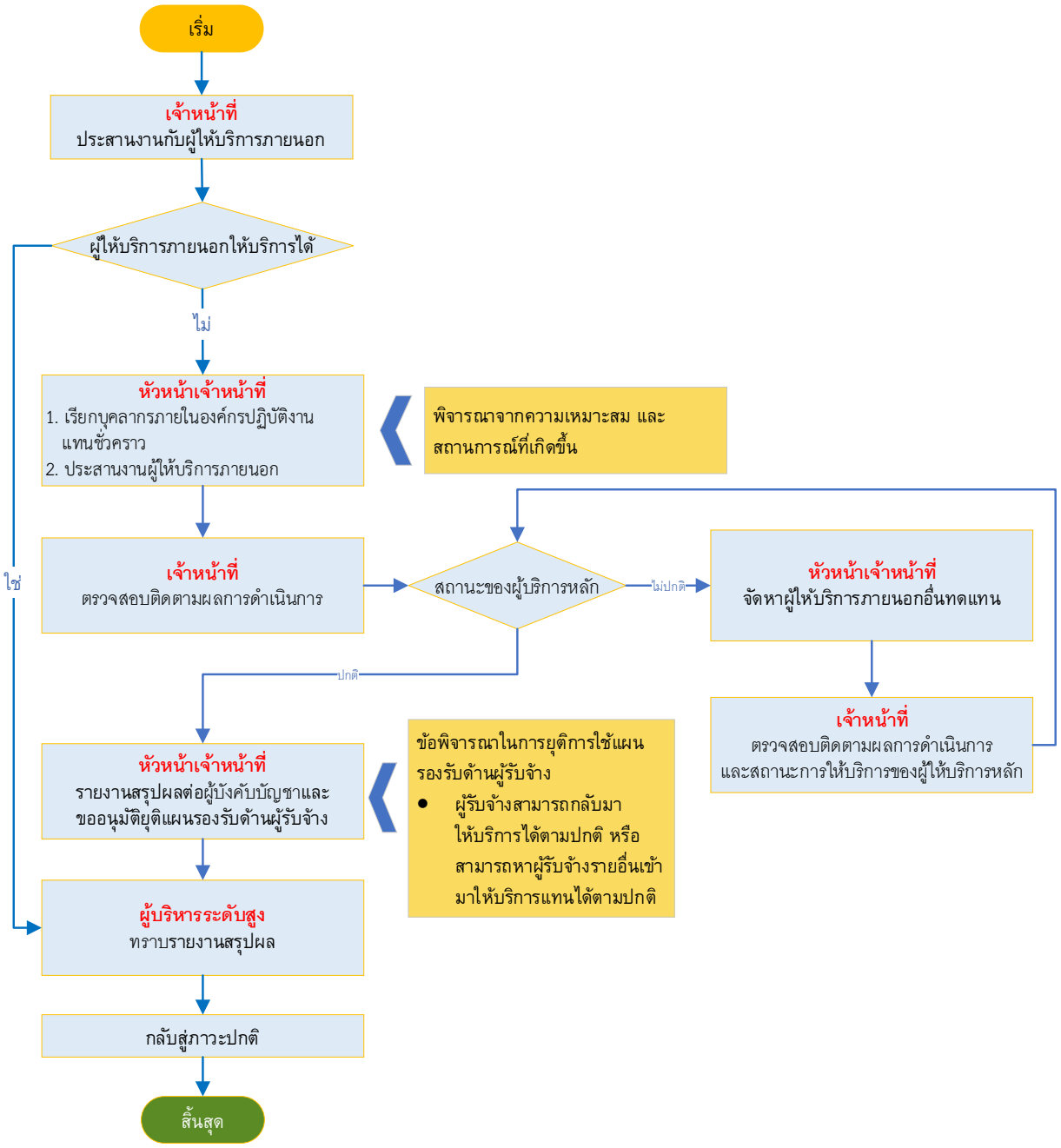
4.2.3 แผนรองรับด้านข้อมูล

หากการประเมินผลกระทบและความเสียหายภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อข้อมูล ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



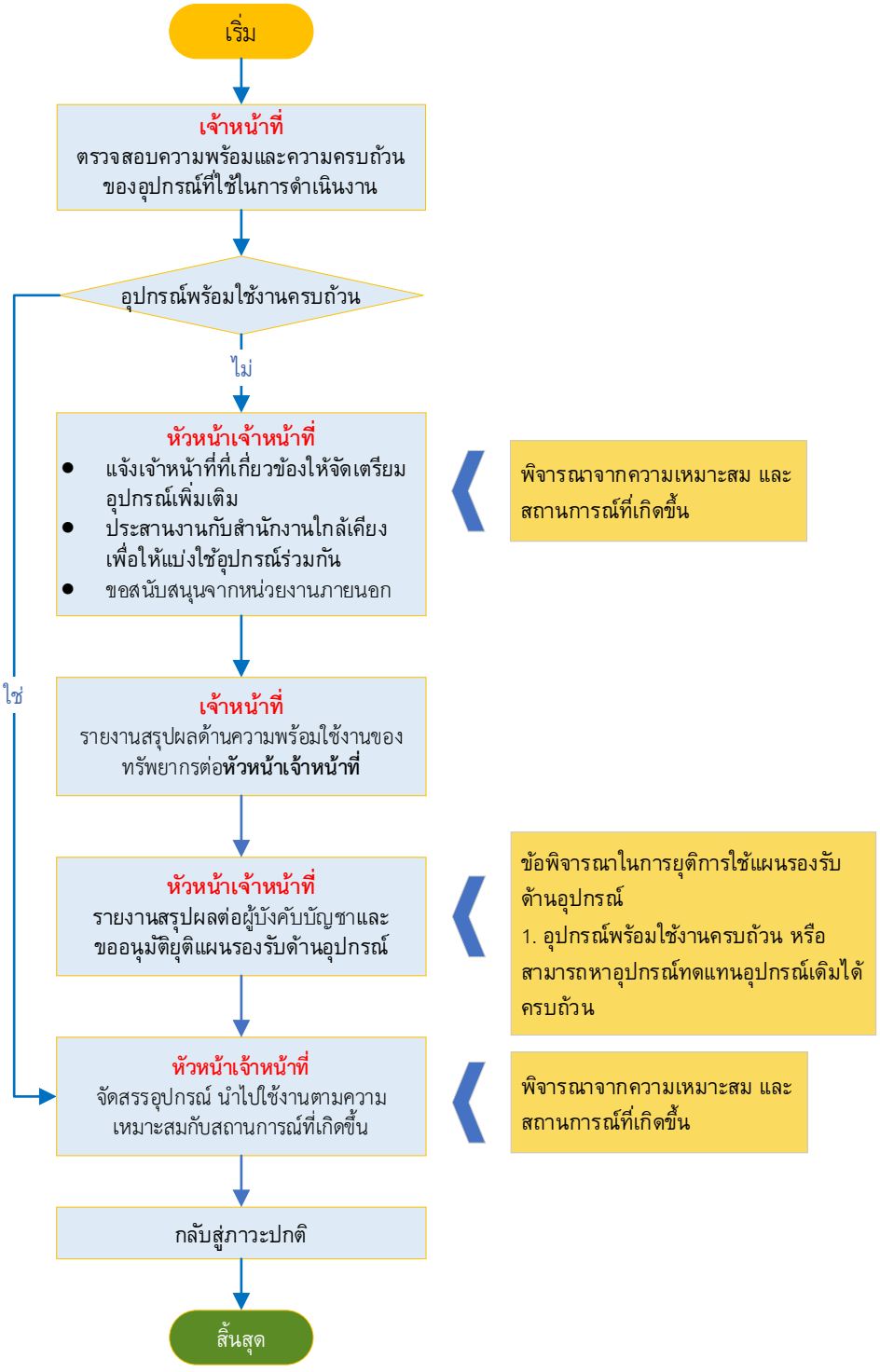
4.2.4 แผนรองรับด้านผู้รับจ้าง

หากการประเมินผลกระทบและความเสียหายภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อผู้รับจ้าง ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



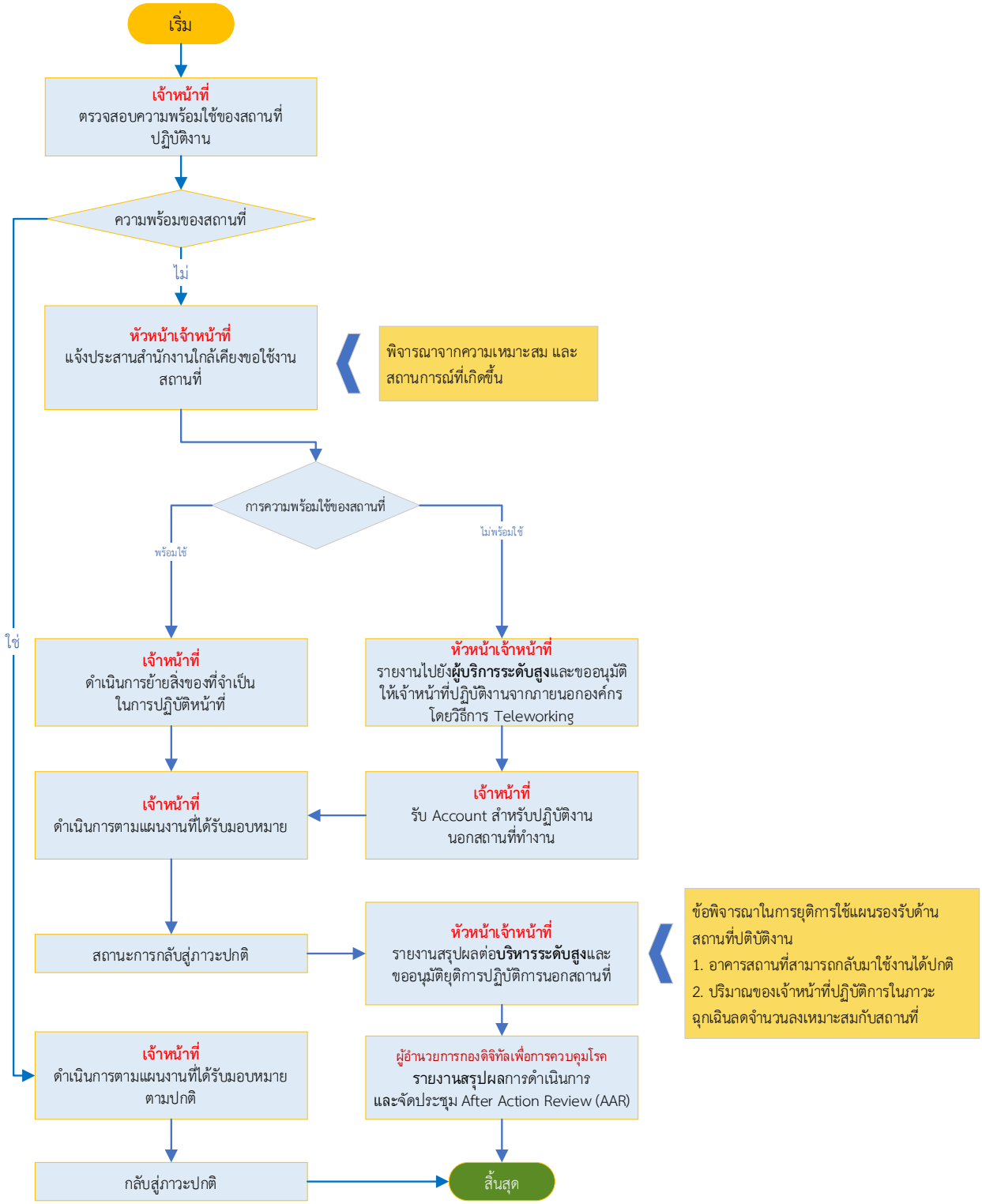
4.2.5 แผนรองรับด้านอุปกรณ์

หากการประเมินผลกระทบและความเสียหายภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่ออุปกรณ์ ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



4.2.6 แผนรองรับด้านสถานที่ปฏิบัติงาน

หากการประเมินผลกระทบและความเสียหายภายในภาพรวมพบว่า เหตุการณ์ที่เกิดขึ้นส่งผลกระทบต่อสถานที่ปฏิบัติงาน ให้ดำเนินการตามขั้นตอนปฏิบัติ ดังนี้



4.3 ลำดับความสำคัญในการฟื้นคืนสภาพ

ลำดับความสำคัญของกระบวนการหลักในการฟื้นคืนสภาพ โดยพิจารณาจากกิจกรรมหรือกระบวนการหลัก ระยะเวลา และระดับการฟื้นคืนที่จำเป็นในการดำเนินธุรกิจอย่างต่อเนื่อง โดยใช้การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis: BIA) ซึ่งหมายถึง การวิเคราะห์และวัดผลกระทบทางธุรกิจหรือความสูญเสียทางธุรกิจที่เกิดจากการหยุดชะงักของการดำเนินธุรกิจ โดยมีสามารถจัดลำดับได้ตามปัจจัยดังต่อไปนี้

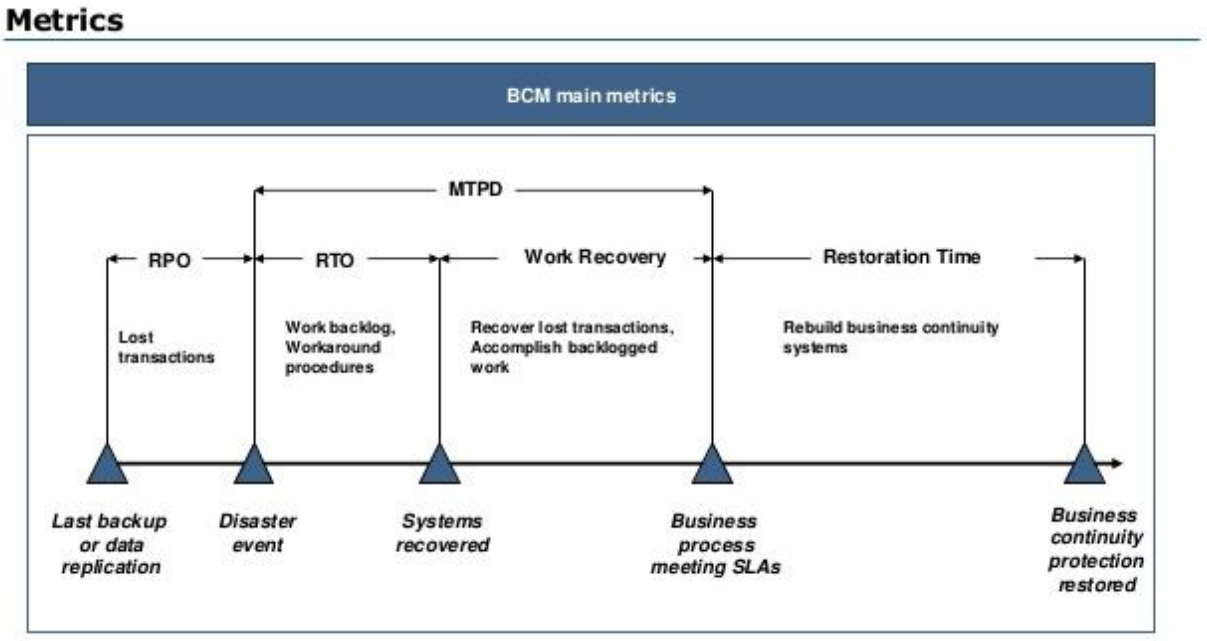
1. ระยะเวลาการหยุดชะงักที่ยอมได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) หมายถึง ระยะเวลาที่ระบบงานหยุดชะงักที่ยอมรับได้สูงสุดหากเกินกำหนดเวลานี้แล้วจะไม่สามารถทำให้ธุรกิจกลับคืนสู่สภาพปกติได้

2. ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives: RTO) หมายถึง ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้ผลิตภัณฑ์ บริการ และกิจกรรมหรือกระบวนการ กลับคืนสู่สภาพปกติหลังเกิดเหตุการณ์

3. ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) หมายถึง จุดเวลาเป้าหมายที่ข้อมูลจะได้รับการกู้กลับคืนมา เพื่อให้กิจกรรมเดินหน้าต่อไปได้ หรือ สามารถยอมรับการสูญหายของข้อมูลได้นานที่สุดเท่าไหร่

ลำดับ	กระบวนการ	RTO	MTPD	RPO	หมายเหตุ
1.	อีเมล	30 นาที	1 ชั่วโมง	-	ควบคุมผ่าน SLA กับผู้ให้บริการ
2.	อินเทอร์เน็ต	30 นาที	1 ชั่วโมง	-	มีมากกว่า อินเทอร์เน็ตลิงก์ 1 ที่ทำงาน มีระบบ Monitoring หากเกิดปัญหาผู้รับผิดชอบจะดำเนินการแก้ปัญหา และติดต่อผู้ให้บริการที่รับผิดชอบ และสามารถใช้มากกว่า 1 ช่องทางในการออกอินเทอร์เน็ต
3.	อุปกรณ์ภายในศูนย์ข้อมูล (Data Center) ทางกายภาพ ได้แก่ เครื่องสำรองไฟฟ้า, เครื่องปรับอากาศแบบควบคุมความชื้น, ระบบดับเพลิงอัตโนมัติ, ระบบแจ้งเตือนความผิดปกติในห้อง Data Center	8 ชั่วโมง	24 ชั่วโมง		มีระบบ Monitoring หากเกิดปัญหา ผู้รับผิดชอบจะดำเนินการแก้ปัญหา และติดต่อผู้ให้บริการที่รับผิดชอบ และมีอุปกรณ์ที่ทำงานทดแทนกันได้

ลำดับ	กระบวนการ	RTO	MTPD	RPO	หมายเหตุ
4.	เครื่องคอมพิวเตอร์แม่ข่าย (Servers), ระบบ Active Directory, DHCP Server, ระบบ Monitor ของ Servers อุปกรณ์เครือข่าย (Network Devices), ระบบตรวจสอบเครือข่าย และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security) ได้แก่ Firewall, IPS/IDS	8 ชั่วโมง	24 ชั่วโมง	-	มีระบบ Monitoring หากเกิดปัญหา ผู้รับผิดชอบจะดำเนินการแก้ปัญหา และติดต่อผู้ให้บริการที่รับผิดชอบ และมีอุปกรณ์ที่ทำงานทดแทนกันได้



ภาพที่ 5 BCM metrics

5. ระดับของแผนและเกณฑ์การพิจารณาและแนวทางการปฏิบัติงานตามระดับความเสี่ยง

การจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ กรมควบคุมโรค ในภาวะโรคระบาด มีการแบ่งระดับความรุนแรงและกำหนดแนวทางปฏิบัติที่ชัดเจน เพื่อให้องค์กรสามารถตอบสนองได้อย่างเหมาะสม และไม่ตื่นตระหนกจนเกินไป โดยทั่วไปแล้ว สามารถแบ่งระดับความเสี่ยงได้ 3 ระดับ พร้อมเกณฑ์และแนวทางการปฏิบัติ ดังนี้

ระดับความเสี่ยง	เกณฑ์พิจารณาและการใช้แผน	แนวทางการปฏิบัติงาน
ระดับที่ 1 ความเสี่ยงต่ำ (Risk Monitoring)	มีการแพร่ระบาดในวงจำกัด หรือมีรายงาน ผู้ติดเชื้อในพื้นที่ห่างไกลจากสำนักงาน	1. ทบทวนและปรับปรุงข้อมูลติดต่อของทีมงานของทุกคนให้เป็นปัจจุบัน 2. ตรวจสอบความพร้อมของอุปกรณ์ที่เกี่ยวข้อง 3. แจ้งให้เจ้าหน้าที่ให้ทราบถึงสถานการณ์และมาตรการเบื้องต้นขององค์กร

ระดับที่ 2 ความเสี่ยงปานกลาง (Initial Response)	มีการแพร่ระบาดในพื้นที่ใกล้เคียงสำนักงาน หรือเริ่มมีมาตรการจำกัดการเดินทาง	1. ทดสอบความสามารถในการทำงานจากระยะไกล 2. จำกัดการเดินทางที่ไม่จำเป็นของทีมงาน 3. เพิ่มการเฝ้าระวังด้านความปลอดภัยทางไซเบอร์
ระดับที่ 3 ความเสี่ยงสูง (Emergency Response)	มีการแพร่ระบาดในวงกว้าง หรือมีคำสั่งให้ล็อกดาวน์พื้นที่ และไม่สามารถเดินทางเข้ามาที่สำนักงานได้	1. สั่งการให้เจ้าหน้าที่ทำงานจาระยะไกล 2. ทีมงานต้องพร้อมปฏิบัติหน้าที่จากระยะไกล 3. มีการสื่อสารแนวทางปฏิบัติที่ปลอดภัย 4. เพิ่มการเฝ้าระวังด้านความปลอดภัยทางไซเบอร์

6. เกณฑ์การเริ่มต้นการตอบโต้ภาวะฉุกเฉิน (Criteria for BCP Activation)

การตัดสินใจที่จะเริ่มใช้แผน BCP (Business Continuity Plan) เพื่อให้มั่นใจว่าการตอบโต้จะเกิดขึ้นในเวลาที่เหมาะสมและได้ผลลัพธ์ที่มีประสิทธิภาพสูงสุด ที่ส่งผลกระทบโดยตรงต่อการดำเนินงานขององค์กร โดยสามารถแบ่งออกได้เป็น 2 กลุ่มหลัก ได้แก่ เกณฑ์ด้านบุคลากร และ เกณฑ์ด้านการดำเนินงาน

6.1 เกณฑ์ด้านบุคลากร (Personnel-based Criteria)

หัวข้อการตัดสินใจ	เกณฑ์การตัดสินใจ
การขาดแคลนบุคลากรที่สำคัญ	เมื่อมีจำนวนเจ้าหน้าที่ในส่วนงานไม่สามารถมาปฏิบัติงานได้ตามปกติเกินกว่าร้อยละ 30 ของอัตรากำลังคนในทีมเจ้าหน้าที่
ข้อจำกัดในการเดินทาง	เมื่อมีคำสั่งอย่างเป็นทางการจากหน่วยงานภาครัฐที่จำกัดการเดินทางเข้า-ออกพื้นที่ ซึ่งส่งผลกระทบต่อความสามารถในการเดินทางมาปฏิบัติงานของบุคลากรในวงกว้าง

6.2 เกณฑ์ด้านการดำเนินงาน (Operational-based Criteria)

หัวข้อการตัดสินใจ	เกณฑ์การตัดสินใจ
การเข้าถึงสถานที่ปฏิบัติงาน	สถานที่หลักไม่สามารถใช้งานได้ หรือไม่ปลอดภัยสำหรับการปฏิบัติงานตามปกติ เช่น เกิดเหตุการณ์ไฟไหม้ น้ำท่วม หรืออาคารถูกปิดเนื่องจากการปนเปื้อน
ความล้มเหลวของระบบสำคัญ	ระบบหรือโครงสร้างพื้นฐานด้านเทคโนโลยีสารสนเทศ ที่สำคัญต่อภารกิจหลักขององค์กรไม่สามารถทำงานได้ หรือมีความเสี่ยงสูงที่จะล้มเหลวในระยะเวลาอันใกล้
การขัดข้องของระบบสาธารณูปโภค	ระบบสาธารณูปโภคหลัก เช่น ไฟฟ้า ประปา หรือเครือข่ายอินเทอร์เน็ต ถูกขัดข้องเป็นเวลานานจนส่งผลกระทบต่อการปฏิบัติงาน
ภัยคุกคามทางไซเบอร์	องค์กรเผชิญกับการโจมตีทางไซเบอร์ในระดับรุนแรง เช่น Ransomware ที่ส่งผลกระทบต่อข้อมูล หรือการดำเนินงานของระบบที่สำคัญ

7. ข้อพิจารณาในการยุติการใช้แผนประคองกิจการ (Business Continuity Plan)

การยุติการใช้แผนประคองกิจการ (Business Continuity Plan) จะสามารถดำเนินการได้ ในกรณีที่เหตุฉุกเฉินหรือ ภัยพิบัติเข้าสู่ภาวะปกติ และพร้อมดำเนินงานตามขั้นตอนการย้ายระบบกลับสู่สภาวะปกติ โดยพิจารณาแผนรองรับในแต่ละด้าน ดังต่อไปนี้

แผนรองรับ	เกณฑ์การยุติการใช้แผนประคองกิจการ Business Continuity Plan
ด้านบุคลากร	บุคลากรหลักสามารถกลับมาปฏิบัติงานได้ตามปกติ หรือสามารถจัดหาบุคลากรทดแทนที่สามารถปฏิบัติงานแทนได้
ด้านเทคโนโลยีสารสนเทศ	ระบบเทคโนโลยีสารสนเทศสามารถกลับมาใช้งานได้ตามปกติ สามารถเข้าระบบงานได้ตามปกติ
ด้านผู้รับจ้าง	ผู้ให้บริการสามารถกลับมาให้บริการได้ตามปกติหรือสามารถหาผู้บริการรายอื่นเข้ามาให้บริการแทนได้ตามปกติ
ด้านอุปกรณ์	อุปกรณ์พร้อมใช้งานครบถ้วนหรือสามารถหาอุปกรณ์ทดแทนอุปกรณ์เดิมได้ครบถ้วน
สถานที่ปฏิบัติงาน	อาคารสถานที่สามารถกลับมาใช้งานได้ปกติ หรือปริมาณของเจ้าหน้าที่ปฏิบัติการในภาวะฉุกเฉินลดจำนวนลงเหมาะสมกับสถานที่ สามารถรองรับได้

8. วิธีการบันทึกข้อมูล

ในกรณีที่เกิดอุบัติการณ์หรือเหตุการณ์ที่อาจส่งผลให้การดำเนินงานของ DDC Data Center กรมควบคุมโรค เกิดการหยุดชะงัก เป็นเหตุให้กรมควบคุมโรค ประกาศใช้แผนประคองกิจการ (Business Continuity Plan) คณะกรรมการรักษาความมั่นคงปลอดภัยสารสนเทศ (Cyber Security Committee) กำหนดผู้รับผิดชอบ เช่น หัวหน้ากลุ่มฯ เป็นต้น เพื่อรับผิดชอบในการบันทึกข้อมูลสำคัญเกี่ยวกับอุบัติการณ์ การดำเนินการ และการตัดสินใจที่ดำเนินการไปแล้ว เพื่อนำไปใช้วิเคราะห์สาเหตุ แนวทางการแก้ไขและปรับปรุงในอนาคต โดยข้อมูลที่สำคัญสามารถสรุปได้ดังตารางต่อไปนี้

ลำดับ	วันที่/เวลา	เหตุการณ์/การดำเนินการ	ผู้รับผิดชอบ	ผู้อนุมัติ	หมายเหตุ

ตัวอย่างแบบฟอร์มบันทึกข้อมูล

8.1 เอกสารสำหรับบันทึก

ลำดับที่	รหัสเอกสาร	ชื่อเอกสาร
1	FRM-DDDC-021	แบบฟอร์มบันทึกข้อมูลเหตุการณ์ภัยคุกคาม

8.2 เอกสารที่เกี่ยวข้อง

ลำดับที่	รหัสเอกสาร	ชื่อเอกสาร
1	PLA-DDDC-001	แผนการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ หัวข้อ 6.3 ขั้นการระงับภัยคุกคามทางไซเบอร์ การปราบปรามภัยคุกคามทางไซเบอร์ และการฟื้นฟูระบบงานที่ได้รับผลกระทบ (containment, eradication, and recovery)

ภาคผนวก ก ทรัพยากรที่สำคัญ

รายการทรัพยากรที่สำคัญในการดำเนินงานซึ่งจำแนกออกเป็นด้านบุคลากร เทคโนโลยีสารสนเทศ ข้อมูล ผู้รับจ้าง และอุปกรณ์ สามารถสรุปได้ดังต่อไปนี้

ก.1 ความต้องการด้านบุคลากร

กำหนดตามภารกิจ กลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์	รายชื่อบุคลากรที่เกี่ยวข้อง							
	หัวหน้ากลุ่ม / นายชัยรัตน์ ปรีชากร							
	นาย อัษฎางค์ โชติมัย	นาย นันทพล พุ่มไสว	นางสาว กนิษฐ์นาถ นรภัทรพงศ์	นาย วิชิต ลักษณะวิลาศ	นางสาววรัญญา ธรรมศรีทิพย์	นาย ขวัญชัย จริยาณวัตร	จ่าสิบตรี ชัยรัฐ เอมะรุจิ	นายธนดล รุ่งแจ้ง
1. งานด้านดูแลระบบเครือข่ายของกรม (Network & Security)	**	*	*	*	*	*		
2. ความมั่นคงปลอดภัย (Security)	**	*	**	*	*	*		
3. งานดูเซิร์ฟเวอร์ (Server Monitoring)	**	*	*	*		*		
4. งานดูแลระบบเครื่องแม่ข่ายและเครื่องแม่ข่ายเสมือน (VMware Workstation)	**	*	*	*	*	*		
5. ดูแลนโยบายความมั่งคงเครือข่ายสารสนเทศ (Network Policy) บน Firewall	**	*	*	*				
6. ดูแลระบบบริหารทรัพยากรผ่านเครือข่าย (Active Directory)	*	*	**	*	*	*		
7. งานบริการ (Service)	*	*	**	*	*	*	*	
8. ระบบการสื่อสารแบบรวมศูนย์ (workD Platform)	*	*	**	*	*			
9. จดโดเมน (Domain)	**	*	*	*	*	*		
10. เครือข่ายส่วนตัวเหมือน (VPN)	**	*	*	*				
11. ตรวจสอบช่องโหว่ (VA)	*	**	*	*		*		

กำหนดตามภารกิจ กลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์	รายชื่อบุคลากรที่เกี่ยวข้อง							
	หัวหน้ากลุ่ม / นายชัยรัตน์ ปรีชากร							
	นาย อัษฎางค์ โชติมัย	นาย นันทพล พุ่มไสว	นางสาว กนิษฐ์นาถ นรภัทรพงศ์	นาย วิชิต ลักษณะวิลาศ	นางสาววรัญญา ธรรมศรีทิพย์	นาย ขวัญชัย จริยาณวัตร	จ่าสิบตรี ชัยรัฐ เอมะรุจิ	นายธนดล รุ่งแจ้ง
12. การทดสอบเจาะระบบ (Penetration Testing)	**	*	*	*		*		
13. งานสนับสนุนระบบประชุมทางไกล (Video Conference)	*	*	*	*	*	*	**	
14. ISO/IEC 27001	**	*	*	*	*	*	*	
15. ระบบสำรองข้อมูล (Backup)	*	*		**				
16. บำรุง รักษา และตรวจเช็คความพร้อมใช้งาน (Data Center Environmental Monitoring) ของระบบดังนี้ - เครื่อง Generator - เครื่องสำรองไฟ UPS - ระบบไฟฟ้าภายในห้อง Data Center - ระบบเครื่องดับเพลิงอัตโนมัติ - ระบบปรับอากาศและความชื้นภายในห้อง Data Center - ระบบรักษาความปลอดภัย กล้องวงจรปิด	*	*	*	**	*	*	*	
17. ทำโครงการภายใต้ กลุ่มเครือข่ายคอมพิวเตอร์ฯ	*	*	*	**	*	*	*	
18. ดูแลลวัสดุคอมพิวเตอร์		*	*		*		**	
19. จัดทำรายงาน 5ล้าน	*	*	*	**	*	**	*	
พัฒนาระบบ Web Service								

กำหนดตามภารกิจ กลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์	รายชื่อบุคลากรที่เกี่ยวข้อง							
	หัวหน้ากลุ่ม / นายชัยรัตน์ ปรีชากร							
	นาย อัษฎางค์ โชติมัย	นาย นันทพล พุ่มไสว	นางสาว กนิษฐ์นาถ นรภัทรพงศ์	นาย วิชิต ลักษณะวิลาศ	นางสาววรัญญา ธรรมศรีทิพย์	นาย ขวัญชัย จริยาณวัตร	จ่าสิบตรี ชัยรัฐ เอมะรุจิ	นายธนดล รุ่งแจ้ง
1. พัฒนาระบบขอใช้ VM Server	**							
2. พัฒนาระบบ AD			**					
3. พัฒนาระบบ VPN				**				
4. พัฒนาระบบจอง Conference ขั้นที่ 2		**						
5. พัฒนาระบบขออีเมลภาครัฐ					**			
6. พัฒนาระบบขอ Domain Name System						**		
7. งานพัฒนาระบบการเข้าห้อง data center	**							
8. งานพัฒนาภาพรวม User Interface ระบบ Service		**						
9. ระบบขออีเมลภาครัฐ เฟส 2 (dashboard)					**			
10. ระบบเก็บข้อมูล Data Center และ Event Case Tacking	**							
11. ระบบจัดเก็บวัสดุคอมพิวเตอร์	**							
12. ระบบขอใช้พื้นที่หน้า authentication			**					
13. ระบบแจ้งเตือนผลการ backup ใน line notification					**			
14. one page dashboard ระบบ service		**						

กำหนดตามภารกิจ กลุ่มเครือข่ายคอมพิวเตอร์และความมั่นคงปลอดภัยทางไซเบอร์	รายชื่อบุคลากรที่เกี่ยวข้อง							
	หัวหน้ากลุ่ม / นายชัยรัตน์ ปรีชากร							
	นาย อัษฎางค์ โชติมัย	นาย นันทพล พุ่มไสว	นางสาว กนิษฐ์นาถ นรภัทรพงศ์	นาย วิชิต ลักษณะวิลาศ	นางสาววรัญญา ธรรมศรีทิพย์	นาย ขวัญชัย จริยาณวัตร	จ่าสิบตรี ชัยรัฐ เอมะรุจิ	นายธนดล รุ่งแจ้ง

หมายเหตุ

** ผู้รับผิดชอบหลัก (มี 1 คนเท่านั้น)

* ผู้รับผิดชอบรอง (มีหลายคน)

ก.2 การทบทวนสิทธิ์ Admin ให้สอดคล้องกับอุปกรณ์/ระบบ

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษะนะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยถนัดตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
1	Firewall 1100E ID 1	S.Admin		Admin	Admin	Admin	Admin	Admin	Admin	Admin		Admin								
2	Firewall 1100E ID 2	S.Admin		Admin	Admin	Admin	Admin	Admin	Admin	Admin		Admin								
3	Server AD	S.Admin			Admin	Admin	Admin	Admin	Admin	Admin		Admin								
4	DHCP SERVER	S.Admin			Admin												Disable			

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
5	DNS 41.250	S.Admin			Admin															
6	DNS 41.240	S.Admin			Admin															
7	DNS 100.250	S.Admin			Admin															
8	DNS 100.240	S.Admin			Admin															

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทัพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
9	IPS	S.Admin	Viewer		Admin							Admin								
10	VMWARE	S.Admin			Admin							Admin	Backup connect	Admin			Admin			
11	Analyzer	S.Admin	Admin	Admin	Admin	Admin	Admin	Admin	Admin	Admin										
12	ITOP	S.Admin			Admin		Admin	Admin												

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logfythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
13	Ruckus WIFI DDC	S.Admin			Admin	Admin						Admin								
14	CISCO WLC	S.Admin			Admin							Admin								
15	Core SW 24	S.Admin			Admin							Admin					Admin			
16	Core SW 48	S.Admin			Admin							Admin								

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
17	L3 vlan 100 sw 1	S.Admin			Admin															
18	L3 vlan 100 sw 2	S.Admin			Admin															
19	L3 vlan 2 sw 1	S.Admin			Admin															
20	L3 vlan 2 sw 2	S.Admin			Admin															

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
21	L3 vlan VM sw 1	S.Admin			Admin															
22	L3 vlan VM sw 2	S.Admin			Admin															
23	L3 GIN SWITCH	S.Admin			Admin															
24	L2 Vlan 190 DHCP	S.Admin			Admin															

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทรัพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarwind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
25	L2 MOPH	S.Admin			Admin															
26	L2 MGMT	S.Admin			Admin															
27	L2 POE AP Commit room	S.Admin			Admin															
28	Solarwinds SERVER				Admin		S.Admin					Admin								

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะนวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarwind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
29	Solarwinds WEB			Admin	Admin	Admin	**S.Admin**	Admin	Admin	Admin		Admin				Admin					
30	Logrhythm system monitor SIEM	**S.Admin**			Admin	Admin	Admin	Admin	Admin	Admin							Admin					
31	Logrhythm Server	**S.Admin**			Admin			Admin									Admin					
32	NETEVID LOG CENTER	**S.Admin**			Admin			Admin					Admin					user / operuser /				

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยรัฐ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarvind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
33	Veeam Backup				Admin			Admin	**S.Admin**				Admin							backup vm	
34	Vutlan Monitor & Control Systems				Admin	**S.Admin**	Admin	Admin	Admin	Admin											
35	DR Site Firewall	**S.Admin**			Admin							Admin									
36	Cloud HM System	**S.Admin**		Admin	Admin			Admin				Admin									Admin

ลำดับที่	รายการอุปกรณ์/ระบบ (อ้างอิงรายการทรัพย์สินในขอบเขต)	รายการสิทธิ์																		
		Default Account ATSADANG CHOTIMAI	ผู้อำนวยการกองดิจิทัลเพื่อการควบคุมโรค	นายชัยรัตน์ ปรีชากร CHAIRAT PREECHAKORN	นายอัษฎางค์ โชติมัย ATSADANG CHOTIMAI	นายวิจิต ลักษณะวิลาศ WICHIT LUXSANAVILAS	นางสาวกนิษฐ์นาถ นรภัทรพงศ์ KANITNAT NARAPATTARAPONG	นายนันทพล พุ่มไสว NUNTAPOL POOMSAWAI	นางสาววรัญญา ธรรมศรีทิพย์ Waranya Thamsritip	นายขวัญชัย จริยาณวัตร KWANCHAI JARIYANAWAT	จ่าสิบตรี ชัยวัฒ เอมะรุจิ SM3 CHAIRATE EMARUCHI	ธนดล รุ่นแจ้ง Thanadon Runsjchaeng Technology Infrastructure	TGS Enterprise Networks	Monster Connect	Solarwind Thailand Mr.Adisorn	Logrhythm Mr.Vu	Default	network.itc@ddc.mail.go.th	ddc.sophos@outlook.com	ddcbackup	Cloud HM UIH
37	อุปกรณ์ IPS ID 1 และ 2	S.Admin			Admin			Admin				Admin								
38	อุปกรณ์ IDS	S.Admin			Admin			Admin				Admin								
39	อุปกรณ์ WAF ID 1 และ 2	S.Admin			Admin			Admin				Admin								

ก.3 ความต้องการด้านเทคโนโลยีสารสนเทศ

ลำดับ	งาน	ทำงาน Manual/offline	เอกสารที่จำเป็น
1	ระบบ Facilities	ไม่ได้	1. แบบผังแสดงการเชื่อมต่ออุปกรณ์ในระบบต่างๆ 2. คู่มือการ Configuration อุปกรณ์ต่างๆ
2	ระบบ Servers and Storage Systems	ไม่ได้	
3	ระบบ Network Systems	ไม่ได้	

ก.4 ความต้องการด้านข้อมูล

ลำดับ	ทรัพยากร	จำนวน		หมายเหตุ
		ขั้นต่ำที่ดำเนินการได้	สถานการณ์ปกติ	
ทีมงานดูแลระบบ Facilities				
1	ระบบ Facilities	N/A	N/A	
ทีมงานดูแลระบบ				
1	ระบบ Servers and Storage Systems, Network Systems	N/A	N/A	
ทีมงานดูแลระบบ Internet and IT Security				
1	ระบบ Internet and IT Security	N/A	N/A	

ก.5 ความต้องการด้านผู้รับจ้าง

ลำดับ	ผู้ให้บริการภายนอก	การเตรียมการรองรับเหตุหยุดการชะงัก
1	บริษัทผู้ให้บริการบำรุงรักษาอุปกรณ์ในระบบ Facilities, ระบบ Servers and Storage Systems, Network Systems และระบบ Security	- จัดให้พนักงานเข้าร่วมดำเนินการกับบริษัทฯในลักษณะ On The Job Training - จัดให้พนักงานเข้ารับการ configuration อุปกรณ์ในระบบต่างๆอย่างต่อเนื่องเพื่อพัฒนาทักษะของพนักงานให้เข้าใจในงานมากขึ้น

ลำดับ	ผู้ให้บริการภายนอก	การเตรียมการรองรับเหตุหยุดการชะงัก
2	บริษัทผู้ให้บริการวงจรสื่อสาร IP-VPN (วงจรสื่อสารสำรอง)	- ตรวจสอบว่าวงจรสื่อสาร IP-VPN (วงจรสื่อสารสำรอง) พร้อมใช้งานหรือไม่
3	บริษัทผู้ให้บริการ Internet (Internet Service Provider : ISP)	- ตรวจสอบว่าวงจรInternetพร้อมใช้งานหรือไม่

ก.6 ความต้องการด้านอุปกรณ์

ลำดับ	ทรัพยากร	จำนวน		หมายเหตุ
		สถานการณ์ปกติ	ขั้นต่ำที่ดำเนินการได้	
ทีมงานดูแลระบบ Facilities				
1	โทรศัพท์	2	1	
2	คอมพิวเตอร์	2	1	
ทีมงานดูแลระบบ Servers and Storage Systems, Network Systems				
1	โทรศัพท์	2	1	
2	คอมพิวเตอร์	2	1	
ทีมงานดูแลระบบ Internet and IT Security				
1	โทรศัพท์	2	1	
2	คอมพิวเตอร์	2	1	

ก.7 ข้อมูลการติดต่อสื่อสาร

รายการข้อมูลการติดต่อสื่อสารของบุคลากรที่เกี่ยวข้องสามารถสรุปได้ดังต่อไปนี้

1) ผู้บริหาร

ลำดับ	ชื่อ-สกุล	ตำแหน่ง/หน่วยงาน	หมายเลขโทรศัพท์
1	นายแพทย์ภาณุมาศ ญาณเวทย์สกุล	อธิบดีกรมควบคุมโรค	0 2590 3351
2	นายแพทย์ดิเรก ขำแป้น	รองอธิบดีกรมควบคุมโรค	0 2590 3003
3	นายแพทย์นิติ เหตานุรักษ์	รองอธิบดีกรมควบคุมโรค	0 2590 3809
4	นายแพทย์สุทัศน์ โชตนะพันธ์	รองอธิบดีกรมควบคุมโรค	0 2590 3004
5	นายแพทย์เอนก มุ่งอ้อมกลาง	รองอธิบดีกรมควบคุมโรค	0 2590 3390

2) ผู้มีส่วนได้ส่วนเสียอื่นภายใน

ลำดับ	หน่วยงาน	การสื่อสารระหว่างกัน
1	หน่วยงานสังกัดกรมควบคุมโรค	1. หนังสือราชการ 2. การประชุม 3. ทางโทรศัพท์ 4. E-mail
2	บุคลากรกรมควบคุมโรค	1. หนังสือราชการ 2. การประชุม 3. ทางโทรศัพท์ 4. E-mail 5. กระดานสนทนาที่ให้คำแนะนำ/คำปรึกษา/ตอบข้อสงสัย
3	สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.)	1. การประชุม 2. ทางโทรศัพท์

ลำดับ	หน่วยงาน	การสื่อสารระหว่างกัน
		3. หนังสือราชการ 4. E-mail

3) หน่วยงานด้านความมั่นคงปลอดภัย

ลำดับ	หน่วยงาน	หมายเลขโทรศัพท์
1	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต)	02 123 1212
2	สำนักงานปลัดกระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	02 141 6993
3	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข	02 590 2180 ต่อ 112, 316
4	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	02 142 6888

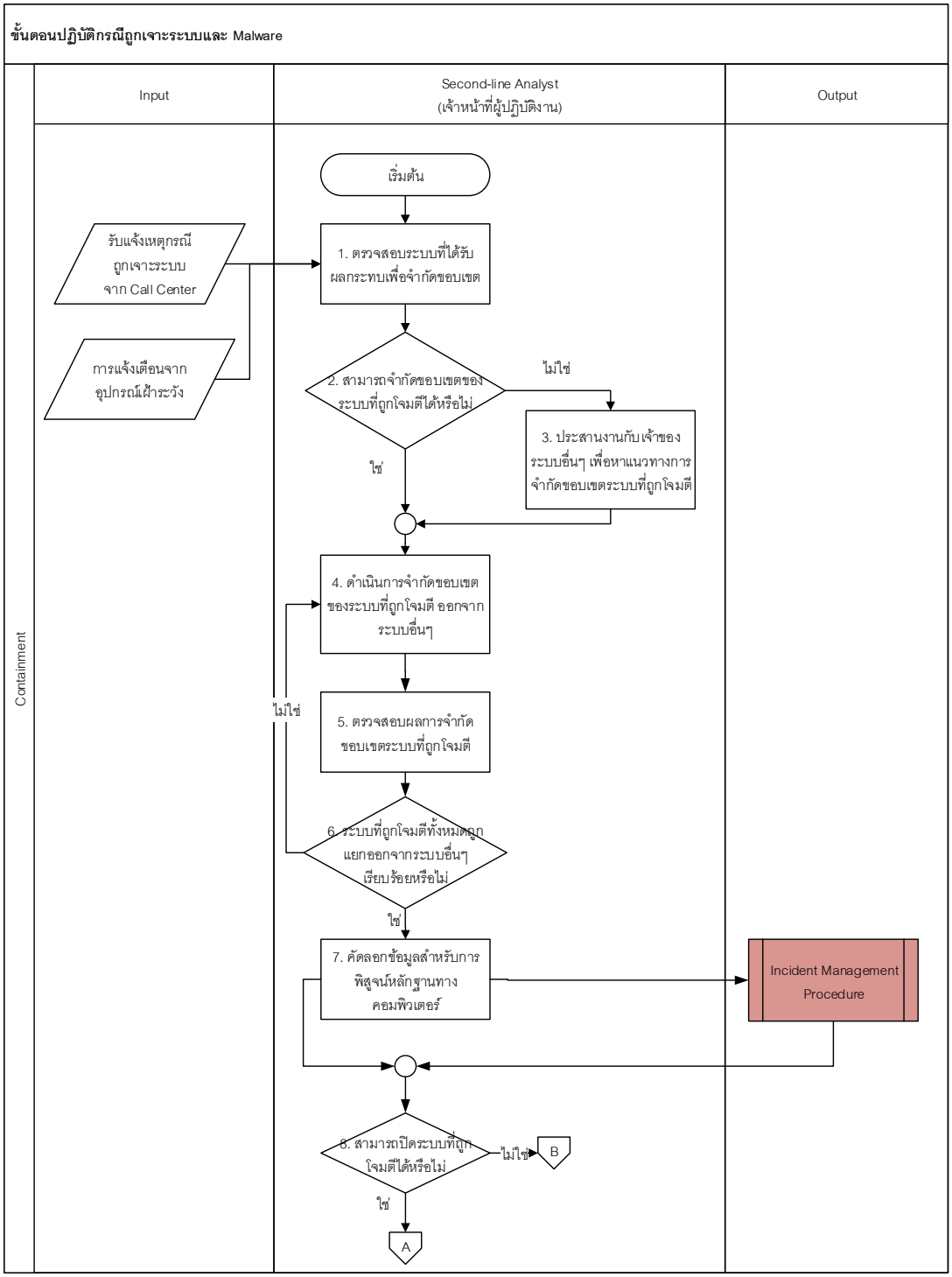
4) ผู้ให้บริการภายนอก

ลำดับ	รายชื่อผู้ให้บริการภายนอก	หมายเลขโทรศัพท์	หัวข้อการให้บริการ
1	United Information Highway Company Limited (UIH)	08 5339 5555 02 016 5000	จ้างเหมาเชื่อมโยงระบบเครือข่ายทั้งหน่วยงานส่วนกลางและส่วนภูมิภาคของกรมควบคุมโรค
2	IDEA Quest Co.Ltd	08 1713 8222	จ้างบำรุงรักษาระบบปรับอากาศแบบควบคุมอุณหภูมิ และความชื้น
3	บริษัท จัสเทล เน็ทเวิร์ค จำกัด (JasTel)	02 100 3183	การจ้างเหมาบริการสัญญาณอินเทอร์เน็ตความเร็วสูง แบบ Leased Line
4	บริษัท เทคโนโลยี อินฟราสตรัคเจอร์ จำกัด	09 8789 2551	อุปกรณ์ระบบเครือข่าย
5	บริษัท อลาร์ม ซีสเต็ม โซลูชั่น จำกัด	09 6813 3686	ระบบดับเพลิง

ลำดับ	รายชื่อผู้ให้บริการภายนอก	หมายเลขโทรศัพท์	หัวข้อการให้บริการ
6	บริษัท พิลเล่อร์ (ประเทศไทย) จำกัด	08 1830 1024	เครื่องกำเนิดไฟฟ้า GENARATOR
7	บริษัท ซีเอสพีเอ็ม (ประเทศไทย) จำกัด	0 2503 9596	จ้างบำรุงรักษาเครื่องสำรองไฟฟ้า UPS
8	บริษัท ซีนิธคอมพ์ จำกัด	02 273 0995	โปรแกรมป้องกันไวรัส
9	บริษัท ไอเน็กซ์ บรอดแบนด์ จำกัด	06 5929 8059	บริการพื้นที่ติดตั้งเครื่องแม่ข่าย (Co-Location)
10	บริษัท บีบี คอนเน็ค จำกัด	02 953 1111	บริการ Cloud Computing

ภาคผนวก ข ขั้นตอนการตอบสนองต่อภัยทางไซเบอร์

ข.1 ขั้นตอนปฏิบัติสำหรับกรณีถูกเจาะระบบและ Malware

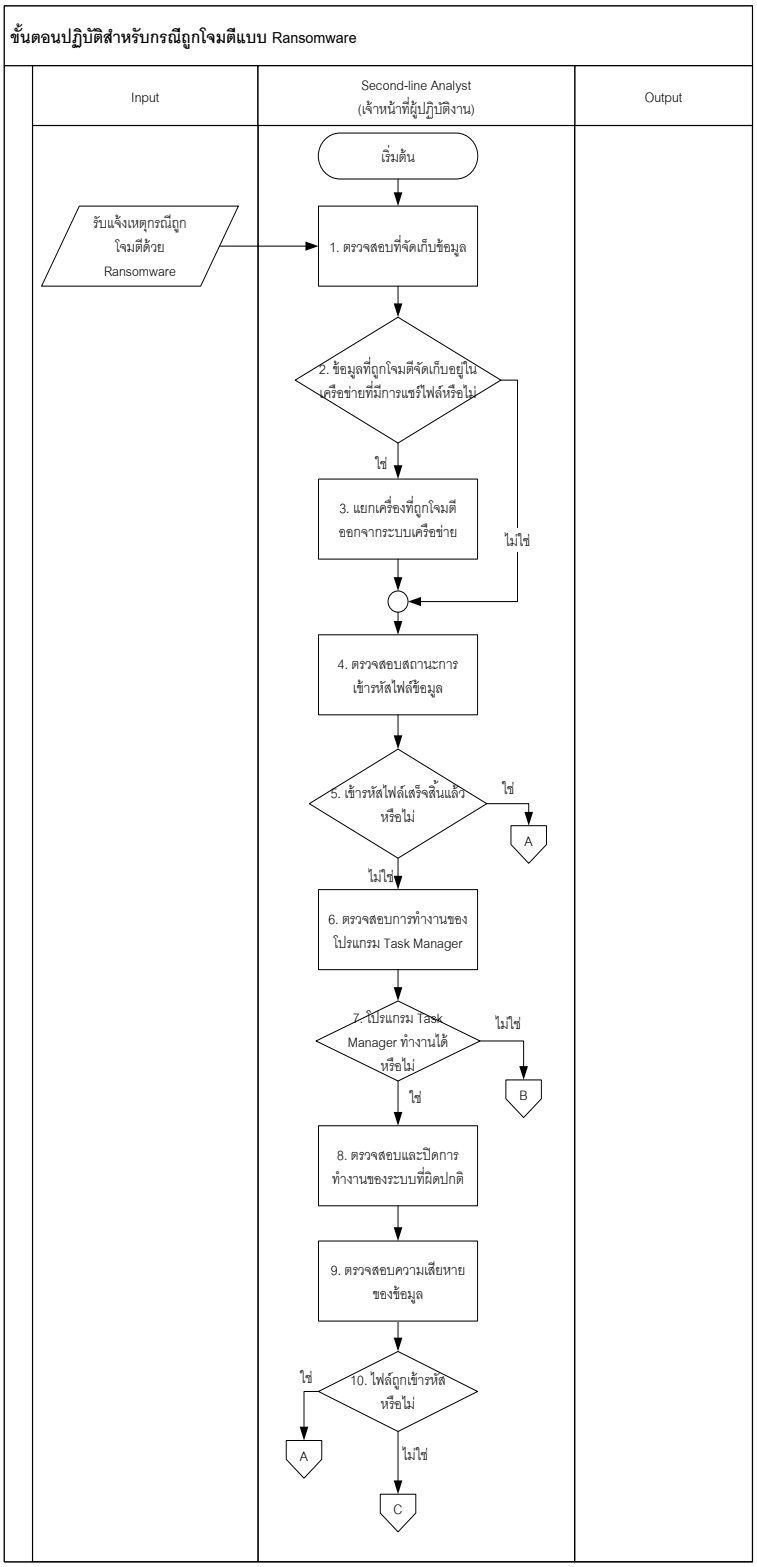


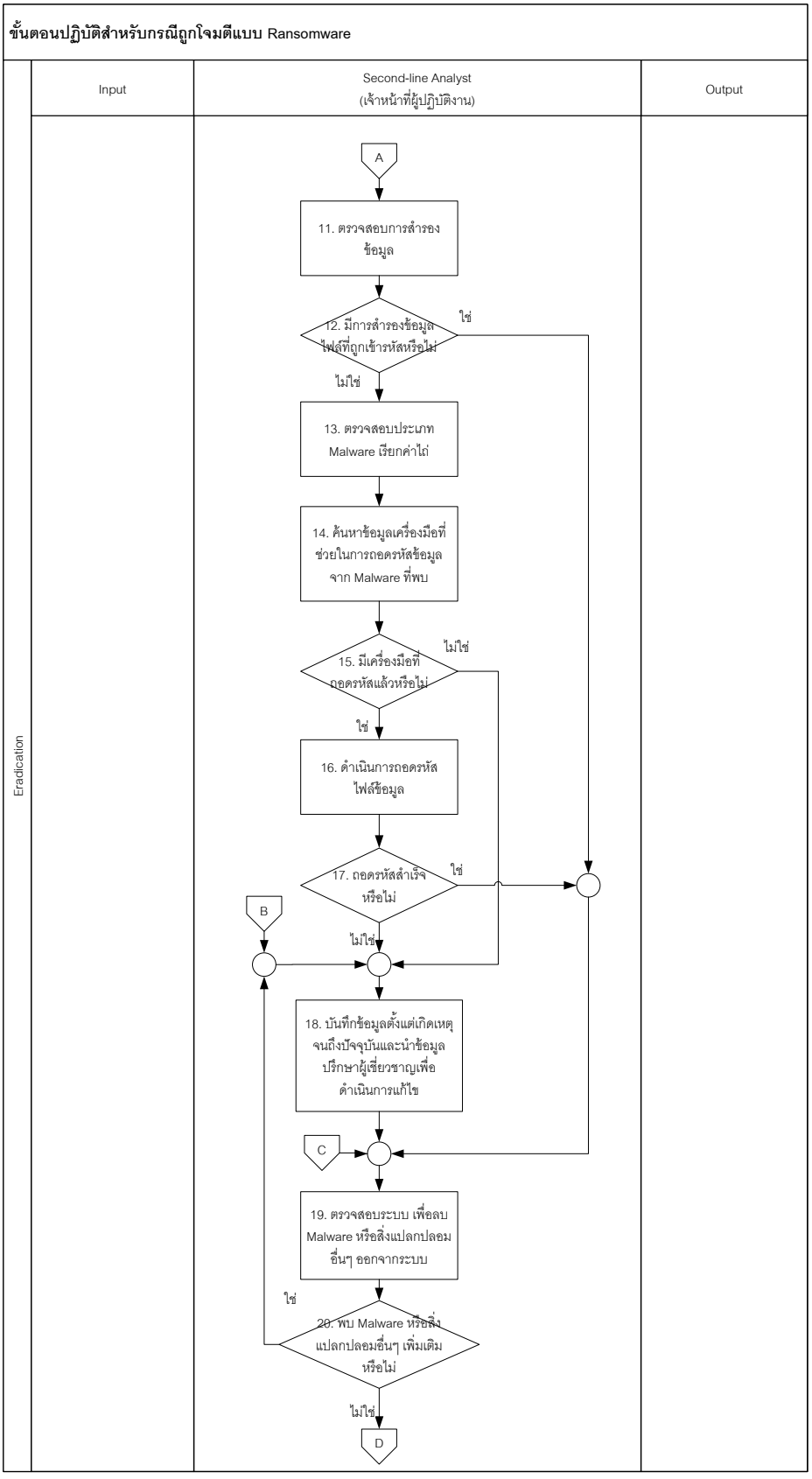
รายละเอียดขั้นตอนปฏิบัติสำหรับกรณีถูกเจาะระบบและ Malware

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ตรวจสอบระบบที่ได้รับผลกระทบเพื่อจำกัดขอบเขต	Second-line Analyst รับทราบการแจ้งเหตุกรณีถูกเจาะระบบหรือกรณีถูกโจมตีด้วย Malware และตรวจสอบระบบที่ได้รับผลกระทบ เพื่อจำกัดขอบเขต ผลกระทบที่เกิดขึ้น และตรวจสอบระบบงานที่เกี่ยวข้อง เพื่อพิจารณาวิธีการแบ่งแยกระบบที่ถูกโจมตีออกจากระบบอื่น ๆ
2	สามารถจำกัดขอบเขตของระบบที่ถูกโจมตีได้หรือไม่	■ กรณีที่สามารถแบ่งแยกระบบงานที่ถูกโจมตีออกจากระบบอื่นได้โดยไม่ส่งผลกระทบต่อการดำเนินงานของระบบอื่น ให้ดำเนินการตามขั้นตอนที่ 4 ■ กรณีที่ไม่สามารถแบ่งแยกระบบงานที่ถูกโจมตีออกจากระบบอื่นได้ ให้ดำเนินการตามขั้นตอนที่ 3
3	ประสานงานกับเจ้าของระบบอื่น ๆ เพื่อหาแนวทางการจำกัดขอบเขตระบบที่ถูกโจมตี	Second-line Analyst ประสานงานกับเจ้าของระบบงานอื่น ๆ ที่เกี่ยวข้อง หรือเชื่อมต่อกับระบบที่ถูกโจมตี เพื่อหารือถึงแนวทางการลดผลกระทบ และความเสียหายที่อาจจะเกิดขึ้นกับระบบ และดำเนินการตามขั้นตอนที่ 4
4	ดำเนินการจำกัดขอบเขตของระบบที่ถูกโจมตี ออกจากระบบอื่น ๆ	Second-line Analyst แบ่งแยกระบบที่ถูกโจมตีออกจากระบบอื่น ๆ เช่น การแยกระบบเครือข่าย (Network Segment) เป็นต้น
5	ตรวจสอบผลการจำกัดขอบเขตระบบที่ถูกโจมตี	Second-line Analyst ตรวจสอบการจำกัดขอบเขตระบบที่ถูกโจมตี และระบบที่ได้ผลกระทบจากการโจมตีทั้งหมดออกจากระบบงานอื่น ๆ
6	ระบบที่ถูกโจมตีทั้งหมดถูกแยกออกจากระบบอื่น ๆ เรียบร้อยหรือไม่	■ กรณีที่สามารถแยกระบบที่ถูกโจมตีทั้งหมด ออกจากระบบอื่นได้ครบถ้วน ให้ดำเนินการตามขั้นตอนที่ 7 ■ กรณีที่ไม่สามารถแยกระบบที่ถูกโจมตีทั้งหมด ออกจากระบบอื่นได้ครบถ้วน ให้ดำเนินการตามขั้นตอนที่ 4
7	คัดลอกข้อมูลสำหรับการพิสูจน์หลักฐานทางคอมพิวเตอร์	Second-line Analyst ดำเนินการสำเนาข้อมูลเพื่อให้พิสูจน์หลักฐานทางคอมพิวเตอร์ (Forensic) จากระบบที่ถูกโจมตี และตรวจสอบการบันทึกข้อมูลเกี่ยวกับการตอบสนองต่อการโจมตีเบื้องต้นทั้งหมด เพื่อให้แน่ใจว่ามีการบันทึกข้อมูลอย่างถูกต้องครบถ้วนและเป็นปัจจุบัน ทั้งนี้หลักฐานข้อมูลที่เกี่ยวข้องต่าง ๆ ต้องถูกจัดเก็บไว้อย่างปลอดภัย อ้างอิง ขั้นตอนการเก็บรวบรวมหลักฐาน (Collection of evidence) และพิจารณาว่าสามารถปิดระบบที่ถูกโจมตีได้หรือไม่

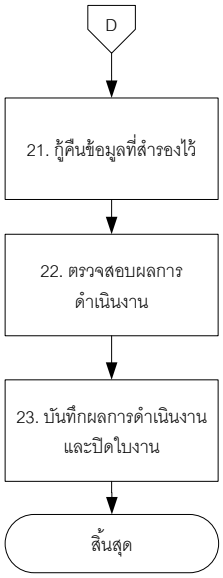
ลำดับที่	ขั้นตอน	คำอธิบาย
8	สามารถปิดระบบที่ถูกโจมตีได้หรือไม่	■ กรณีที่สามารถปิดระบบได้ ให้ดำเนินการตามขั้นตอนที่ 10 ■ กรณีที่ไม่สามารถปิดระบบได้ ให้ดำเนินการตามขั้นตอนที่ 9
9	ตรวจสอบระบบเพื่อทำการ Reimage และ Hardening ระบบ	Second-line Analyst ตรวจสอบระบบที่ถูกโจมตีว่าสามารถ Reimage และ Hardening ได้หรือไม่
10	สามารถ Reimage และ Hardening ได้หรือไม่	■ กรณีที่ระบบสามารถ Reimage และ Hardening ได้ ให้ดำเนินการตามขั้นตอนที่ 12 ■ กรณีที่ระบบไม่สามารถ Reimage และ Hardening ได้ ให้ดำเนินการตามขั้นตอนที่ 11
11	ขอคำปรึกษาจากผู้เชี่ยวชาญเพื่อดำเนินการแก้ไข	Second-line Analyst รวบรวมข้อมูลรายละเอียดเหตุการณ์ที่พบ เพื่อขอข้อมูลเพิ่มเติมจากผู้เชี่ยวชาญ เพื่อดำเนินการแก้ไขต่อไป และเมื่อแก้ไขได้แล้วเสร็จให้ดำเนินการตามขั้นตอนที่ 16
12	ดำเนินการ Reimage และ Hardening ระบบ	Second-line Analyst ดำเนินการ Reimage และ Hardening ระบบ เช่น การอัพเดท patches การตรวจสอบและปิด port ที่ไม่ใช้งาน เป็นต้น เพื่อเป็นการป้องกันระบบ และลดความเสี่ยงจากการถูกโจมตี
13	ตรวจสอบผลการ Reimage และ Hardening	Second-line Analyst สอบทานผลการ Reimage และ Hardening ระบบ เพื่อให้แน่ใจว่าไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ คงเหลืออยู่
14	พบ Malware หรือสิ่งแปลกปลอมอื่นๆ หรือไม่	■ กรณีที่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ให้บันทึก Malware และสิ่งที่ตรวจพบ และดำเนินการตามขั้นตอนที่ 12 ■ กรณีที่ไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ให้ดำเนินการตามขั้นตอนที่ 15
15	ดำเนินการกู้คืนระบบ	Second-line Analyst ดำเนินการกู้คืนระบบ (restore) กลับสู่การดำเนินงานปกติ ตรวจสอบผลการดำเนินงาน และบันทึกผล
16	กำหนดระยะเวลาในการเฝ้าระวังระบบ	Second-line Analyst กำหนดระยะเวลาในการเฝ้าระวังระบบ เพื่อให้แน่ใจว่า ระบบสามารถทำงานได้ตามปกติ ไม่ถูกโจมตีซ้ำด้วยวิธีเดิม
17	สรุปผลการดำเนินงาน	Second-line Analyst สรุปผลการดำเนินงาน รายงานต่อผู้ที่เกี่ยวข้อง และดำเนินการบันทึกปิดใบงาน

ข.2 ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Ransomware





ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Ransomeware

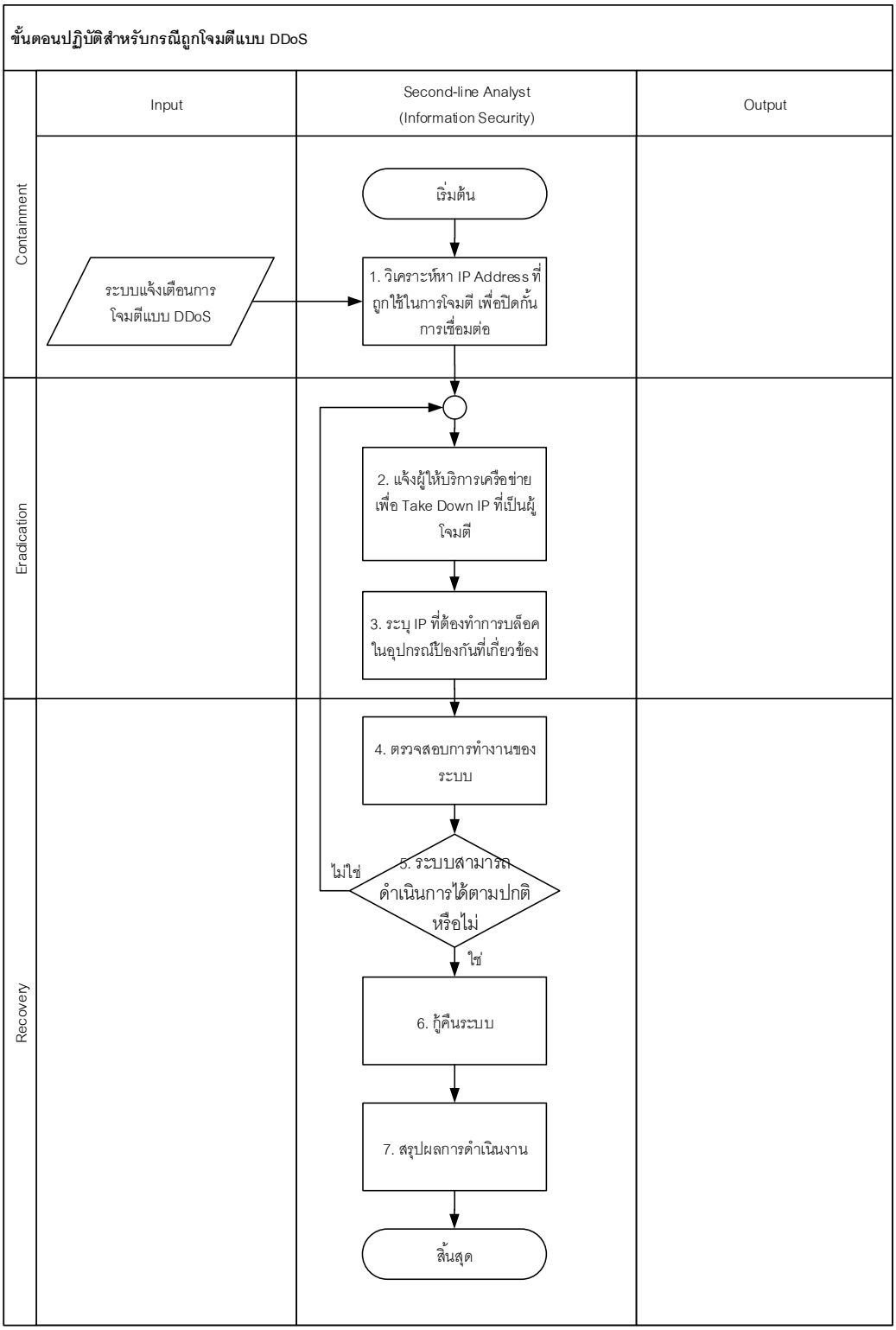
	Input	Second-line Analyst (เจ้าหน้าที่ผู้ปฏิบัติงาน)	Output
Recovery			

รายละเอียดขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Ransomware

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ตรวจสอบที่จัดเก็บข้อมูล	Second-line Analyst ตรวจสอบที่จัดเก็บข้อมูล โดยพิจารณาว่าข้อมูลที่ถูกโจมตีจัดเก็บอยู่ในระบบเครือข่ายที่มีการแชร์ไฟล์หรือไม่
2	ข้อมูลที่ถูกโจมตีจัดเก็บอยู่ในเครือข่ายที่มีการแชร์ไฟล์หรือไม่	■ กรณีที่ข้อมูลที่ถูกโจมตีจัดเก็บอยู่ในระบบเครือข่าย ให้ดำเนินการตามขั้นตอนที่ 3 ■ กรณีที่ข้อมูลที่ถูกโจมตีไม่จัดเก็บอยู่ในระบบเครือข่าย ให้ดำเนินการตามขั้นตอนที่ 4
3	แยกเครื่องที่ถูกโจมตีออกจากระบบเครือข่าย	Second-line Analyst แยกเครื่องที่ถูกโจมตีออกจากระบบเครือข่ายทั้งหมด เพื่อจำกัดขอบเขตของระบบที่ถูกโจมตี และกำจัดขอบเขตของระบบที่ได้รับผลกระทบ
4	ตรวจสอบสถานะการเข้ารหัสไฟล์ข้อมูล	Second-line Analyst ตรวจสอบสถานการณ์เข้ารหัสไฟล์ข้อมูล เพื่อตรวจสอบว่าข้อมูลถูกเข้ารหัสจนเสร็จสิ้นแล้วหรือไม่
5	เข้ารหัสไฟล์เสร็จสิ้นแล้วหรือไม่	■ กรณีที่ไฟล์ถูกเข้ารหัสจนเสร็จสิ้นแล้ว ให้ดำเนินการตามขั้นตอนที่ 11 ■ กรณีที่ไฟล์ยังเข้ารหัสไม่แล้วเสร็จ ให้ดำเนินการตามขั้นตอนที่ 6
6	ตรวจสอบการทำงานของโปรแกรม Task Manager	Second-line Analyst ตรวจสอบการทำงานของโปรแกรม Task Manager เพื่อพิจารณาว่ายังสามารถทำงานได้อยู่หรือไม่
7	โปรแกรม Task Manager ทำงานได้หรือไม่	■ กรณีที่โปรแกรม Task Manager ยังสามารถทำงานได้ ให้ดำเนินการตามขั้นตอนที่ 8 ■ กรณีที่โปรแกรม Task Manager ไม่สามารถทำงานได้ ให้ดำเนินการตามขั้นตอนที่ 18
8	ตรวจสอบและปิดการทำงานของระบบที่ผิดปกติ	Second-line Analyst ตรวจสอบและปิดการทำงานของระบบหรือ Process ที่ผิดปกกติ
9	ตรวจสอบความเสียหายของข้อมูล	Second-line Analyst ตรวจสอบความเสียหายของข้อมูลเพื่อพิจารณาว่ามีไฟล์ที่ถูกเข้ารหัสหรือไม่
10	ไฟล์ถูกเข้ารหัสหรือไม่	■ กรณีพบไฟล์ที่ถูกเข้ารหัส ให้ดำเนินการตามขั้นตอนที่ 11 ■ กรณีไม่พบไฟล์ที่ถูกเข้ารหัส ให้ดำเนินการตามขั้นตอนที่ 19
11	ตรวจสอบการสำรองข้อมูล	Second-line Analyst ตรวจสอบว่าข้อมูลที่ถูกเข้ารหัสมีการสำรองข้อมูลไว้หรือไม่
12	มีการสำรองข้อมูลไฟล์ที่ถูกเข้ารหัสหรือไม่	■ กรณีที่มีการสำรองข้อมูลไว้ ให้ดำเนินการตามขั้นตอนที่ 19 ■ กรณีที่ไม่มีการสำรองข้อมูลไว้ ให้ดำเนินการตามขั้นตอนที่ 13
13	ตรวจสอบประเภท Malware เรียกค่าไถ่	Second-line Analyst ตรวจสอบประเภท Malware ที่ใช้ในการเข้ารหัสข้อมูลเพื่อเรียกค่าไถ่ เพื่อใช้เป็นข้อมูลในการค้นหาเครื่องมือในการถอดรหัส

ลำดับที่	ขั้นตอน	คำอธิบาย
14	ค้นหาข้อมูลเครื่องมือที่ช่วยในการถอดรหัสข้อมูลจาก Malware ที่พบ	Second-line Analyst ค้นหาข้อมูลเครื่องมือ ที่ใช้ในการถอดรหัสข้อมูล อ้างอิงประเภท Malware ที่ใช้ในการเข้ารหัสข้อมูล เทียบกับข้อมูลจากการแลกเปลี่ยนข้อมูลและอุปกรณ์ในการถอนรหัสจากสถาบันที่มีความน่าเชื่อถือ
15	มีเครื่องมือที่ถอดรหัสแล้วหรือไม่	■ กรณีที่มีเครื่องมือที่ถอดรหัสได้ ให้ดำเนินการตามขั้นตอนที่ 16 ■ กรณีที่ไม่มีเครื่องมือที่ถอดรหัสได้ ให้ดำเนินการตามขั้นตอนที่ 18
16	ดำเนินการถอดรหัสไฟล์ข้อมูล	Second-line Analyst ดำเนินการถอดรหัสข้อมูล
17	ถอดรหัสสำเร็จหรือไม่	■ กรณีที่ถอดรหัสสำเร็จ ให้ดำเนินการตามขั้นตอนที่ 19 ■ กรณีที่ถอดรหัสไม่สำเร็จ ให้ดำเนินการตามขั้นตอนที่ 18
18	บันทึกข้อมูลตั้งแต่เกิดเหตุจนถึงปัจจุบันและนำข้อมูลปรึกษาผู้เชี่ยวชาญเพื่อดำเนินการแก้ไข	Second-line Analyst เก็บรวบรวมข้อมูลตั้งแต่เกิดเหตุจนถึงปัจจุบัน เพื่อนำข้อมูลต่าง ๆ เป็นหลักฐานอ้างอิงและนำข้อมูลไปปรึกษาผู้เชี่ยวชาญเพื่อดำเนินการแก้ไขปัญหา
19	ตรวจสอบระบบ เพื่อลบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ออกจากระบบ	Second-line Analyst ตรวจสอบระบบ เพื่อทำการกำจัด Malware หรือสิ่งแปลกปลอมในระบบทั้งหมด
20	พบ Malware หรือสิ่งแปลกปลอมอื่นๆ เพิ่มเติมหรือไม่	■ กรณีที่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตามขั้นตอนที่ 18 ■ กรณีที่ไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตามขั้นตอนที่ 21
21	กู้คืนข้อมูลที่สำรองไว้	Second-line Analyst กู้คืนข้อมูลที่สำรองไว้ และตรวจสอบผลการกู้คืนข้อมูลไว้
22	ตรวจสอบผลการดำเนินงาน	Second-line Analyst ตรวจสอบผลการดำเนินงานของข้อมูลเพื่อให้แน่ใจว่าสามารถดำเนินการกู้คืนข้อมูลได้แล้วเสร็จ
23	บันทึกผลการดำเนินงานและปิดใบงาน	Second-line Analyst บันทึกผลการดำเนินงาน และปิดใบงาน

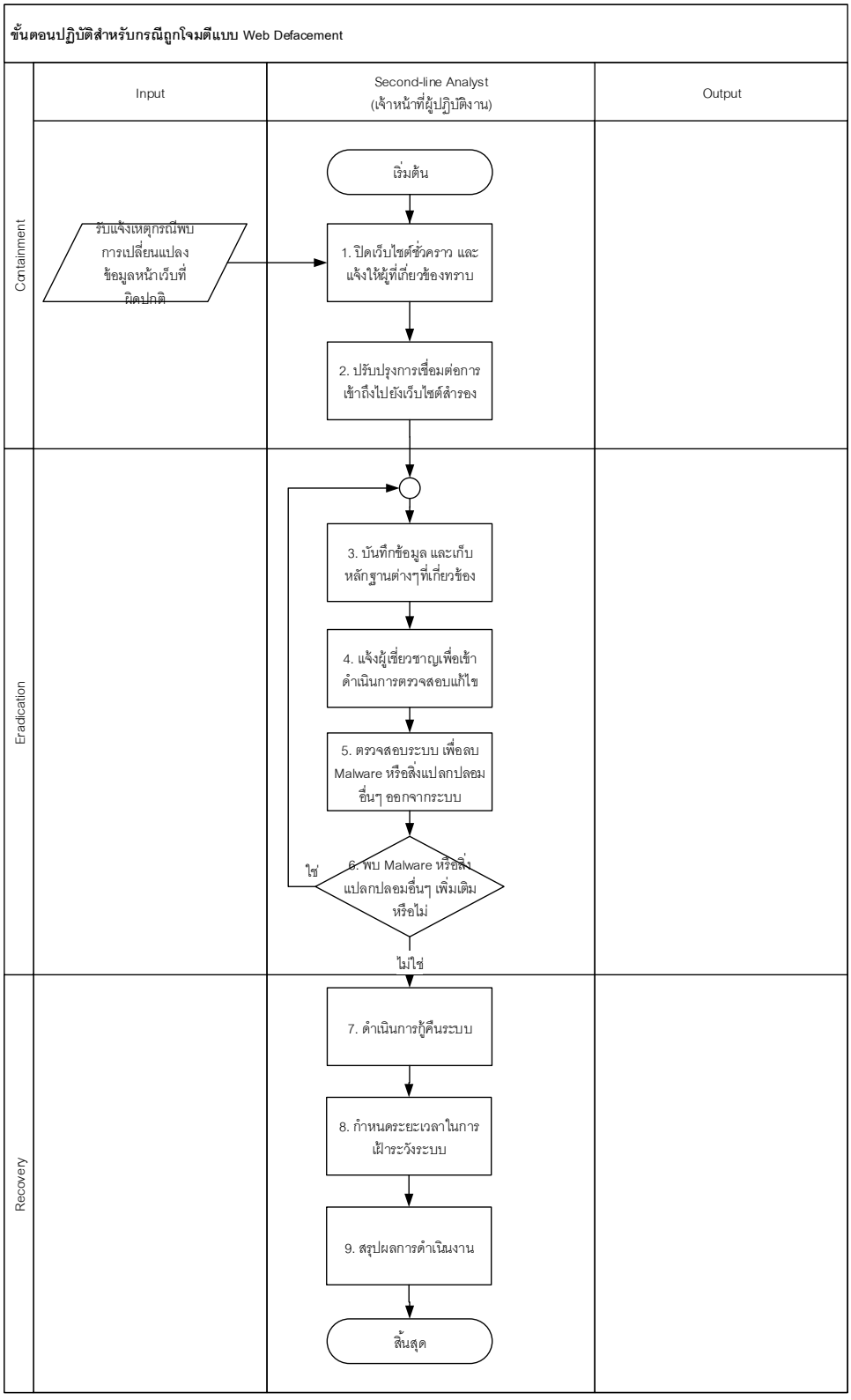
ข.3 ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ DDoS



รายละเอียดขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ DDoS

ลำดับที่	ขั้นตอน	คำอธิบาย
1	วิเคราะห์หา IP Address ที่ถูกใช้ในการโจมตี เพื่อปิดกั้นการเชื่อมต่อ	Second-line Analyst วิเคราะห์เพื่อกำหนด IP Address ที่ถูกใช้ในการโจมตี
2	แจ้งผู้ให้บริการเครือข่าย เพื่อ Take Down IP ที่เป็นผู้โจมตี	Second-line Analyst ประสานงานกับผู้ให้บริการระบบเครือข่าย เพื่อ Take Down IP ที่เป็นผู้โจมตี
3	ระบุ IP ที่ต้องทำการบล็อคในอุปกรณ์ป้องกันที่เกี่ยวข้อง	Second-line Analyst ตรวจสอบการกำหนดข้อมูล DDoS traffic ในอุปกรณ์เครือข่าย เพื่อป้องกันการโจมตี และใช้เป็นข้อมูลในการวิเคราะห์ข้อมูลลักษณะการโจมตี
4	ตรวจสอบการทำงานของระบบ	Second-line Analyst สอบทานการทำงานของระบบที่ถูกโจมตี เพื่อให้แน่ใจว่า ระบบสามารถกลับมาทำงานได้ตามปกติ โดยการตรวจสอบข้อมูลเบื้องต้นดังนี้ ■ ตรวจสอบ traffic flow เพื่อให้แน่ใจว่าเป็นการเชื่อมต่อตามปกติ ไม่มีการเชื่อมต่อที่ผิดสังเกต ■ ตรวจสอบการดำเนินงานของระบบที่ถูกโจมตีว่าสามารถใช้งานได้ตามปกติ ■ ตรวจสอบประสิทธิภาพการให้บริการของโครงสร้างพื้นฐาน เพื่อให้แน่ใจว่าสามารถให้บริการได้ตามปกติ ตรวจสอบระบบที่เกี่ยวข้องเพื่อให้แน่ใจว่าไม่เกิดความเสียหายเพิ่มเติม
5	ระบบสามารถดำเนินการได้ตามปกติหรือไม่	■ กรณีที่ระบบสามารถดำเนินการได้ตามปกติ ให้ดำเนินการตามขั้นตอนที่ 9 ■ กรณีที่ระบบยังไม่สามารถดำเนินงานได้ตามปกติ ให้ดำเนินการตามขั้นตอนที่ 4
6	กู้คืนระบบ	Second-line Analyst ดำเนินการกู้คืนระบบ และปรับปรุงระบบเครือข่ายเข้าสู่การดำเนินงานตามปกติ
7	สรุปผลการดำเนินงาน	Second-line Analyst สรุปผลการดำเนินงาน รายต่อผู้ที่เกี่ยวข้องและดำเนินการบันทึกปิดใบงาน

ข.4 ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Web Defacement

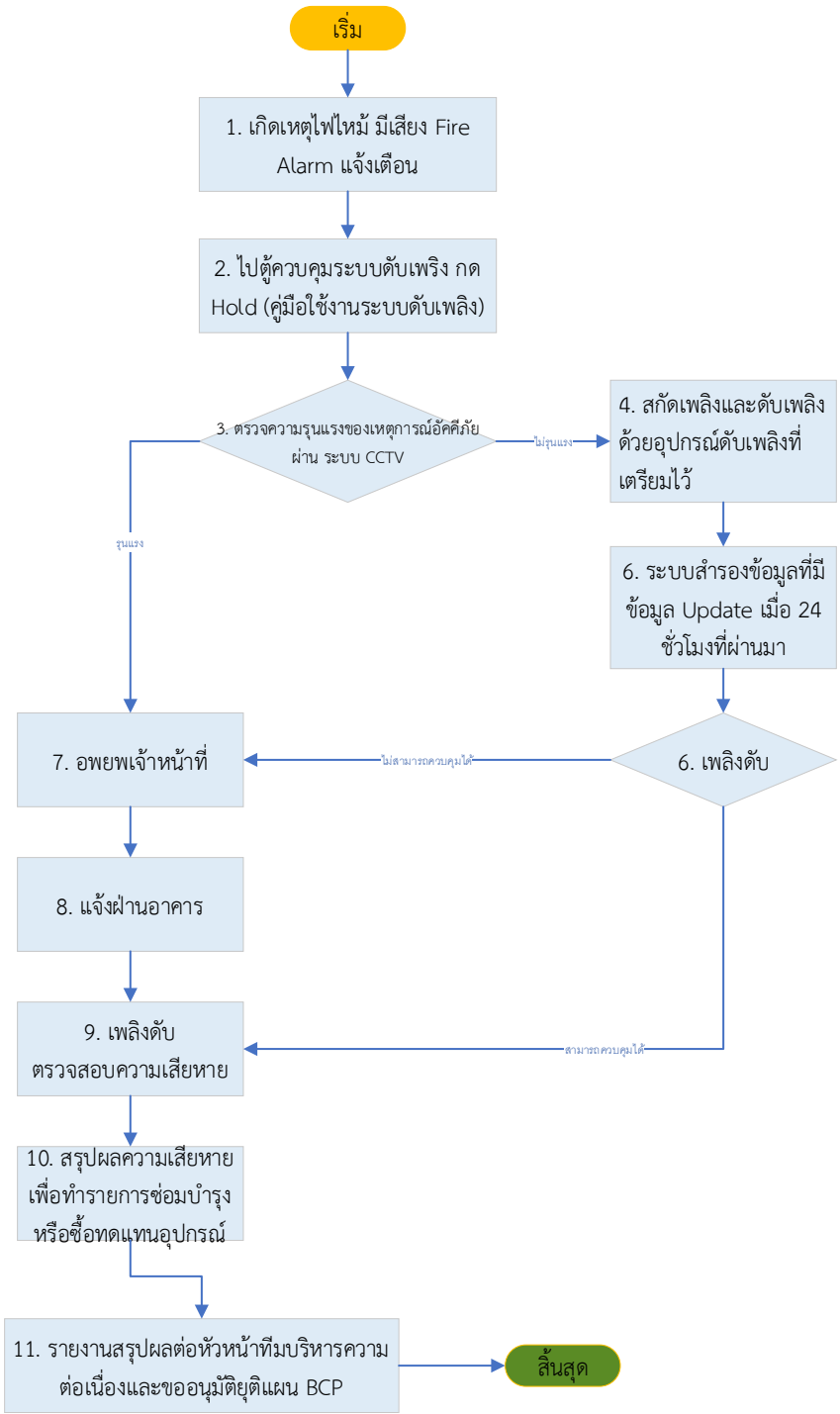


รายละเอียดขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Web Defacement

ลำดับที่	ขั้นตอน	คำอธิบาย
1	ปิดเว็บไซต์ชั่วคราว และแจ้งให้ผู้ที่เกี่ยวข้องทราบ	Second-line Analyst ปิดการเข้าถึง (off-line) หน้าเว็บไซต์ที่ถูกโจมตีทันที โดยไม่ต้องปิดระบบ เพื่อรักษาสภาพข้อมูล สำหรับการเก็บข้อมูลพิสูจน์หลักฐานทางคอมพิวเตอร์ และแจ้งสถานการณ์ให้ผู้ที่เกี่ยวข้องทราบ
2	ปรับปรุงการเชื่อมต่อการเข้าถึงไปยังเว็บไซต์สำรอง	Second-line Analyst ปรับการเชื่อมต่อเว็บออกจากระบบเครือข่ายอื่น ๆ ที่เกี่ยวข้อง สร้างเว็บเพจใหม่เพื่อแสดงสถานะอยู่ระหว่างการปรับปรุงเว็บไซต์ (Maintenance) และ redirect การเข้าถึงหน้าเว็บไปที่หน้าแสดงสถานะนั้น
3	บันทึกข้อมูล และเก็บหลักฐานต่าง ๆ ที่เกี่ยวข้อง	Second-line Analyst เก็บบันทึกข้อมูลหลักฐาน ของเครื่องแม่ข่าย (Server) ที่ถูกโจมตีเพื่อทำการพิสูจน์หลักฐานทางคอมพิวเตอร์ และเก็บบันทึกข้อมูล Log จากระบบเครือข่ายและเครื่องแม่ข่ายที่ถูกโจมตีเพื่อวิเคราะห์หาสาเหตุและวิธีที่ใช้ในการโจมตี
4	แจ้งผู้เชี่ยวชาญเพื่อเข้าดำเนินการตรวจสอบแก้ไข	Second-line Analyst แจ้งผู้เชี่ยวชาญ และนำส่งข้อมูลหลักฐานเพื่อดำเนินการตรวจสอบ และปรับปรุงแก้ไข
5	ตรวจสอบระบบ เพื่อลบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ออกจากระบบ	Second-line Analyst ตรวจสอบระบบ เพื่อทำการกำจัด Malware หรือสิ่งแปลกปลอมในระบบทั้งหมด
6	พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติมหรือไม่	■ กรณีที่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตามขั้นตอนที่ 3 ■ กรณีที่ไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตามขั้นตอนที่ 7
7	ดำเนินการกู้คืนระบบ	Second-line Analyst ดำเนินการกู้คืนระบบ (restore) กลับสู่การดำเนินงานปกติ ทำการตรวจสอบช่องโหว่ อัพเดท patchทดสอบการทำ Penetration testing บนเว็บไซต์ที่กู้คืน และทำ Hardening ตรวจสอบผลการดำเนินงาน ปรับปรุงการเข้าถึงเว็บไซต์จากแสดงหน้าจอการปรับปรุงเว็บไซต์ (Maintenance) ให้สามารถเข้าถึงเว็บไซต์ได้ตามปกติ และบันทึกผล
8	กำหนดระยะเวลาในการเฝ้าระวังระบบ	Second-line Analyst กำหนดระยะเวลาในการเฝ้าระวังระบบ เพื่อให้แน่ใจว่า ระบบสามารถทำงานได้ตามปกติ ไม่ถูกโจมตีซ้ำด้วยวิธีเดิม
9	สรุปผลการดำเนินงาน	Second-line Analyst สรุปผลการดำเนินงาน รายต่อผู้ที่เกี่ยวข้องและดำเนินการบันทึกปิดใบงาน

ภาคผนวก ค ขั้นตอนการตอบสนองต่อภัยธรรมชาติและภัยที่เกิดจากมนุษย์

ค.1 ขั้นตอนปฏิบัติสำหรับกรณีอัคคีภัย

เหตุการณ์	รายละเอียด
	1. ทราบเหตุไฟไหม้จากการสัญญาณแจ้งเตือนหรือสังเกตถึงความผิดปกติเช่น ควันไฟ กลิ่นไหม้ 2. ไปตู้ควบคุมระบบดับเพลิงกด HOLD (คู่มือใช้งานระบบดับเพลิง) 3. ตรวจความรุนแรงของเหตุการณ์อัคคีภัย ผ่านระบบ CCTV 4. กรณีไม่รุนแรงให้สกัดเพลิงและดับเพลิงด้วยอุปกรณ์ดับเพลิงที่เตรียมไว้ 5. กรณีมีเวลาในดำเนินงานให้สำรองข้อมูล ปิดระบบหรือย้ายไปยังระบบสำรองนอกสถานที่ตามลำดับความสำคัญเท่าที่ทำได้เพื่อป้องกันความเสียหายของข้อมูล 6. ระบบสำรองข้อมูลที่มีข้อมูล Update เมื่อ 24 ชั่วโมงที่ผ่านมา 7. กรณีไม่สามารถควบคุมเพลิงได้ด้วยอุปกรณ์ที่เตรียมไว้ให้อพยพเจ้าหน้าที่เพื่อความปลอดภัย 8. หลังจากอพยพเจ้าหน้าที่ ให้เจ้าหน้าที่ดับเพลิงปฏิบัติงาน 9. หลังจากเพลิงดับให้ตรวจสอบความเสียหาย 10. สรุปผลความเสียหายเพื่อทำรายการซ่อมบำรุงหรือซื้อทดแทนอุปกรณ์ 11. รายงานสรุปผลต่อหัวหน้าทีมบริหารความต่อเนื่องและขออนุมัติยุติแผน BCP

ข้อปฏิบัติเบื้องต้นสำหรับเจ้าหน้าที่ทั่วไปกรณีอัคคีภัย

1. รีบออกจากอาคารอย่างเป็นระเบียบโดยเร็วที่สุด และไม่ควรกลับเข้าไปในอาคารอีก

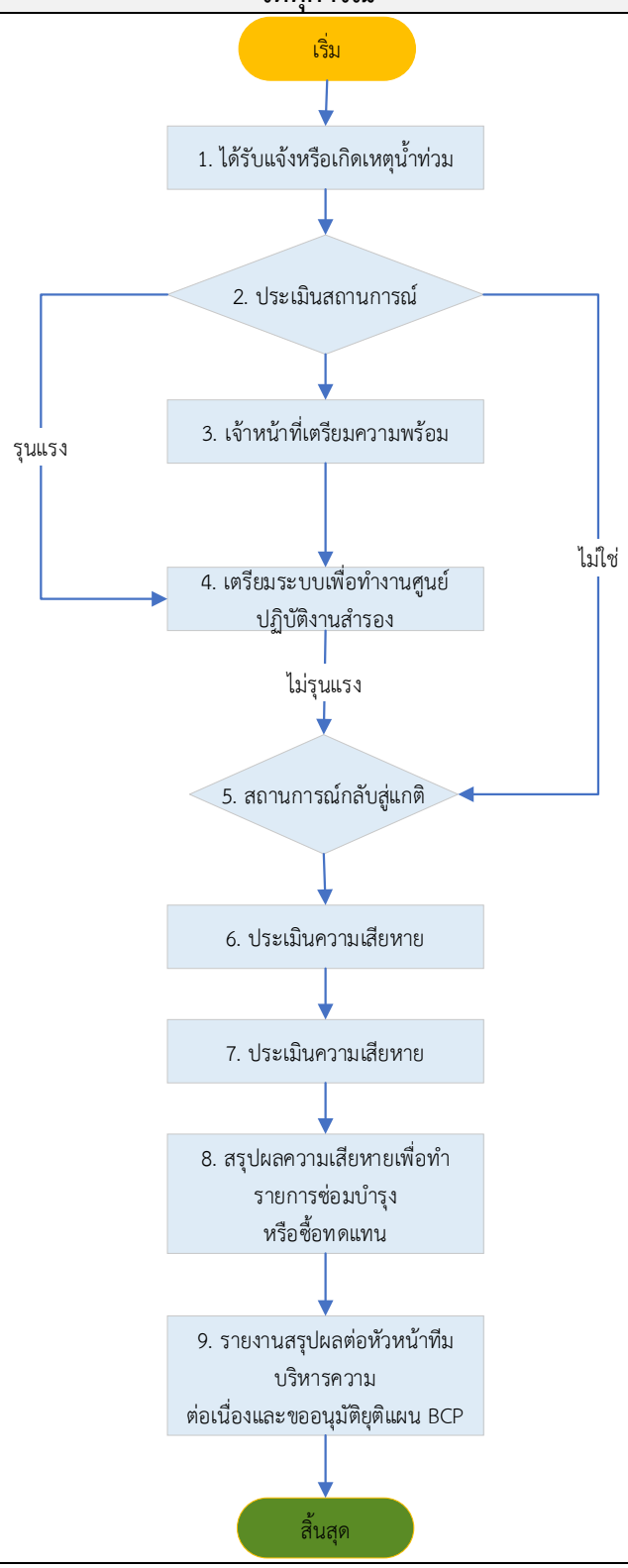
2. หากต้องอพยพออกจากห้อง ควรใช้มือสัมผัสบริเวณผนังหรืออังใกล้ ๆ ลูกบิดประตู ถ้ามีความร้อนสูง แสดงว่าเกิดเพลิงไหม้บริเวณใกล้ ๆ ห้ามเปิดประตูโดยเด็ดขาด

3. ควรหนีไฟลงด้านล่างของอาคาร โดยใช้บันไดหนีไฟด้านนอกอาคาร เนื่องจากลักษณะบันไดภายในอาคารเป็นเหมือนช่อง โพรง ที่เสริมให้เปลวไฟพุ่งขึ้น และลุกลามอย่างรวดเร็ว

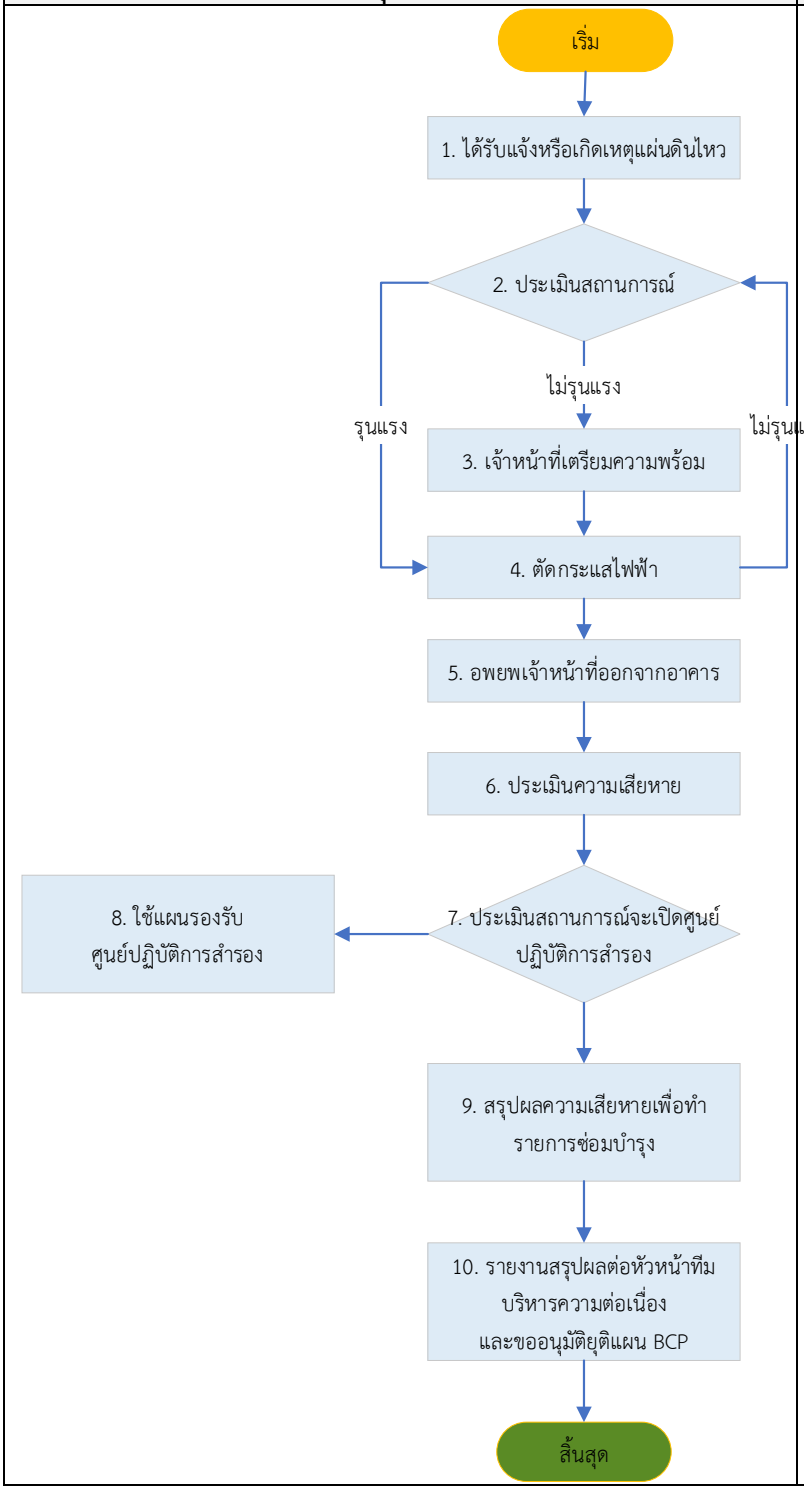
4. ห้ามใช้ลิฟต์ เพราะขณะเกิดเพลิงไหม้ ไฟฟ้าจะดับ ทำให้ลิฟต์ค้างจะทำให้ด้านในของตัวลิฟต์ไม่มีอากาศ

5. หากเส้นทางหนีไฟเต็มไปด้วยกลุ่มควันให้ใช้ผ้าชุบน้ำมาคลุมตัว และปิดจมูก ป้องกันการสำลักควัน

ค.2 ขั้นตอนปฏิบัติสำหรับกรณีอุทกภัย

เหตุการณ์	รายละเอียด
	1. ได้รับแจ้งหรือเกิดเหตุน้ำท่วม 2. แจ้งข่าวสารและประเมินสถานการณ์ว่าจำเป็นต้องอพยพพร้อมทั้งตรวจสอบระบบไฟฟ้ายังสามารถใช้งานได้ตามปกติหรือไม่ 3. เตรียมความพร้อม ติดตามข่าวสารอย่างใกล้ชิด 4. กรณีสถานการณ์รุนแรงจำเป็นต้องอพยพเจ้าหน้าที่ออกจากพื้นที่ ให้เตรียมการช่องทางเพื่อ Remote ทำงานจากภายนอกได้ 5. ประเมินสถานการณ์กลับสู่ปกติหรือตรวจสอบสถานการณ์ ความคืบหน้าเตรียมความพร้อมหากได้รับแจ้งให้อพยพ 6. ประเมินความเสียหายที่อาจเกิดขึ้นหลังเหตุการณ์น้ำท่วม ทำความสะอาดสถานที่ 7. จัดทำรายงานสรุปผลความเสียหายซ่อมบำรุงหรือซื้อทดแทนอุปกรณ์ 8. สรุปผลความเสียหายเพื่อทำรายการซ่อมบำรุงหรือซื้อทดแทนอุปกรณ์ 9. รายงานสรุปผลต่อหัวหน้าทีมบริหารความต่อเนื่องและขออนุมัติยุติแผน BCP

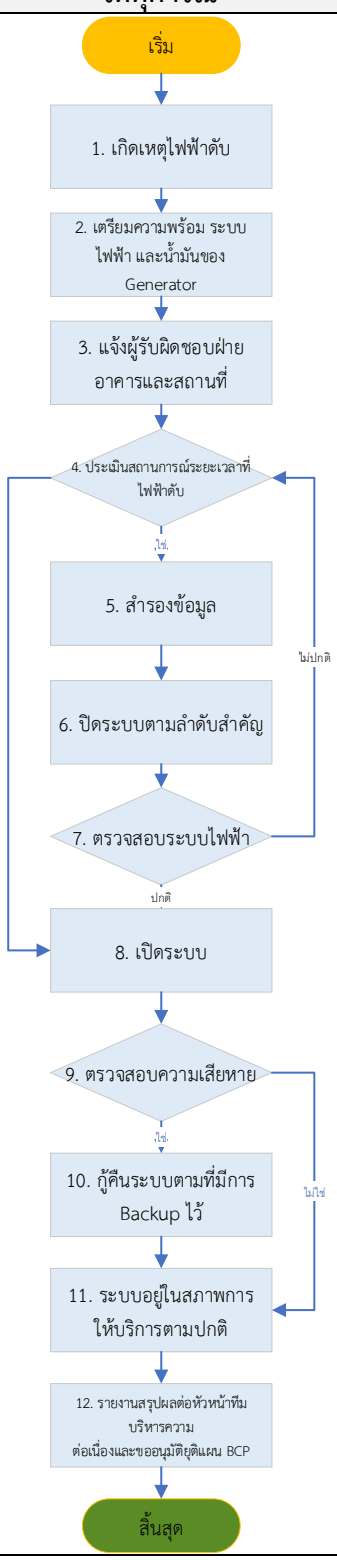
ค.3 ขั้นตอนปฏิบัติสำหรับกรณีแผ่นดินไหว และอาคารถล่ม

เหตุการณ์	รายละเอียด
	1. ได้รับแจ้งหรือเกิดเหตุแผ่นดินไหว 2. แจ้งข่าวสารและประเมินสถานการณ์ว่าจำเป็นต้องอพยพหรือระบบไฟฟ้ายังสามารถใช้งานได้ตามปกติหรือไม่ 3. เจ้าหน้าที่รับมือเหตุการณ์อย่างมีสติ ออกห่างจากประตูระเบียง และหน้าต่าง 4. กรณีสถานการณ์รุนแรงมีคำสั่งให้อพยพให้ตัดระบบไฟฟ้าเพื่อป้องกันเหตุไฟไหม้ 5. อพยพเจ้าหน้าที่ออกจากอาคาร 6. ประเมินความเสียหายที่อาจเกิดขึ้นหลังเหตุการณ์ 7. ประเมินสถานการณ์จะเปิดศูนย์ปฏิบัติการสำรอง 8. ถ้าสถานการณ์ความเสียหายรุนแรงเปิดใช้แผนรองรับการเปิดศูนย์ปฏิบัติการสำรอง 9. ถ้าสถานการณ์ความเสียหายไม่รุนแรงสรุปผลความเสียหาย 10. รายงานสรุปผลต่อหัวหน้าทีมบริหารความต่อเนื่องและขออนุมัติยุติแผน BCP

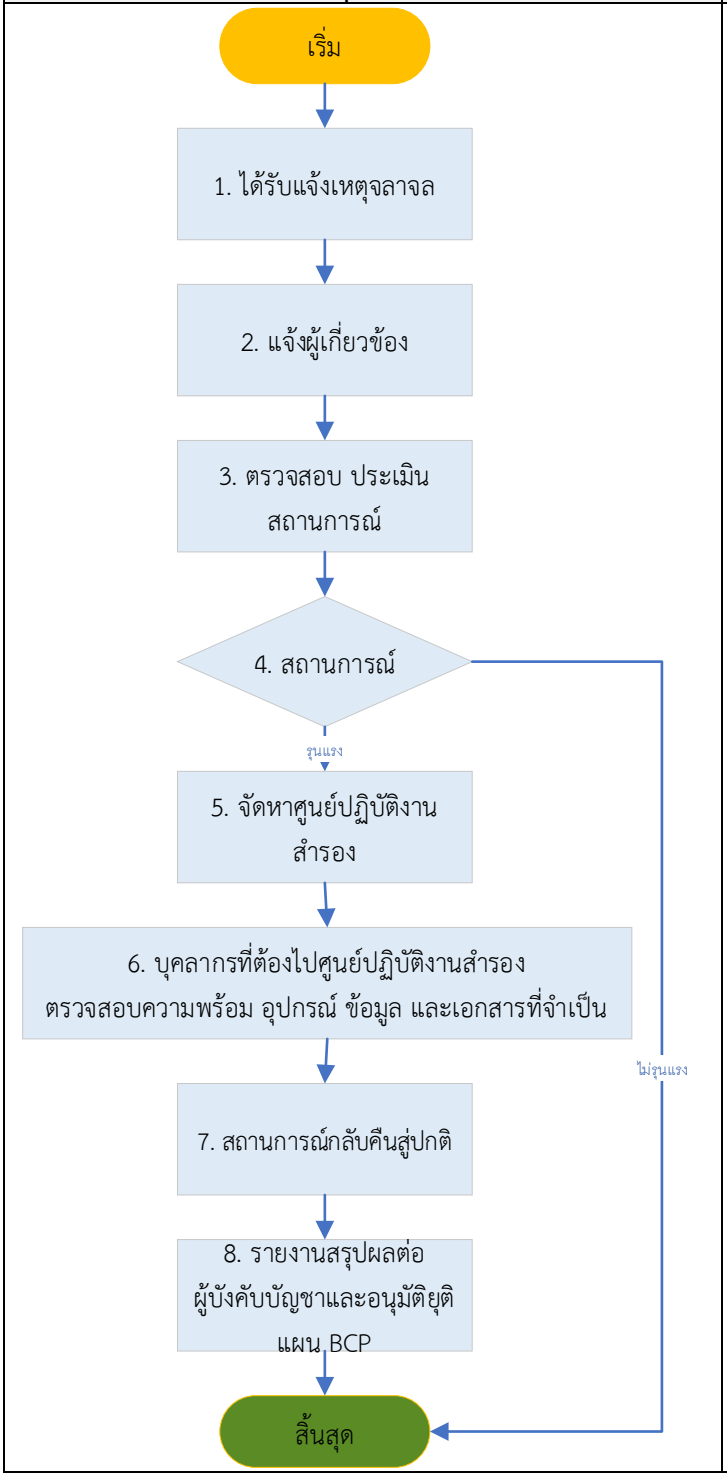
ข้อปฏิบัติเบื้องต้นสำหรับเจ้าหน้าที่ทั่วไปกรณีแผนดินไหว

1. พยายามควบคุมสติอยู่อย่างสงบ หากอยู่ในอาคารที่มีโครงสร้างแข็งแรง ให้อยู่ห่างจากประตู ระเบียง และหน้าต่าง หากอยู่ในอาคารสูง ควรตั้งสติและรีบออกจากอาคารโดยเร็ว
2. ห้ามใช้ลิฟต์โดยเด็ดขาดขณะเกิดแผ่นดินไหว

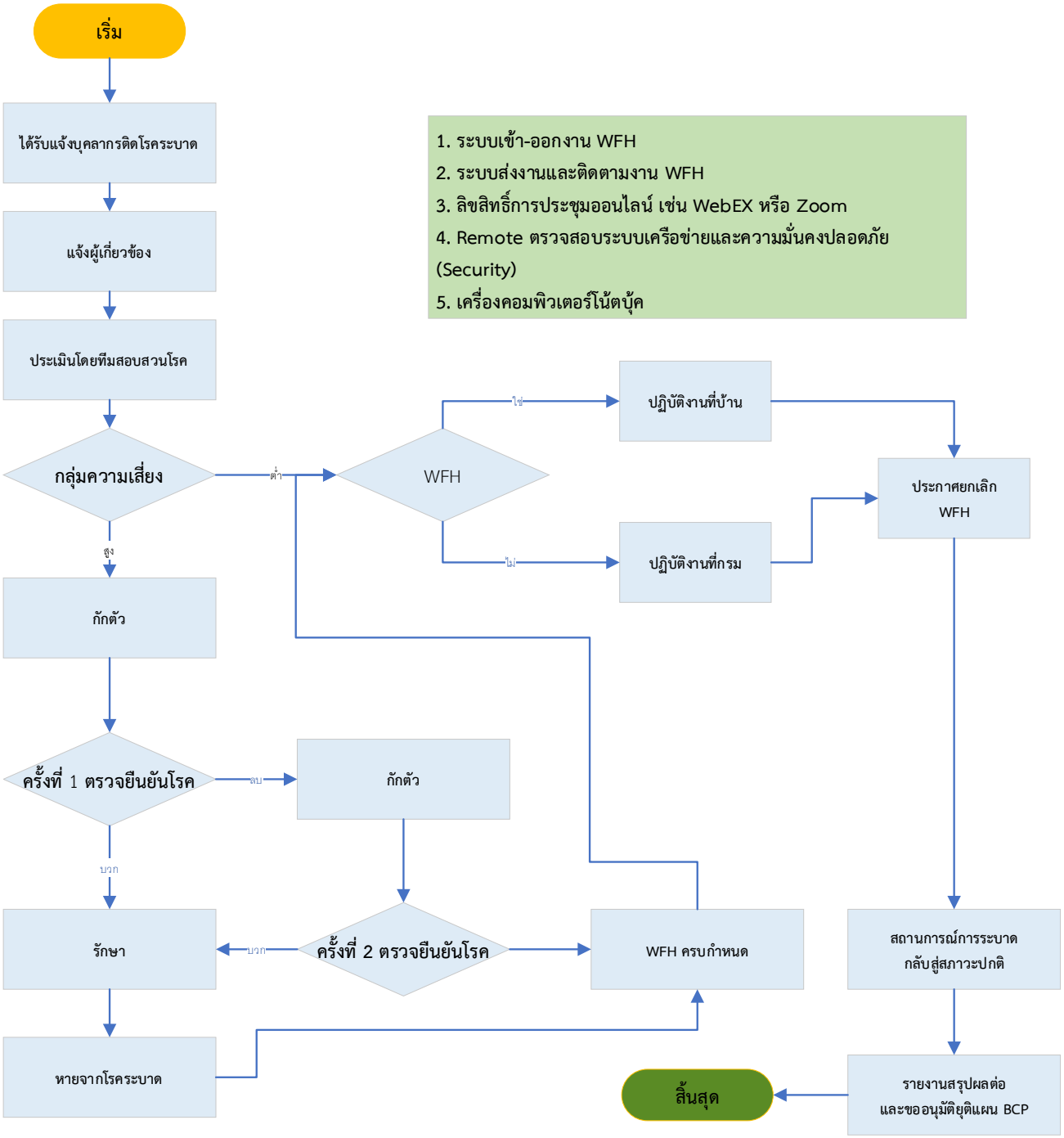
ค.4 ขั้นตอนปฏิบัติสำหรับกรณีไฟฟ้าดับในวงกว้าง

เหตุการณ์	รายละเอียด
	1. เกิดเหตุไฟฟ้าดับหรือขัดข้อง 2. เจ้าหน้าที่เตรียมความพร้อม เช็คปริมาณไฟสำรองจาก UPS และน้ำมันของ Generator 3. ติดต่อฝ่ายอาคารสถานที่เพื่อรับทราบปัญหาและระยะเวลาการแก้ไขปัญหาไฟฟ้า 4. ประเมินสถานการณ์ระยะเวลาที่ไฟฟ้าดับอยู่ในเกณฑ์ที่กำหนดหรือไม่ 5. สำรองข้อมูลที่มีความสำคัญหรือการดำเนินงานที่ค้างอยู่ของเครื่องคอมพิวเตอร์แม่ข่าย 6. ปิดระบบเพื่อป้องการความเสียหายในกรณีเครื่องสำรองไฟไม่เพียงพอ โดยลำดับตามความสำคัญของระบบงาน 7. ตรวจสอบการทำงานของไฟฟ้าเป็นระยะ พร้อมประสานงานผู้เกี่ยวข้องติดตามการแก้ไขปัญหา หากยังไม่สามารถแก้ไขปัญหาได้ให้ทำการสำรองข้อมูลและปิดระบบตามความสำคัญต่อไป 8. หลังจากไฟฟ้ากลับมาใช้งานได้ตามปกติให้เปิดระบบที่ปิดไป 9. ตรวจสอบการทำงานของระบบว่าทำงานได้ตามปกติ หรือเกิดความเสียหายหลังจากเหตุการณ์หรือไม่ 10. กรณีระบบเสียหายหรือเกิดความสูญเสียข้อมูลให้ทำการกู้คืนระบบตามที่มีการ Backup ไว้ 11. ระบบอยู่ในสภาพการให้บริการตามปกติ 12. จัดทำรายงานผลการดำเนินงานและจัดเก็บบันทึกรายงาน รายงานสรุปผลต่อหัวหน้าทีมบริหารความต่อเนื่องและขออนุมัติยุติแผน BCP

ค.5 ขั้นตอนปฏิบัติสำหรับกรณีจลาจล การชุมชุม หรือเหตุการณ์ความไม่สงบ

เหตุการณ์	รายละเอียด
	1. เกิดเหตุจลาจล การชุม หรือเหตุการณ์ความไม่สงบ 2. แจ้งประสานงานไปยังผู้เกี่ยวข้อง 3. ตรวจสอบและประเมินสถานการณ์ 3. กรณีไม่รุนแรงให้เจ้าหน้าที่ปฏิบัติงาน 4. กรณีรุนแรงให้อพยพเจ้าหน้าที่ไปยังศูนย์ปฏิบัติงานสำรอง 5. จัดหาพื้นที่สำรองสำหรับการปฏิบัติงาน 6. เจ้าหน้าที่ที่ไปปฏิบัติงานศูนย์ปฏิบัติงานสำรองตรวจสอบความพร้อมอุปกรณ์ ข้อมูลเอกสารที่จำเป็น 7. สถานการณ์กลับคืนสู่ปกติ จึงดำเนินการสำรวจความเสียหายของศูนย์ปฏิบัติงานหลัก 8. รายงานสรุปผลต่อหัวหน้าทีมบริหารความต่อเนื่องและขออนุมัติยุติแผน BCP

ค.6 ขั้นตอนปฏิบัติสำหรับกรณีโรคระบาดต่อเนื่องร้ายแรง



เมื่อเกิดเหตุการณ์**โรคระบาดต่อเนื่องร้ายแรง** ส่งผลให้บุคลากรป่วยด้วยโรคระบาด เพื่อบริหารความต่อเนื่องภารกิจองค์กร ได้กำหนดร้อยละบุคลากร และพื้นที่ปฏิบัติงานเป็นสถานที่ปฏิบัติงานหลัก และสำรองดังตาราง

ลำดับที่	ฉากทัศน์ (Scenario)	พื้นที่ปฏิบัติงานที่กำหนด
1	กรณีเพื่อพบผู้ป่วยที่เข้าเกณฑ์สอบสวนโรค (Patient under investigation : PUI) ในสถานที่ปฏิบัติงาน 1 คน	- สถานที่ปฏิบัติงานหลัก ร้อยละ 70 - สถานที่ปฏิบัติงานสำรอง (บ้าน หรือที่พักที่หน่วยงานจัดไว้) ร้อยละ 30
2	กรณีเพื่อพบผู้ป่วยที่เข้าเกณฑ์สอบสวนโรค (Patient under investigation : PUI) ในสถานที่ปฏิบัติงานมากกว่า 5 คน	- สถานที่ปฏิบัติงานหลัก ร้อยละ 50 - สถานที่ปฏิบัติงานสำรอง (บ้าน หรือที่พักที่หน่วยงานจัดไว้) ร้อยละ 50
3	กรณีมีการระบาดซ้ำภายใน 28 วัน หลังจากมีมาตรการกักตัวครบ 14 วันแล้ว	- สถานที่ปฏิบัติงานหลัก ร้อยละ 30 - สถานที่ปฏิบัติงานสำรอง (บ้าน หรือที่พักที่หน่วยงานจัดไว้) ร้อยละ 70