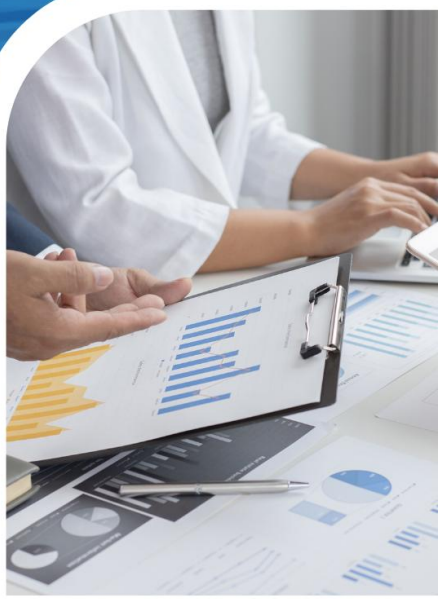
กรมวิทยาศาสตร์การแพทย์
Department of Medical Sciences

แผนบริหารความต่อเนื่อง ด้านระบบเทคโนโลยีสารสนเทศ (IT BUSINESS CONTINUITY PLAN) กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข



จัดทำโดย

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
กรมวิทยาศาสตร์การแพทย์

มิถุนายน 2568

แผนบริหารความต่อเนื่องด้านระบบเทคโนโลยีสารสนเทศ
กรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข

กรมวิทยาศาสตร์การแพทย์นำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ ระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตีจากผู้ไม่ประสงค์ดี ไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่าง ๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของกรมวิทยาศาสตร์การแพทย์

แผนบริหารความต่อเนื่องด้านระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) จัดทำขึ้น เพื่อให้ “**กรมวิทยาศาสตร์การแพทย์**” สามารถนำแผนไปใช้ปฏิบัติงานในสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการมุ่งร้ายต่อองค์กร โดยไม่ให้สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินดังกล่าวส่งผลกระทบต่อการปฏิบัติงานหรือไม่สามารถให้บริการได้อย่างต่อเนื่องของกรมวิทยาศาสตร์การแพทย์ รวมไปถึง การรับมือเหตุภัยคุกคามทางไซเบอร์ของกรมวิทยาศาสตร์การแพทย์ ตามมาตรา 44 แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562 ซึ่งการที่กรมวิทยาศาสตร์การแพทย์ไม่มีกระบวนการรองรับภัยคุกคามสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินดังกล่าวข้างต้นนั้น อาจส่งผลกระทบทั้งในด้านเศรษฐกิจการเงิน การให้บริการ สังคม ชุมชน สิ่งแวดล้อม ตลอดจนชีวิตและทรัพย์สินของประชาชน เป็นต้น

ดังนั้น การจัดทำแผนบริหารความต่อเนื่องจึงเป็นสิ่งสำคัญที่จะช่วยให้กรมวิทยาศาสตร์การแพทย์สามารถรับมือกับสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินที่ไม่คาดคิด และทำให้กระบวนการที่สำคัญ (Critical Business Process) สามารถกลับมาดำเนินการได้อย่างปกติ หรือตามระดับการให้บริการที่กำหนดไว้ ซึ่งจะช่วยลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อหน่วยงานได้

วัตถุประสงค์ (Objectives)

1. เพื่อเตรียมความพร้อมในการรับมือกับสภาวะวิกฤต
2. เพื่อเตรียมการรับมือเหตุภัยคุกคามทางไซเบอร์ที่เกิดขึ้น
3. เพื่อเป็นแนวทางในการบริหารความต่อเนื่องของบุคลากรกรมวิทยาศาสตร์การแพทย์
4. เพื่อลดผลกระทบจากการหยุดชะงักในการดำเนินงานหรือการให้บริการ
5. เพื่อบรรเทาความเสียหายให้อยู่ระดับที่ยอมรับได้
6. เพื่อให้ประชาชน เจ้าหน้าที่ และผู้มีส่วนได้ส่วนเสีย(Stakeholders) มีความเชื่อมั่นในศักยภาพของกรมวิทยาศาสตร์การแพทย์ แม้กรมวิทยาศาสตร์การแพทย์ต้องเผชิญกับเหตุการณ์ร้ายแรงและส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

สมมติฐาน (Assumptions)

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐาน ดังต่อไปนี้

1. เหตุการณ์ฉุกเฉินที่เกิดขึ้นในช่วงเวลาสำคัญต่าง ๆ แต่มิได้ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการจัดเตรียมไว้
2. ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารรับผิดชอบในการสำรองระบบสารสนเทศต่าง ๆ โดยระบบสารสนเทศ
   สำรองมิได้รับผลกระทบจากเหตุการณ์ฉุกเฉินเหมือนกับระบบสารสนเทศหลัก
3. “บุคลากร” ที่ถูกระบุในเอกสารฉบับนี้ หมายถึง เจ้าหน้าที่และพนักงานทั้งหมดของกรมวิทยาศาสตร์การแพทย์

ขอบเขต (Scope)

แผนบริหารความต่อเนื่องฉบับนี้ใช้รองรับสถานการณ์ กรณีเกิดสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินทางด้านเทคโนโลยีสารสนเทศและข้อมูลดิจิทัลของ (กรมวิทยาศาสตร์การแพทย์) รวมถึงบุคคลหรืออุปกรณ์ใดๆ ซึ่งเข้าถึงระบบสารสนเทศ และข้อมูลดิจิทัลดังกล่าว ของกรมวิทยาศาสตร์การแพทย์ ประกอบด้วยเหตุการณ์ต่อไปนี้

- เหตุการณ์อุทกภัยและวาตภัย
- เหตุการณ์อัคคีภัย
- เหตุการณ์ชุมนุมประท้วง/จลาจล
- เหตุการณ์โรคระบาด
- เหตุการณ์แผ่นดินไหว
- ระบบไฟฟ้าขัดข้อง
- ระบบโครงสร้างพื้นฐานขัดข้อง (SERVER, Network)
- การโจมตีทางไซเบอร์

การวิเคราะห์ทรัพยากรที่สำคัญ

สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้นเพื่อให้กรมวิทยาศาสตร์การแพทย์สามารถบริหารจัดการการดำเนินงานของกรมวิทยาศาสตร์การแพทย์ให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงเป็นสิ่งจำเป็นและต้องระบุไว้ในแผนบริหารความต่อเนื่อง ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบใน 5 ด้าน ดังนี้

1. **ผลกระทบด้านอาคาร/สถานที่ปฏิบัติงานหลัก** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายหรือไม่สามารถใช้สถานที่ปฏิบัติงานหลักได้ และส่งผลให้บุคลากรไม่สามารถเข้าไปปฏิบัติงานได้ชั่วคราวหรือระยะยาว
2. **ผลกระทบด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้
3. **ผลกระทบด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ
4. **ผลกระทบด้านบุคลากรหลัก** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ
5. **ผลกระทบด้านคู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย** หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

เหตุการณ์สภาวะวิกฤต	ผลกระทบ				
	ด้านอาคาร/สถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	ด้านเทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	ด้านบุคลากรหลัก	ผลกระทบด้านคู่ค้า/ผู้ให้บริการที่สำคัญ/ผู้มีส่วนได้ส่วนเสีย
เหตุการณ์อุทกภัยและวาตภัย	✓	✓	✓	✓	✓
เหตุการณ์อัคคีภัย	✓	✓	✓	✓	✓
เหตุการณ์ชุมนุมประท้วง/จลาจล	✓	✓	✓	✓	✓
เหตุการณ์แผ่นดินไหว	✓	✓	✓	✓	✓
เหตุการณ์โรคระบาด	✓		✓	✓	✓
เหตุการณ์ระบบไฟฟ้าขัดข้อง		✓	✓		✓
การโจมตีทางไซเบอร์			✓	✓	✓

แผนบริหารความต่อเนื่องฉบับนี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องเกิดขึ้นจากการดำเนินงานปกติ และเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของกรมวิทยาศาสตร์การแพทย์เนื่องจากกรมวิทยาศาสตร์การแพทย์ยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม โดยผู้บริหารของกรมวิทยาศาสตร์การแพทย์ หรือผู้บริหารของแต่ละสำนัก/ศูนย์/กลุ่ม สามารถรับผิดชอบและดำเนินการได้ด้วยตนเอง

บทบาทหน้าที่และโครงสร้างทีมรับมือสถานการณ์ฉุกเฉิน

<u>ผู้รับแจ้งเหตุการณ์ฉุกเฉินภายในหน่วยงาน</u>

การติดต่อของผู้รับแจ้งเหตุการณ์ฉุกเฉินภายในหน่วยงาน กรณีเมื่อมีการตรวจพบ หรือมีการรายงานเหตุการณ์เกี่ยวกับฉุกเฉินด้านเทคโนโลยีสารสนเทศโดยควรมีผู้รับแจ้งเหตุฯ หลัก รวมถึงช่องทางหลักในการติดต่อและเตรียมผู้รับแจ้งเหตุฯ คนที่สอง รวมถึงช่องทางสำรองสำหรับกรณีที่ไม่สามารถติดต่อผู้รับแจ้งเหตุคนแรกได้ โดยหน่วยงานควรจะกำหนดให้มีผู้ทำหน้าที่รับแจ้งเหตุฯ คลอบคลุมตลอดระยะเวลา 24 ชั่วโมง/ 7 วัน ตาม ภาคผนวก 1

<u>กรณีเป็นเหตุฉุกเฉินด้านภัยคุกคามทางไซเบอร์ ให้ปฏิบัติตาม แผนรับมือเหตุภัยคุกคามทางไซเบอร์กรมวิทยาศาสตร์การแพทย์</u>

<u>โครงสร้างทีมรับมือเหตุการณ์ที่ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (Incident Response Team : IRT)</u>

กรมวิทยาศาสตร์การแพทย์ใช้โครงสร้างการรับมือเหตุการณ์แบบรวมศูนย์ (Centralize) โดยรายชื่อของบุคลากรที่มีความเกี่ยวข้องกับการรับมือ พร้อมทั้งโครงสร้างทีมรับมือฯ ดังนี้ ตามภาคผนวก 1

<u>หน่วยงานภายนอกที่เกี่ยวข้อง</u>

ลำดับ	ชื่อ – นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
1	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ	02-142-6888 ncert@ncsa.or.th https://www.ncsa.or.th 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษา	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	ประสานงานแจ้งเหตุให้ความช่วยเหลือภัยคุกคามทางไซเบอร์
2	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT)	health-cirt@moph.go.th https://health-cirt.moph.go.th Line Official : @health-cirt ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข อาคาร ๒ ชั้น ๑	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT)	หน่วยงานกำกับดูแล
3	ThaiCERT	02-114-3531 (24 ชั่วโมง) thaicert@ncsa.or.th https://www.thaicert.or.th 120 หมู่ 3 อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7 ศูนย์ราชการเฉลิมพระเกียรติ 80	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ Thailand Computer Emergency Response Team (ThaiCERT)	แจ้งเหตุและติดตามข่าวสารด้านภัยคุกคามไซเบอร์

ลำดับ	ชื่อ – นามสกุล	ช่องทางการติดต่อสื่อสาร	หน่วยงาน	ความเกี่ยวข้อง
4	PCPC	02-142-1033, 02-141-6993 saraban@pdpc.or.th https://www.pdpc.or.th 120 หมู่ 3 ศูนย์ราชการเฉลิมพระเกียรติ 80 พรรษาฯ อาคารรัฐประศาสนภักดี (อาคารบี) ชั้น 7	สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส. หรือ PCPC)	กำกับดูแลด้านข้อมูลส่วนบุคคล
5	กรมสอบสวนคดีพิเศษ	02-831-9888 dsi@dsi.go.th https://www.dsi.go.th อาคารกรมสอบสวนคดีพิเศษ เลขที่ 128 ถนนแจ้งวัฒนะ แขวงทุ่งสองห้อง เขตหลักสี่ กรุงเทพฯ 10210	กรมสอบสวนคดีพิเศษ (DSI)	ติดตามดำเนินงานด้านกฎหมาย
6	Techknowledge	02-513-9415-6contact@techknowledge-th.com 72 อาคารพีเอวี ชั้น 2 ซอยลาดพร้าว 42 ถนนลาดพร้าว แขวงสามเสนนอก เขตห้วยขวาง กรุงเทพมหานคร 10310	บริษัท เทคโนวเลจ คอนซัลติง จำกัด	ผู้รับจ้างภายนอก Network Monitoring กรมวิทยาศาสตร์การแพทย์
7	GMS Support Center	GMS Support Center gms@ncsa.or.th	สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.) ภายใต้โครงการ GMS	ผู้ให้บริการด้านความมั่นคงปลอดภัยไซเบอร์

ทั้งนี้ ขั้นตอนการทีมรับมือฯ ให้มีบุคคลดังต่อไปนี้ทำหน้าที่สนับสนุนการดำเนินการของแผนรับมือฯ ฉบับนี้ ตาม Call tree

ทีมงานแผนความต่อเนื่อง (Business Continuity Plan Team)

เพื่อให้แผนบริหารความต่อเนื่อง (BCP) ของกรมวิทยาศาสตร์การแพทย์ กระทรวงสาธารณสุข สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพและเกิดประสิทธิผล จะต้องจัดตั้งทีมงานบริหารความต่อเนื่อง (BCP Team) ขึ้น โดย BCP Team ประกอบด้วยโครงสร้าง ดังนี้

1. หัวหน้าคณะบริหารความต่อเนื่อง (รองอธิบดีปฏิบัติหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)
2. ผู้ประสานงานคณะบริหารความต่อเนื่อง (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นหัวหน้าคณะผู้ประสานงาน, ฝ่ายการเจ้าหน้าที่, ฝ่ายพัสดุ และศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เป็นคณะทำงาน)
3. หัวหน้าทีมบริหารความต่อเนื่อง (แบ่งออกเป็น 35 ทีม จากหน่วยงานภายในกรมวิทยาศาสตร์การแพทย์) โดยรายละเอียดช่องทางการติดต่อตาม **ภาคผนวก 1**

กลยุทธ์ความต่อเนื่องทางธุรกิจ (Business Continuity Strategy)

กลยุทธ์ความต่อเนื่อง เป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน 5 ด้าน ดังตารางที่ 2

ตารางที่ 2 กลยุทธ์ความต่อเนื่อง (Business Continuity Strategy) และ**ความต้องการด้านทรัพยากรที่จำเป็นในการบริหารความต่อเนื่อง**

ทรัพยากร	กลยุทธ์ความต่อเนื่อง
อาคาร/สถานที่ปฏิบัติงานหลัก	ในกรณีที่ความเสียหายขยายเป็นวงกว้าง กำหนดให้ใช้พื้นที่ปฏิบัติงานสำรอง ณ สถานที่ ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี (ศูนย์คอมพิวเตอร์สำรอง) โดยมีการประสานงาน และการเตรียมความพร้อมล่วงหน้า
วัสดุอุปกรณ์ที่สำคัญ/การจัดหาจัดส่งวัสดุอุปกรณ์ที่สำคัญ	• กำหนดให้มีการจัดหาคอมพิวเตอร์สำรอง ที่มีคุณลักษณะเหมาะสมกับการใช้งาน พร้อมอุปกรณ์ที่สามารถเชื่อมโยงต่อผ่านอินเตอร์เน็ตเข้าสู่ระบบเทคโนโลยีของหน่วยงานกลางได้ • กำหนดให้มีการประสานงานระหว่างผู้ให้บริการเครือข่ายในการจัดเส้นทางของระบบเครือข่ายคอมพิวเตอร์ • กำหนดให้ใช้คอมพิวเตอร์แบบพกพา (Laptop/Notebook)ของเจ้าหน้าที่ของหน่วยงานได้เป็นการชั่วคราว หากมีความจำเป็นเร่งด่วนในช่วงระหว่างการจัดหาคอมพิวเตอร์สำรอง ทั้งนี้ ต้องได้รับอนุญาตจากหัวหน้าคณะบริหารความต่อเนื่องในการกู้คืนก่อน
เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ	• กรมวิทยาศาสตร์การแพทย์มอบหมายให้ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รับผิดชอบจัดเตรียมและให้มีระบบงานเทคโนโลยีหรือระบบสารสนเทศสำรอง และเทคโนโลยีประชุมทางไกลจากภายนอกกรม • ปฏิบัติงานโดยไม่ใช้ระบบงานเทคโนโลยี (Manual) ไปก่อนแล้วจึงป้อนข้อมูลเข้าในระบบเมื่อกลับคืนสู่สภาวะปกติ
บุคลากรหลัก	• กำหนดให้ใช้บุคลากรสำรอง ทดแทนภายในหน่วยงานหรือกลุ่มงานเดียวกัน • กำหนดให้ใช้บุคลากรนอกหน่วยงานหรือกลุ่มงานในกรณีที่บุคลากรไม่เพียงพอหรือขาดแคลน
ลูกค้า/ผู้มีส่วนได้ส่วนเสีย	กำหนดหมายเลขติดต่อ สถานที่ที่สามารถติดต่อได้ และข่าวสารที่สำคัญในกรณีเกิดเหตุการณ์ฉุกเฉิน หรือภัยพิบัติ ให้ลูกค้า/ผู้มีส่วนได้ส่วนเสียรับทราบ

การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) เป็นการวิเคราะห์ช่วงระยะเวลาของการหยุดชะงักเมื่อสภาวะวิกฤต/ภัยคุกคามเริ่มส่งผลกระทบกับการดำเนินงานของหน่วยงานโดยแบ่งเกณฑ์การ ประเมินความเสี่ยง (Risk Assessment) และวิเคราะห์เหตุการณ์ที่ทำให้เกิดการหยุดชะงัก (Incident) โดยประเมินจากความเสี่ยงที่ได้จากแบบประเมินความเสี่ยงสำหรับวิเคราะห์ความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ (Risk Assessment: RA)

เกณฑ์การให้คะแนนประเมินความเสี่ยง (Risk Assessment)

ความรุนแรง (S)

คะแนน	ผลกระทบหยุดการปฏิบัติงาน	ผลกระทบด้านการเงินที่เสียหายหรือสูญเสีย
1	ไม่หยุดการปฏิบัติงาน	ไม่เกิดมูลค่าเสียหาย
2	หยุดการปฏิบัติงานไม่เกิน 2 ชั่วโมง	มูลค่าเสียหายไม่เกิน 100,000 บาท
3	หยุดการปฏิบัติงานไม่เกิน 2 ชั่วโมง – 1 วัน	มูลค่าเสียหายไม่เกิน 100,000 -1,000,000 บาท
4	หยุดการปฏิบัติงาน 2 วัน – 7 วัน	มูลค่าเสียหายไม่เกิน 1,000,000 -10,000,000 บาท
5	หยุดการปฏิบัติงานมากกว่า 7 วัน	มูลค่าเสียหายเกิน 10,000,000 บาท

ความถี่ในการเกิดอุบัติการณ์ (L)

คะแนน	ผลกระทบ
1	ไม่เคยเกิดขึ้นเลย
2	เกิดขึ้นในช่วง 1 ปี ขึ้นไป
3	เกิดขึ้นในช่วง 6 เดือนถึง 1 ปี
4	เกิดขึ้นในช่วง 3 เดือนถึง 6 เดือน
5	เกิดขึ้นในช่วง 1 เดือนถึง 3 เดือน

การควบคุมในปัจจุบัน (D)

คะแนน	ผลกระทบ
1	มีการควบคุมจัดทำเป็นเอกสารและมีการนำไปปฏิบัติและ/หรือมีการซ้อมจริง
2	มีการควบคุมแล้ว ผู้ที่เกี่ยวข้องเข้าใจ มีการปฏิบัติจริง
3	มีการควบคุมแล้วและพอเข้าใจแต่มีการปฏิบัติบ้างไม่ปฏิบัติบ้าง
4	มีการควบคุมแล้วแต่ไม่มีประสิทธิภาพและผู้ที่เกี่ยวข้องเข้าใจ
5	ไม่มีการควบคุมอุบัติการณ์นี้เลย

เกณฑ์การตัดสินใจ

คะแนน (S X L X D)	ระดับความเสี่ยง	Risk Reduction
60 ขึ้นไป	Unacceptable	BCP
40 ถึง 59	Medium	Operational Control
น้อยกว่า 40 ลงมา	Accept	N/A

ทั้งนี้กรมวิทยาศาสตร์การแพทย์ ได้มีการทบทวนการวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis) ข้างต้นปีละ 1 ครั้งและนำมาวิเคราะห์ผลกระทบทางธุรกิจเพื่อนำมาใช้กำหนดแนวทางปฏิบัติสำหรับบริการที่สำคัญ ดังตารางผลกระทบทางธุรกิจ (Business Impact Analysis)

ผลกระทบทางธุรกิจ (Business Impact Analysis)

กระบวนการหลัก/กิจกรรมสำคัญ	MTPD	MTPD	RTO	RPO	ระยะเวลาของการตอบสนองต่อเหตุการณ์		
					ระยะสั้น	ระยะกลาง	ระยะยาว
การให้บริการระบบการเงินการคลัง(Fin-AD)	unacceptable	3h	2h	1d	1-2d	7d	30d
การให้บริการระบบใบเสร็จอิเล็กทรอนิกส์(Dmsc Payment)	unacceptable	3h	2h	1d	1-2d	7d	30d
การให้บริการระบบทดสอบความชำนาญ(DMSc PT)	unacceptable	3h	2h	1d	1-2d	7d	30d
การให้บริการระบบบริหารสินทรัพย์ (AMS)	unacceptable	7h	4h	1d	1-2d	7d	30d
การให้บริการระบบ DMSc QR Code	medium	1d	7h	1d	1-2d	7d	30d
การให้บริการระบบสืบค้นหมายเลขโทรศัพท์ออนไลน์ (DMSc Phone)	medium	1d	7h	1d	1-2d	7d	30d
การให้บริการระบบสารบรรณอิเล็กทรอนิกส์ (e-Saraban)	medium	6h	3h	1d	1-2d	7d	30d
ระบบจัดการองค์ความรู้ (KMIS)	accept	7d	7d	1d	1-2d	7d	30d
ระบบ GLP Doc	accept	7d	7d	1d	7d	14d	30d

กระบวนการหลัก/กิจกรรมสำคัญ	MTPD	MTPD	RTO	RPO	ระยะเวลาของการตอบสนองต่อเหตุการณ์		
					ระยะสั้น	ระยะกลาง	ระยะยาว
งานบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย	unacceptable	3h	2h	-	1-2d	7d	30d
บริการระบบเครือข่ายคอมพิวเตอร์	medium	4h	2h	-	1-2d	7d	30d
งานบริหารจัดการสมาชิกเครือข่าย	unacceptable	3h	2h	1d	1-2d	7d	30d
ระบบสารสนเทศทรัพยากรบุคคลระดับกรม (DPIS)	unacceptable	6h	4h	1d	1-2d	7d	30d
ระบบสนับสนุนพระราชบัญญัติเชื้อโรคและพิษจากสัตว์ออนไลน์	unacceptable	6h	4h	1d	1-2d	7d	30d
ระบบแจ้งเงินเดือนและหักภาษี ณ ที่จ่ายออนไลน์ (Payslip and Tax)	unacceptable	6h	4h	1d	1-2d	7d	30d
การให้บริการระบบ DMSc Data Center	unacceptable	6h	4h	1d	1-2d	7d	30d
การให้บริการระบบการจัดซื้อจัดจ้าง (e-Procurement)	unacceptable	6h	4h	1d	1-2d	7d	30d
การให้บริการระบบจัดการเอกสารอิเล็กทรอนิกส์(SmartDI)	unacceptable	6h	3h	1d	7d	7d	30d
การให้บริการระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus)	unacceptable	7h	4h	1d	7d	7d	30d

กระบวนการหลัก/กิจกรรมสำคัญ	MTPD	MTPD	RTO	RPO	ระยะเวลาของการตอบสนองต่อเหตุการณ์		
					ระยะสั้น	ระยะกลาง	ระยะยาว
การให้บริการระบบยานพาหนะออนไลน์ (Vehicle Online)	unacceptable	6h	3h	1d	7d	7d	30d
Dmsc Data Catalog	medium	10h	4h	1d	7d	7d	30d
การให้บริการระบบสารสนเทศ Co-lab2	medium	7h	4h	1d	7d	7d	30d
ระบบบริการช่วยเหลือผู้ใช้งาน(HelpDesk)	medium	7h	3h	1d	1-2d	7d	30d
การให้บริการระบบกรมวิทย์ With You	medium	7h	3h	1d	1-2d	7d	30d

สำหรับกระบวนการอื่น ๆ ที่ประเมินแล้ว อาจไม่ได้รับผลกระทบต่อกรมวิทยาศาสตร์การแพทย์มาก หรือมีความยืดหยุ่น สามารถชะลอการดำเนินงานและให้บริการได้ ผู้บริหารของหน่วยงานประเมินความจำเป็นและเหมาะสมโดยกระบวนงานที่ประเมินผลกระทบระดับกลาง (Medium) ให้ทำการสำรองข้อมูลไว้ ณ ศูนย์สำรองข้อมูล (ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี ทั้งนี้ หากมีความจำเป็น ให้ปฏิบัติตามแนวทางการบริหารความต่อเนื่องเช่นเดียวกับกระบวนการหลัก

การประมาณระยะเวลาที่ระบบหยุดชะงัก (Estimated Downtime**)** กรมวิทยาศาสตร์การแพทย์ได้จำแนกประเภทของระยะเวลาที่ระบบหยุดชะงัก ดังนี้

- ระยะเวลานานที่สุดที่ยอมให้การปฏิบัติงานทางธุรกิจหยุดชะงัก **(Maximum Tolerable Period Disruption: MTPD)** หมายถึง ช่วงภาวะฉุกเฉินที่องค์กรต้องรีบเร่งแก้ไขด้วยการใช้บุคคล/เครื่องมือ/วัสดุอุปกรณ์/สถานที่/สิ่งใด ๆ มาทดแทนเพื่อระงับการหยุดชะงัก และทำให้องค์กรสามารถดำเนินงานหรือให้บริการต่อไปได้ในภาวะปกติ แต่อาจยังไม่กลับสู่การดำเนินงานตามปกติ
- ความต่อเนื่องทางธุรกิจขั้นต่ำสุด **(Minimum Business Continuity Objective: MBCO)** หมายถึง ระดับต่ำสุดของการบริการ และ/หรือ ผลิตภัณฑ์ที่กรมวิทยาศาสตร์การแพทย์ยอมรับ โดยยังคงสามารถดำเนินงานได้ในระหว่างเกิดการหยุดชะงัก
- ระยะเวลาที่สามารถกู้คืนระบบให้สามารถใช้งานได้ **(Recovery Time Objective: RTO)** หมายถึง ระยะเวลาที่องค์กรยอมรับได้ในการกู้คืนระบบในกรณีที่เกิดเหตุฉุกเฉินขึ้น ซึ่งเป็นค่าที่ถูกกำหนดโดยเจ้าของระบบ ต้องให้ผู้บริหารระดับสูงรับรู้ และยอมรับในค่า RTO ที่ถูกกำหนดขึ้น
- จุดที่ยอมรับให้ข้อมูลสูญหายได้ **(Recovery Point Objective: RPO)** หมายถึง การกำหนดว่ายอมให้ข้อมูลสูญหายได้นานเท่าใดโดยจะไม่ส่งผลเสียหายต่อการดำเนินงาน หรือทำให้การปฏิบัติงานขาดความต่อเนื่อง/เสียหายน้อยที่สุด

ที่มา: http://www.uih.co.th/knowledge/view/406#sthash.nwOLnlS9.dpuf
แผนการบริหารความต่อเนื่องทางธุรกิจของการทางพิเศษแห่งประเทศไทย
(Business Continuity Plan: BCP)

การวิเคราะห์เพื่อกำหนดความต้องการทรัพยากรที่สำคัญ แบ่งออกเป็น 4 ด้าน ดังนี้

1. **ความต้องการด้านสถานที่ปฏิบัติงานสำรอง (Working Space Requirement)** ดังตารางที่ 4

ตารางที่ 4 การระบุพื้นที่การปฏิบัติงานสำรอง

ประเภททรัพยากร	สถานที่	4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
พื้นที่ปฏิบัติงานสำรอง	สถานที่ที่สะดวกในการปฏิบัติงาน	16 ตร.ม.	16 ตร.ม.	16 ตร.ม.	30 ตร.ม	30 ตร.ม

2. **ความต้องการด้านวัสดุอุปกรณ์ (Equipment & Supplies Requirement)** ดังตารางที่ 5

ตารางที่ 5 การระบุจำนวนวัสดุอุปกรณ์

ประเภททรัพยากร	แหล่งที่มา	4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
เครื่องคอมพิวเตอร์แบบพกพา	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	4 เครื่อง	4 เครื่อง	4 เครื่อง	8 เครื่อง	8 เครื่อง
คอมพิวเตอร์แม่ข่ายพร้อมโปรแกรมที่จำเป็น	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	2 ชุด	2 ชุด	2 ชุด	2 ชุด	2 ชุด
อุปกรณ์กระจายสัญญาณพร้อมสายสัญญาณเครือข่าย	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	2 ชุด	2 ชุด	2 ชุด	2 ชุด	2 ชุด
อุปกรณ์ป้องกันการบุกรุกเครือข่าย/router	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	1 ชุด	1 ชุด	1 ชุด	1 ชุด	1 ชุด
โทรศัพท์เคลื่อนที่ตามสิทธิที่ได้รับการจัดสรร	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง	1 เครื่อง
ปลั๊กราง	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	3 ตัว	3 ตัว	3 ตัว	3 ตัว	5 ตัว
Projector Portable	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	1 ตัว	1 ตัว	1 ตัว	1 ตัว	1 ตัว
External hard disk	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	2 ตัว	2 ตัว	2 ตัว	2 ตัว	2 ตัว
Thumb drive	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	1 ตัว	1 ตัว	1 ตัว	1 ตัว	1 ตัว

3. **ความต้องการด้านเทคโนโลยีสารสนเทศและข้อมูล (IT & Information Requirement)**
ดังตารางที่ 6

ตารางที่ 6 การระบุความต้องการด้านเทคโนโลยี

ประเภททรัพยากร	แหล่งที่มา	4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
E-mail	สำนักงานรัฐบาลอิเล็กทรอนิกส์	✓	✓	✓	✓	✓
ระบบงานสารบรรณเชื่อมโยง	สำนักปลัดกระทรวงสาธารณสุข	✓	✓	✓	✓	✓
ระบบ NSW	กระทรวงดิจิทัลฯ		✓	✓	✓	✓
ระบบ iLab+	กรมวิทยาศาสตร์การแพทย์	✓	✓	✓	✓	✓
e-GP (ระบบจัดซื้อจัดจ้าง)	กรมบัญชีกลาง	✓	✓	✓	✓	✓
GFMIS (ระบบเบิกจ่ายเงิน)	กรมบัญชีกลาง	✓	✓	✓	✓	✓

4. **ความต้องการด้านบุคลากรสำหรับความต่อเนื่องเพื่อปฏิบัติงาน (Personnel Requirement)**
ดังตารางที่ 7

ตารางที่ 7 การระบุจำนวนบุคลากรหลักที่จำเป็น

ประเภททรัพยากร	4 ชั่วโมง	1 วัน	1 สัปดาห์	2 สัปดาห์	1 เดือน
จำนวนบุคลากรปฏิบัติงานที่ สำนักงาน/สถานที่ปฏิบัติงานสำรอง	5 คน	5 คน	10 คน	20 คน	20 คน

หมายเหตุ ไม่รวมผู้บริหารระดับสูง

กระบวนการแจ้งเหตุฉุกเฉิน Call Tree

กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกในคณะบริหารความต่อเนื่องและทีมงานบริหารความต่อเนื่องที่เกี่ยวข้องตามรายชื่อที่ปรากฏในตารางข้อมูลรายชื่อ โดยมีวัตถุประสงค์เพื่อการบริหารจัดการขั้นตอนในการติดต่อบุคลากรภายหลังจากมีการประกาศเหตุการณ์ฉุกเฉินหรือภาวะวิกฤตของกรมวิทยาศาสตร์การแพทย์ จุดเริ่มต้นของกระบวนการ Call Tree จะเริ่มจากผู้ประสบเหตุรายงานต่อเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร หรือ ผู้ดูแลระบบ จากนั้นผู้ดูแลระบบแจ้งให้ผู้ประสานงานคณะบริหารความต่อเนื่อง รับทราบและรายงานต่อ หัวหน้าคณะบริหารความต่อเนื่อง โดยหัวหน้าคณะบริหารความต่อเนื่อง สังการณ์ผู้ประสานงานคณะบริหารความต่อเนื่อง โดยผู้ประสานงานฯ จะแจ้งให้หัวหน้าทีมบริหารความต่อเนื่องรับทราบ เหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง ตามสายงานการบังคับบัญชาของแต่ละสายงานรวมไปถึงแจ้งข้อสังการณ์ไปยังผู้ดูแลระบบเพื่อเตรียมความพร้อม จากนั้นหัวหน้ากลุ่มงานมีหน้าที่แจ้งไปยังบุคลากรภายใต้การบังคับบัญชาของตนรับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่องของหน่วยงานที่ได้รับผลกระทบ ตามรายชื่อและช่องทางติดต่อสื่อสารที่ได้ระบุในแผนความต่อเนื่อง

ในกรณีที่ไม่สามารถติดต่อหัวหน้าทีมได้ ให้ติดต่อไปยังบุคลากรสำรอง โดยพิจารณา

1.สภาวะไม่วิกฤต ให้ปฏิบัติดังนี้

- ถ้าเหตุการณ์เกิดขึ้นในเวลาราชการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของสำนักงานเป็นช่องทางแรก
- ถ้าเหตุการณ์เกิดขึ้นนอกเวลาราชการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
- ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบ ดังต่อไปนี้:

1. สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและการประกาศใช้แผนความต่อเนื่อง
2. เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับผู้บริหารของหน่วยงานทีมงานบริหารความต่อเนื่อง
3. ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่องต่อไป เช่น สถานที่รวมพลในกรณีที่มีการย้ายสถานที่ทำการ
4. รวบรวมหลักฐานเพื่อใช้ในการสืบคดี เช่น เครื่องที่ถูก ransomware, traffic log network, log windows, log database ของระบบงาน เพื่อรายงานต่อหน่วยงานกำกับดูแล

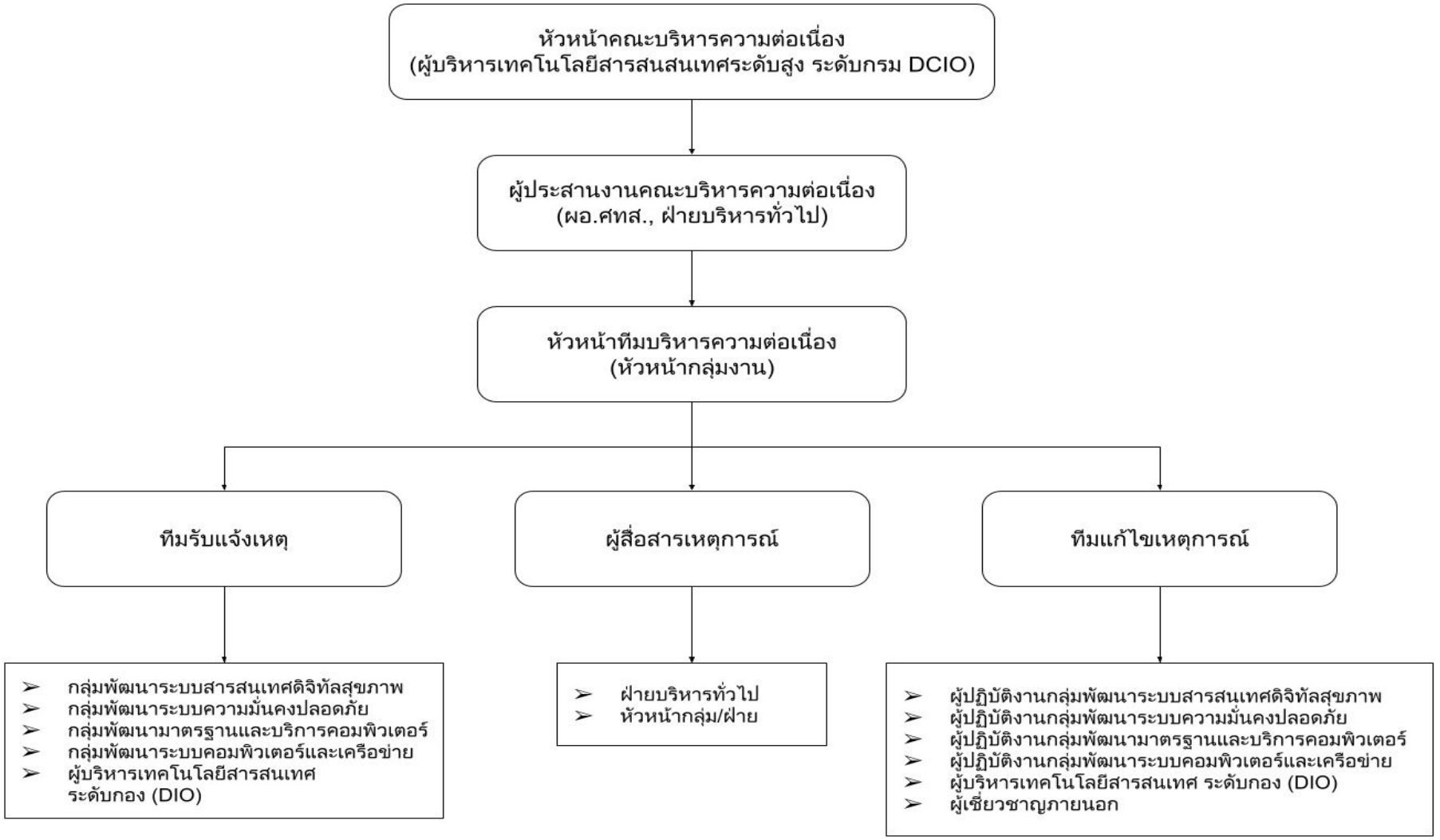
2.ในสภาวะวิกฤต ให้ปฏิบัติดังนี้

- ถ้าเหตุการณ์เกิดขึ้นในเวลาราชการ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์ของสำนักงานเป็นช่องทางแรก
- ถ้าเหตุการณ์เกิดขึ้นนอกเวลาราชการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการติดต่อบุคลากรหลักโดยติดต่อผ่านเบอร์โทรศัพท์มือถือเป็นช่องทางแรก
- ถ้าสามารถติดต่อบุคลากรหลักได้ให้แจ้งข้อมูลแก่บุคลากรหลักของหน่วยงานทราบ ดังต่อไปนี้:

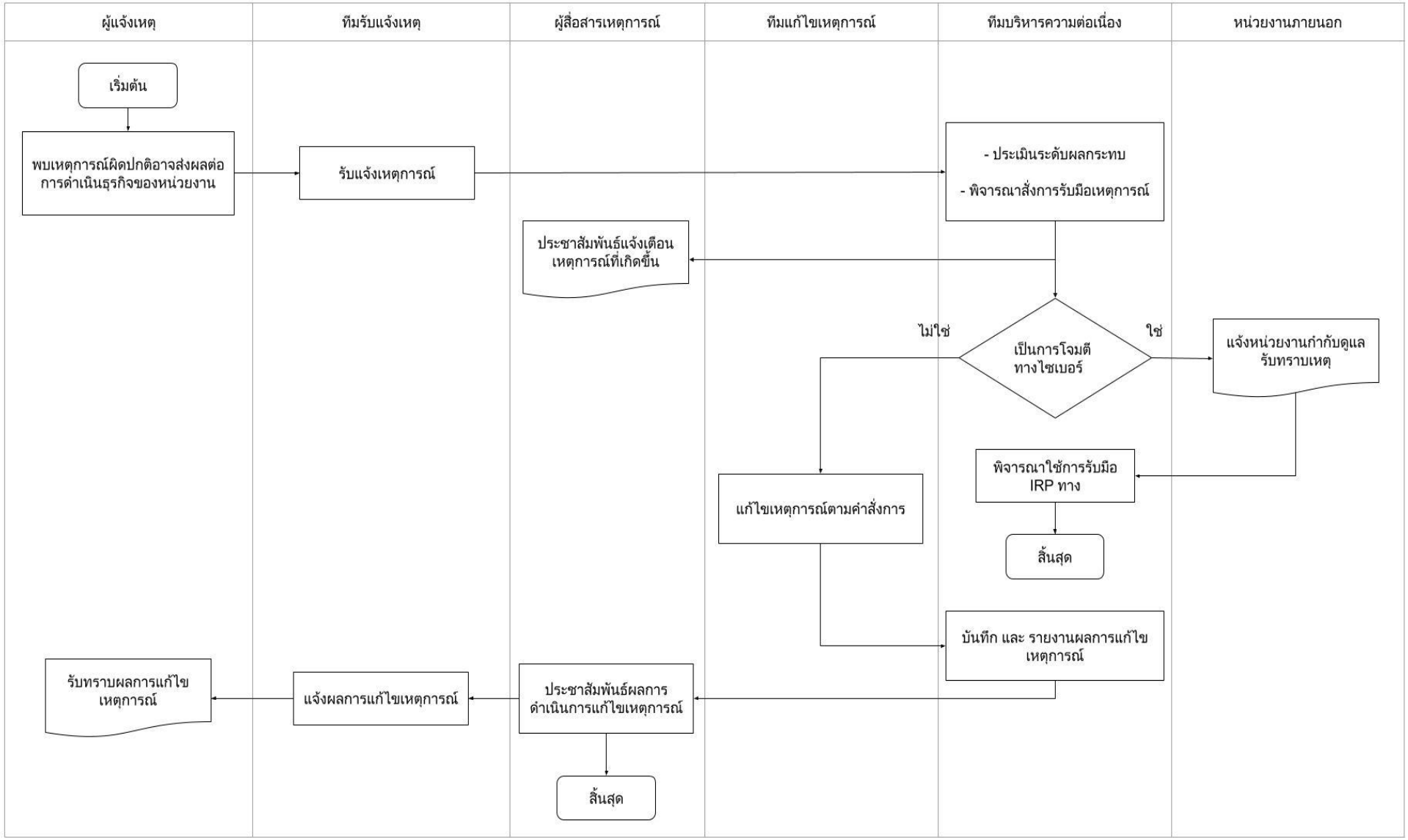
1. สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินและรายงานต่อหน่วยงานกำกับดูแล
   1.1 ศูนย์ประสานการรักษาความมั่นคงปลอดภัยไซเบอร์ด้านสาธารณสุข (Health CERT)
   โทร 02 590 1201
   1.2 สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ
   โทร. 02-502-7831 ,02-502-7835, thnca@ncsa.or.th
   1.3 สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล
   โทร. 02-1421033, 02-1416993, saraban@pdpc.or.th
2. เวลาและสถานที่สำหรับการนัดประชุมเร่งด่วนของหน่วยงาน สำหรับผู้บริหารของหน่วยงานและทีมงานบริหารความต่อเนื่อง
3. ขั้นตอนการปฏิบัติงาน เพื่อบริหารความต่อเนื่อง
4. รวบรวมหลักฐานเพื่อใช้ในการสืบคดี เช่น เครื่องที่ถูก ransomware, traffic log network, log windows, log database ของระบบงาน เพื่อรายงานต่อหน่วยงานกำกับดูแล

ภายหลังจากได้รับการตอบรับจากบุคลากรหลักครบถ้วนตามผังการติดต่อ (Call Tree) หัวหน้าทีมบริหารความต่อเนื่องมีหน้าที่โทรกลับไปแจ้งยังผู้ประสานงานคณะบริหารความต่อเนื่อง เพื่อรวบรวมสรุปความพร้อมของหน่วยงานในการบริหารความต่อเนื่อง รวมทั้งความปลอดภัยในชีวิตและทรัพย์สินของหน่วยงานและเจ้าหน้าที่ทั้งหมดในหน่วยงาน ทีมบริหารความต่อเนื่องมีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อให้เป็นปัจจุบันอยู่ตลอดเวลา เพื่อให้กระบวนการติดต่อเจ้าหน้าที่ภายในหน่วยงานสามารถดำเนินได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่ เกิดเหตุการณ์ฉุกเฉินและมีการประกาศใช้แผนความต่อเนื่อง

แผนผังกระบวนการแจ้งเหตุฉุกเฉิน Call Tree



ขั้นตอนการเผชิญเหตุการณ์ผิดปกติที่อาจส่งผลต่อการงานของกรม



ขั้นตอนการบริหารความต่อเนื่องและกอบกู้กระบวนการ

วันที่ 1 (ภายใน 24 ชั่วโมง) การตอบสนองต่อเหตุการณ์ทันที

ในการปฏิบัติการใด ๆ ให้บุคลากรของสำนักต่าง ๆ คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่น และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด (ใส่เครื่องหมาย ✓ ในช่องดำเนินการแล้วเสร็จ)

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
1. แจ้งเหตุฉุกเฉิน วิกฤต ตามกระบวนการ call tree ให้กับหัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์	หัวหน้าคณะบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
2. จัดประชุมทีมบริหารต่อเนื่อง เพื่อประเมินความเสียหาย ผลกระทบต่อการดำเนินงาน การให้บริการ และทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง	ทีมประสานงาน/ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
3. ทบทวนกระบวนงานที่มีความเร่งด่วน หรือส่งผลกระทบอย่างสูงหากไม่ดำเนินการ และพิจารณาว่าจำเป็นต้องทำให้ระบบดำเนินงานได้อย่างต่อเนื่อง หรือปฏิบัติด้วยมือ (Manual Processing) ได้	ทีมประสานงาน/ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
4.ดำเนินการกู้คืนระบบเทคโนโลยีสารสนเทศที่สำรองข้อมูลไว้ ณ ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี ขึ้นมาใช้งานหรือย้ายระบบที่สำคัญขึ้นให้บริการ ณ ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี	ทีมผู้ดูแลระบบ	
5. ระบุและสรุปรายชื่อบุคลากรในหน่วยงาน ที่ได้รับผลกระทบจากเหตุการณ์	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
6. รายงานหัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์ทราบโดยครอบคลุมประเด็นดังนี้ • จำนวนและรายชื่อบุคลากรที่ได้รับผลกระทบจากเหตุการณ์ • ความเสียหายและผลกระทบต่อการดำเนินงานและการให้บริการ • ทรัพยากรสำคัญที่ต้องใช้ในการบริหารความต่อเนื่อง • กระบวนงานที่มีความเร่งด่วนและส่งผลกระทบอย่างสูงหากไม่ดำเนินการ และจำเป็นต้องดำเนินงานหรือปฏิบัติงานด้วยมือ • รายงานผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม เพื่อรับทราบและพิจารณาอนุมัติดำเนินการปฏิบัติงานและกิจกรรมต่าง ๆ	ทีมประสานงาน/หัวหน้าทีมบริหารความต่อเนื่องของสำนักต่าง ๆ	
7. สื่อสารและรายงานสถานการณ์แก่บุคลากรในกรมให้ทราบ และหากมีผลกระทบถึงการให้บริการประชาชนดำเนินการสื่อสารประชาสัมพันธ์/ แถลงข่าว ให้ประชาชนผู้เกี่ยวข้องตามเนื้อหาและข้อความที่ได้รับการพิจารณาและเห็นชอบจากคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์แล้ว	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
8. ประเมินและระบุกระบวนการหลัก และงานเร่งด่วนที่จำเป็นต้องดำเนินการให้แล้วเสร็จ ภายใน 1 – 5 วันข้างหน้า	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
9. ประเมินศักยภาพและความสามารถของกรม ในการดำเนินงานเร่งด่วนในข้อ 7 ภายใต้ข้อจำกัดและสภาวะวิกฤตพร้อมระบุทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่องตามแผนการจัดหาทรัพยากร	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
10. รายงานความคืบหน้าให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบ และขออนุมัติดำเนินการแจ้ง NCERT ในกรณีที่เป็นภัยคุกคามทางไซเบอร์	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
11. ติดต่อและประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่ ● สถานที่ปฏิบัติงานสำรอง ● วัสดุอุปกรณ์ที่สำคัญ ● เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ● บุคลากรหลัก ● ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
12. บันทึก และทบทวนกิจกรรม งานต่าง ๆ ที่ทีมบริหารความต่อเนื่องของสำนักต่าง ๆ ต้องดำเนินการ (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลา) อย่างสม่ำเสมอ	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
13. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการ สำหรับในวันถัดไป ให้กับบุคลกรหลักในกรม เพื่อรับทราบและดำเนินการ เช่น แจ้งวัน เวลา และสถานที่ปฏิบัติงานสำรอง	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
14. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์อย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

วันที่ 1-2 การตอบสนองในระยะสั้น

ในการปฏิบัติการใด ๆ ให้บุคลากรของสำนักต่าง ๆ คำนึงถึงความปลอดภัยในชีวิตของตนเองและบุคลากรอื่น และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
15. ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็นและระยะเวลาที่ต้องใช้ในการกอบกู้คืน	ทีมประสานงาน/ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
16. ตรวจสอบกับหน่วยงาน ความพร้อมและข้อจำกัดในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่ ● สถานที่ปฏิบัติงานสำรอง ● วัสดุอุปกรณ์ที่สำคัญ ● เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ● บุคลากรหลัก ● ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
17. รายงานหัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์ในเรื่องความพร้อม ข้อจำกัด และข้อเสนอแนะในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
18. ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่ ● สถานที่ปฏิบัติงานสำรอง ● วัสดุอุปกรณ์ที่สำคัญ ● เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ● บุคลากรหลัก ● ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	ทีมประสานงาน/ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
19. ดำเนินงานและให้บริการ ภายใต้ทรัพยากรที่จัดหา เพื่อบริหารความต่อเนื่อง ● สถานที่ปฏิบัติงานสำรอง ● วัสดุอุปกรณ์ที่สำคัญ ● เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ ● บุคลากรหลัก ● ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
20. ดำเนินการกอบกู้และจัดหาข้อมูลและรายงานต่าง ๆ ที่จำเป็นต้องใช้ในการดำเนินงานและให้บริการพร้อมให้ความร่วมมือกับ NCERT ในกรณีที่เป็นภัยคุกคามทางไซเบอร์	ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร	
21.แจ้งสถานการณ์และแนวทางในการบริหารความต่อเนื่องแก่หน่วยงาน ผู้รับบริการ ที่ได้รับผลกระทบ	ทีมประสานงาน/ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
22. บันทึก และทบทวนกิจกรรมงานต่าง ๆ ที่ทีมงานบริหารความต่อเนื่องของหน่วยงานดำเนินการ (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลา) อย่างสม่ำเสมอ	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
23. แจ้งสรุปสถานการณ์และขั้นตอนการดำเนินการต่อไป สำหรับในวันถัดไป ให้กับบุคลากรในสำนัก	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
24. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์อย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

วันที่ 8 การตอบสนองระยะกลาง (1 สัปดาห์)

ในการปฏิบัติการใด ๆ ให้บุคลากรของสำนักต่าง ๆ คำนึงถึงความปลอดภัยในชีวิตขอตนเองและบุคลากรอื่น ๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
25. ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความจำเป็น ระยะเวลาที่ต้องใช้ในการกอบกู้คืน	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
26. ระบุทรัพยากรที่จำเป็นต้องใช้ เพื่อดำเนินงานและใช้บริการตามปกติ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
27. รายงานหัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์ในเรื่องสถานภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบและทรัพยากรที่จำเป็นต้องใช้เพ่อดำเนินงานและให้บริการตามปกติ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
28. ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ • สถานที่ปฏิบัติงานสำรอง • วัสดุอุปกรณ์ที่สำคัญ • เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ • บุคลากรหลัก • ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
29. แจ้งสรุปสถานการณ์และการเตรียมความพร้อมด้านทรัพยากรต่าง ๆ เพื่อดำเนินงานและให้บริการตามปกติ ให้กับบุคลากรในสำนัก	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
30. บันทึกและทบทวนกิจกรรมและงานต่าง ๆ ของทีมงานบริหารความต่อเนื่องของสำนัก (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลาอย่างสม่ำเสมอ	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
31. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริการความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์อย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

การตอบสนองระยะกลาง (2 สัปดาห์)

ในการปฏิบัติการใด ๆ ให้บุคลากรของสำนักต่าง ๆ คำนึงถึงความปลอดภัยในชีวิตขอตนเองและบุคลากรอื่น ๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด

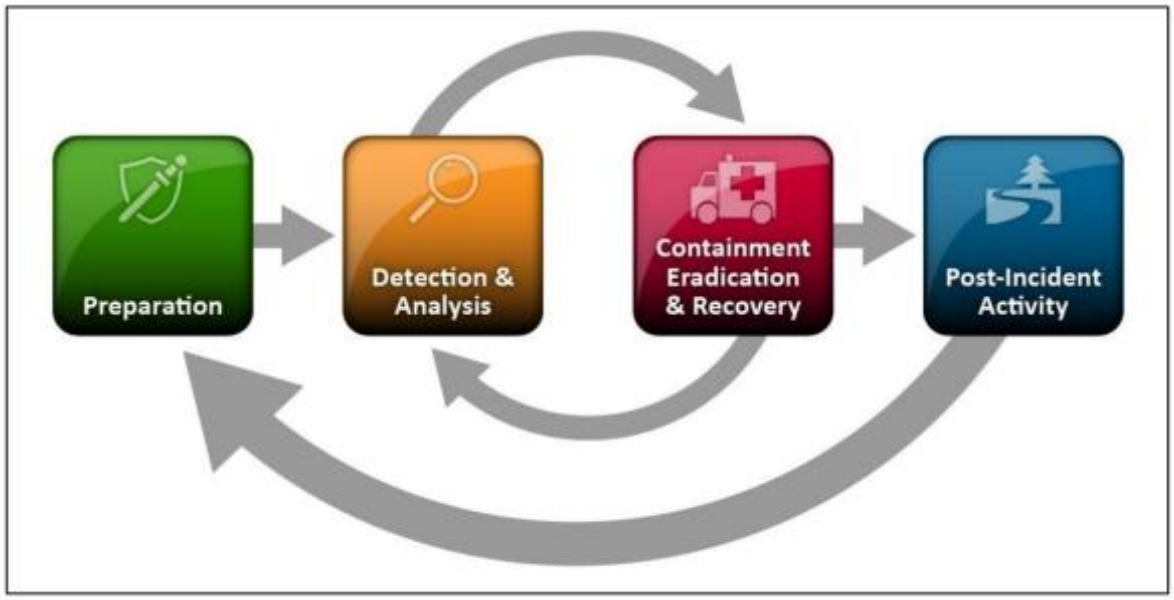
ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
32. ติดตามสถานะภาพการกอบกู้คืนมาของทรัพยากรที่ได้รับผลกระทบ และประเมินความสามารถในการกลับไป ใช้ระบบหลักตามปกติ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
33. ระบุทรัพยากรที่จำเป็นต้องใช้ เพื่อดำเนินงานและใช้บริการตามปกติ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
34. รายงานหัวหน้าคณะบริหารความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์ในเรื่องสถานภาพการกลับไปใช้ระบบหลักาของกรม ทรัพยากรที่ได้รับผลกระทบและทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
35. ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้เพื่อดำเนินงานและให้บริการตามปกติ • สถานที่ปฏิบัติงานสำรอง • วัสดุอุปกรณ์ที่สำคัญ • เทคโนโลยีสารสนเทศและข้อมูลที่สำคัญ • บุคลากรหลัก • ผู้รับบริการ/ผู้มีส่วนได้ส่วนเสีย	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
36. แจ้งสรุปสถานการณ์และการเตรียมความพร้อมด้านทรัพยากรต่าง ๆ เพื่อดำเนินงานและให้บริการตามปกติ ให้กับบุคลากรในกรม	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
37. บันทึกและทบทวนกิจกรรมและงานต่าง ๆ ของทีมงานบริหารความต่อเนื่องของสำนัก (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลาอย่างสม่ำเสมอ	ทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
38. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริการความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์อย่างสม่ำเสมอ ตามที่ได้กำหนดไว้	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

การตอบสนองระยะกลาง (1 เดือน)

ในการปฏิบัติการใด ๆ ให้บุคลากรของสำนักต่าง ๆ คำนึงถึงความปลอดภัยในชีวิตขอตนเองและบุคลากรอื่น ๆ และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่กำหนดขึ้นโดยกรมวิทยาศาสตร์การแพทย์อย่างเคร่งครัด

ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการแล้วเสร็จ
39. ทดสอบการนำระบบคืนสู่สภาวะปกติ	ผู้ดูแลระบบ (System Admin/DBA)/ผู้เกี่ยวข้องดำเนินการแก้ไขทางเทคนิค	
40. ติดตามผลการทดสอบ	หัวหน้าฝ่ายพัฒนาระบบคอมพิวเตอร์/หัวหน้าฝ่ายพัฒนาระบบสารสนเทศ	
41. บันทึกและทบทวนกิจกรรมและงานต่าง ๆ ของทีมงานบริหารความต่อเนื่องของสำนัก (พร้อมระบุรายละเอียดผู้ดำเนินการ และเวลาอย่างสม่ำเสมอ	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	
42. รายงานความคืบหน้าให้แก่หัวหน้าคณะบริการความต่อเนื่องของกรมวิทยาศาสตร์การแพทย์	หัวหน้าทีมบริหารความต่อเนื่องของหน่วยงานต่าง ๆ	

<u>กรณีภัยคุกคามทางไซเบอร์มีขั้นการตรวจจับและวิเคราะห์ภัยคุกคามทางไซเบอร์ (Detection and Analysis)</u> ดังนี้



แผนจัดการดำเนินธุรกิจอย่างต่อเนื่อง

สถานการณ์วิกฤต (Critical Situation):	นิยาม หรือ ลักษณะ
ระบบงานภายในกรมวิทยาศาสตร์การแพทย์ไม่สามารถใช้งานได้ก่อให้เกิดปัญหาการปฏิบัติงานล่าช้าหรือหยุดชะงัก	ระบบงานภายในกรมวิทยาศาสตร์การแพทย์ที่สำคัญ ซึ่งใช้ระบบคอมพิวเตอร์ในการประมวลผลไม่สามารถใช้งานได้ มีผลให้การดำเนินการของกรม ในส่วนที่ต้องใช้ระบบงานนั้นในการปฏิบัติงานหรือให้บริการต้องหยุดชะงัก
วิกฤตการณ์ (Crisis)	**นิยาม หรือ ลักษณะ**
1. เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้	เครื่องแม่ข่ายหลักไม่สามารถให้บริการได้เนื่องจากชำรุด/ภัยพิบัติทางธรรมชาติ /โรคระบาด/ ชุมนุมประท้วง/จลาจล ทำให้ระบบงานทุกระบบในส่วนงานสารสนเทศ ที่ใช้ระบบคอมพิวเตอร์ในการประมวลผลและเชื่อมต่อกับเครือข่ายคอมพิวเตอร์ ไม่สามารถใช้งานได้ มีผลให้การดำเนินการของกรมวิทยาศาสตร์การแพทย์ที่ต้องใช้ระบบสารสนเทศในการปฏิบัติงานหรือให้บริการต้อง หยุดชะงัก
2. ระบบเครือข่ายคอมพิวเตอร์และการสื่อสารข้อมูล ไม่สามารถใช้งานได้	ระบบเครือข่ายคอมพิวเตอร์ระหว่างอาคารสำนักงาน ไม่สามารถใช้งานได้เนื่องจากอุปกรณ์ในระบบเครือข่ายและ/หรือซอฟต์แวร์ในระบบขัดข้องหรือระบบเครือข่ายถูกบุกรุก หรือสายสัญญาณสื่อสารเสียหายทำให้การใช้งานสื่อสารข้อมูลของระบบงานต่าง ๆ ในส่วนงานสารสนเทศ หยุดชะงัก
3. ระบบสารสนเทศ ของกรมวิทยาศาสตร์การแพทย์ ไม่สามารถใช้งานได้ - ระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus) - ระบบใบเสร็จอิเล็กทรอนิกส์ (DMSc Payment) - การให้บริการระบบกรมวิทย์ With You - ระบบบริหารจัดการครุภัณฑ์ (AMS) -ระบบสารบรรณ (Contents)	ระบบสารสนเทศ ของกรมวิทยาศาสตร์ การแพทย์ไม่สามารถใช้งานได้เนื่องจากเครื่องแม่ข่ายและอุปกรณ์ขัดข้องหรือโปรแกรมระบบงานขัดข้อง หรือฐานข้อมูลขัดข้องมีผลให้การปฏิบัติงาน ในส่วนที่ต้องใช้ระบบงานในการปฏิบัติงานหรือให้บริการต้องหยุดชะงัก

วิกฤตการณ์ (Crisis)	นิยาม หรือ ลักษณะ
4. ระบบสารสนเทศถูกโจมตีทางไซเบอร์ - ระบบใบเสร็จอิเล็กทรอนิกส์ (DMSc Payment) - ระบบการเงินการคลัง (Fin-AD) - ระบบจัดซื้อจัดจ้าง (e-procurement) - ระบบสารบรรณ (Contents) - ระบบ GLP Document - ระบบ Website กรมวิทยาศาสตร์การแพทย์ และระดับหน่วยงานภายใน - ระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus) - ระบบกรมวิทย์ with you - ระบบบริหารจัดการครุภัณฑ์ (AMS)	ระบบสารสนเทศ ของกรมวิทยาศาสตร์ การแพทย์ ไม่สามารถใช้งานได้เนื่องจากถูกโจมตีโดยผู้ไม่ประสงค์ดี (Hacker) ในส่วนที่ต้องใช้ระบบงานในการปฏิบัติงานหรือให้บริการต้องหยุดชะงัก

รายละเอียดแผนการจัดการดำเนินธุรกิจอย่างต่อเนื่อง

1. วิกฤตการณ์: เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้ /ชำรุด

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้เนื่องจากเกิดอุบัติเหตุเช่นไฟไหม้ หรือเกิด อุบัติภัย เช่น แผ่นดินไหวหรือน้ำท่วม หรือเกิด วินาศกรรม จลาจล ทำให้ระบบงานสารสนเทศบางระบบ ไม่สามารถใช้งานได้ หรือไม่สามารถให้บริการได้ นาน 24 ชั่วโมง	- ผู้ดูแลระบบเตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองให้สามารถใช้ระบบงานได้ภายใน 24 ชั่วโมง - ประสานงานกับทุกหน่วยงานที่ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรอง

1.1 แผนรับมือสถานะการณ์ฉุกเฉิน (Incident Response Plan)

***<u>กรณี</u>* เครื่องคอมพิวเตอร์แม่ข่ายชำรุด และเครื่องคอมพิวเตอร์แม่ข่ายระบบสมาชิกเครือข่าย (Domain Active Directory) ชำรุด**

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง	10 นาที
2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์หลักและรายงานความเสียหายให้ทราบพร้อมขอปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง หรือเครื่องคอมพิวเตอร์แม่ข่ายสำรอง ประสานงานบริหารทั่วไปประชาสัมพันธ์สถานการณ์	30 นาที
3. ผู้ดูแลระบบเตรียมระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์สำรองเพื่อให้สามารถใช้งานได้และแจ้งทีมเพื่อทดสอบระบบสารสนเทศ	2 ชั่วโมง
4. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 3	20 นาที
รวม RTO	**3 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบมีหน้าที่ตรวจสอบความเสียหายระบบคอมพิวเตอร์ ระบบงานระบบเครือข่าย ที่ศูนย์คอมพิวเตอร์หลัก เตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง ประสานงานกับผู้ใช้ระบบงาน และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

ผู้ใช้ระบบงาน (หน่วยงานต่าง ๆ) เตรียมความพร้อมปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรองหรือเครื่องคอมพิวเตอร์แม่ข่ายสำรอง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

โทรศัพท์ ยานพาหนะ(ขนย้ายพนักงานและอุปกรณ์) เครื่องคอมพิวเตอร์แม่ข่ายสำรอง ระบบสื่อสารข้อมูล

1.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถดำเนินงานต่อเนื่องไม่หยุดชะงักภายใต้ภาวะปกติ แต่ยังไม่กลับสู่การดำเนินการตามปกติ

- ปฏิบัติงานโดยใช้ระบบคอมพิวเตอร์สำรองที่ติดตั้ง ณ ศูนย์คอมพิวเตอร์สำรองทำงานทดแทน

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบดำเนินการตรวจสอบการใช้ระบบคอมพิวเตอร์สำรองโดยนำเข้าข้อมูลที่ได้สำรองไว้ล่าสุด	20 นาที
2. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ใช้ระบบงานทดสอบและตรวจสอบระบบงานจากการปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองหรือใช้เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และนำเข้าข้อมูลให้เป็นปัจจุบันมากที่สุด	15 นาที
3. ผู้ใช้ระบบงานปฏิบัติงาน/ให้บริการโดยใช้ระบบคอมพิวเตอร์ ณ ศูนย์คอมพิวเตอร์สำรอง โดยใช้เครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์อื่น ๆ ร่วมกัน	10 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	15 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**4 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดใช้งานระบบคอมพิวเตอร์สำรองและประสานงานกับผู้ใช้ระบบงานในการทดสอบระบบงาน และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

ผู้ใช้ระบบงานทดสอบและตรวจสอบความถูกต้องข้อมูล นาเข้าข้อมูลให้เป็นปัจจุบันและปฏิบัติงาน/ให้บริการโดยใช้ระบบคอมพิวเตอร์สำรอง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

1.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	**กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว**
การกอบกู้คืนห้องควบคุมเครือข่ายคอมพิวเตอร์และเครื่องแม่ข่ายหลักที่ไม่สามารถใช้งานได้เนื่องจากเกิดอุบัติเหตุเช่นไฟไหม้ หรือเกิด อุบัติภัย เช่น แผ่นดินไหวหรือน้ำท่วม หรือเกิด วินาศกรรม จลาจล ทำให้ระบบงานสารสนเทศบางระบบให้สามารถใช้งานได้เป็นปกติ	- สำรวจความเสียหายที่เกิดขึ้นเพิ่มเติม เพื่อจัดหาระบบคอมพิวเตอร์และระบบเครือข่ายพร้อมอุปกรณ์เพื่อติดตั้งทดแทนในส่วนที่เสียหาย - ติดตั้ง ทดสอบและตรวจสอบระบบงานที่ศูนย์คอมพิวเตอร์หลักให้พร้อมใช้งาน - ดำเนินการให้ผู้ใช้ระบบงานสามารถปฏิบัติงาน/ให้บริการได้ตามปกติ

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ดูแลระบบสำรวจความเสียหายที่เกิดขึ้นเพิ่มเติม และรายงานต่อผู้ประสานงานทีมบริหารความต่อเนื่อง (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อขออนุมัติดำเนินการจัดหาระบบคอมพิวเตอร์และระบบเครือข่ายพร้อมอุปกรณ์เพื่อติดตั้ง ทดแทนในส่วนที่เสียหาย ต่อหัวหน้าคณะบริหารความต่อเนื่อง (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)
2. ผู้ดูแลระบบ ดำเนินการติดตั้ง ระบบเครือข่ายคอมพิวเตอร์ และระบบสารสนเทศทุกระบบพร้อมทั้ง ทดสอบและตรวจสอบให้พร้อมใช้งาน
3. ผู้ดูแลระบบทำการสำรองข้อมูลจากศูนย์คอมพิวเตอร์สำรองมาที่ศูนย์คอมพิวเตอร์หลัก
4. ผู้ดูแลระบบ ประสานงานผู้ใช้ระบบงานทดสอบ ตรวจสอบความพร้อมและแจ้งกำหนดการการเปิดใช้ระบบที่ศูนย์คอมพิวเตอร์หลัก
5. ผู้ดูแลระบบ รายงานผู้บังคับบัญชาและขอเปิดใช้งานระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์หลัก
6. ผู้ประสานงานทีมบริหารความต่อเนื่อง (ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) รายงานและขออนุมัติเพื่อเปิดใช้ระบบงานที่ศูนย์คอมพิวเตอร์หลักและแจ้งผู้เกี่ยวข้อง ต่อหัวหน้าคณะบริหารความต่อเนื่อง (ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ดำเนินการจัดหาระบบคอมพิวเตอร์และระบบเครือข่ายพร้อมอุปกรณ์และซอฟต์แวร์เพื่อติดตั้ง ทดแทนในส่วนที่เสียหายและสำรองข้อมูลจากศูนย์คอมพิวเตอร์สำรองมาที่ศูนย์คอมพิวเตอร์หลักพร้อมทดสอบและประสานงานแจ้งผู้ใช้ระบบงาน

ผู้ใช้ระบบงานตรวจสอบการใช้งานร่วมกับผู้ดูแลระบบ

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายพร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

1.4 การซ้อมแผน

หลักการและแนวทางในการซ้อมแผน

ดำเนินการซ้อมแผนปีละ 1 ครั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคาร 1 ชั้น 3

กำหนดการฝึกซ้อม: เดือนมิถุนายน – กรกฎาคม ของทุกปี

2. วิกฤตการณ์: ระบบเครือข่ายคอมพิวเตอร์และการสื่อสารข้อมูลไม่สามารถใช้งานได้

2.1 แผนรับมือสถานะการณ์ฉุกเฉิน (Incident Response Plan)

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
ระบบเครือข่ายคอมพิวเตอร์และสื่อสารข้อมูล ไม่สามารถใช้งานได้เนื่องจากอุปกรณ์ในระบบเครือข่ายและ/หรือซอฟต์แวร์ในระบบขัดข้องหรือ ระบบเครือข่าย ถูกบุกรุก หรือสายสัญญาณสื่อสารเสียหาย นาน 4 ชั่วโมง (ยกเว้นวันหยุดราชการ)	-ตรวจสอบหาสาเหตุและประสานงานกับบริษัทที่ให้บริการบำรุงรักษาเพื่อซ่อมแซมแก้ไข - เตรียมความพร้อมในการใช้ระบบเครือข่ายสื่อสารสำรอง/อุปกรณ์เครือข่ายสำรอง - ประสานงานแจ้งผู้ใช้ระบบงานทราบ

<u>กรณี</u> อุปกรณ์เครือข่ายหลักชำรุด

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง	10 นาที
2.ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบเครือข่ายคอมพิวเตอร์	20 นาที
3. ผู้ดูแลระบบนำอุปกรณ์เครือข่ายหลักสำรองที่ดำเนินการตั้งค่าเริ่มต้นของอุปกรณ์เพื่อให้สามารถใช้งานได้กับระบบของกรมวิทยาศาสตร์ มาติดตั้ง	40 นาที
4.ย้ายสายสัญญาณจากอุปกรณ์เครือข่ายเดิมที่ชำรุด มาไว้ที่อุปกรณ์เครือข่ายสำรอง และทดสอบการเชื่อมต่อกับระบบต่าง ๆ ภายในระบบเครือข่าย ซึ่งจะสามารถใช้งานได้เพียง อาคาร 1 ITC zone อาคาร 2 อาคาร 4 อาคาร 8 อาคาร 9 อาคาร 9 ITC zone อาคาร 10 และ อาคาร 14 (port fiber optic ของอุปกรณ์มีจำนวนจำกัด 8 ช่อง)	40 นาที
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	10 นาที
รวม RTO	**2 ชั่วโมง**

***<u>กรณี</u>* สาย fiber optic ระหว่างกรมวิทยาศาสตร์การแพทย์กับสำนักงานปลัดกระทรวงสาธารณสุขขาด**

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้อง	10 นาที
2.ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบเครือข่ายคอมพิวเตอร์	25 นาที
3. ผู้ดูแลระบบดำเนินการตั้งค่าระบบเครือข่ายคอมพิวเตอร์ ให้ผู้ใช้งานสามารถใช้งานระบบ internet ได้จากสายสื่อสารข้อมูลเช่าของกรมและประสานขอสนับสนุน Public IP จากผู้ให้บริการสายสัญญาณเช่า	30 นาที
4.ผู้ดูแลระบบ ดำเนินการเปลี่ยนการตั้งค่า Public IP จากของสำนักงานปลัดกระทรวงสาธารณสุขมาเป็นของผู้ให้บริการสายสัญญาณเช่าตรวจสอบการใช้งานของระบบงานที่สำคัญ ได้แก่ iLABplus กรมวิทย์ With you Dmsc Payment ระบบงานสารบรรณ เว็บไซต์กรม	40 นาที
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	15 นาที
รวม RTO	**2 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ มีหน้าที่ตรวจสอบระบบเครือข่ายคอมพิวเตอร์และการสื่อสารข้อมูล ประสานงานกับบริษัทที่ให้บริการบำรุงรักษาหรือบริษัทผู้ให้บริการระบบเครือข่ายเพื่อแก้ไขปัญหา

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

โทรศัพท์ อุปกรณ์เครือข่ายสำรอง

2.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถดำเนินงานต่อเนื่องไม่หยุดชะงักภายใต้ภาวะปกติ แต่ยังไม่กลับสู่การดำเนินการตามปกติ

-ปฏิบัติงานโดยใช้อุปกรณ์เครือข่ายหลักสำรอง

- ปฏิบัติงานโดยใช้สายสื่อสารข้อมูลเช่า

กรณี อุปกรณ์เครือข่ายหลักชำรุด

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบดำเนินการเฝ้าระวังจากระบบเฝ้าระวังระบบเครือข่ายคอมพิวเตอร์ ตรวจสอบการทำงานของระบบเครือข่าย การเชื่อมต่อกับ DNS Firewall และระบบสารสนเทศ	1 ชั่วโมง
2. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ใช้ระบบงานทดสอบการใช้ระบบงานโดยประชาสัมพันธ์ผู้ปฏิบัติงานสามารถปฏิบัติงานได้ตามอาคาร อาคาร 1 ITC zone อาคาร 2 อาคาร 4 อาคาร 8 อาคาร 9 อาคาร 9 ITC zone อาคาร 10 และ อาคาร 14 เท่านั้น	1 ชั่วโมง
3. ฝ่ายสนับสนุนและบริการวิชาการจัดตั้งจุดบริการใช้งานคอมพิวเตอร์และเครือข่ายชั่วคราวสำหรับผู้ใช้งานอาคารที่ไม่สามารถใช้งานได้ (อาคาร 1 Zone อื่น) ชั่วคราว	1 ชั่วโมง
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	1 ชั่วโมง
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**4 ชั่วโมง**

กรณี สาย fiber optic ระหว่างกรมวิทยาศาสตร์การแพทย์กับสำนักงานปลัดกระทรวงสาธารณสุขขาด

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบ ดำเนินการเปลี่ยนการตั้งค่า Public IP จากของสำนักงานปลัดกระทรวงสาธารณสุขมาเป็นของผู้ให้บริการสายสัญญาณเช่าตรวจสอบการใช้งานของระบบงานให้ครบทุกระบบ	30 นาที
2. ผู้ดูแลระบบประสานผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ของสำนักงานปลัดกระทรวงสาธารณสุขให้ตรวจสอบและจัดเส้นทางสื่อสารข้อมูลมาทางสาย fiber optic สำรองพร้อมทดสอบการเชื่อมต่อกับอุปกรณ์ของกรม	30 นาที
3.ผู้ดูแลระบบ ดำเนินการคืนค่า Public IP ให้ครบทุกระบบและทดสอบการใช้งาน	2 ชั่วโมง
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**4 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ(ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดใช้งานระบบคอมพิวเตอร์สำรองและประสานงานกับผู้ใช้ระบบงานในการทดสอบระบบงาน และรายงานผลการดำเนินการต่อผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

2.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว
กอบกู้คืนระบบเครือข่ายคอมพิวเตอร์และเครื่องแม่ข่ายหลัก ไม่สามารถใช้งานได้เนื่องจากเกิดอุบัติเหตุเช่นไฟไหม้ หรือเกิดอุบัติภัย เช่น แผ่นดินไหวหรือน้ำท่วม หรือเกิดวินาศกรรม จลาจล ให้ระบบงานสารสนเทศสามารถใช้งานได้ปกติ	ดำเนินการซ่อมแซมแก้ไขอุปกรณ์เครือข่ายและเครื่องแม่ข่ายหลัก ประสานงานควบคุมให้บริษัทฯ หรือหน่วยงานที่ให้บริการเครือข่าย แก้ไขปัญหา ให้แล้วเสร็จภายในเวลาที่กำหนด

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ดูและระบบรายงานผลการดำเนินงานในข้อ 2.2 ให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง
2. ผู้ดูแลระบบเตรียมตรวจสอบความเสียหายระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์เครือข่ายหลักหรือสายสัญญาณ และทำการแก้ไขซ่อมแซม ส่งเปลี่ยนอุปกรณ์กับบริษัทที่รับประกันอุปกรณ์หรือจัดหาอุปกรณ์ทดแทนเพื่อให้สามารถใช้งานได้ปกติ
3. ดำเนินการติดตั้งอุปกรณ์ หรือสายสัญญาณ ทดแทน พร้อมทดสอบให้สามารถใช้งานได้เป็นปกติ
4. แจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งหัวหน้าคณะบริหารความต่อเนื่องผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้องทราบ

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ประสานงานและควบคุมการดาเนินการของบริษัทฯ ในการซ่อมแซมแก้ไขระบบเครือข่ายและเครื่องแม่ข่ายหลักให้แล้วเสร็จ ทดสอบการใช้งานและกำหนดให้กลับมาใช้เครือข่ายหลัก

ผู้ใช้ระบบงาน ปฏิบัติงานโดยใช้ระบบเครือข่ายและเครื่องแม่ข่ายหลัก แจ้งผู้ดูแลระบบกรณีเกิดปัญหาการใช้งาน

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

อุปกรณ์เครือข่าย สายสัญญาณ เครื่องแม่ข่าย พร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

2.4 การซ้อมแผน

หลักการและแนวทางในการซ้อมแผน

ดำเนินการซ้อมแผนปีละ 1 ครั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคาร 1 ชั้น 3

กำหนดการฝึกซ้อม: เดือนมิถุนายน – กรกฎาคม ของทุกปี

3. วิกฤตการณ์: ระบบสารสนเทศ ของกรมวิทยาศาสตร์การแพทย์ไม่สามารถใช้งานได้

3.1 แผนรับมือสถานะการณ์ฉุกเฉิน (Incident Response Plan)

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
ระบบสารสนเทศของกรมขัดข้องไม่สามารถใช้งานได้	- ผู้ดูแลระบบเตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองให้สามารถใช้ระบบงานได้ภายใน 7 ชั่วโมง - ประสานงานกับทุกหน่วยงานที่ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรอง

<u>กรณี</u> **ระบบสารสนเทศ** iLab Plus, Co-lab2 **ขัดข้อง, ไฟดับ**

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้องทราบ	5 นาที
2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของเครื่องคอมพิวเตอร์แม่ข่าย	10 นาที
3. ผู้ดูแลระบบดำเนินการตรวจสอบเครื่องแม่ข่ายเตรียมความพร้อมอุปกรณ์ในการกู้ระบบจากข้อมูลระบบ iLab Plus, Co-lab2	45 นาที
4. ผู้ดูแลระบบดำเนินการกู้ระบบจากข้อมูลระบบ iLab Plus ,Co-lab2สำรอง ตรวจสอบ Source Program และทดสอบระบบ	2.45 ชั่วโมง
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	15 นาที
รวม RTO	**4 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ มีหน้าที่ตรวจสอบความเสียหายระบบคอมพิวเตอร์ ระบบงานระบบเครือข่าย ที่ศูนย์คอมพิวเตอร์หลัก เตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง ประสานงานกับผู้ใช้ระบบงาน และรายงานผลการดำเนินการต่อผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)

ผู้ใช้ระบบงาน (หน่วยงานต่าง ๆ) เตรียมความพร้อมปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรอง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

โทรศัพท์ ยานพาหนะ(ขนย้ายพนักงานและอุปกรณ์)

3.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถดำเนินงานต่อเนื่องไม่หยุดชะงักภายใต้ภาวะปกติ แต่ยังไม่กลับสู่การดำเนินการตามปกติ

ปฏิบัติงานโดยใช้ระบบคอมพิวเตอร์สำรองที่ติดตั้ง ณ ศูนย์คอมพิวเตอร์สำรองทำงานทดแทน

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบดำเนินการตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายระบบ iLab Plus / Co-lab2/ กรมวิทย์ With You ที่ทำงาน backup ไว้ที่ศูนย์คอมพิวเตอร์สำรอง	45 นาที
2. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) กู้คืนระบบให้สามารถใช้งานได้ที่ศูนย์คอมพิวเตอร์สำรอง และทดสอบระบบประชาสัมพันธ์ให้ผู้ใช้งานใช้งานจาก Public IP	2.45 ชั่วโมง
3. ฝ่ายพัฒนาระบบคอมพิวเตอร์ แก้ไข Domain Name ให้ตรงกับ Public IP ของศูนย์คอมพิวเตอร์สำรอง	1 ชั่วโมง
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	2 ชั่วโมง
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**7 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดใช้งานระบบคอมพิวเตอร์สำรองและประสานงานกับผู้ใช้ระบบงานในการทดสอบระบบงาน และรายงานผลการดำเนินการต่อหัวหน้าคณะบริหารความต่อเนื่อง

(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้อง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

3.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	**กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว**
กอบกู้คืนระบบเครือข่ายคอมพิวเตอร์และเครื่องแม่ข่ายหลัก ไม่สามารถใช้งานได้เนื่องจากเกิดอุบัติเหตุเช่นไฟไหม้ หรือเกิดอุบัติภัย เช่น แผ่นดินไหวหรือน้ำท่วม หรือเกิดวินาศกรรม จลาจล ให้ระบบงานสารสนเทศสามารถใช้งานได้ปกติ	ดำเนินการซ่อมแซมแก้ไขอุปกรณ์เครือข่ายและเครื่องแม่ข่ายหลัก ประสานงานควบคุมให้บริษัทฯ หรือหน่วยงานที่ให้บริการเครือข่าย แก้ไขปัญหา ให้แล้วเสร็จภายในเวลาที่กำหนด

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง

2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบสารสนเทศที่ศูนย์คอมพิวเตอร์หลักและรายงานความเสียหายให้ทราบ

3. ผู้ดูแลระบบเตรียมตรวจสอบความเสียหายระบบสารสนเทศและเครื่องแม่ข่ายหลัก และย้ายระบบกลับมายังศูนย์คอมพิวเตอร์หลัก เพื่อให้สามารถใช้งานได้ปกติ

4. แจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งหัวหน้าคณะบริหารความต่อเนื่องผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้องทราบ

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ประสานงาน ตรวจสอบ และควบคุมการดำเนินการของบริษัทฯ ในการแก้ไขระบบทดสอบการใช้งานและกำหนดให้กลับมาใช้ระบบหลัก

ผู้ใช้ระบบงาน ปฏิบัติงานโดยใช้ระบบสารสนเทศและเครื่องแม่ข่ายหลัก แจ้งผู้ดูแลระบบกรณีเกิดปัญหาการใช้งาน

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

อุปกรณ์เครือข่าย สายสัญญาณ เครื่องแม่ข่าย พร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

3.4 การซ้อมแผน

หลักการและแนวทางในการซ้อมแผน

ดำเนินการซ้อมแผนปีละ 1 ครั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคาร 1 ชั้น 3 และอาคาร 9 ชั้น 8

กำหนดการฝึกซ้อม: เดือนมิถุนายน – กรกฎาคม ของทุกปี

4. วิกฤตการณ์: ระบบสารสนเทศ ถูกโจมตีทางไซเบอร์

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
ระบบสารสนเทศ ไม่สามารถใช้งานได้ หรือไม่สามารถให้บริการได้เนื่องจากถูกโจมตีทางไซเบอร์ - ระบบใบเสร็จอิเล็กทรอนิกส์ (DMSc Payment) - ระบบการเงินการคลัง (Fin-AD) - ระบบจัดซื้อจัดจ้าง (e-procurement) - ระบบสารบรรณ (Contents) - ระบบ GLP Document - ระบบ Website กรมวิทยาศาสตร์การแพทย์ และระดับหน่วยงานภายใน - ระบบกรมวิทย์ with you - ระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus) - ระบบบริหารจัดการครุภัณฑ์ (AMS)	- ผู้ดูแลระบบเตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองให้สามารถใช้ระบบงานได้ภายใน 3 ชั่วโมง - ประสานงานกับทุกหน่วยงานที่ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบสำรองจากศูนย์คอมพิวเตอร์สำรอง

4.1 แผนรับมือสถานะการณ์ฉุกเฉิน (Incident Response Plan)

4.1.1 ***กรณี*** ระบบการเงินการคลัง กรมวิทยาศาสตร์การแพทย์(Fin-AD), ระบบใบเสร็จอิเล็กทรอนิกส์ (DMSc Payment)

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้องทราบ	5 นาที
2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบสารสนเทศ	10 นาที
3. ผู้ดูแลระบบดำเนินการตรวจสอบเครื่องแม่ข่ายและ logs ระบบเครือข่ายคอมพิวเตอร์ , Web Application Firewall log antivirus หาเส้นทางที่ถูกโจมตี และปิดกั้นการเข้าถึงชั่วคราว	45 นาที
4. ผู้ดูแลระบบดำเนินการกู้ระบบจากข้อมูลระบบ DMSc Payment ระบบ Fin-AD สำรอง ตรวจสอบ Source Program และทดสอบระบบ	50 นาที
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	10 นาที
รวม RTO	**2 ชั่วโมง**

4.1.2 *<u>กรณี</u>* ระบบสารบรรณ (Contents)**,** ระบบ GLP Document, ระบบ Website กรมวิทยาศาสตร์การแพทย์ และระดับหน่วยงานภายใน

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้องทราบ	5 นาที
2.ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตี	10 นาที
3. ผู้ดูแลระบบดำเนินการแก้ไขเบื้องต้น และตรวจสอบ log การโดนโจมตี จาก firewall ,log antivirus	45 นาที
4.หากเจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้ให้ติดต่อหน่วยงานที่เกี่ยวข้องเข้าตรวจสอบแก้ไขปัญหา และเริ่มการกู้คืนระบบจากระบบสำรอง	1.50 ชั่วโมง
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	10 นาที
รวม RTO	**3 ชั่วโมง**

4.1.3 *<u>กรณี</u>* ระบบ กรมวิทย์ With You

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้องทราบ	5 นาที
2.ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตี	10 นาที
3. ผู้ดูแลระบบดำเนินการแก้ไขเบื้องต้น และตรวจสอบ log การโดนโจมตี จาก firewall, log antivirus	45 นาที
4.หากเจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้ให้ติดต่อหน่วยงานที่เกี่ยวข้องเข้าตรวจสอบแก้ไขปัญหา และเริ่มการกู้คืนระบบจากระบบสำรอง	1.50 ชั่วโมง
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	10 นาที
รวม RTO	**3 ชั่วโมง**

4.1.4 *<u>กรณี</u>* ระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus), ระบบบริหารจัดการครุภัณฑ์กรมวิทยาศาสตร์การแพทย์ (AMS)

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ที่เกี่ยวข้องทราบ	5 นาที
2.ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของเครื่องคอมพิวเตอร์แม่ข่ายที่ถูกโจมตี	10 นาที
3. ผู้ดูแลระบบดำเนินการแก้ไขเบื้องต้น และตรวจสอบ log การโดนโจมตี จาก firewall, log antivirus	45 นาที
4.หากเจ้าหน้าที่ไม่สามารถแก้ไขปัญหาได้ให้ติดต่อหน่วยงานที่เกี่ยวข้องเข้าตรวจสอบแก้ไขปัญหา และเริ่มการกู้คืนระบบจากระบบสำรอง	1.50 ชั่วโมง
5. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 4	10 นาที
รวม RTO	**4 ชั่วโมง**

4.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถดำเนินงานต่อเนื่องไม่หยุดชะงักภายใต้ภาวะปกติ แต่ยังไม่กลับสู่การดำเนินการตามปกติ

ปฏิบัติงานโดยใช้ระบบคอมพิวเตอร์สำรองที่ติดตั้ง ณ ศูนย์คอมพิวเตอร์สำรองทำงานทดแทน

4.2.1 กรณีระบบการเงินการคลัง กรมวิทยาศาสตร์การแพทย์(Fin-AD), ระบบใบเสร็จอิเล็กทรอนิกส์ (DMSc Payment)

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) กู้คืนระบบให้สามารถใช้งานได้ที่ศูนย์คอมพิวเตอร์สำรอง และทดสอบระบบ ประชาสัมพันธ์ให้ผู้ใช้งานใช้งานจาก IP และแก้ไขช่องโหว่เพื่อปิดกั้นการถูกโจมตีจากผู้ไม่ประสงค์ดี	40 นาที
2. ฝ่ายพัฒนาระบบคอมพิวเตอร์ แก้ไข Domain Name ให้ตรงกับ IP ของศูนย์คอมพิวเตอร์สำรอง และปิดกั้นการใช้งานจากภายนอก ให้ใช้งานผ่านเครือข่ายภายในเท่านั้น	5 นาที
3. ผู้ดูแลระบบแจ้ง ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อขออนุมัติจากหัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม) รายงานต่อ Nation CERT NCSA	5 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	10 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**3 ชั่วโมง**

4.2.2 กรณีระบบ ระบบสารบรรณ (Contents)**,** ระบบ GLP Document, ระบบ Website กรมวิทยาศาสตร์การแพทย์ และระดับหน่วยงานภายใน

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) กู้คืนระบบให้สามารถใช้งานได้ที่ศูนย์คอมพิวเตอร์สำรอง และทดสอบระบบประชาสัมพันธ์ให้ผู้ใช้งานใช้งานจาก Public IP และแก้ไขช่องโหว่เพื่อปิดกั้นการถูกโจมตีจากผู้ไม่ประสงค์ดี	2.30 ชั่วโมง
2. ฝ่ายพัฒนาระบบคอมพิวเตอร์ แก้ไข Domain Name ให้ตรงกับ Public IP ของศูนย์คอมพิวเตอร์สำรอง	5 นาที
3. ผู้ดูแลระบบแจ้ง ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อขออนุมัติจากหัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม) รายงานต่อ Nation CERT NCSA	5 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	20 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**6 ชั่วโมง**

1. กรณีระบบ กรมวิทย์ With You

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) กู้คืนระบบให้สามารถใช้งานได้ที่ศูนย์คอมพิวเตอร์สำรอง และทดสอบระบบประชาสัมพันธ์ให้ผู้ใช้งานใช้งานจาก Public IP และแก้ไขช่องโหว่เพื่อปิดกั้นการถูกโจมตีจากผู้ไม่ประสงค์ดี	3.30 ชั่วโมง
2. ฝ่ายพัฒนาระบบคอมพิวเตอร์ แก้ไข Domain Name ให้ตรงกับ Public IP ของศูนย์คอมพิวเตอร์สำรอง	5 นาที
3. ผู้ดูแลระบบแจ้ง ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อขออนุมัติจากหัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม) รายงานต่อ Nation CERT NCSA	5 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	20 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**7 ชั่วโมง**

2.ระบบรับส่งตัวอย่างเพื่อตรวจวิเคราะห์ (iLab Plus), ระบบบริหารจัดการครุภัณฑ์ กรมวิทยาศาสตร์การแพทย์ (AMS)

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) กู้คืนระบบให้สามารถใช้งานได้ที่ศูนย์คอมพิวเตอร์สำรอง และทดสอบระบบประชาสัมพันธ์ให้ผู้ใช้งานใช้งานจาก Public IP และแก้ไขช่องโหว่เพื่อปิดกั้นการถูกโจมตีจากผู้ไม่ประสงค์ดี	2.30 ชั่วโมง
2. ฝ่ายพัฒนาระบบคอมพิวเตอร์ แก้ไข Domain Name ให้ตรงกับ Public IP ของศูนย์คอมพิวเตอร์สำรอง	5 นาที
3. ผู้ดูแลระบบแจ้ง ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) เพื่อขออนุมัติจากหัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม) รายงานต่อ Nation CERT NCSA	5 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	20 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**7 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดใช้งานระบบคอมพิวเตอร์สำรองและประสานงานกับผู้ใช้ระบบงานในการทดสอบระบบงาน และรายงานผลการดำเนินการต่อหัวหน้าคณะบริหารความต่อเนื่อง
(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้อง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

4.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว
กอบกู้คืนระบบสารสนเทศและเครื่องแม่ข่ายหลัก ไม่สามารถใช้งานได้เนื่องจากถูกโจมตีทางไซเบอร์ ให้ระบบงานสารสนเทศสามารถใช้งานได้ปกติ	ดำเนินการกู้คืนข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่สำรองไว้ ณ ศูนย์คอมพิวเตอร์สำรอง (ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี) ประสานงานควบคุมให้บริษัทฯ หรือหน่วยงานที่ เกี่ยวข้อง แก้ไขปัญหา ให้แล้วเสร็จภายในเวลาที่กำหนด

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง

2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์หลักและรายงานความเสียหายให้ทราบ

3. ผู้ดูแลระบบเตรียมตรวจสอบความเสียหายระบบสารสนเทศและเครื่องแม่ข่ายหลัก และทำการตรวจสอบช่องโหว่ของระบบสารสนเทศ และย้ายระบบกลับมายังศูนย์คอมพิวเตอร์หลัก เพื่อให้สามารถใช้งานได้ปกติ

4. แจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งหัวหน้าคณะบริหารความต่อเนื่องผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้องทราบ

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ประสานงานและควบคุมการดำเนินการแก้ไขระบบสารสนเทศและเครื่องแม่ข่ายหลักให้แล้วเสร็จ ทดสอบการใช้งานและกำหนดให้กลับมาใช้เครื่องคอมพิวเตอร์แม่ข่ายหลัก

ผู้ใช้ระบบงาน ปฏิบัติงานโดยใช้ระบบสารสนเทศและเครื่องแม่ข่ายหลัก แจ้งผู้ดูแลระบบกรณีเกิดปัญหาการใช้งาน

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

อุปกรณ์เครือข่าย สายสัญญาณ เครื่องคอมพิวเตอร์แม่ข่าย พร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

5. วิกฤตการณ์: ระบบสารสนเทศด้านข้อมูลรั่วไหล

5.1 แผนรับมือสถานการณ์ฉุกเฉิน สถานะการณ์ด้านข้อมูลรั่วไหล (Incident Data Leak Plan)

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
ระบบสารสนเทศข้อมูลหรือข้อมูลส่วนบุคคลรั่วไหล	- ผู้ดูแลระบบรับแจ้งเหตุข้อมูลหรือข้อมูลส่วนบุคคลรั่วไหล - รายงานเหตุต่อหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) ทราบรายละเอียดข้อมูลที่รั่วไหล - รายงานเหตุต่อหน่วยงานที่ใช้ระบบสารสนเทศ ปฏิบัติงาน - DPO รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล โทร. 02-1421033, 02-1416993 e-mail : saraban@pdpc.or.th - ตรวจสอบหาสาเหตุการรั่วไหลของข้อมูล
รวม RTO	72 ชั่วโมง

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้พบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง

2. แจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งหัวหน้าคณะบริหารความต่อเนื่องผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้อง ทราบเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (Data Protection Officer) รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

3. แจ้งเตือนบุคคลที่ถูกละเมิดข้อมูลส่วนตัว

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ดำเนินการแก้ไขการเข้าถึงระบบสารสนเทศและเครื่องแม่ข่ายหลักจนกว่าจะมีการจัดการช่องโหว่ของระบบให้แล้วเสร็จ

ผู้ใช้ระบบงาน ปฏิบัติงานโดยใช้ระบบสารสนเทศและเครื่องแม่ข่ายหลัก รายงานเหตุต่อหน่วยงานที่ใช้ระบบสารสนเทศ ปฏิบัติงาน

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

อุปกรณ์เครือข่าย สายสัญญาณ เครื่องคอมพิวเตอร์แม่ข่าย พร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

5.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถกลับมาดำเนินงานได้การตามปกติ

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ทีมรับแจ้งเหตุได้รับแจ้งเหตุข้อมูลส่วนบุคคลรั่วไหล	20 นาที
2. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ทำการตรวจสอบตัวอย่างข้อมูลส่วนบุคคลที่รั่วไหล และนำรายงานต่อหัวหน้ากลุ่มงาน	60 นาที
3. DPO รายงานต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล	60 นาที
4.ทีมแก้ไขเหตุการณ์ตรวจสอบช่องโหว่การรั่วไหล และปิดช่องโหว่การรั่วไหล	60 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**4 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดดูตัวอย่างข้อมูลที่อ้างว่าได้รั่วไหลจากกรมวิทยาศาสตร์การแพทย์ และประเมินความเป็นได้ว่าข้อมูลได้รั่วไหลจากระบบสารสนเทศใด เมื่อไร และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

Data protection officer(DPO) ตรวจสอบความถูกต้องของรายงาน และ รายงานเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ทีมแก้ไขเหตุการณ์ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่ ระบุต้นเหตุระบบสารสนเทศที่ทำให้ข้อมูลส่วนบุคคลรั่วไหล ระบุช่องโหว่การรั่วไหลข้อมูล ตลอดจนปิดช่องโหว่การรั่วไหลข้อมูล และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

5.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว
การปิดช่องโหว่การรั่วไหลของข้อมูลส่วนบุคคล ทำให้ระบบงานสารสนเทศบางระบบให้สามารถใช้งานได้เป็นปกติ	- สำรวจระบบสารสนเทศที่เกิดการรั่วไหลข้อมูลส่วนบุคคล - ดำเนินการให้ผู้ใช้ระบบงานสามารถปฏิบัติงาน/ให้บริการได้ตามปกติ

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ดูแลระบบสำรวจระบบสารสนเทศที่เกิดการรั่วไหลของข้อมูลส่วนบุคคล และหาสาเหตุการรั่วไหล ตลอดจนปิดช่องโหว่การรั่วไหลข้อมูลส่วนบุคคล
2. ผู้ดูแลระบบ รายงานผู้บังคับบัญชา
3. Data protection officer(DPO) ตรวจสอบความถูกต้องของรายงาน และ รายงานเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดดูตัวอย่างข้อมูลที่อ้างว่าได้รั่วไหลจากกรมวิทยาศาสตร์การแพทย์ และประเมินความเป็นได้ว่าข้อมูลได้รั่วไหลจากระบบสารสนเทศใด เมื่อไร และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

Data protection officer(DPO) ตรวจสอบความถูกต้องของรายงาน และ รายงานเหตุการณ์รั่วไหลของข้อมูลส่วนบุคคลต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล

ทีมแก้ไขเหตุการณ์ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่ ระบุต้นเหตุระบบสารสนเทศที่ทำให้ข้อมูลส่วนบุคคลรั่วไหล ระบุช่องโหว่การรั่วไหลข้อมูล ตลอดจนปิดช่องโหว่การรั่วไหลข้อมูล และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการ**ปฏิบัติงาน:**

เครื่องคอมพิวเตอร์แม่ข่ายพร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

5.4 การซ้อมแผน

หลักการและแนวทางในการซ้อมแผน

ดำเนินการซ้อมแผนปีละ 1 ครั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคาร 1 ชั้น 3

กำหนดการฝึกซ้อม: เดือนมิถุนายน – กรกฎาคม ของทุกปี

6. วิกฤตการณ์: ระบบสารสนเทศจากเหตุแผ่นดินไหว (Earthquake Recovery Plan)

6.1 แผนรับมือสถานะการณ์ฉุกเฉิน (Incident Response Plan) สถานการณ์ ระบบเทคโนโลยีสารสนเทศใช้งานไม่ได้จากเหตุแผ่นดินไหว

นิยามของภาวะฉุกเฉิน	กลยุทธ์ในการปฏิบัติงานเมื่อเกิดภาวะฉุกเฉิน
เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้เนื่องจากแผ่นดินไหว ทำให้ระบบงานสารสนเทศบางระบบ ไม่สามารถใช้งานได้ หรือไม่สามารถให้บริการได้	- ผู้ดูแลระบบเตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองให้สามารถใช้ระบบงานได้ภายใน 4 ชั่วโมง - ประสานงานกับทุกหน่วยงานที่ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรอง

***<u>กรณี</u>* เครื่องคอมพิวเตอร์แม่ข่าย และระบบสารสนเทศกรมวิทยาศาสตร์การแพทย์ ไม่สามารถใช้งานได้**

ขั้นตอนและวิธีการปฏิบัติงาน:	ระยะเวลา
1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง	10 นาที
2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์หลักและรายงานความเสียหายให้ทราบพร้อมขอปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง หรือเครื่องคอมพิวเตอร์แม่ข่ายสำรอง ประสานงานบริหารทั่วไปประชาสัมพันธ์สถานการณ์	30 นาที
3. ผู้ดูแลระบบเตรียมระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์สำรองเพื่อให้สามารถใช้งานได้และแจ้งทีมเพื่อทดสอบระบบสารสนเทศ	2 ชั่วโมง
4. หัวหน้าคณะบริหารความต่อเนื่อง(ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง)/ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งผู้ใช้ระบบสารสนเทศปฏิบัติงานโดยใช้ระบบจากขั้นตอนที่ 3	20 นาที
รวม RTO	**3 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบมีหน้าที่ตรวจสอบความเสียหายระบบคอมพิวเตอร์ ระบบงานระบบเครือข่าย ที่ศูนย์คอมพิวเตอร์หลัก เตรียมความพร้อมปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรอง ประสานงานกับผู้ใช้ระบบงาน และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

ผู้ใช้ระบบงาน (หน่วยงานต่าง ๆ) เตรียมความพร้อมปฏิบัติงานโดยใช้ศูนย์คอมพิวเตอร์สำรองหรือเครื่องคอมพิวเตอร์แม่ข่ายสำรอง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

โทรศัพท์ ยานพาหนะ(ขนย้ายพนักงานและอุปกรณ์) เครื่องคอมพิวเตอร์แม่ข่ายสำรอง ระบบสื่อสารข้อมูล

6.2 แผนดำเนินการต่อเนื่อง (Continuity Plan)

กลยุทธ์ในการปฏิบัติงานหลังพ้นภาวะฉุกเฉินเพื่อ ให้สามารถดำเนินงานต่อเนื่องไม่หยุดชะงักภายใต้ภาวะปกติ แต่ยังไม่กลับสู่การดำเนินการตามปกติ

- ปฏิบัติงานโดยใช้ระบบคอมพิวเตอร์สำรองที่ติดตั้ง ณ ศูนย์คอมพิวเตอร์สำรองทำงานทดแทน

ขั้นตอนและวิธีการปฏิบัติงาน:	**ระยะเวลา**
1. ผู้ดูแลระบบดำเนินการตรวจสอบการใช้ระบบคอมพิวเตอร์สำรองโดยนำเข้าข้อมูลที่ได้สำรองไว้ล่าสุด	20 นาที
2. ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) และผู้ใช้ระบบงานทดสอบและตรวจสอบระบบงานจากการปฏิบัติงานที่ศูนย์คอมพิวเตอร์สำรองหรือใช้เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และนำเข้าข้อมูลให้เป็นปัจจุบันมากที่สุด	15 นาที
3. ผู้ใช้ระบบงานปฏิบัติงาน/ให้บริการโดยใช้ระบบคอมพิวเตอร์ ณ ศูนย์คอมพิวเตอร์สำรอง โดยใช้เครื่องคอมพิวเตอร์ลูกข่ายและอุปกรณ์อื่น ๆ ร่วมกัน	10 นาที
4.ผู้ดูแลระบบตรวจสอบเฝ้าระวังและติดตามการใช้งานและแก้ไขปัญหาขณะใช้งานจนระบบมีความเสถียร	15 นาที
รวม MTPD (นับเวลาต่อเนื่องจาก RTO)	**4 ชั่วโมง**

หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ (ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มีหน้าที่เปิดใช้งานระบบคอมพิวเตอร์สำรองและประสานงานกับผู้ใช้ระบบงานในการทดสอบระบบงาน และรายงานผลการดำเนินการต่อผู้บังคับบัญชา

ผู้ใช้ระบบงานทดสอบและตรวจสอบความถูกต้องข้อมูล นาเข้าข้อมูลให้เป็นปัจจุบันและปฏิบัติงาน/ให้บริการโดยใช้ระบบคอมพิวเตอร์สำรอง

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

เครื่องคอมพิวเตอร์แม่ข่ายสำรอง และเครื่องคอมพิวเตอร์ลูกข่ายพร้อมอุปกรณ์

6.3 แผนฟื้นตัวจากความเสียหาย (Disaster Recovery Plan)

นิยามของภาวะฟื้นตัว	**กลยุทธ์ในการปฏิบัติงานเพื่อให้ฟื้นตัวจากวิกฤตและกลับสู่การดำเนินงานตามปกติได้โดยเร็ว**
กู้คืนระบบสารสนเทศและเครื่องแม่ข่ายหลักไม่สามารถใช้งานได้ เนื่องจากเหตุแผ่นดินไหว ให้ระบบงานสารสนเทศสามารถใช้งานได้ปกติ	ดำเนินการกู้คืนข้อมูลเครื่องคอมพิวเตอร์แม่ข่ายที่สำรองไว้ ณ ศูนย์คอมพิวเตอร์สำรอง (ศูนย์วิทยาศาสตร์การแพทย์ที่ 4 สระบุรี) ประสานงานควบคุมให้บริษัทฯ หรือหน่วยงานที่เกี่ยวข้อง แก้ไขปัญหา ให้แล้วเสร็จภายในเวลาที่กำหนด

ขั้นตอนและวิธีการปฏิบัติงาน:

1. ผู้ประสบเหตุแจ้งเหตุฉุกเฉินให้กับหัวหน้าทีมบริหารความต่อเนื่อง (ผู้อำนวยการ/หัวหน้ากลุ่ม) เพื่อแจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร)และผู้ที่เกี่ยวข้อง

2. ผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) มอบหมายผู้ดูแลระบบสำรวจความเสียหายของระบบคอมพิวเตอร์ที่ศูนย์คอมพิวเตอร์หลักและรายงานความเสียหายให้ทราบ

3. ผู้ดูแลระบบเตรียมตรวจสอบความเสียหายระบบสารสนเทศและเครื่องแม่ข่ายหลัก และย้ายระบบกลับมายังศูนย์คอมพิวเตอร์หลัก เพื่อให้สามารถใช้งานได้ปกติ

4. แจ้งผู้ประสานงานทีมบริหารความต่อเนื่อง(ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร) ประสานงานแจ้งหัวหน้าคณะบริหารความต่อเนื่องผู้บริหารเทคโนโลยีสารสนเทศระดับสูง) และผู้ที่เกี่ยวข้องทราบ

หน้าที่และความรับผิดชอบของผู้ปฏิบัติงาน/ผู้เกี่ยวข้อง:

ผู้ดูแลระบบ ประสานงานและควบคุมการดำเนินการแก้ไขระบบสารสนเทศและเครื่องแม่ข่ายหลักให้แล้วเสร็จ ทดสอบการใช้งานและกำหนดให้กลับมาใช้เครื่องคอมพิวเตอร์แม่ข่ายหลัก

ผู้ใช้ระบบงาน ปฏิบัติงานโดยใช้ระบบสารสนเทศและเครื่องแม่ข่ายหลัก แจ้งผู้ดูแลระบบกรณีเกิดปัญหาการใช้งาน

เครื่องมือ/วัสดุอุปกรณ์/สิ่งอำนวยความสะดวกในการปฏิบัติงาน:

อุปกรณ์เครือข่าย สายสัญญาณ เครื่องคอมพิวเตอร์แม่ข่าย พร้อมอุปกรณ์อื่น ๆ ที่เกี่ยวข้อง

6.4. การซ้อมแผน

หลักการและแนวทางในการซ้อมแผน

ดำเนินการซ้อมแผนปีละ 1 ครั้ง ณ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อาคาร 1 ชั้น 3 และอาคาร 9 ชั้น 8

กำหนดการฝึกซ้อม: เดือนมิถุนายน – กรกฎาคม ของทุกปี

ลงชื่อ.....ผู้จัดทำ
(นายอดิศักดิ์ แก้วสุกแท้)
นักวิชาการคอมพิวเตอร์ปฏิบัติการ
5 มิถุนายน 2568

ลงชื่อ.....ผู้ทบทวน
(นางสาวชุติมา โพธิ์ป้อม)
นักวิชาการคอมพิวเตอร์ชำนาญการ
5 มิถุนายน 2568

ลงชื่อ.....ผู้เสนอ
(นายอาคม สาลี)
ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
10 มิถุนายน 2568

ลงชื่อ.....ผู้อนุมัติ
(นายพิเชฐ บัญญัติ)
รองอธิบดีกรมวิทยาศาสตร์การแพทย์
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม
11 มิถุนายน 2568


ICT
Information and Communication Technology Center