



**การบริหารความต่อเนื่องทางธุรกิจ
(Business Continuity Management : BCM)
และแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
(Business Continuity Plan : BCP)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. 2569**



โดย ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร



www.otp.go.th



การบริหารความต่อเนื่องทางธุรกิจ
(Business Continuity Management : BCM)
และแผนความต่อเนื่องทางธุรกิจด้านเทคโนโลยีสารสนเทศ
(Business Continuity Plan : BCP)
ของสำนักงานนโยบายและแผนการขนส่งและจราจร
ประจำปีงบประมาณ พ.ศ. ๒๕๖๙

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร
สำนักงานนโยบายและแผนการขนส่งและจราจร

สารบัญ

เรื่อง	หน้า
ส่วนที่ ๑ แผนบริหารความต่อเนื่องทางธุรกิจ และการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศของ สนข.	
๑. บทนำ	๑
๒. วัตถุประสงค์	๒
๓. ขอบเขตการดำเนินงานของแผนความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ	๒
๔. การระบุผลกระทบต่อทรัพยากรที่สำคัญขององค์กร	๒
๕. สรุปผลกระทบจากเหตุการณ์ต่อทรัพยากรที่สำคัญ	๓
๖. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis หรือ BIA)	๔
๗. สรุปผลกระทบจากเหตุการณ์ต่อทรัพยากรที่สำคัญ	๔
๘. การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง	๗
๙. กลไกการบริหารความต่อเนื่องในสภาวะวิกฤตของ สนข.	๑๐
๑๐. โครงสร้างของทีมงาน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.	๑๒
๑๑. การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง	๑๗
๑๒. ขั้นตอนการบริหารความต่อเนื่องและการกอบกู้กระบวนการ	๑๘
ส่วนที่ ๒ แผนและแนวทางปฏิบัติในสถานการณ์ฉุกเฉินจากสภาวะวิกฤตต่าง ๆ	
๑. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์แผ่นดินไหว หรืออาคารถล่ม	๒๕
๒. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อัคคีภัย (กรณีเพลิงไหม้ภายในห้องเซิร์ฟเวอร์)	๒๖
๓. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อัคคีภัย (กรณีเพลิงไหม้ตัวอาคาร สนข.)	๒๗
๔. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อุทกภัย	๒๘
๕. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ไฟฟ้าดับ (กรณีทราบล่วงหน้าหรือได้รับแจ้งล่วงหน้า)	๒๙
๖. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ไฟฟ้าดับ (กรณีไม่ทราบล่วงหน้า)	๓๐
๗. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์จลาจล การชุมนุมประท้วง หรือเหตุการณ์ความไม่สงบ	๓๑
๘. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์โรคระบาด	๓๒
๙. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์	๓๓

สารบัญรูป

เรื่อง	หน้า
รูปที่ ๑ หลักเกณฑ์การกำหนดค่า MTD RPO และ RTO	๔
รูปที่ ๒ การกำหนดค่า MTD RPO และ RTO ของ สนข.	๘
รูปที่ ๓ ขั้นตอนการปฏิบัติประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.	๑๑
รูปที่ ๔ โครงสร้างทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ)	๑๒
รูปที่ ๕ ทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ) ของ สนข.	๑๔
รูปที่ ๖ กระบวนการพิจารณาเพื่อเริ่ม Call Tree	๑๕
รูปที่ ๗ กระบวนการแจ้งเหตุฉุกเฉินในสถานการณ์ Call Tree	๑๕
รูปที่ ๘ ขั้นตอนการบริหารความต่อเนื่องต่อเนื่องและการตอบสนองต่อเหตุการณ์	๑๘
รูปที่ ๙ ขั้นตอนการบริหารความต่อเนื่องต่อเนื่องและการตอบสนองต่อเหตุการณ์ (ต่อ)	๑๙

สารบัญตาราง

เรื่อง	หน้า
ตารางที่ ๑	สรุปผลกระทบจากเหตุการณ์และทรัพยากรที่สำคัญ
ตารางที่ ๒	หลักเกณฑ์สำหรับพิจารณาระดับความรุนแรง
ตารางที่ ๓	ช่วงคะแนนระดับความรุนแรงของผลกระทบ
ตารางที่ ๔	สรุปผลกระทบจากเหตุการณ์ต่อทรัพยากรที่สำคัญของ สนช.
ตารางที่ ๕	Risk Heat Map ๕x๕
ตารางที่ ๖	หลักเกณฑ์การพิจารณาผลกระทบจากการหยุดชะงักของระบบงาน บริการอิเล็กทรอนิกส์
ตารางที่ ๗	ระยะเวลาสูงสุดที่ยอมรับได้ในการหยุดชะงักของระบบงานอิเล็กทรอนิกส์
ตารางที่ ๘	การกำหนดค่า MTD RPO และ RTO
ตารางที่ ๙	เกณฑ์การพิจารณายุติการใช้แผนการบริหารความต่อเนื่อง ด้านระบบเทคโนโลยีสารสนเทศ
ตารางที่ ๑๐	รายชื่อบุคลากรและบทบาทของทีมบริหารความต่อเนื่อง (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ)
ตารางที่ ๑๑	การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง

ส่วนที่ ๑ : แผนบริหารความต่อเนื่องทางธุรกิจ และการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศของ สนข.

๑. บทนำ

มติคณะรัฐมนตรี เมื่อวันที่ ๒๔ เมษายน ๒๕๕๕ เห็นชอบแนวทางและมาตรการที่กำหนดให้หน่วยงานของรัฐดำเนินการบริหารความพร้อมต่อสภาวะวิกฤต เพื่อให้สามารถปฏิบัติภารกิจหลักหรืองานบริการที่สำคัญอย่างต่อเนื่องภายใต้สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ และมอบหมายให้สำนักงานคณะกรรมการพัฒนาระบบราชการ (ก.พ.ร.) เป็นหน่วยงานหลักในการสนับสนุนการดำเนินการให้แก่หน่วยงานของรัฐ

ระเบียบสำนักนายกรัฐมนตรีว่าด้วยการปฏิบัติงานนอกสถานที่ตั้งของส่วนราชการ พ.ศ. ๒๕๖๕ และหนังสือสำนักงาน ก.พ. ที่ นร. ๑๐๑๒.๒/ว ๑๘ ลงวันที่ ๓๐ ตุลาคม ๒๕๖๕ เรื่อง แนวทางการปฏิบัติราชการที่รองรับชีวิตและการทำงานวิถีใหม่ มีแนวทางการดำเนินงานโดยให้หน่วยงานปรับรูปแบบและขั้นตอนวิธีการทำงานให้สอดคล้องกับสถานการณ์และตอบสนองต่อความต้องการของผู้รับบริการ เพื่อให้การปฏิบัติราชการของหน่วยงานของรัฐมีความยืดหยุ่น คล่องตัว มีประสิทธิภาพ โดยใช้ประโยชน์จากเทคโนโลยีดิจิทัล โดยมีรูปแบบการทำงาน ๓ รูปแบบ ได้แก่ ๑) การปฏิบัติงานในสถานที่ตั้งของส่วนราชการโดยการเหลื่อมเวลาทำงาน ๒) การปฏิบัติงานในสถานที่ตั้งของส่วนราชการโดยการนับชั่วโมงการทำงาน และ ๓) การปฏิบัติงานนอกสถานที่ตั้งของส่วนราชการ (Work from anywhere : WFA)

ศูนย์เทคโนโลยีสารสนเทศการขนส่งและจราจร (ศทท.) ซึ่งเป็นหน่วยงานภายใต้สังกัดของสำนักงานนโยบายและแผนการขนส่งและจราจร (สนข.) มีหน้าที่ดูแลรับผิดชอบข้อมูลสารสนเทศ ระบบเทคโนโลยีสารสนเทศ และโครงสร้างพื้นฐานทางด้านดิจิทัลของ สนข. ได้เริ่มดำเนินการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) มาตั้งแต่ปี พ.ศ. ๒๕๕๗ และมีการทบทวนอย่างต่อเนื่องเป็นประจำทุกปี ดังนี้

ปี พ.ศ. ๒๕๖๗ มีการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติด้านเทคโนโลยีสารสนเทศ ประจำปี พ.ศ. ๒๕๖๖ โดยมีการปรับปรุงเนื้อหาเพิ่มเติมให้มีความสอดคล้องและเป็นไปตามมาตรา ๔๔ แห่งพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ และได้เปลี่ยนชื่อใหม่เป็น “แผนความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศของ สนข. (Business Continuity Plan : BCP)” ซึ่งต่อไปนี้จะเรียกว่า “แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.” ซึ่งเป็นส่วนหนึ่งของประมวลแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. และสอดคล้องกับแนวปฏิบัติการรักษาความมั่นคงปลอดภัยไซเบอร์ของ สนข. จัดทำขึ้นเพื่อให้ ศทท. นำไปใช้ในการตอบสนองต่อสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่เกิดจากภัยธรรมชาติ อุบัติเหตุ อุบัติการณ์ โรคระบาด หรือการมุ่งร้ายต่อหน่วยงานโดยไม่ให้สถานการณ์ดังกล่าวส่งผลให้ภารกิจหลักหรืองานบริการที่สำคัญของ สนข. ต้องหยุดชะงักลงบางส่วนหรือทั้งหมด

ปี พ.ศ. ๒๕๖๙ มีการทบทวนแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. ให้สอดคล้องกับสถานการณ์และบริบทในปัจจุบันที่เปลี่ยนแปลงไปไม่ว่าจะเป็นสถานการณ์ฉุกเฉินด้านสาธารณสุข (โรคระบาด) การจัดหาสถานที่ปฏิบัติงานสำรองหรือการจัดเตรียมระบบเทคโนโลยีสารสนเทศสำรอง (DR Site) การปรับเปลี่ยนนโยบายและโครงสร้างการบริหารหน่วยงาน การดำเนินงานตามแนวทางการทำงานวิถีใหม่ (Work from Anywhere) ตลอดจนการเพิ่มความพร้อมในการรับมือกับความเสี่ยงด้านภัยพิบัติ (Disaster) และภัยคุกคามทางไซเบอร์ (Cyber Attack) ในโลกยุคปัจจุบัน

ทั้งนี้ หาก ศทท. ขาดแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. อาจส่งผลกระทบในด้านต่าง ๆ อาทิ ด้านการให้บริการ ด้านการบริหารจัดการ ด้านชื่อเสียง/ภาพลักษณ์ ด้านกฎหมาย และด้านงบประมาณ ดังนั้น การจัดทำแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. จึงเป็นสิ่งสำคัญที่จะช่วยให้ สนข. สามารถตอบสนองต่อภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ทำให้ภารกิจหลักหรืองานบริการที่สำคัญของ สนข. สามารถให้บริการได้อย่างต่อเนื่องอย่างน้อยที่สุดในระดับที่กำหนดไว้ รวมทั้งลดระดับความรุนแรงของผลกระทบที่จะเกิดขึ้นต่อ สนข. ได้

๒. วัตถุประสงค์

๒.๑ เพื่อใช้เป็นแนวทางในการบริหารจัดการความต่อเนื่อง

๒.๒ เพื่อให้ สนข. มีการเตรียมความพร้อมล่วงหน้าในการรับมือกับสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่เกิดขึ้น และลดผลกระทบจากการหยุดชะงักในการดำเนินธุรกิจหรือการให้บริการ

๒.๓ เพื่อบรรเทาความเสียหายให้อยู่ในระดับที่ยอมรับได้ เช่น ผลกระทบด้านเศรษฐกิจการเงิน การให้บริการ สังคม ชุมชน และสิ่งแวดล้อม ตลอดจนชีวิตและทรัพย์สินของประชาชน

๒.๔ เพื่อให้ผู้มีส่วนได้ส่วนเสีย (Stakeholders) มีความเชื่อมั่นในศักยภาพของ สนข. แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงและ ส่งผลกระทบจนทำให้การดำเนินงานต้องหยุดชะงัก

๓. ขอบเขตการดำเนินงานของแผนความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศของ สนข. จัดทำขึ้นสำหรับ สนข. เพื่อใช้กู้คืนระบบงานให้กลับคืนสู่สภาพปกติ (Recovery) และบริการหลัก (Critical Service) โดยมีรายละเอียดดังนี้

(๑) อุปกรณ์ภายในห้องปฏิบัติการศูนย์ข้อมูล (DATA CENTER)

(๒) เครื่องคอมพิวเตอร์แม่ข่าย (Servers) อุปกรณ์เครือข่าย (Network Devices) และระบบรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ (IT Security)

(๓) ระบบงานสารสนเทศอิเล็กทรอนิกส์

แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. นี้ ใช้รองรับกรณีเกิดสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินในพื้นที่ของ สนข. ด้วยเหตุการณ์ต่อไปนี้

๓.๑ เหตุการณ์อัคคีภัย

๓.๒ เหตุการณ์แผ่นดินไหว หรืออาคารถล่ม

๓.๓ เหตุการณ์อุทกภัย

๓.๔ เหตุการณ์ไฟฟ้าดับเป็นวงกว้าง

๓.๕ เหตุการณ์จลาจล การชุมนุมประท้วง หรือเหตุการณ์ความไม่สงบ

๓.๖ เหตุการณ์โรคระบาดติดต่อร้ายแรง

๓.๗ เหตุการณ์ภัยคุกคามทางไซเบอร์ เช่น การถูกเจาะระบบ การถูกโจมตีจากภัยต่าง ๆ เช่น malware Ransomware DDoS และ Web Defacement

๔. การระบุผลกระทบต่อทรัพยากรที่สำคัญขององค์กร

สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินมีหลากหลายรูปแบบ ดังนั้นเพื่อให้ สนข. สามารถบริหารการดำเนินงานขององค์กรให้มีความต่อเนื่อง การจัดหาทรัพยากรที่สำคัญจึงมีความจำเป็นและต้องระบุไว้ในแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. ซึ่งการเตรียมการทรัพยากรที่สำคัญจะพิจารณาจากผลกระทบใน ๕ ด้าน ดังนี้

ด้านที่ ๑ สถานที่ปฏิบัติงานหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้สถานที่ปฏิบัติงานหลักได้รับความเสียหายจนไม่สามารถใช้งานได้ และส่งผลให้บุคลากรไม่สามารถเข้าปฏิบัติงานได้ชั่วคราวหรือระยะยาว ซึ่งรวมทั้งการที่ผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียไม่สามารถเข้าถึงสถานที่ให้บริการของหน่วยงานด้วย

ด้านที่ ๒ วัสดุอุปกรณ์ที่จำเป็น หมายถึง เหตุการณ์ ที่เกิดขึ้นทำให้ไม่สามารถใช้งานวัสดุอุปกรณ์ที่สำคัญ หรือไม่สามารถจัดหา/จัดส่งวัสดุอุปกรณ์ที่สำคัญได้

ด้านที่ ๓ ข้อมูลและระบบเทคโนโลยีสารสนเทศที่สำคัญ หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้ระบบงานเทคโนโลยี หรือระบบสารสนเทศ หรือข้อมูลที่สำคัญไม่สามารถนำมาใช้ในการปฏิบัติงานได้ตามปกติ

ด้านที่ ๔ บุคลากรหลัก หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้บุคลากรหลักไม่สามารถมาปฏิบัติงานได้ตามปกติ

ด้านที่ ๕ ผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย หมายถึง เหตุการณ์ที่เกิดขึ้นทำให้คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียไม่สามารถติดต่อหรือให้บริการหรือส่งมอบงานได้

๔.๑ การประเมินความเสี่ยงและภัยคุกคาม

สนช. ได้ประเมินความเสี่ยงและภัยคุกคามที่มีโอกาสเกิดในพื้นที่ปฏิบัติงาน และส่งผลกระทบรุนแรงต่อองค์กร โดยทบทวนกิจกรรม/กระบวนการทำงาน รวมถึงระดับผลกระทบต่อองค์กร ในกรณีที่กิจกรรม/กระบวนการทำงานดังกล่าวต้องหยุดชะงัก หากเกิดสภาวะวิกฤต โดยสามารถสรุปผลกระทบจากเหตุการณ์และทรัพยากรที่สำคัญได้ ดังนี้

ตารางที่ ๑ สรุปผลกระทบจากเหตุการณ์และทรัพยากรที่สำคัญ

ความเสี่ยงและภัยคุกคาม	ผลกระทบ				
	สถานที่ปฏิบัติงานหลัก	วัสดุอุปกรณ์ที่จำเป็น	ข้อมูลและระบบเทคโนโลยีสารสนเทศที่สำคัญ	บุคลากรหลัก	ผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย
เหตุการณ์แผ่นดินไหว หรืออาคารถล่ม	✓	✓	✓	✓	
เหตุการณ์อัคคีภัย	✓	✓	✓	✓	
เหตุการณ์อุทกภัย	✓	✓	✓	✓	✓
เหตุการณ์ไฟฟ้าดับเป็นวงกว้าง			✓		
เหตุการณ์จลาจล การชุมนุมประท้วง หรือเหตุการณ์ความไม่สงบ	✓	✓	✓	✓	
เหตุการณ์โรคระบาดติดต่อร้ายแรง	✓	✓	✓	✓	✓
เหตุการณ์ภัยคุกคามทางไซเบอร์		✓	✓	✓	✓

๕. หลักเกณฑ์และวิธีการประกาศใช้แผน

กำหนดให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ระดับกรม (DCIO) หรือผู้บริหารจัดการความมั่นคงปลอดภัยไซเบอร์ (HoIS) ประจำ สนช. เป็นผู้มีความอำนาจในการพิจารณาการประกาศใช้และยุติการใช้แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศฉบับนี้ โดยหลักเกณฑ์ในการพิจารณาประกาศใช้แผนอาจพิจารณาจากระดับความรุนแรงของผลกระทบ ความเสียหาย และโอกาสที่การดำเนินงานของระบบเทคโนโลยีสารสนเทศของ สนช. จะเกิดการหยุดชะงัก ภายหลังจากการดำเนินการแก้ไขสถานการณ์เบื้องต้นตามขั้นตอน

การปฏิบัติที่อยู่ในแผนการจัดการอุบัติการณ์ (Incident Management Plan: IMP) แล้วเสร็จ โดยมีการสื่อสารกับผู้บริหารของผู้ที่ได้รับผลกระทบรับทราบ จากนั้นผู้บริหารจะแจ้งให้ผู้ที่เกี่ยวข้องรับทราบ

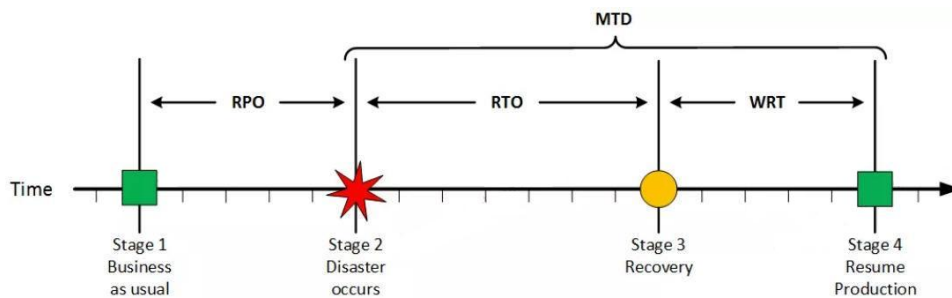
๖. การวิเคราะห์ผลกระทบทางธุรกิจ (Business Impact Analysis หรือ BIA) ประกอบด้วย

๖.๑ การวิเคราะห์ช่วงระยะเวลาของการหยุดชะงักเมื่อสภาวะวิกฤต/ภัยคุกคามเริ่มส่งผลกระทบกับการดำเนินงานของระยะเวลาของกิจกรรมต่าง ๆ ของหน่วยงาน ซึ่งกำหนดค่า RTO, MTPD และ RPO

๑) ระยะเวลาการหยุดชะงักที่ยอมรับได้สูงสุด (Maximum Tolerable Period of Disruption : MTPD) หมายถึง ระยะเวลาที่ระบบงานหยุดชะงักที่ยอมรับได้สูงสุดหากเกินกำหนดเวลานี้แล้วจะไม่สามารถทำให้ระบบงานของ สนข. กลับคืนสู่สภาพปกติได้

๒) ระยะเวลาเป้าหมายในการฟื้นคืนสภาพ (Recovery Time Objectives : RTO) หมายถึง ระยะเวลาเป้าหมายที่ใช้ในการดำเนินการเพื่อให้กระบวนการดำเนินงาน กลับคืนสู่สภาพปกติหลังเกิดเหตุการณ์

๓) ระยะเวลาสูงสุดที่ยอมให้ข้อมูลเสียหาย (Recovery Point Objective : RPO) หมายถึง จุดเวลาเป้าหมายสามารถยอมรับการสูญหายของข้อมูลได้นานที่สุดเท่าไร



รูปที่ ๑ หลักเกณฑ์การกำหนดค่า MTD RPO และ RTO

๗. สรุปผลกระทบจากเหตุการณ์ต่อทรัพยากรที่สำคัญ

เมื่อได้วิเคราะห์ข้อมูลเพื่อระบุความเสี่ยงและภัยคุกคามที่มีโอกาสเกิดขึ้นในพื้นที่ปฏิบัติงานและส่งผลกระทบต่อทรัพยากรที่สำคัญ ๕ ด้าน ได้แก่ (๑) สถานที่ปฏิบัติงานหลัก (๒) ด้านวัสดุอุปกรณ์ที่จำเป็น (๓) ด้านข้อมูลและระบบเทคโนโลยีสารสนเทศ (๔) ด้านบุคลากรหลัก และ (๕) ด้านผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ทั้งนี้ได้กำหนดหลักเกณฑ์สำหรับการพิจารณาโอกาสที่สถานการณ์จะเกิดขึ้น (likelihood) ผลกระทบ (Impact) ต่อทรัพยากรแต่ละด้าน และช่วงคะแนน ดังนี้

ตารางที่ ๒ หลักเกณฑ์สำหรับพิจารณาระดับความรุนแรง

ระดับ	โอกาสที่จะเกิดขึ้น (ความถี่ที่จะเกิดขึ้นโดยเฉลี่ย)	ผลกระทบ
สูงมาก (๕)	เกิดขึ้นเป็นประจำ หรือ เกิดมากกว่า ๑ ครั้งต่อปี	- สถานที่ปฏิบัติงานและระบบสาธารณูปโภคหลักเสียหายทั้งหมด
		- ไม่มีวัสดุ/อุปกรณ์สำรอง และไม่สามารถจัดหาได้ภายในระยะเวลาที่กำหนด ส่งผลให้กระบวนการหลักหยุดชะงักทันที
		- ระบบงานหลักหยุดชะงักทั้งหมด/สูญเสียข้อมูลสำคัญแบบถาวร
		- บุคลากรไม่สามารถเข้ามาปฏิบัติงานได้ทั้งหมด/ภารกิจหยุดชะงัก
		- ไม่สามารถติดต่อ/ให้บริการ/รับบริการได้ทั้งหมด

ระดับ	โอกาสที่จะเกิดขึ้น (ความถี่ที่จะเกิดขึ้นโดยเฉลี่ย)	ผลกระทบ
สูง (๔)	เกิดขึ้นค่อนข้างบ่อย หรือ เกิดประมาณ ๑ ครั้งต่อปี	<ul style="list-style-type: none"> - สถานที่ปฏิบัติงานและระบบสาธารณูปโภคหลักส่วนใหญ่เสียหาย แต่ยังใช้งานได้บางส่วน - มีวัสดุ/อุปกรณ์สำรองจำกัด หรือมีผู้จัดหาทดแทนเพียงรายเดียว การจัดส่งล่าช้าเกินระยะเวลาที่ยอมรับได้ (เกิน RTO) ส่งผลกระทบต่อภารกิจหลักบางส่วน - ระบบงานหลักส่วนใหญ่หยุดชะงัก/สูญเสียข้อมูลสำคัญเกินกว่าระดับที่ยอมรับได้ - มีบุคลากรเฉพาะบางส่วนเข้ามาปฏิบัติงาน/ภารกิจหลักบางส่วนหยุดชะงัก - สามารถรื้อติดต่อ/ให้บริการ/รับบริการได้บางส่วน
ปานกลาง (๓)	เกิดขึ้นได้ในบางช่วงเวลา หรือ เกิด ๑ ครั้งในรอบ ๒ - ๓ ปี	<ul style="list-style-type: none"> - สถานที่ปฏิบัติงานและระบบสาธารณูปโภคหลักเสียหายบางส่วน - มีวัสดุ/อุปกรณ์สำรองเพียงพอในระยะสั้น แต่หากเหตุการณ์ยืดเยื้อ จะเริ่มกระทบการดำเนินงาน การจัดส่งล่าช้าแต่ยังควบคุมได้ - ระบบงานหลักบางส่วนหยุดชะงัก/สูญเสียข้อมูลสำคัญในระดับที่ยอมรับได้ - บุคลากรต้องสลับกันเข้ามาปฏิบัติงาน/ภารกิจล่าช้า - สามารถรื้อติดต่อ/ให้บริการ/รับบริการได้ตามช่วงระยะเวลาที่กำหนด
น้อย (๒)	เกิดขึ้นต่ำหรือ เกิด ๑ ครั้งในรอบ ๓ - ๕ ปี	<ul style="list-style-type: none"> - สถานที่ปฏิบัติงานและระบบสาธารณูปโภคหลักเสียหายเล็กน้อย - มีวัสดุ/อุปกรณ์สำรองเพียงพอสำหรับระยะเวลาหนึ่ง และสามารถจัดหาทดแทนได้จากหลายแหล่ง แม้มีความล่าช้าแต่ไม่กระทบภารกิจหลัก - ระบบงานหลักขัดข้องเล็กน้อย/ไม่มีข้อมูลสำคัญสูญหายแต่ได้รับความเสียหาย - บุคลากรส่วนใหญ่สามารถเข้ามาปฏิบัติงานได้/ไม่กระทบภารกิจหลัก - สามารถรื้อติดต่อ/ให้บริการ/รับบริการได้เกือบทั้งหมด
น้อยมาก (๑)	แทบไม่เคยเกิดขึ้น หรือ เกิดน้อยกว่า ๑ ครั้งใน ๕ ปี หรือไม่เคยเกิดมาก่อน	<ul style="list-style-type: none"> - สถานที่ปฏิบัติงานและระบบสาธารณูปโภคหลักไม่ได้รับความเสียหาย - มีวัสดุ/อุปกรณ์สำรองเพียงพอต่อการใช้งาน และมีผู้จัดหาหลายราย สามารถจัดส่งได้ตามปกติ - ไม่กระทบกับระบบงานหลักเลย/ไม่มีข้อมูลสำคัญสูญหายและเสียหาย - บุคลากรสามารถเข้ามาปฏิบัติงานได้ตามปกติ/ภารกิจสามารถดำเนินการได้ตามปกติ - สามารถรื้อติดต่อ/ให้บริการ/รับบริการได้ทั้งหมดตามปกติ

ตารางที่ ๓ ช่วงคะแนนระดับความรุนแรงของผลกระทบ

ช่วงคะแนน	ระดับ	สัญลักษณ์สี	ความหมาย
๒๐ - ๒๕	ระดับสูงมาก		มีโอกาสเกิดสูงมากและมีผลกระทบรุนแรงต่อภารกิจหลัก อาจทำให้องค์กรหยุดชะงัก สูญเสียข้อมูลจำนวนมาก หรือกระทบต่อความมั่นคงขององค์กร
๑๒ - ๑๙	ระดับสูง		มีโอกาสเกิดค่อนข้างสูงและ/หรือมีผลกระทบรุนแรงอาจกระทบภารกิจหลัก ภาพลักษณ์ หรือความเชื่อมั่นขององค์กร
๖ - ๑๑	ระดับปานกลาง		มีโอกาสเกิดขึ้นหรือมีผลกระทบในระดับที่เริ่มกระทบการดำเนินงาน บางส่วน แต่ยังสามารถควบคุมและบริหารจัดการได้
๑ - ๕	ระดับต่ำ		มีโอกาสเกิดต่ำและ/หรือมีผลกระทบจำกัด ไม่ส่งผลกระทบต่อภารกิจหลักขององค์กรอย่างมีนัยสำคัญ

ตารางที่ ๔ สรุปผลกระทบจากเหตุการณ์ต่อทรัพยากรที่สำคัญของ สนช.

เหตุการณ์	โอกาสที่จะเกิดขึ้น	ผลกระทบ				
		ด้านสถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่จำเป็น	ด้านข้อมูลและระบบเทคโนโลยีสารสนเทศ	ด้านบุคลากรหลัก	ด้านผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย
เหตุการณ์แผ่นดินไหวหรืออาคารถล่ม	น้อยมาก (๑)	สูงมาก (๕)	สูงมาก (๕)	สูงมาก (๕)	สูงมาก (๕)	น้อยมาก (๑)
เหตุการณ์อัคคีภัย	น้อยมาก (๑)	สูงมาก (๕)	สูงมาก (๕)	สูงมาก (๕)	สูงมาก (๕)	น้อยมาก (๑)
เหตุการณ์อุทกภัย	น้อยมาก (๑)	น้อย (๒)	ปานกลาง (๓)	น้อยมาก (๑)	น้อย (๒)	น้อย (๒)
เหตุการณ์ไฟฟ้าดับเป็นวงกว้าง	น้อย (๒)	น้อยมาก (๑)	น้อยมาก (๑)	สูงมาก (๕)	น้อยมาก (๑)	น้อยมาก (๑)
เหตุการณ์จราจลการชุมนุมประท้วง* หรือเหตุการณ์ความไม่สงบ**	น้อยมาก (๑)	น้อย (๒)	ปานกลาง (๓)	น้อยมาก (๑)	สูง (๔)	น้อยมาก (๑)
เหตุการณ์โรคระบาดติดต่อร้ายแรง	น้อยมาก (๑)	น้อยมาก (๑)	ปานกลาง (๓)	น้อยมาก (๑)	สูง (๔)	สูง (๔)
เหตุการณ์ภัยคุกคามทางไซเบอร์	สูง (๔)	น้อยมาก (๑)	น้อยมาก (๑)	สูงมาก (๕)	สูง (๔)	น้อย (๒)

หมายเหตุ : * หมายถึง การชุมนุมโดยชอบธรรมตามกฎหมาย ไม่มีการใช้ความรุนแรงหรือกำลังทำลายทรัพย์สิน

** หมายถึง การก่อความไม่สงบ มักมีการใช้ความรุนแรงหรือกำลังทำลายทรัพย์สิน

จัดระดับความรุนแรงโดยคำนวณตามสูตร Risk Score = Likelihood × Impact

ตารางที่ ๕ Risk Heat Map ๕x๕

		ผลกระทบ (Impact)				
		ด้านสถานที่ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ที่จำเป็น	ด้านข้อมูลสารสนเทศและระบบเทคโนโลยี	ด้านบุคลากรหลัก	ด้านรับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย
โอกาสที่จะเกิดขึ้น (likelihood)	แผ่นดินไหว หรือ อาคารถล่ม	๑x๕ (๕)	๑x๕ (๕)	๑x๕ (๕)	๑x๕ (๕)	๑x๑ (๑)
	อัคคีภัย	๑x๕ (๕)	๑x๕ (๕)	๑x๕ (๕)	๑x๕ (๕)	๑x๑ (๑)
	อุทกภัย	๑x๒ (๒)	๑x๓ (๓)	๑x๑ (๑)	๑x๒ (๒)	๑x๒ (๒)
	ไฟฟ้าดับเป็นวงกว้าง	๒x๑ (๒)	๒x๑ (๒)	๒x๕ (๑๐)	๒x๑ (๒)	๒x๑ (๒)
	จราจล การชุมนุมประท้วง* หรือเหตุการณ์ความไม่สงบ**	๑x๒ (๒)	๑x๓ (๓)	๑x๑ (๑)	๑x๔ (๔)	๑x๑ (๑)
	โรคระบาดติดต่อร้ายแรง	๑x๑ (๑)	๑x๓ (๓)	๑x๑ (๑)	๑x๔ (๔)	๑x๔ (๔)
	ภัยคุกคามทางไซเบอร์	๔x๑ (๔)	๔x๑ (๔)	๔x๕ (๒๐)	๔x๔ (๑๖)	๔x๒ (๘)

แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. นี้ ไม่รองรับการปฏิบัติงานในกรณีที่เหตุขัดข้องเกิดขึ้นจากการปฏิบัติงานปกติและเหตุขัดข้องดังกล่าวไม่ส่งผลกระทบในระดับสูงต่อการดำเนินงานและการให้บริการของ สนข. เนื่องจาก ศพท. ยังสามารถจัดการหรือปรับปรุงแก้ไขสถานการณ์ได้ภายในระยะเวลาที่เหมาะสม

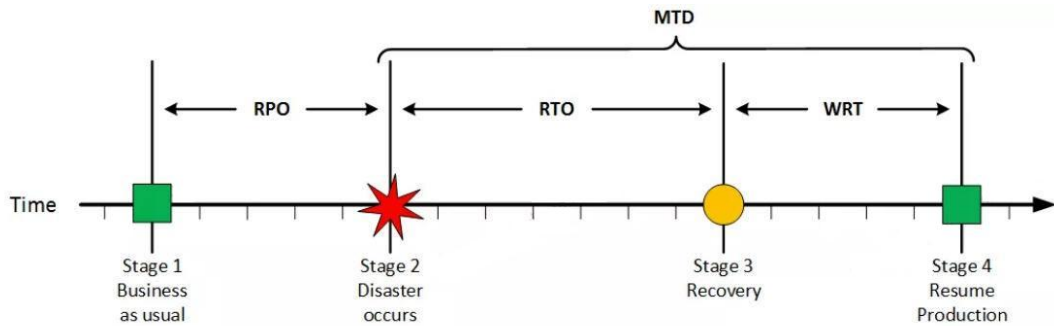
๘. ผลกระทบต่อกระบวนการทำงานหรือการให้บริการ

การวิเคราะห์เพื่อประเมินผลกระทบต่อกระบวนการทำงานหรือการให้บริการ (Business Impact Analysis : BIA) พบว่า มีระบบงานบริการอิเล็กทรอนิกส์ จำนวน ๑๘ ระบบ ที่ส่งผลกระทบต่อกระบวนการทำงานหรือบริการที่สำคัญ สนข. ต้องประเมินระดับผลกระทบในแต่ละช่วงระยะเวลาของการหยุดชะงักที่ไม่สามารถปฏิบัติงานได้ว่าเริ่มส่งผลกระทบเมื่อระบบเริ่มหยุดชะงักไปแล้วเป็นระยะเวลาเท่าใด เพื่อพิจารณา กำหนดค่า MTD^๑ RPO^๒ และ RTO^๓ สำหรับใช้ในแผนการกู้คืนภัยพิบัติ (Disaster Recovery Plan) ซึ่งแบ่งออกเป็น ๕ ช่วงระยะเวลา ได้แก่ ๑ ชั่วโมง / ๖ ชั่วโมง / ๑๒ ชั่วโมง / ๒๔ ชั่วโมง / ๔๘ ชั่วโมง

^๑ Maximum Tolerable Downtime (MTD) คือ ระยะเวลาสูงสุดที่กระบวนการสามารถหยุดชะงักได้ก่อนเกิดผลกระทบรุนแรง

^๒ Recovery Point Objective (RPO) คือ ปริมาณข้อมูลที่ยอมให้สูญเสียได้

^๓ Recovery Time Objective (RTO) คือ ระยะเวลาที่ต้องฟื้นฟูระบบให้กลับมาใช้งานได้



รูปที่ ๒ การกำหนดค่า MTD RPO และ RTO ของ สนข.

ตารางที่ ๖ หลักเกณฑ์การพิจารณาผลกระทบจากการหยุดชะงักของระบบงานบริการอิเล็กทรอนิกส์

ระดับผลกระทบ	หลักเกณฑ์การพิจารณา
สูงมาก	<ul style="list-style-type: none"> - ไม่มีระบบงานสำรองทำงานทดแทน - กระบวนการทำงานหรือการให้บริการหยุดทำงานทั้งหมด ไม่สามารถดำเนินการได้
สูง	<ul style="list-style-type: none"> - มีระบบสำรองแต่สามารถรองรับการทำงานได้เพียงบางส่วน - กระบวนการทำงานหรือการให้บริการดำเนินการได้เพียงบางส่วน เกิดความล่าช้า หรือสะสมงานจำนวนมาก
ปานกลาง	<ul style="list-style-type: none"> - มีวิธีทดแทน เช่น Manual Process - กระบวนการทำงานหรือการให้บริการยังดำเนินการได้ แต่ประสิทธิภาพลดลงอย่างชัดเจน
ต่ำ	<ul style="list-style-type: none"> - ระบบขัดข้องบางฟังก์ชัน มีระบบสำรองรองรับได้เกือบทั้งหมด - กระบวนการทำงานหรือการให้บริการดำเนินต่อไปได้โดยมีผลกระทบเล็กน้อย
ต่ำมาก	<ul style="list-style-type: none"> - มีระบบงานสำรองที่ทำงานทดแทนได้ทันที - กระบวนการทำงานหรือการให้บริการสามารถดำเนินงานได้อย่างต่อเนื่องตามปกติ

ตารางที่ ๗ ระยะเวลาสูงสุดที่ยอมรับได้ในการหยุดชะงักของระบบงานอิเล็กทรอนิกส์

ระบบงานบริการอิเล็กทรอนิกส์	ระดับผลกระทบ	ระยะเวลาหยุดชะงักที่ยอมรับได้ (MTD)				
		๑ ชม.	๒ ชม.	๑๒ ชม.	๒๔ ชม.	๔๘ ชม.
๑. ระบบเว็บท่า (Web Portal)	ต่ำ				✓	
๒. ระบบรายงานผลการดำเนินงานภายใน สนข. (TRS)	ต่ำมาก					✓
๓. ระบบนำทางการเดินทางด้วยขนส่งสาธารณะภายในกรุงเทพมหานครและปริมณฑล (NAMTANG)	สูง		✓			
๔. ระบบฐานข้อมูลสารสนเทศด้านการขนส่งและจราจรเพื่อประเมินขีดความสามารถการแข่งขันของประเทศ (TPI)	ต่ำมาก					✓
๕. แบบจำลองด้านการขนส่งและจราจรระดับประเทศ (National Model : NAM)	ต่ำ				✓	
๖. แบบจำลองการด้านการขนส่งและการจราจรระดับกรุงเทพมหานครและปริมณฑล (Extended Bangkok Urban Area Model : eBUM)	ต่ำ				✓	

ระบบงานบริการอิเล็กทรอนิกส์	ระดับ ผลกระทบ	ระยะเวลาหยุดชะงักที่ยอมรับได้ (MTD)				
		๑ ชม.	๖ ชม.	๑๒ ชม.	๒๔ ชม.	๔๘ ชม.
๗. ระบบห้องสมุดอัตโนมัติ สนข. (OTP Automated Library)	ต่ำมาก					✓
๘. ระบบสารสนเทศทรัพยากรบุคคล สนข. (DPIS)	ต่ำมาก					✓
๙. ระบบสแกนใบหน้าเพื่อลงเวลาทำงาน (OTP Face Scan)	สูง		✓			
๑๐. ระบบโพลภายใน สนข. (OTP POLL)	ต่ำมาก					✓
๑๑. ระบบพิสูจน์ตัวตน	สูง		✓			
๑๒. ระบบเบอร์โทรศัพท์ติดต่อภายใน สนข.	ต่ำมาก					✓
๑๓. ระบบบริหารจัดการเอกสาร สนข. (OTP Document Management : ODM)	ต่ำ				✓	
๑๔. ระบบบริหารจัดการข้อมูลส่วนบุคคล สนข. (OTP Private Cloud)	ปานกลาง			✓		
๑๕. ระบบตรวจสอบพัสดุครุภัณฑ์ สนข. (OTP Inventory)	ต่ำมาก					✓
๑๖. ระบบแจ้งเตือนการประชุมผ่านสื่ออิเล็กทรอนิกส์ ของ สนข.	ปานกลาง			✓		
๑๗. ระบบงานบริหารสำนักงานอัตโนมัติ (e-Office)	สูง		✓			
๑๘. ระบบการเรียนการสอนออนไลน์ของ สนข. (OTP E-Learning)	ต่ำมาก					✓

ตารางที่ ๘ การกำหนดค่า MTD RPO และ RTO

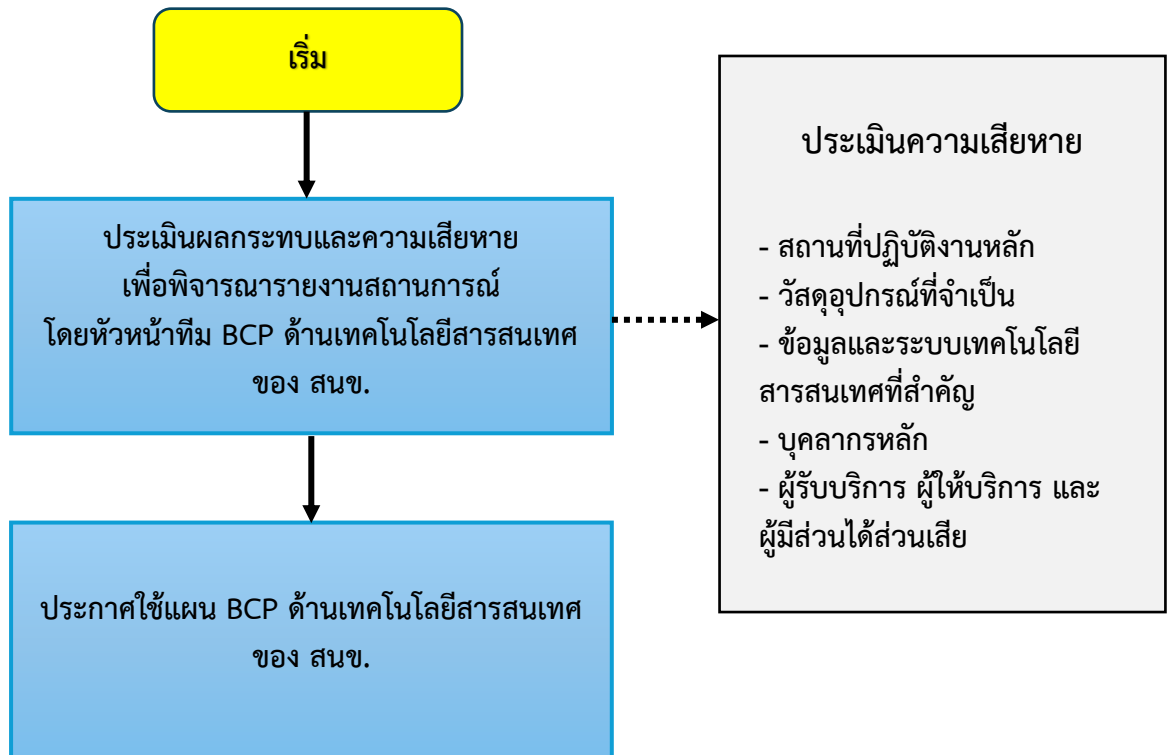
ลำดับที่	กระบวนการหลัก / ระบบงานบริการอิเล็กทรอนิกส์	ระดับ ผลกระทบ	MTPD (ชั่วโมง)	RTO (ชั่วโมง)	RPO (ชั่วโมง)
๑	ระบบเว็บท่า (Web Portal)	ต่ำ	๒๔	๑๒	๘
๒	ระบบรายงานผลการดำเนินงานภายใน สนข. (TRS)	ต่ำมาก	๔๘	๒๔	๑๒
๓	ระบบนำทางการเดินทางด้วยขนส่งสาธารณะ ภายในกรุงเทพมหานครและปริมณฑล (NAMTANG)	สูง	๖	๔	๑
๔	ระบบฐานข้อมูลสารสนเทศด้านการขนส่งและ จราจรเพื่อประเมินขีดความสามารถแข่งขันของ ประเทศ (TPI)	ต่ำมาก	๔๘	๒๔	๑๒
๕	แบบจำลองด้านการขนส่งและจราจรระดับประเทศ (National Model : NAM)	ต่ำ	๒๔	๑๒	๘
๖	แบบจำลองการด้านการขนส่งและการจราจร ระดับกรุงเทพมหานครและปริมณฑล (Extended Bangkok Urban Area Model : eBUM)	ต่ำ	๒๔	๑๒	๘

ลำดับที่	กระบวนการหลัก / ระบบงานบริการอิเล็กทรอนิกส์	ระดับผลกระทบ	MTPD (ชั่วโมง)	RTO (ชั่วโมง)	RPO (ชั่วโมง)
๗	ระบบห้องสมุดอัตโนมัติ สนข. (OTP Automated Library)	ต่ำมาก	๔๘	๒๔	๑๒
๘	ระบบสารสนเทศทรัพยากรบุคคล สนข. (DPIS)	ต่ำมาก	๔๘	๒๔	๑๒
๙	ระบบสแกนใบหน้าเพื่อลงเวลาทำงาน (OTP Face Scan)	สูง	๖	๔	๑
๑๐	ระบบโพลภายใน สนข. (OTP POLL)	ต่ำมาก	๔๘	๒๔	๑๒
๑๑	ระบบพิสูจน์ตัวตน	สูง	๖	๔	๑
๑๒	ระบบเบร็ทโทรศัพท์ติดต่อภายใน สนข.	ต่ำมาก	๔๘	๒๔	๑๒
๑๓	ระบบบริหารจัดการเอกสาร สนข. (OTP Document Management : ODM)	ต่ำ	๒๔	๑๒	๘
๑๔	ระบบบริหารจัดการข้อมูลส่วนบุคคล สนข. (OTP Private Cloud)	ปานกลาง	๑๒	๘	๔
๑๕	ระบบตรวจสอบพัสดุครุภัณฑ์ สนข. (OTP Inventory)	ต่ำมาก	๔๘	๒๔	๑๒
๑๖	ระบบแจ้งเตือนการประชุมผ่านสื่ออิเล็กทรอนิกส์ ของ สนข.	ปานกลาง	๑๒	๘	๔
๑๗	ระบบงานบริหารสำนักงานอัตโนมัติ (e-Office)	สูง	๖	๔	๑
๑๘	ระบบการเรียนการสอนออนไลน์ของ สนข. (OTP E-Learning)	ต่ำมาก	๔๘	๒๔	๑๒

๙. กลไกการบริหารความต่อเนื่องในภาวะวิกฤตของ สนข.

แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. เป็นแนวปฏิบัติที่จะช่วยให้การตอบสนองต่อสภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ที่เกิดจากภัยธรรมชาติ อุบัติเหตุ อุบัติการณ์ โรคระบาด หรือการมุ่งร้ายต่อหน่วยงานไม่ส่งผลกระทบทำให้ภารกิจหลักหรืองานบริการที่สำคัญของ สนข. ต้องหยุดชะงักลงบางส่วนหรือทั้งหมด รวมถึงการลดผลกระทบต่อเป้าหมายของสนข. ให้อยู่ในระดับที่ยอมรับได้ โดยแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. จัดทำขึ้นตามแนวทางการบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Management : BCM) ที่สอดคล้องกับมาตรฐานสากล BS ๒๕๙๙๙ (Business Continuity Management (BCP) Standard) หมายถึง รหัสมาตรฐานของ British Standards Institution (BSI) ที่องค์กรทั่วโลกยอมรับและนำไปใช้ ซึ่ง สนข. ได้กำหนดแนวทางการบริหารความต่อเนื่องในภาวะวิกฤติโดยได้แต่งตั้งทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ หรือ “ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ” ประกอบด้วย หัวหน้าทีมผู้ประสานงาน และทีมงาน โดยจะต้องร่วมมือกันดูแล ติดตาม ปฏิบัติงาน และกู้คืนข้อมูลและระบบเทคโนโลยีสารสนเทศของ สนข. ภายใต้สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินต่าง ๆ ให้กลับสู่สภาวะปกติได้โดยเร็ว

๙.๑ ขั้นตอนการปฏิบัติประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.



รูปที่ ๓ ขั้นตอนการปฏิบัติประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.

๙.๒ ข้อพิจารณาในการยุติการใช้การบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (Business Continuity Plan)

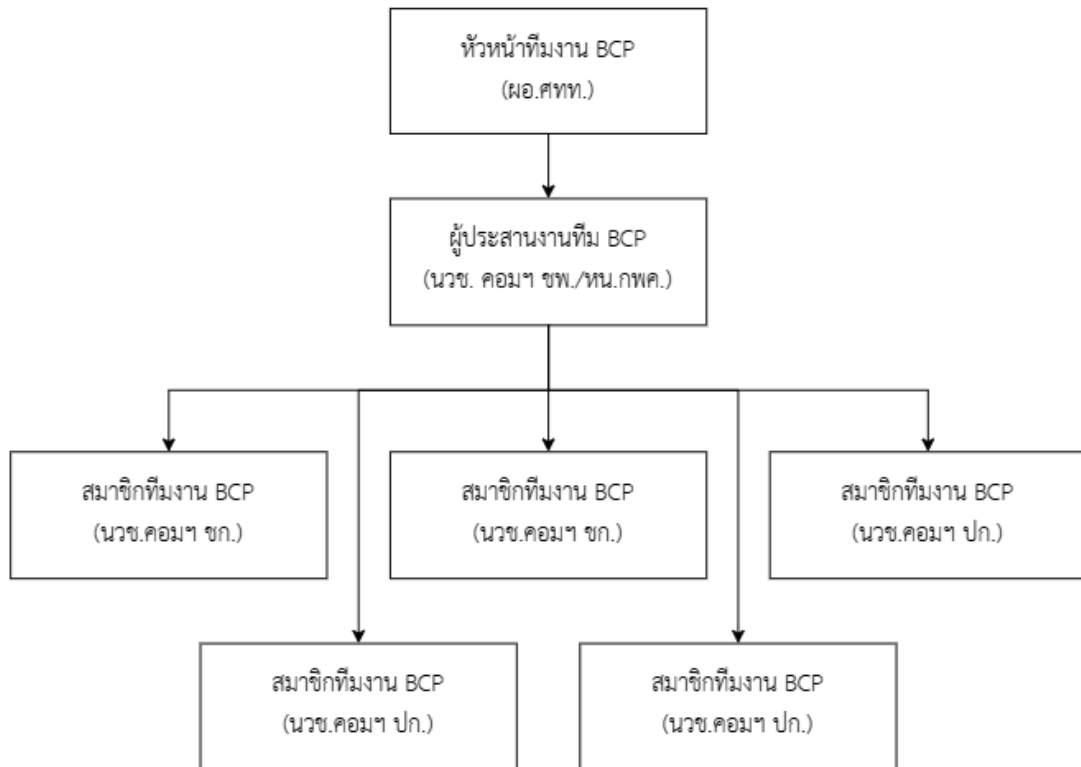
การยุติการใช้การบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ Business Continuity Plan จะสามารถดำเนินการได้ ในกรณีที่เหตุฉุกเฉินหรือภัยพิบัติเข้าสู่ภาวะปกติ และพร้อมดำเนินงานตามขั้นตอนการย้ายระบบกลับสู่สภาวะปกติ โดยพิจารณาแต่ละด้าน

ตารางที่ ๙ เกณฑ์การพิจารณายุติการใช้แผนการบริหารความต่อเนื่องด้านระบบเทคโนโลยีสารสนเทศ

ด้าน	เกณฑ์การพิจารณา
บุคลากร	บุคลากรหลักสามารถกลับมาปฏิบัติงานได้ตามปกติ หรือสามารถจัดหาบุคลากรทดแทนที่สามารถปฏิบัติงานแทนได้
เทคโนโลยีสารสนเทศ	ระบบเทคโนโลยีสารสนเทศสามารถกลับมาใช้งานได้ตามปกติ สามารถเข้าระบบงานได้ตามปกติ
ผู้รับจ้าง	ผู้ให้บริการสามารถกลับมาให้บริการได้ตามปกติหรือสามารถหาผู้บริการรายอื่นเข้ามาให้บริการแทนได้ตามปกติ
อุปกรณ์	อุปกรณ์พร้อมใช้งานครบถ้วนหรือสามารถหาอุปกรณ์ทดแทนอุปกรณ์เดิมได้ครบถ้วน

๑๐. โครงสร้างของทีมงาน BCP ด้านเทคโนโลยีสารสนเทศของ สนช.

๑๐.๑ โครงสร้างของทีมงาน BCP ด้านเทคโนโลยีสารสนเทศกำหนดไว้ ดังนี้



รูปที่ ๔ โครงสร้างทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ)

๑๐.๒ บทบาทหน้าที่ของ ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ กำหนดไว้ ดังนี้

(๑) หัวหน้าทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ คือ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ การขนส่งและจราจร (ผอ.ศทท.) มีหน้าที่

- (๑.๑) กำหนดนโยบาย กำกับ ดูแล และติดตามผลตามแผนดำเนินการกิจอย่างต่อเนื่อง
- (๑.๒) ประเมินลักษณะ ขอบเขต และแนวโน้มของอุบัติการณ์ที่เกิดขึ้น
- (๑.๓) พิจารณาตัดสินใจประกาศใช้แผนดำเนินการกิจอย่างต่อเนื่อง

(๒) ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศ คือ หัวหน้ากลุ่มพัฒนาระบบคอมพิวเตอร์ และเครือข่าย (หน.กพค.) มีหน้าที่

(๒.๑) รายงานข้อมูลข่าวสารหรือเหตุการณ์ที่อาจนำมาซึ่งแนวโน้มการเกิดอุบัติการณ์แก่ หัวหน้าทีม BCP ทราบ

(๒.๒) แจ้งให้ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ ปฏิบัติตามขั้นตอน แนวทางของ แผนดำเนินการกิจอย่างต่อเนื่องฯ ตามที่ประกาศใช้

(๒.๓) ติดตามและประเมินผลการดำเนินการตามแผนดำเนินการกิจอย่างต่อเนื่องฯ

(๓) ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ คือ เจ้าหน้าที่กลุ่มพัฒนาระบบคอมพิวเตอร์ และเครือข่าย ที่ปฏิบัติหน้าที่เป็นทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ มีหน้าที่ ดังนี้

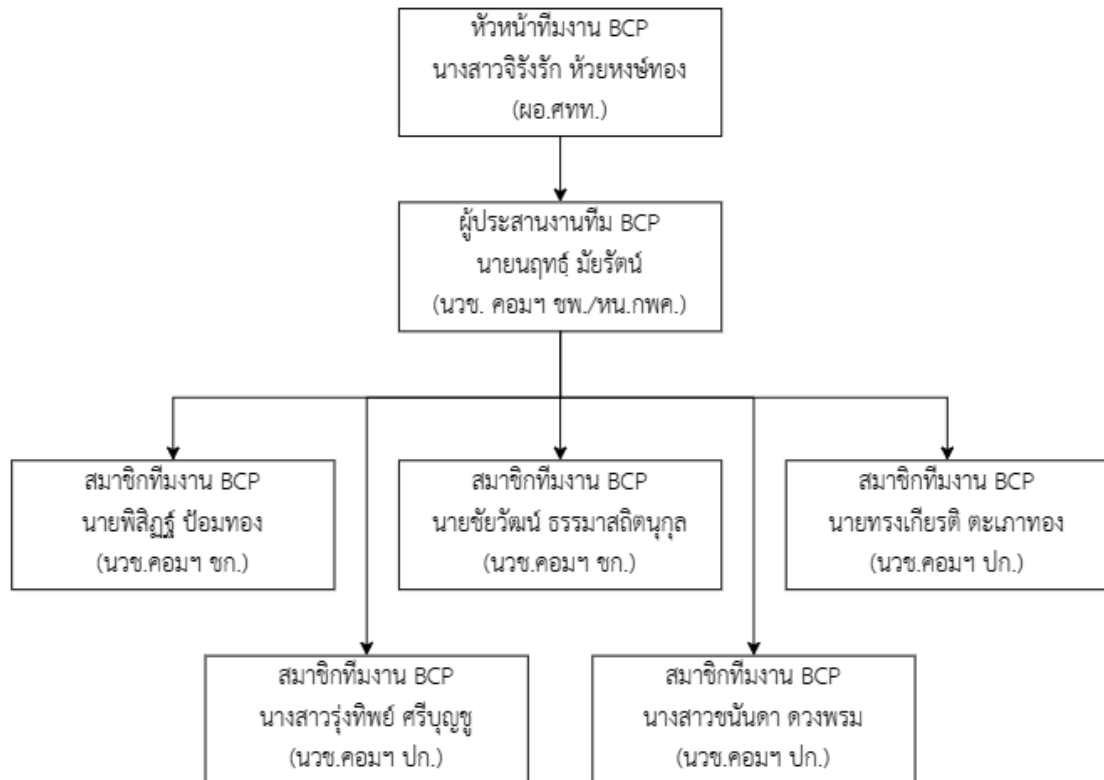
(๓.๑) ดำเนินการตามขั้นตอนและแนวทางการบริหารความต่อเนื่องฯ

(๓.๒) สรรหาทรัพยากรที่ได้กำหนดไว้ในแผนดำเนินการกิจอย่างต่อเนื่องฯ

ตารางที่ ๑๐ รายชื่อบุคลากรและบทบาทของทีมบริหารความต่อเนื่อง (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ)

บุคลากรหลัก	บทบาท	บุคลากรสำรอง
ชื่อ-นามสกุล (เบอร์โทร)		ชื่อ-นามสกุล (เบอร์โทร)
๑. นางสาวจิรัชกร ห้วยหงษ์ทอง ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๐๘ ๐๘ ๑๑๓๘ ๓๘๔๐	หัวหน้าทีมงาน BCP	๑. นายนฤทีร์ มัยรัตน์ ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๕ ๐๙ ๔๙๑๕ ๑๕๓๖
๒. นายนฤทีร์ มัยรัตน์ ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๕ ๐๙ ๔๙๑๕ ๑๕๓๖	ผู้ประสานงานทีม BCP	๒. นายชัยวัฒน์ ธรรมาสถิตนุกูล ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๑๔ ๐๘ ๑๒๐๖ ๕๒๕๔
๓. นายพิสิฐ ป้อมทอง ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๕๑๐ ๐๖ ๔๕๙๔ ๙๔๓๙	สมาชิกทีมงาน BCP	-
๔. นายชัยวัฒน์ ธรรมาสถิตนุกูล ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๑๔ ๐๘ ๑๒๐๖ ๕๒๕๔	สมาชิกทีมงาน BCP	-
๕. นายทรงเกียรติ ตะเภาทอง ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๔๕ ๐๙ ๓๒๔๕ ๕๓๔๒	สมาชิกทีมงาน BCP	-
๖. นางสาวรุ่งทิพย์ ศรีบุญชู ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๔๕ ๐๘ ๓๔๓๒ ๕๖๒๕	สมาชิกทีมงาน BCP	-
๗. นางสาวชนันดา ดวงพรหม ๐ ๒๒๑๕ ๑๕๑๕ ต่อ ๔๐๘๑ ๐๙ ๓๕๓๖ ๖๓๖๔	สมาชิกทีมงาน BCP	-

ทั้งนี้ ในกรณีที่บุคลากรหลักไม่สามารถปฏิบัติหน้าที่ได้ ให้บุคลากรสำรองรับผิดชอบปฏิบัติหน้าที่ในบทบาทของบุคลากรหลัก ปรากฏดังรูปที่ ๒ แผนผังทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ (ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ) ของ สนช.



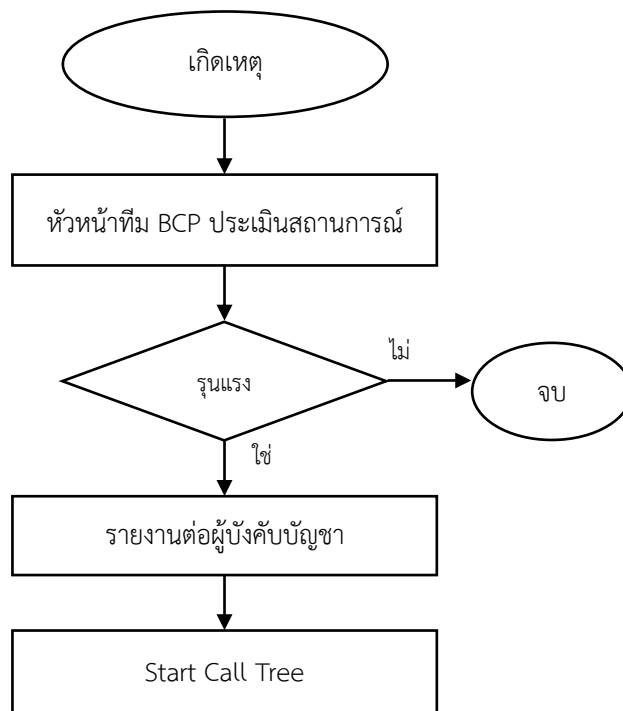
รูปที่ ๕ ทีมบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ
(ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ) ของ สนข.

๑๐.๓ การสื่อสารในสภาวะวิกฤตของ สนข. กำหนดไว้ ดังนี้

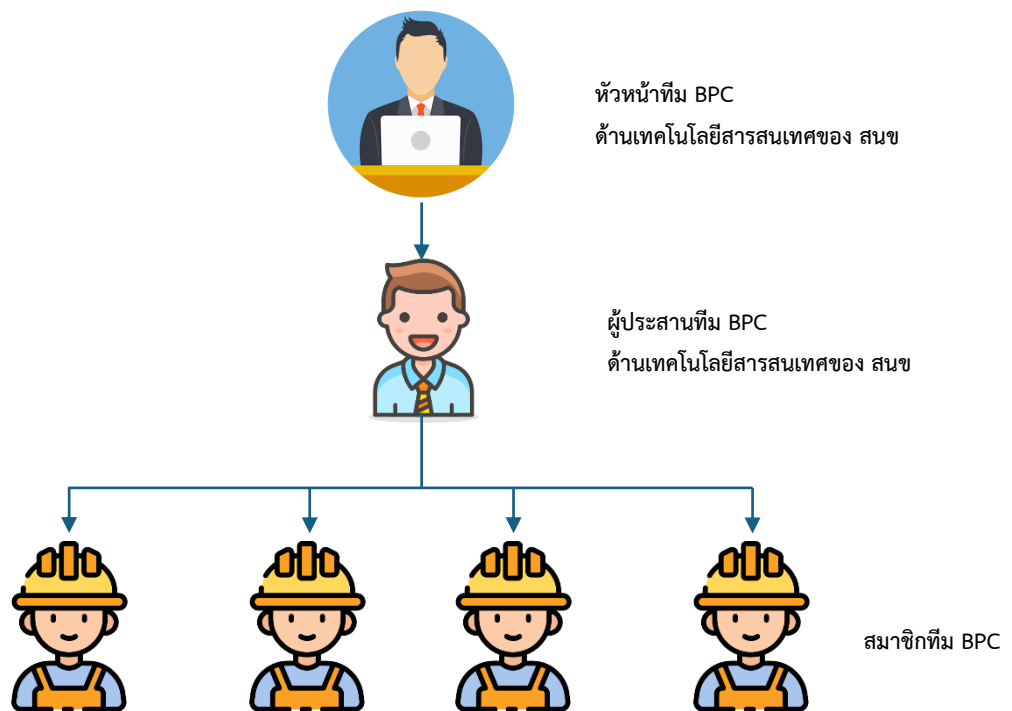
เมื่อเกิดสภาวะวิกฤตจนทำให้ไม่สามารถปฏิบัติงานได้ตามปกติ การสื่อสารในสภาวะวิกฤตที่มีประสิทธิภาพ จะช่วยให้ผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสียมีความเชื่อมั่นในศักยภาพของ สนข. แม้หน่วยงานต้องเผชิญกับเหตุการณ์ร้ายแรงแต่การขับเคลื่อนภารกิจของ สนข. จะยังคงสามารถดำเนินงานได้อย่างต่อเนื่องตามปกติ สามารถบรรลุเป้าหมายที่กำหนดได้อย่างมีประสิทธิภาพและประสิทธิผล ดังนั้น สนข. จึงกำหนดให้มีกระบวนการสื่อสารในสภาวะวิกฤตที่มีประสิทธิภาพ

๑๐.๔ กระบวนการสั่งการและสื่อสารในสภาวะวิกฤต (Call Tree)

กระบวนการ Call Tree คือ กระบวนการแจ้งเหตุฉุกเฉินให้กับสมาชิกทีมงาน BCP ด้านเทคโนโลยีสารสนเทศตามผังรายชื่อ โดยมีวัตถุประสงค์เพื่อบริหารจัดการขั้นตอนในการติดต่อกับสมาชิกในทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ ภายหลังจากมีการประกาศใช้งานแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. ซึ่งมีขั้นตอนกำหนดไว้ ดังนี้



รูปที่ ๖ กระบวนการพิจารณาเพื่อเริ่ม Call Tree



รูปที่ ๗ กระบวนการแจ้งเหตุฉุกเฉินในสถานการณ์ Call Tree

กระบวนการ Call Tree จะเริ่มต้นที่หัวหน้าทีมงาน BCP ด้านเทคโนโลยีสารสนเทศแจ้งให้ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศทราบถึงเหตุการณ์ฉุกเฉิน และการประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. จากนั้น ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศจะแจ้งให้สมาชิกได้รับทราบเหตุการณ์ฉุกเฉินและการประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข. ภายใต้สภาวะวิกฤติ และเหตุการณ์ฉุกเฉินผ่านช่องทางการติดต่อสื่อสารที่ได้กำหนดไว้ในแผนฯ ของ สนข. จำนวน ๓ ช่องทาง ได้แก่ ๑) กลุ่ม line “ข่าวสาร สนข.” ๒) เสียงตามสาย และ ๓) เว็บไซต์ของ สนข. โดยพิจารณา ดังนี้

๑๐.๔.๑ หากเหตุการณ์เกิดขึ้นในเวลาทำการให้ดำเนินการ ดังต่อไปนี้

(๑) ติดต่อผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศเป็นลำดับแรก โดยให้ติดต่อผ่านเบอร์โทรศัพท์หน่วยงานเป็นช่องทางแรก และเบอร์โทรศัพท์เคลื่อนที่เป็นช่องทางถัดมา

(๒) หากไม่สามารถติดต่อผู้ประสานงานหลักของทีม BCP ด้านเทคโนโลยีสารสนเทศได้ ให้ดำเนินการติดต่อผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศ (สำรอง) แทน โดยติดต่อผ่านเบอร์โทรศัพท์หน่วยงานเป็นช่องทางแรก และเบอร์โทรศัพท์เคลื่อนที่เป็นช่องทางถัดมา

๑๐.๔.๒ หากเหตุการณ์เกิดขึ้นนอกเวลาทำการหรือสถานที่ปฏิบัติงานหลักได้รับผลกระทบ ให้ดำเนินการตามขั้นตอนเช่นเดียวกับข้อ ๑๐.๔.๑

๑๐.๔.๓ ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศแจ้งข้อมูลให้แก่สมาชิกภายในทีมงาน BCP ด้านเทคโนโลยีสารสนเทศทราบ ดังต่อไปนี้

(๑) สรุปสถานการณ์ของเหตุการณ์ฉุกเฉินที่เกิดขึ้น ระดับความรุนแรง และความเสียหายในเบื้องต้น

(๒) วัน เวลา และสถานที่สำหรับการนัดหมายทีมงาน BCP ด้านเทคโนโลยีสารสนเทศเพื่อประชุมเร่งด่วน

(๓) การประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศและดำเนินการตามขั้นตอนต่อไป

๑๐.๔.๔ ภายหลังจากได้รับการตอบรับจากทีมงาน BCP ด้านเทคโนโลยีสารสนเทศครบถ้วนตามผังการติดต่อ (Call Tree) เรียบร้อยแล้ว ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศจะต้องแจ้งกลับไปยังหัวหน้าทีมงาน BCP ด้านเทคโนโลยีสารสนเทศเพื่อตรวจสอบความปลอดภัยของชีวิตและทรัพย์สินของบุคลากร ด้าน IT ทั้งหมด รวบรวมและสรุปความพร้อมของ สนข. ในการปฏิบัติตามแผน BCP ด้านเทคโนโลยีสารสนเทศของ สนข.

๑๐.๔.๕ ทีมงาน BCP ด้านเทคโนโลยีสารสนเทศ มีหน้าที่ในการปรับปรุงข้อมูลสำหรับการติดต่อ (Call Tree) ให้เป็นปัจจุบันอยู่เสมอ เพื่อให้กระบวนการติดต่อทีมงาน BCP ด้านเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและสำเร็จลุล่วงภายในระยะเวลาที่คาดหวัง ในกรณีที่เกิดเหตุการณ์ฉุกเฉิน และมีการประกาศใช้แผน BCP ด้านเทคโนโลยีสารสนเทศ นอกจากการมีกระบวนการแจ้งเหตุฉุกเฉินในสถานการณ์ Call Tree ที่มีประสิทธิภาพแล้ว การสื่อสารกับผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย ก็ถือเป็นสิ่งสำคัญอย่างยิ่งที่จะทำให้เกิดความเชื่อมั่นในการดำเนินงานและให้บริการของ สนข. ในสภาวะวิกฤติ และเหตุการณ์ฉุกเฉินต่าง ๆ เนื่องจากผู้รับบริการ ผู้ให้บริการ และผู้มีส่วนได้ส่วนเสียจะต้องการรับรู้ข้อมูลอย่างชัดเจน ครบถ้วนถูกต้อง และรวดเร็ว

๑๑. การกำหนดกลยุทธ์ในการสร้างความต่อเนื่อง

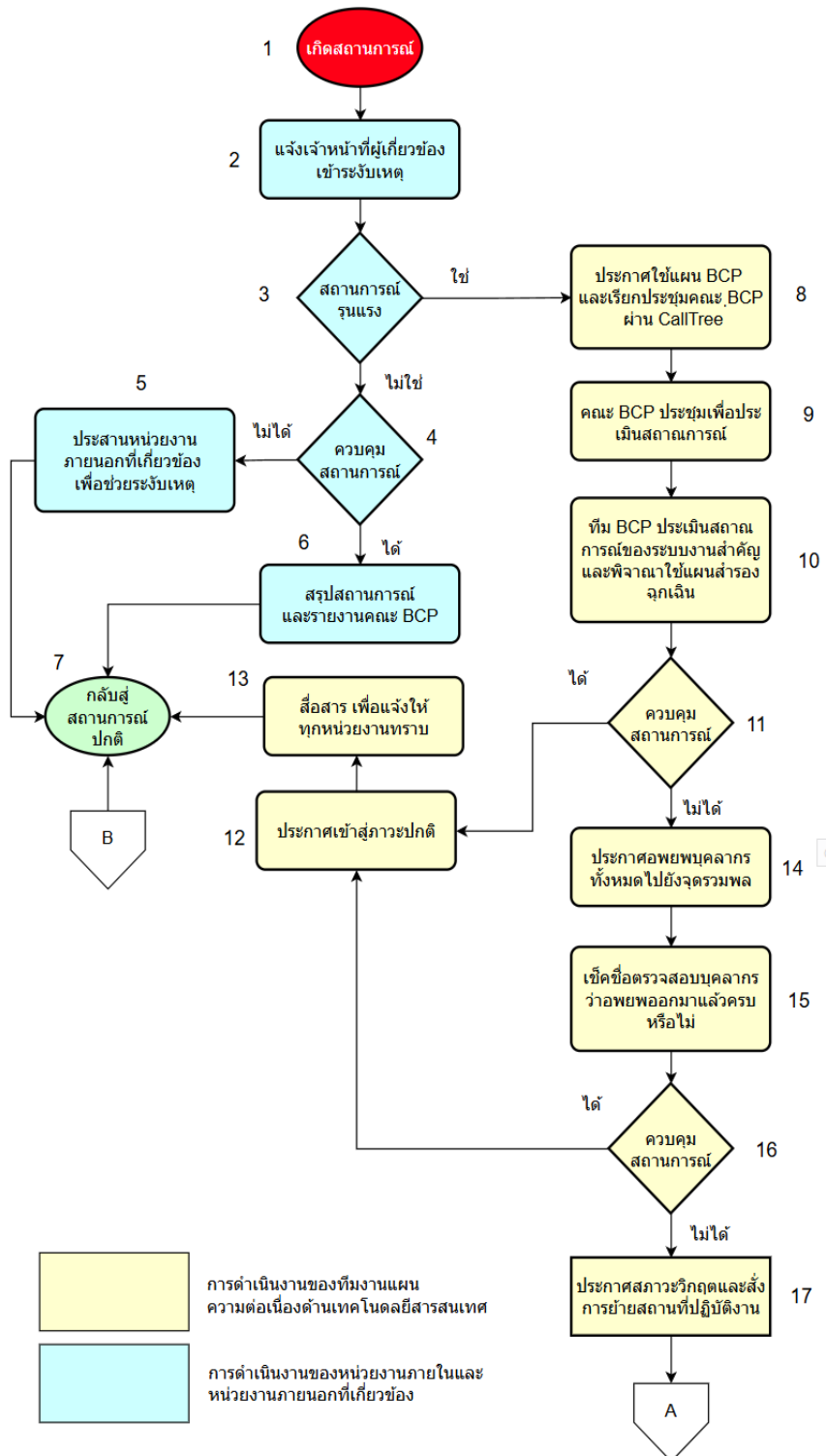
กลยุทธ์ความต่อเนื่องเป็นแนวทางในการจัดหาและบริหารจัดการทรัพยากรให้มีความพร้อมเมื่อเกิดสภาวะวิกฤต ซึ่งพิจารณาทรัพยากรใน ๕ ด้าน ดังนี้

ตารางที่ ๑๑ การกำหนดกลยุทธ์ความต่อเนื่อง

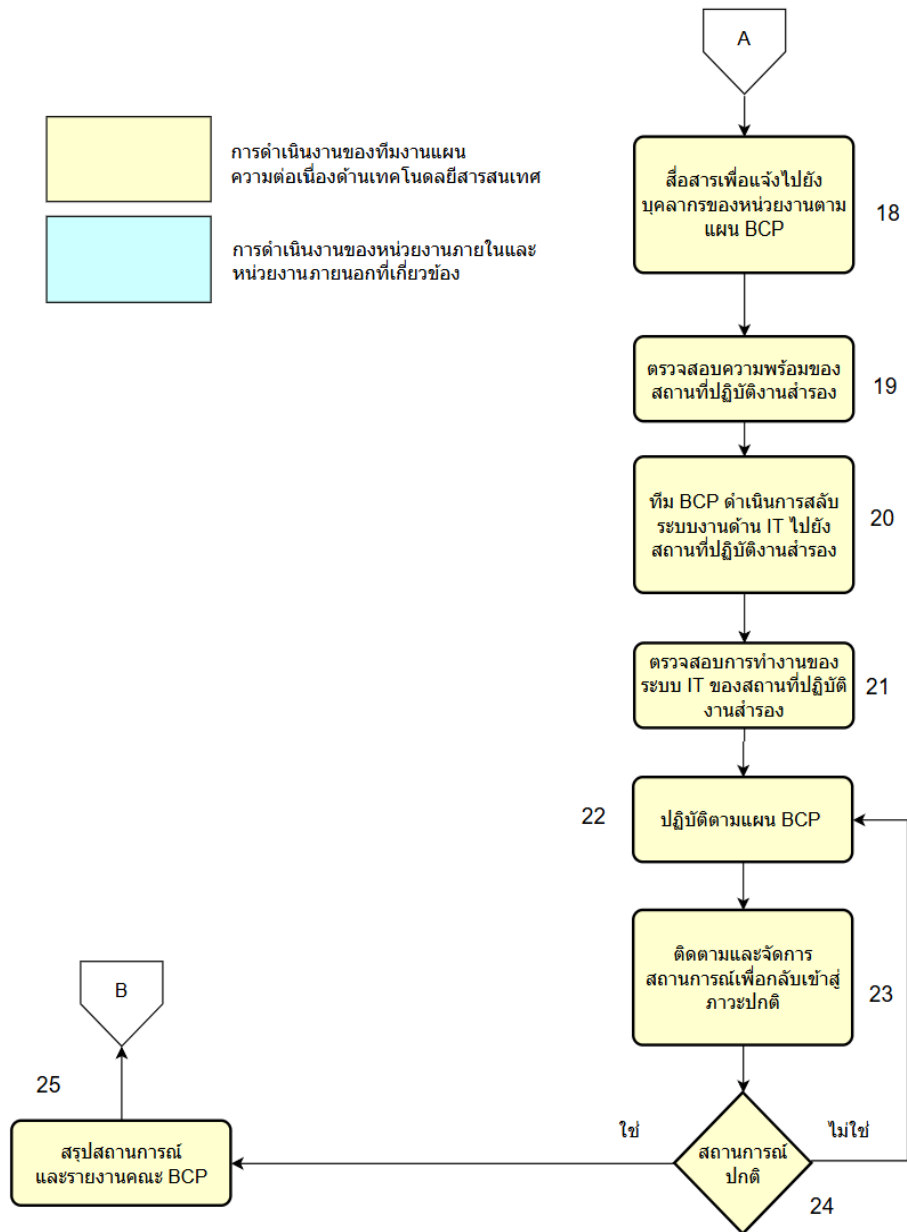
ทรัพยากร	กลยุทธ์ความต่อเนื่อง
ด้านสถานที่ปฏิบัติงานหลัก	๑. หากโครงสร้างอาคารของสถานที่ปฏิบัติงานหลักได้รับความเสียหายจนไม่สามารถใช้ปฏิบัติงานได้ และจำเป็นต้องใช้สถานที่ปฏิบัติงานสำรอง ให้พิจารณามาตรการ ดังต่อไปนี้
	๒. จัดหาและเตรียมอาคาร/สถานที่ปฏิบัติงานสำรองจากหน่วยงานราชการอื่น ๆ ในกระทรวงคมนาคม หรือหน่วยงานราชการอื่น ๆ
	๓. จัดหาและเตรียมอาคาร/สถานที่ปฏิบัติงานสำรองกับภาคเอกชน อาทิ โรงแรม สำนักงาน
	๔. กำหนดแนวทางให้บุคลากรปฏิบัติงานที่บ้านพัก (Work from Home)
ด้านวัสดุอุปกรณ์ที่จำเป็น	๑. จัดเตรียมเครื่องมือและอุปกรณ์สำรอง เพื่อใช้ในสภาวะวิกฤตและเหตุการณ์ฉุกเฉิน
	๒. ทำข้อตกลงกับหน่วยงานราชการหรือภาคเอกชน เพื่อขอยืมเครื่องมือและอุปกรณ์
	๓. ดำเนินการจัดซื้อเครื่องมือและอุปกรณ์ ผ่านกระบวนการจัดซื้อจัดจ้างพิเศษ
ด้านข้อมูลสารสนเทศและระบบเทคโนโลยี	๑. ประสานงานกับหน่วยงานเทคโนโลยี เพื่อจัดเตรียมและให้มีระบบงานเทคโนโลยีหรือระบบสารสนเทศสำรอง
	๒. ปฏิบัติงานโดยไม่ใช้ระบบงานเทคโนโลยี (Manual) ไปก่อน แล้วจึงป้อนข้อมูลเข้าในระบบเมื่อกลับคืนสู่สภาวะปกติ
	๓. จัดหาพื้นที่บนระบบ Cloud หรือ Server ของหน่วยงาน เพื่อให้เจ้าหน้าที่จัดเก็บข้อมูล และสามารถปฏิบัติงานนอกสำนักงานได้
	๔. พัฒนาระบบการให้บริการของหน่วยงาน เป็นระบบ e-service
ด้านบุคลากรหลัก	๑. กำหนดให้มีบุคลากรหลักและบุคลากรสำรองทำงานทดแทนกันได้ในสภาวะวิกฤต
	๒. กำหนดแนวทางและกลุ่มบุคลากรที่สามารถขอให้ช่วยปฏิบัติงานชั่วคราวจากหน่วยงานราชการอื่น ๆ ในกระทรวงคมนาคม
ด้านผู้รับบริการ/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย	๑. กำหนดให้มีคู่ค้า/ผู้ให้บริการสำรอง/ผู้มีส่วนได้ส่วนเสีย เพื่อเรียกใช้บริการได้ในสภาวะวิกฤต
	๒. พิจารณากระจายความเสี่ยง โดยมีคู่ค้า/ผู้ให้บริการ มากกว่า ๑ ราย สำหรับให้บริการแก่หน่วยงาน

๑๒ ขั้นตอนการบริหารความต่อเนื่องและการกอบกู้กระบวนการ

ขั้นตอนการบริหารความต่อเนื่องและการตอบสนองต่อเหตุการณ์ทันทีภายใน ๒๔ ชั่วโมง มีดังนี้



รูปที่ ๘ ขั้นตอนการบริหารความต่อเนื่องต่อเนื่องและการตอบสนองต่อเหตุการณ์



รูปที่ ๙ ขั้นตอนการบริหารความต่อเนื่องต่อเนื่องและการตอบสนองต่อเหตุการณ์ (ต่อ)

วันที่ ๑ (ภายใน ๒๔ ชั่วโมง) การตอบสนองต่อเหตุการณ์ทันที

ในการปฏิบัติการใด ๆ ให้ทีมงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและผู้อื่น และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่ สนข. กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอน ที่	กิจกรรม	บทบาท ความรับผิดชอบ	ดำเนินการ	
			แล้วเสร็จ	ยังไม่เสร็จ
๑	ผู้ประสานงานทีม BCP ด้านเทคโนโลยีสารสนเทศ แจ้งเหตุฉุกเฉิน ตามผังรายชื่อและเบอร์โทรศัพท์ ของกระบวนการ Call Tree ให้กับหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ และสมาชิกภายในทีมทราบ		☐	☐
๒	ประชุมทีมงานอย่างเร่งด่วน เพื่อประเมินความเสียหาย ผลกระทบต่อการดำเนินงาน การให้บริการ และทรัพยากร สำคัญที่จำเป็นต้องใช้ในการดำเนินการบริหารความต่อเนื่อง ด้านเทคโนโลยีสารสนเทศ		☐	☐
๓	ทบทวนกระบวนการงานที่มีความเร่งด่วน หรือส่งผลกระทบ อย่างสูงหากไม่ทำการดำเนินการ และจำเป็นต้องดำเนินงาน หรือปฏิบัติด้วยมือ (Manual Processing)		☐	☐
๔	สำรวจ ระบุ และสรุปรายชื่อสมาชิก BCP Team ด้านเทคโนโลยีสารสนเทศที่ได้รับบาดเจ็บ หรือเสียชีวิต หรือไม่พร้อมปฏิบัติหน้าที่		☐	☐
๕	รายงานหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศทราบ โดยครอบคลุมประเด็น ดังนี้ - จำนวนและรายชื่อสมาชิก BCP Team ด้านเทคโนโลยี สารสนเทศที่ได้รับบาดเจ็บ/เสียชีวิต/ไม่สามารถปฏิบัติงานได้ - ความเสียหายและผลกระทบต่อการดำเนินงาน และการให้บริการระบบงานสารสนเทศ - ทรัพยากรสำคัญที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ด้านเทคโนโลยีสารสนเทศ - กระบวนการที่มีความเร่งด่วนและส่งผลกระทบอย่างสูง หากไม่ดำเนินการและจำเป็นต้องดำเนินงานหรือปฏิบัติงาน ด้วยมือ		☐ ☐ ☐ ☐	☐ ☐ ☐ ☐
๖	สื่อสารและรายงานสถานการณ์แก่สมาชิกภายในทีม BCP ด้านเทคโนโลยีสารสนเทศให้ทราบตามเนื้อหาและข้อความ ที่ได้รับการพิจารณาและเห็นชอบจากหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศแล้ว		☐	☐
๗	ประเมินและระบุกระบวนการหลักและงานเร่งด่วนที่จำเป็นต้อง ดำเนินการให้แล้วเสร็จภายใน ๑- ๕ วัน ข้างหน้า		☐	☐
๘	ประเมินศักยภาพและความสามารถของ สนข. ในการดำเนินงาน เร่งด่วนข้างต้นภายใต้ข้อจำกัดและสภาวะวิกฤต พร้อมระบุ ทรัพยากรที่จำเป็นต้องใช้ในแผนดำเนินธุรกิจอย่างต่อเนื่อง สำหรับการบริหารความพร้อมต่อสภาวะวิกฤตของ สนข.		☐	☐

ขั้นตอน ที่	กิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการ	
			แล้วเสร็จ	ยังไม่เสร็จ
๙	รายงานความคืบหน้าให้แก่หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศทราบ พร้อมขออนุมัติการดำเนินงานหรือปฏิบัติงานด้วยมือ (Manual Processing) สำหรับกระบวนการที่มีความเร่งด่วนและส่งผลกระทบอย่างสูงหากไม่ดำเนินการ		☐	☐
๑๐	ติดต่อและประสานงานกับหน่วยงานที่เกี่ยวข้องในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในการบริหารความต่อเนื่อง ได้แก่ <ul style="list-style-type: none"> - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - ข้อมูลและระบบเทคโนโลยีสารสนเทศ - บุคลากรหลัก - ด้านผู้ให้บริการหรือผู้มีส่วนได้ส่วนเสีย 		☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
๑๑	พิจารณาดำเนินการหรือปฏิบัติงานด้วยมือ (Manual Processing) เฉพาะงานเร่งด่วน หากไม่ดำเนินการจะส่งผลกระทบอย่างสูงและไม่สามารถรอได้ ทั้งนี้ต้องได้รับการอนุมัติ		☐	☐
๑๒	ระบุหน่วยงานที่เป็นคู่ค้า/ผู้ให้บริการสำหรับงานเร่งด่วนเพื่อแจ้งสถานการณ์และแนวทางในการบริหารงานให้มีความต่อเนื่องตามความเห็นของทีม BCP ด้านเทคโนโลยีสารสนเทศ		☐	☐
๑๓	บันทึก (Log Book) และทบทวนกิจกรรมและงานต่าง ๆ ที่ต้องดำเนินการ (พร้อมระบุรายละเอียด ผู้ดำเนินการ และเวลา) อย่างสม่ำเสมอ		☐	☐
๑๔	สรุปสถานการณ์และขั้นตอนการดำเนินการสำหรับในวันถัดไป เพื่อแจ้งให้กับบุคลากร สนข. รับทราบและดำเนินการ อาทิ วัน เวลา และสถานที่ปฏิบัติงานสำรอง		☐	☐
๑๕	รายงานความคืบหน้าให้แก่หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศทราบอย่างสม่ำเสมอหรือตามที่ได้กำหนดไว้		☐	☐

วันที่ ๒-๗ การตอบสนองในระยะสั้น

ในการปฏิบัติการใด ๆ ให้ทีมงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและผู้อื่น และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่ สนข. กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอน ที่	ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการ	
			แล้วเสร็จ	ยังไม่เสร็จ
๑	ติดตามสถานะการกู้คืน (Recovery) ทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็น และระยะเวลาที่ต้องใช้ในการกู้คืน (MTD)		☐	☐

ขั้นตอน ที่	ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการ	
			แล้วเสร็จ	ยังไม่เสร็จ
๒	ตรวจสอบความพร้อมและข้อกำหนดในการจัดหาทรัพยากร ที่จำเป็นต้องใช้ในแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับ การบริหารความพร้อมต่อสภาวะวิกฤตของ สนข. ได้แก่ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - ข้อมูลและระบบเทคโนโลยีสารสนเทศ - บุคลากรหลัก - ด้านผู้ให้บริการหรือผู้มีส่วนได้ส่วนเสีย		☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
๓	รายงานหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมประเด็นความพร้อม ข้อกำหนด และข้อเสนอแนะ ในการจัดหาทรัพยากรที่จำเป็นต้องใช้ในแผนดำเนินธุรกิจ อย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤต ของ สนข.		☐	☐
๔	ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ ในแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหาร ความพร้อมต่อสภาวะวิกฤตของ สนข. ได้แก่ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - ข้อมูลและระบบเทคโนโลยีสารสนเทศ - บุคลากรหลัก - ด้านผู้ให้บริการหรือผู้มีส่วนได้ส่วนเสีย		☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
๕	ดำเนินการจัดหาข้อมูลและรายงานต่าง ๆ ที่จำเป็นต้องใช้ ในการดำเนินงานและให้บริการ		☐	☐
๖	ดำเนินงานและให้บริการภายใต้ทรัพยากรที่จัดหา เพื่อการบริหารความพร้อมต่อสภาวะวิกฤตของ สนข. ดังต่อไปนี้ - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - ข้อมูลและระบบเทคโนโลยีสารสนเทศ - บุคลากรหลัก - ด้านผู้ให้บริการหรือผู้มีส่วนได้ส่วนเสีย		☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
๗	แจ้งสถานการณ์และแนวทางในการบริหารความพร้อม ต่อสภาวะวิกฤตของ สนข. แก่บุคลากร/ผู้ให้บริการ/ ผู้มีส่วนได้ส่วนเสีย ที่ได้รับผลกระทบ		☐	☐
๘	บันทึก (Log Book) และทบทวนกิจกรรมและงานต่าง ๆ พร้อมระบุรายละเอียด ผู้ดำเนินการ และเวลา (อย่างสม่ำเสมอ)		☐	☐
๙	สรุปสถานการณ์และขั้นตอนการดำเนินการสำหรับในวันถัดไป เพื่อแจ้งให้กับบุคลากร สนข. รับทราบและดำเนินการ อาทิ วัน เวลา และสถานที่ปฏิบัติงานสำรอง		☐	☐
๑๐	รายงานความคืบหน้าให้แก่หัวหน้าทีม BCP ด้านเทคโนโลยี สารสนเทศทราบ อย่างสม่ำเสมอ หรือตามที่ได้กำหนดไว้		☐	☐

วันที่ ๘ การตอบสนองระยะกลาง (๑ สัปดาห์)

ในการปฏิบัติการใด ๆ ให้ทีมงาน คำนึงถึงความปลอดภัยในชีวิตของตนเองและผู้อื่น และปฏิบัติตามแนวทางและแผนเผชิญเหตุและขั้นตอนการปฏิบัติงานที่ สนข. กำหนดขึ้นอย่างเคร่งครัด

ขั้นตอน ที่	ขั้นตอนและกิจกรรม	บทบาทความรับผิดชอบ	ดำเนินการ	
			แล้วเสร็จ	ยังไม่เสร็จ
๑	ติดตามสถานะการกู้คืน (Recovery) ทรัพยากรที่ได้รับผลกระทบ ประเมินความจำเป็น และระยะเวลาที่ต้องใช้ในการกู้คืน (MTD)		☐	☐
๒	ระบุทรัพยากรที่จำเป็นต้องใช้เพื่อการดำเนินงานและให้บริการ		☐	☐
๓	รายงานหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ โดยครอบคลุมประเด็น สถานะการกู้คืน (Recovery) ทรัพยากรที่ได้รับผลกระทบ และทรัพยากรที่จำเป็นต้องใช้ในแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤตของ สนข.		☐	☐
๔	ประสานงานและดำเนินการจัดหาทรัพยากรที่จำเป็นต้องใช้ในแผนดำเนินธุรกิจอย่างต่อเนื่องสำหรับการบริหารความพร้อมต่อสภาวะวิกฤตของ สนข. ได้แก่ <ul style="list-style-type: none"> - สถานที่ปฏิบัติงานสำรอง - วัสดุอุปกรณ์ที่สำคัญ - ข้อมูลและระบบเทคโนโลยีสารสนเทศ - บุคลากรหลัก - ด้านผู้ให้บริการหรือผู้มีส่วนได้ส่วนเสีย 		☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
๕	สรุปสถานการณ์และการเตรียมความพร้อมด้านทรัพยากรต่าง ๆ เพื่อดำเนินงานและให้บริการตามปกติให้กับบุคลากร สนข. รับทราบ		☐	☐
๖	บันทึก (Log Book) และทบทวนกิจกรรมและงานต่าง ๆ พร้อมระบุรายละเอียด ผู้ดำเนินการ และเวลา (อย่างสม่ำเสมอ)		☐	☐
๗	๗ รายงานความคืบหน้าให้แก่หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ ทราบ อย่างสม่ำเสมอ หรือตามที่ได้กำหนดไว้		☐	☐

ส่วนที่ ๒ : แผนและแนวทางปฏิบัติในสถานการณ์ฉุกเฉินจากสภาวะวิกฤตต่าง ๆ

สถานการณ์ฉุกเฉินจากสภาวะวิกฤตต่าง ๆ ได้แก่

๑. เหตุการณ์แผ่นดินไหว หรืออาคารถล่ม
๒. เหตุการณ์อัคคีภัย
๓. เหตุการณ์อุทกภัย
๔. เหตุการณ์ไฟฟ้าดับเป็นวงกว้าง
๕. เหตุการณ์จลาจล การชุมนุมประท้วง หรือเหตุการณ์ความไม่สงบ
๖. เหตุการณ์โรคระบาดติดต่อร้ายแรง
๗. เหตุการณ์ภัยคุกคามทางไซเบอร์

ขั้นตอน/แนวทางปฏิบัติ

ขั้นตอน/แนวทางปฏิบัติที่ผู้เกี่ยวข้องจะต้องถือปฏิบัติตามช่วงเวลาที่เกิดเหตุการณ์หรือสถานการณ์ฉุกเฉินจากสภาวะวิกฤตในแต่ละเหตุการณ์ แบ่งเป็น ๓ ช่วงเวลา ประกอบด้วย

๑. **ก่อนเกิดเหตุการณ์** มุ่งเน้นที่การเฝ้าระวัง การเตรียมความพร้อม การป้องกันและลดความเสียหาย การเตรียมวัสดุอุปกรณ์ที่จำเป็น การวางแผนจัดอบรมและฝึกซ้อมสถานการณ์จำลอง อย่างน้อยปีละ ๑ ครั้ง

๒. **เมื่อเกิดเหตุการณ์** เข้าสู่สภาวะวิกฤต ซึ่งเป็นผลทำให้การปฏิบัติงานขององค์กรหยุดชะงัก มุ่งเน้นการปฏิบัติตามขั้นตอนให้เป็นที่ไปตามแผน ในเรื่องการแจ้งเตือนและการระงับเหตุ การอพยพ การสื่อสารและการรายงานสถานการณ์ให้ผู้เกี่ยวข้องทราบ

๓. **เมื่อเหตุการณ์กลับเข้าสู่สภาวะปกติ** มุ่งเน้นการฟื้นฟูและการปฏิบัติงานต่อเนื่อง

๑. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์แผ่นดินไหว หรืออาคารถล่ม ดำเนินการ ดังนี้

๑.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๑.๑.๑ ตรวจสอบการยึดอุปกรณ์ภายในตู้ Rack ในห้องเซิร์ฟเวอร์ ชั้น ๔ และตู้ Rack อุปกรณ์เครือข่ายทุกชั้นให้มั่นคงกับพื้นหรือผนัง เพื่อป้องกันการล้มคว่ำหรือหลุดขณะเกิดเหตุสั่นสะเทือน

๑.๑.๒ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือจัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๑.๑.๓ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๑.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๑.๒.๑ ให้เจ้าหน้าที่ดำเนินการตามแผน BCP ของหน่วยงาน

๒.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๑.๓.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์ หากสถานการณ์คลี่คลายและปลอดภัยแล้ว ให้แจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศ เพื่อเข้าตรวจสอบเหตุการณ์และสถานที่

๑.๓.๒ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบพื้นที่ในส่วนที่เกี่ยวข้อง เช่น ห้องเซิร์ฟเวอร์ ห้องจัดเก็บอุปกรณ์

๑.๓.๓ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบทรัพย์สินสารสนเทศ เช่น ระบบคอมพิวเตอร์ ระบบสายสัญญาณ และตู้ Rack จัดเก็บอุปกรณ์

๑.๓.๔ ในกรณีเกิดความเสียหายขึ้นกับพื้นที่หรือทรัพย์สินสารสนเทศให้รายงานความเสียหายทั้งหมดต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ

๑.๓.๕ ทดสอบเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๒. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อัคคีภัย (กรณีเพลิงไหม้ภายในห้องเซิร์ฟเวอร์) ดำเนินการ ดังนี้

๒.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๒.๑.๑ ตรวจสอบระบบดับเพลิงอัตโนมัติด้วยสารสะอาด ระบบตรวจจับ และระบบแจ้งเตือนให้พร้อมใช้งานอยู่เสมอ

๒.๑.๒ ตรวจสอบและดูแลระบบไฟฟ้าและระบบเครื่องสำรองไฟฟ้า (UPS) ให้สามารถใช้งานได้เป็นปกติอยู่เสมอ

๒.๑.๓ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือ จัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๒.๑.๔ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๒.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๒.๒.๑ เมื่อตรวจพบเหตุเพลิงไหม้ภายในห้องเซิร์ฟเวอร์ ระบบแจ้งเตือนและระบบดับเพลิงอัตโนมัติด้วยสารสะอาดจะทำงานโดยอัตโนมัติ เพื่อปล่อยสารดับเพลิงดับไฟโดยไม่ทำให้อุปกรณ์ทรัพย์สินสารสนเทศเสียหาย

๒.๒.๒ เมื่อระบบดับเพลิงอัตโนมัติทำงาน ทีม BCP ด้านเทคโนโลยีสารสนเทศตัดกระแสไฟฟ้าที่จ่ายเข้าห้องเซิร์ฟเวอร์เพื่อป้องกันเพลิงลุกลามซ้ำ

๒.๒.๓ หัวหน้าทีม BCP พิจารณาเหตุการณ์ หากกรณีที่เหมาะสมแล้วว่าเหตุสงบลงแล้วให้รายงานผลให้ผู้บริหารทราบ

๒.๒.๔ หากกรณีที่เหมาะสมแล้วยังไม่สามารถควบคุมเหตุได้ ให้เร่งแจ้งเหตุต่อผู้บริหารเพื่อพิจารณาเข้าสู่ภาวะเพลิงไหม้อาคาร และพิจารณาประกาศใช้แผน BCP ของหน่วยงานต่อไป

๓.๒.๕ ปิดกั้นพื้นที่ไม่ให้บุคคลที่ไม่เกี่ยวข้องเข้าห้องเซิร์ฟเวอร์ หรือบริเวณที่เกิดเหตุ

๒.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๒.๓.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์ หากสถานการณ์คลี่คลายและปลอดภัยแล้ว ให้แจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศ เพื่อเข้าตรวจสอบเหตุการณ์และสถานที่

๒.๓.๒ ทีม BCP ด้านเทคโนโลยีสารสนเทศประสานผู้เชี่ยวชาญเพื่อตรวจสอบโครงสร้างพื้นฐานของห้องเซิร์ฟเวอร์

๒.๓.๓ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบทรัพย์สินสารสนเทศ เช่น ระบบคอมพิวเตอร์ ระบบสายสัญญาณ และตู้ Rack จัดเก็บอุปกรณ์ และประเมินความเสียหาย

๒.๓.๔ ในกรณีเกิดความเสียหายขึ้นกับพื้นที่หรือทรัพย์สินสารสนเทศให้รายงานความเสียหายทั้งหมดต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ

๒.๓.๕ หากสำรวจแล้วไม่ได้รับความเสียหายให้ทยอยเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๓. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อัคคีภัย (กรณีเพลิงไหม้ตัวอาคาร สนข.) ดำเนินการ ดังนี้

๓.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๓.๑.๑ ตรวจสอบระบบดับเพลิงอัตโนมัติด้วยสารสะอาด ระบบตรวจจับ และระบบแจ้งเตือนให้พร้อมใช้งานอยู่เสมอ

๓.๑.๒ ตรวจสอบและดูแลระบบไฟฟ้าและระบบเครื่องสำรองไฟฟ้า (UPS) ให้สามารถใช้งานได้เป็นปกติอยู่เสมอ

๓.๑.๓ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือ จัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๓.๑.๔ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๓.๑.๕ ชักซ้อมการอพยพและการประกาศใช้แผน IRP (Incident Response Plan)

๓.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๓.๒.๑ หากตรวจพบเพลิงหรือกลุ่มควันในอาคาร ให้กดสัญญาณแจ้งเหตุและใช้ถังดับเพลิงระงับเหตุเบื้องต้น (หากปลอดภัย)

๓.๒.๒ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ ประเมินว่าไม่สามารถควบคุมสถานการณ์เพลิงไหม้ภายในอาคารได้หรือไม่ หากพบว่าเหตุยังคงดำเนินอยู่ ให้รีบแจ้งเจ้าหน้าที่ทุกคนเพื่อดำเนินการตามแผน BCP ของหน่วยงานทันที

๓.๒.๓ ให้เจ้าหน้าที่ดำเนินการตามแผน BCP ของหน่วยงาน

๓.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๓.๓.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์ หากสถานการณ์คลี่คลายและปลอดภัยแล้ว ให้แจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศ เพื่อเข้าตรวจสอบเหตุการณ์และสถานที่

๓.๓.๒ ทีม BCP ด้านเทคโนโลยีสารสนเทศประสานผู้เชี่ยวชาญเพื่อตรวจสอบโครงสร้างพื้นฐานของห้องเซิร์ฟเวอร์

๓.๓.๓ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบทรัพย์สินสารสนเทศ เช่น ระบบคอมพิวเตอร์ ระบบสายสัญญาณ และตู้ Rack จัดเก็บอุปกรณ์ และประเมินความเสียหาย

๓.๓.๔ ในกรณีเกิดความเสียหายขึ้นกับพื้นที่หรือทรัพย์สินสารสนเทศให้รายงานความเสียหายทั้งหมดต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ

๓.๓.๕ หากสำรวจแล้วไม่ได้รับความเสียหายให้ทยอยเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๔. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์อุทกภัย ดำเนินการ ดังนี้

๔.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๔.๑.๑ ติดตามสถานการณ์จากหน่วยงานที่เกี่ยวข้อง เช่น ประกาศจากกรมอุตุนิยมวิทยา สำนัก
ระบายน้ำอย่างใกล้ชิด

๔.๑.๒ ตรวจสอบจุดเสี่ยงน้ำรั่วซึมภายในห้องเซิร์ฟเวอร์ ชั้น ๔ อาคาร

๔.๑.๓ ตรวจสอบและดูแลการใช้งานเครื่องสำรองไฟฟ้า (UPS) ขนาด ๑๕ กิโลวัตต์แอมป์ (kVA)
จำนวน ๒ เครื่อง ให้สามารถใช้งานได้เป็นปกติ

๔.๑.๔ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือ
จัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๔.๑.๕ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๔.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๔.๒.๑ ขนย้ายทรัพย์สินสารสนเทศที่คาดว่าจะเสียหายจากเหตุน้ำท่วมขึ้นสู่ที่สูง

๔.๒.๒ ปิดระบบงานสำคัญ (Shutdown) และปิดเครื่องเซิร์ฟเวอร์ตามขั้นตอนที่ถูกต้องก่อนมี
การตัดไฟเพื่อป้องกันข้อมูลเสียหาย

๔.๒.๓ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ ติดตามและประเมินสถานการณ์ หากประกาศ
สถานการณ์อุทกภัย หรืออยู่ในสภาวะวิกฤตจนไม่สามารถเข้าปฏิบัติงานได้ หรือมีการประกาศใช้นโยบาย
การปฏิบัติงานจากที่บ้าน (WFH) ให้หัวหน้าทีมแจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศเพื่อเตรียมความพร้อม
ในการเปิดใช้งานระบบเทคโนโลยีสารสนเทศให้สามารถรองรับการปฏิบัติงานนอกสถานที่

๔.๒.๔ เมื่อมีประกาศสถานการณ์อุทกภัยและให้ปฏิบัติงานนอกสถานที่ ให้ทีม BCP ด้าน
เทคโนโลยีสารสนเทศดำเนินการเตรียมความพร้อมเปิดใช้งานระบบเทคโนโลยีสารสนเทศให้สามารถรองรับการ
ปฏิบัติงานนอกสถานที่

๔.๒.๕ เปิดช่องทางติดต่อสื่อสารสำรอง เช่น Line Group หรือ Mobile App เพื่อประสานงาน
หรือให้ความช่วยเหลือเจ้าหน้าที่

๔.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๔.๓.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์ หากสถานการณ์คลี่คลาย
และปลอดภัยแล้ว ให้แจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศ เพื่อเข้าตรวจสอบเหตุการณ์และสถานที่

๔.๓.๒ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบพื้นที่และทรัพย์สินสารสนเทศบริเวณที่
ประสบเหตุ เช่น ระบบคอมพิวเตอร์ ระบบสายสัญญาณ และตู้ Rack จัดเก็บอุปกรณ์

๔.๓.๓ ในกรณีเกิดความเสียหายขึ้นกับพื้นที่หรือทรัพย์สินสารสนเทศให้รายงานความเสียหาย
ทั้งหมดต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ

๔.๓.๔ ทดสอบเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๕. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ไฟฟ้าดับ (กรณีทราบล่วงหน้าหรือได้รับแจ้งล่วงหน้า) ดำเนินการ ดังนี้

๕.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๕.๑.๑ แจ้งหน่วยงานภายใน สนข. เกี่ยวกับช่วงเวลาการดับไฟฟ้า เพื่อให้เจ้าหน้าที่ทราบและสามารถเตรียมความพร้อมเป็นการล่วงหน้า

๕.๑.๒ ดำเนินการทำ Incremental Backup ระบบงานสำคัญล่าสุดก่อนเวลาตัดไฟ เพื่อให้ข้อมูลสำรองที่เป็นปัจจุบันที่สุด

๕.๑.๓ ปิดระบบงานสำคัญ (Shutdown) และปิดเครื่องเซิร์ฟเวอร์ตามขั้นตอนที่ถูกต้องก่อนมีการตัดไฟเพื่อป้องกันข้อมูลเสียหาย

๕.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๕.๒.๑ ก่อนถึงเวลากำหนดดับไฟฟ้า ให้ผู้ดูแลระบบดำเนินการปิดเครื่องเซิร์ฟเวอร์และอุปกรณ์เครือข่ายทั้งหมดให้เรียบร้อยก่อนไฟฟ้าตัด

๕.๒.๒ ให้เจ้าหน้าที่ดำเนินการตามแผน BCP ของหน่วยงาน

๕.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๕.๓.๑ เมื่อไฟฟ้ากลับมา ให้รอประมาณ ๕ - ๑๐ นาที เพื่อให้กระแสไฟนิ่งป้องกันไฟฟ้ากระชากที่อาจทำให้อุปกรณ์เสียหาย

๕.๓.๒ ทดสอบเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๕.๓.๓ ทिम BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบการให้บริการระบบสารสนเทศและอุปกรณ์ทั้งหมด หากตรวจสอบแล้วว่ามีระบบเกิดความเสียหาย ให้รายงานต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศและดำเนินการกู้คืนระบบตามแผนกู้คืนระบบ

๖. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ไฟฟ้าดับ (กรณีไม่ทราบล่วงหน้า) ดำเนินการ ดังนี้

๖.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๖.๑.๑ ดูแลและตรวจสอบประสิทธิภาพการทำงานของระบบเครื่องสำรองไฟฟ้า (UPS) ของห้องเซิร์ฟเวอร์ให้เป็นปกติและมีความพร้อมใช้อยู่เสมอ

๖.๑.๒ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือจัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๖.๑.๓ กำหนดลำดับการปิดเซิร์ฟเวอร์และอุปกรณ์เครือข่ายล่วงหน้า (Shutdown Sequence) เพื่อให้เจ้าหน้าที่ปฏิบัติได้ทันทีเมื่อไฟดับ

๖.๑.๔ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๖.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๖.๒.๑ ทีม BCP ด้านเทคโนโลยีสารสนเทศเร่งดำเนินการปิด (Shutdown) ระบบงานสารสนเทศ อิเล็กทรอนิกส์ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ ตามลำดับความสำคัญ ภายในเวลา ๑๕ นาทีแรกนับจากเกิดเหตุไฟฟ้าดับ เพื่อป้องกันความเสียหาย

๖.๒.๒ หากทราบว่าไฟฟ้าดับเป็นเวลานาน ให้หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศพิจารณาสั่งการให้ดำเนินการตามแผน BCP ของหน่วยงานจนกว่าเหตุการณ์จะกลับเป็นปกติ

๖.๒.๓ หากจำเป็นต้องออกนอกพื้นที่ให้ปิดล็อกห้องเซิร์ฟเวอร์ ห้องเก็บอุปกรณ์ และห้องที่มีทรัพย์สินสารสนเทศอยู่ทั้งหมดเพื่อความปลอดภัยและป้องกันการสูญหาย

๖.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๖.๓.๑ เมื่อไฟฟ้ากลับมาให้รอประมาณ ๕ - ๑๐ นาที เพื่อให้กระแสไฟนิ่งป้องกันไฟฟ้ากระชาก (Surge) ที่อาจทำให้อุปกรณ์เสียหาย

๖.๓.๒ ทดสอบเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๖.๓.๓ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบการให้บริการระบบสารสนเทศและอุปกรณ์ทั้งหมด หากตรวจสอบแล้วว่ามีระบบเกิดความเสียหาย ให้รายงานต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ และดำเนินการกู้คืนระบบตามแผนกู้คืนระบบ

๗. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์จราจร การชุมนุมประท้วง หรือเหตุการณ์ความไม่สงบ ดำเนินการ ดังนี้

๗.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๗.๑.๑ ตรวจสอบระบบกล้องวงจรปิด CCTV ภายในและภายนอกอาคาร ระบบดับเพลิงอัตโนมัติ และระบบรักษาความปลอดภัยในการเข้าถึงพื้นที่ที่มีทรัพย์สินสารสนเทศ

๗.๑.๒ ตรวจสอบและเตรียมความพร้อมระบบสารสนเทศให้มีความพร้อมใช้งาน ในกรณีที่เจ้าหน้าที่ไม่สามารถเข้ามาปฏิบัติงานภายในสถานที่หรือจำเป็นต้องปฏิบัติงานจากภายนอก

๗.๑.๓ เตรียมช่องทางติดต่อสื่อสารสำรอง เช่น Line Group หรือ Mobile App เพื่อประสานงาน หรือให้ความช่วยเหลือเจ้าหน้าที่

๗.๑.๔ ดำเนินการสำรองข้อมูล (Backup) ล่าสุดให้เรียบร้อยตามกฎหมาย ๓-๒-๑

๗.๑.๕ ติดตามข่าวสารหรือสถานการณ์จากหน่วยงานที่เกี่ยวข้อง

๗.๑.๖ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๗.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๗.๒.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศติดตามและประเมินสถานการณ์ หากเป็นเหตุที่ไม่ร้ายแรงสามารถเข้าดำเนินงานในพื้นที่สำนักงานได้ตามปกติ

๗.๒.๒ หากหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์แล้วว่าเป็นเหตุสถานการณ์รุนแรงที่อาจมีผลกระทบแก่ร่างกายเจ้าหน้าที่ หรือทรัพย์สินของราชการ หรือมีคำสั่งให้ออกจากพื้นที่ปฏิบัติงานให้เร่งแจ้งเหตุแก่ทีม BCP ด้านเทคโนโลยีสารสนเทศ

๗.๒.๓ ทีม BCP ด้านเทคโนโลยีสารสนเทศเร่งดำเนินการปิด (Shutdown) ระบบงานสารสนเทศ อิเล็กทรอนิกส์ เครื่องเซิร์ฟเวอร์ และอุปกรณ์ต่าง ๆ ทั้งหมดตามลำดับความสำคัญ เพื่อความปลอดภัยและป้องกันการสูญหาย

๗.๒.๔ ปิดล็อกประตูหรือช่องทางการเข้าถึงพื้นที่ที่มีทรัพย์สินสารสนเทศของหน่วยงาน

๗.๒.๕ ตรวจสอบและเตรียมความพร้อมระบบสารสนเทศให้มีความพร้อมใช้งาน ในกรณีที่เจ้าหน้าที่ไม่สามารถเข้ามาปฏิบัติงานภายในสถานที่หรือจำเป็นต้องปฏิบัติงานจากภายนอก

๗.๒.๖ ให้เจ้าหน้าที่ดำเนินการตามแผน BCP ของหน่วยงาน

๗.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๗.๓.๑ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศประเมินสถานการณ์ หากสถานการณ์คลี่คลายและปลอดภัยแล้ว ให้แจ้งต่อทีม BCP ด้านเทคโนโลยีสารสนเทศ เพื่อเข้าตรวจสอบเหตุการณ์และสถานที่

๗.๓.๒ ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าตรวจสอบพื้นที่และทรัพย์สินสารสนเทศทั้งหมดในบริเวณที่เกิดเหตุ

๗.๓.๓ ในกรณีเกิดความเสียหายขึ้นกับพื้นที่หรือทรัพย์สินสารสนเทศให้รายงานความเสียหายทั้งหมดต่อหัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศ

๗.๓.๔ ทดสอบเปิดระบบงานตามลำดับความสำคัญ (Criticality) โดยอ้างอิงจากแผนกู้คืนระบบ

๘. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์โรคระบาด ดำเนินการ ดังนี้

๘.๑ ก่อนเกิดเหตุ

ในการป้องกันและเตรียมความพร้อม ให้ดำเนินการ ดังนี้

๘.๑.๑ ติดตามสถานการณ์โรคระบาดและการเฝ้าระวังจากหน่วยงานที่เกี่ยวข้อง เช่น กรมควบคุมโรค กระทรวงสาธารณสุข

๘.๑.๒ ตรวจสอบความพร้อมใช้ของระบบเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายให้มีความพร้อมต่อการปฏิบัติงานนอกสถานที่อยู่เสมอ

๘.๑.๓ ตรวจสอบการ Backup ระบบงานสารสนเทศสำคัญและข้อมูล ตามกฎ ๓-๒-๑ หรือ จัดเก็บข้อมูลสำรองไว้ภายนอกสถานที่ (Off-site Storage) เป็นอย่างน้อย

๘.๑.๔ สร้างความเข้าใจและทบทวนแนวทางการดำเนินการให้มีความพร้อมอยู่เสมอ

๘.๒ ขณะเกิดเหตุ

เมื่อเกิดสถานการณ์ ให้ดำเนินการ ดังนี้

๘.๒.๑ เมื่อมีประกาศสถานการณ์โรคระบาดและให้ปฏิบัติงานนอกสถานที่ ให้ทีม BCP ด้านเทคโนโลยีสารสนเทศดำเนินการเตรียมความพร้อมเปิดใช้งานระบบเทคโนโลยีสารสนเทศให้สามารถรองรับการปฏิบัติงานนอกสถานที่

๘.๒.๒ หัวหน้าทีม BCP ด้านเทคโนโลยีสารสนเทศพิจารณาระดับความรุนแรงตามประกาศภาครัฐ หรือข้อสั่งการของหน่วยงานให้เจ้าหน้าที่ปฏิบัติงานนอกสถานที่ทั้งหมด หรือตามสัดส่วนที่เหมาะสม และสามารถพิจารณาจัดทีมเพื่อเข้าดูแลระบบสารสนเทศได้ตามสมควร (หากจำเป็น)

๘.๒.๓ เปิดช่องทางติดต่อสื่อสารสำรอง เช่น Line Group หรือ Mobile App เพื่อประสานงาน หรือให้ความช่วยเหลือเจ้าหน้าที่

๘.๕.๖ ให้เจ้าหน้าที่ดำเนินการตามแผน BCP ของหน่วยงาน

๘.๓ หลังเกิดเหตุ

เมื่อสถานการณ์คลี่คลายหรือกลับสู่ภาวะปกติ ให้ดำเนินการ ดังนี้

๘.๓.๑ ทีม BCP ด้านเทคโนโลยีสารสนเทศตรวจสอบความพร้อมและเปิดใช้งานระบบเทคโนโลยีสารสนเทศ อุปกรณ์เครือข่าย และเครื่องเซิร์ฟเวอร์ ให้รองรับการปฏิบัติงานภายในสถานที่ได้ตามปกติ

๘.๓.๒ ให้ทีม BCP ด้านเทคโนโลยีสารสนเทศเข้าทำงานตามปกติแต่ต้องปฏิบัติตามมาตรการของหน่วยงาน เช่น มาตรการใส่หน้ากากอนามัย มาตรการเว้นระยะห่าง

๙. แนวทางปฏิบัติเมื่อเกิดเหตุการณ์ภัยคุกคามทางไซเบอร์

เหตุภัยคุกคามทางไซเบอร์นั้นเป็นภัยเฉพาะด้านที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน โดยมีปัจจัยและผลกระทบที่แตกต่างจากสถานการณ์ในรูปแบบอื่น ๆ ซึ่งภัยคุกคามทางไซเบอร์สามารถแบ่งประเภทของภัยคุกคามทางไซเบอร์ และรูปแบบการโจมตีได้หลากหลาย โดยในการปฏิบัติหน่วยงานได้มีการกำหนดนโยบายและแนวทางปฏิบัติที่ชัดเจนในการดำเนินการให้ระบบเทคโนโลยีสารสนเทศมีความมั่นคงปลอดภัยแล้ว แต่หากเกิดภัยคุกคามทางไซเบอร์ขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน จำเป็นต้องมีแนวทางในการดำเนินการเพื่อลดผลกระทบที่จะเกิดขึ้น และให้หน่วยงานสามารถดำเนินกิจการได้อย่างต่อเนื่อง โดยมีสถานการณ์และแนวทางขั้นตอนปฏิบัติการถูกโจมตีที่สำคัญ ดังนี้

๙.๑ ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ DDoS

เมื่อเกิดเหตุระบบเทคโนโลยีสารสนเทศถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ในรูปแบบ DDoS ให้ทีม BCP ด้านเทคโนโลยีสารสนเทศดำเนินการ ดังนี้

ลำดับ ที่	แนวทาง / ขั้นตอนปฏิบัติ	คำอธิบาย
๑	วิเคราะห์หา IP Address ที่ถูกใช้ ในการ โจมตีเพื่อทำการปิดกั้นการเชื่อมต่อ	ดำเนินการวิเคราะห์หา IP Address ที่โจมตี DDOS ระบบ สารสนเทศของหน่วยงาน ตั้งค่าป้องกันที่อุปกรณ์ ป้องกันเครือข่าย
๒	แจ้งผู้ให้บริการเครือข่าย เพื่อทำการ Block IP ที่เป็นผู้โจมตี	แจ้งผู้ให้บริการระบบเครือข่ายอินเทอร์เน็ต เพื่อทำการ Block IP ที่โจมตีเครือข่าย สนข.
๓	ตรวจสอบการทำงานของระบบ	ตรวจสอบการทำงานของระบบที่ถูกโจมตีเพื่อให้แน่ใจว่า ระบบสามารถกลับมาทำงานได้ตามปกติ โดยการตรวจสอบข้อมูล เบื้องต้น ดังนี้ - ตรวจสอบ traffic flow เพื่อให้แน่ใจว่าเป็นการเชื่อมต่อ ตามปกติ ไม่มีการเชื่อมต่อที่ผิดปกติ - ตรวจสอบการดำเนินงานของระบบที่ถูกโจมตีว่าสามารถใช้งาน ได้ตามปกติ - ตรวจสอบประสิทธิภาพการให้บริการของโครงสร้างพื้นฐาน เพื่อให้แน่ใจว่าสามารถให้บริการได้ตามปกติ - ตรวจสอบระบบที่เกี่ยวข้องเพื่อให้แน่ใจว่าไม่เกิดความเสียหาย เพิ่มเติม
๔	เมื่อระบบสามารถทำงานได้ตามปกติ	กรณีที่ระบบสามารถดำเนินการได้ตามปกติ ให้ดำเนินการ ตามขั้นตอนที่ ๖
๕	เมื่อระบบสามารถไม่สามารถทำงานได้ ตามปกติ	ดำเนินการกู้คืนระบบตามแผนการกู้คืนระบบ พร้อมทบทวน ปรับปรุงการรักษาความมั่นคงปลอดภัยของระบบเครือข่าย
๖	รายงานผลการดำเนินงาน	สรุปผลการดำเนินงานรายต่อผู้บังคับบัญชาตามลำดับ และผู้ที่เกี่ยวข้อง

๙.๒ ขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Web Defacement

เมื่อเกิดเหตุการณ์ระบบเทคโนโลยีสารสนเทศถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ในรูปแบบ Web Defacement ให้ทีม BCP ด้านเทคโนโลยีสารสนเทศดำเนินการ ดังนี้

ลำดับ ที่	ขั้นตอน	คำอธิบาย
๑	ดำเนินการปิดเว็บไซต์ชั่วคราว พร้อมแจ้งผู้ใช้งานและผู้ที่เกี่ยวข้องทราบ	ปิดการเข้าถึงหน้าเว็บไซต์ที่ถูกโจมตีทันที เพื่อรักษาสภาพข้อมูล สำหรับการเก็บข้อมูลพิสูจน์ หลักฐานทางคอมพิวเตอร์ พร้อมแจ้งสถานการณ์ให้ผู้ที่เกี่ยวข้องทราบ
๒	ดำเนินการเชื่อมต่อการใช้งานไปยังเว็บไซต์สำรอง	ทำการเชื่อมต่อการใช้งานไปยังเว็บไซต์สำรองเพื่อเปิดใช้งานระบบ ให้กลับมาใช้งานได้เป็นการชั่วคราว
๓	บันทึกข้อมูล และเก็บหลักฐานที่เกี่ยวข้อง	เก็บบันทึกข้อมูลหลักฐานของเครื่องแม่ข่าย (Server) ที่ถูกโจมตี เพื่อทำการพิสูจน์หลักฐานทางคอมพิวเตอร์ และเก็บบันทึกข้อมูล Log จากระบบเครือข่ายและเครื่องแม่ข่ายที่ถูกโจมตีเพื่อวิเคราะห์ หาสาเหตุและวิธีที่ใช้ในการโจมตี
๔	แจ้งไปยังหน่วยงานผู้เชี่ยวชาญ เพื่อให้ดำเนินการตรวจสอบแก้ไข	ประสานงานและแจ้งผู้เชี่ยวชาญ ให้ช่วยดำเนินการตรวจสอบ แก้ไขระบบที่ถูกโจมตี พร้อมนำส่งข้อมูลหลักฐานทั้งหมด เพื่อใช้ในการตรวจสอบและปรับปรุงแก้ไข
๕	ตรวจสอบระบบเพื่อลบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ออกจากระบบ	ตรวจสอบระบบเพื่อทำการกำจัด Malware หรือสิ่งแปลกปลอม ในระบบทั้งหมด
๖	ตรวจพบ Malware หรือสิ่งแปลกปลอมอื่น เพิ่มเติม	- กรณีที่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตามขั้นตอนที่ ๓ - กรณีที่ไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ เพิ่มเติม ให้ดำเนินการตาม ขั้นตอน ที่ ๗
๗	ดำเนินการกู้คืนระบบ	ดำเนินการกู้คืนระบบ (Restore) กลับสู่การดำเนินงานปกติ ทำการตรวจสอบช่องโหว่ อัปเดต patch ทดสอบการทำ Penetration testing บนเว็บไซต์ที่กู้คืน และทำ Hardening ตรวจสอบผลการดำเนินงาน ปรับปรุงการเข้าถึงเว็บไซต์ จากแสดงหน้าจอการปรับปรุงเว็บไซต์ (Maintenance) ให้สามารถเข้าถึงเว็บไซต์ได้ตามปกติ
๘	กำหนดระยะเวลาในการเฝ้าระวังระบบ	กำหนดระยะเวลาในการเฝ้าระวังระบบ เพื่อให้แน่ใจว่า ระบบสามารถทำงานได้ตามปกติ ไม่ถูกโจมตีซ้ำด้วยวิธีเดิม
๙	รายงานผลการดำเนินงาน	สรุปผลการดำเนินงานรายต่อผู้บังคับบัญชาตามลำดับ และผู้ที่เกี่ยวข้อง

๙.๓ ขั้นตอนปฏิบัติสำหรับกรณีถูกเจาะระบบและ Malware

เมื่อเกิดเหตุการณ์ระบบเทคโนโลยีสารสนเทศถูกโจมตีด้วยภัยคุกคามทางไซเบอร์ในกรณีถูกเจาะระบบและ Malware ให้ทีม BCP ด้านเทคโนโลยีสารสนเทศดำเนินการ ดังนี้

ลำดับ ที่	ขั้นตอน	คำอธิบาย
๑	ตรวจสอบระบบที่ได้รับผลกระทบเพื่อจำกัดขอบเขต	รับทราบการแจ้งเหตุกรณีถูกเจาะระบบหรือ กรณีถูกโจมตีด้วย Malware และตรวจสอบระบบงานที่เกี่ยวข้องที่ได้รับผลกระทบ เพื่อจำกัดขอบเขตและผลกระทบที่เกิดขึ้น
๒	จำกัดขอบเขตของระบบที่ถูกโจมตี	- กรณีที่ไม่สามารถแบ่งแยกระบบงานที่ถูกโจมตีออกจากระบบอื่นให้ดำเนินการตามขั้นตอนที่ ๓ - กรณีที่สามารถแบ่งแยกระบบงานที่ถูกโจมตีออกจากระบบอื่นได้โดยไม่ส่งผลกระทบต่อการทำงานของระบบอื่น ให้ดำเนินการตามขั้นตอนที่ ๔
๓	ประสานงานกับเจ้าของระบบที่ถูกโจมตีเพื่อหาแนวทางการจำกัดขอบเขตของระบบที่ถูกโจมตี	ประสานงานกับเจ้าของระบบงาน รวมทั้งระบบที่เกี่ยวข้องหรือเชื่อมต่อกับระบบที่ถูกโจมตี เพื่อหาวิธีถึงแนวทางการลดผลกระทบและความเสียหายที่อาจเกิดขึ้นกับระบบ
๔	ดำเนินการจำกัดขอบเขตของระบบที่ถูกโจมตีออกจากระบบอื่น	ดำเนินการแยกระบบที่ถูกโจมตีออกจากระบบงานอื่น เช่น การแยกระบบเครือข่าย การยกเลิกการเชื่อมต่อเครือข่าย เป็นต้น
๕	ตรวจสอบผลการจำกัดขอบเขตระบบที่ถูกโจมตี	ตรวจสอบการจำกัดขอบเขตระบบที่ถูกโจมตี และระบบที่ได้รับผลกระทบจากการโจมตี
๖	คัดลอกและจัดเก็บข้อมูลสำหรับการพิสูจน์หลักฐานทางคอมพิวเตอร์	ดำเนินการสำเนาข้อมูลเพื่อให้พิสูจน์หลักฐานทางคอมพิวเตอร์จากระบบที่ถูกโจมตี และตรวจสอบการบันทึกข้อมูลที่เกี่ยวข้องกับการตอบสนองต่อการโจมตีเบื้องต้นทั้งหมด เพื่อให้แน่ใจว่ามีการบันทึกข้อมูลอย่างถูกต้องครบถ้วนและเป็นปัจจุบัน ทั้งนี้หลักฐานข้อมูลที่เกี่ยวข้องต่าง ๆ ต้องจัดเก็บไว้อย่างปลอดภัย
๗	พิจารณาการปิดระบบที่ถูกโจมตีได้	- กรณีที่ไม่สามารถปิดระบบได้ ให้ดำเนินการตามขั้นตอนที่ ๘ - กรณีที่สามารถปิดระบบได้ ให้ดำเนินการตามขั้นตอนที่ ๙
๘	ตรวจสอบระบบเพื่อทำการ Re-image และ Hardening ระบบ	ตรวจสอบระบบที่ถูกโจมตีว่าสามารถทำ Re-image และ Hardening ได้หรือไม่
๙	กรณีการทำ Re-image และ Hardening	- กรณีที่ระบบไม่สามารถ reimage และ Hardening ได้ ให้ดำเนินการตามขั้นตอนที่ ๑๐ - กรณีที่ระบบสามารถ reimage และ Hardening ได้ ให้ดำเนินการตามขั้นตอนที่ ๑๑
๑๐	ขอคำปรึกษาจากผู้เชี่ยวชาญเพื่อดำเนินการแก้ไข	รวบรวมข้อมูลรายละเอียดเหตุการณ์ที่พบ เพื่อขอข้อมูลเพิ่มเติมจากผู้เชี่ยวชาญ เพื่อดำเนินการแก้ไขต่อไป และเมื่อแก้ไขได้แล้วเสร็จให้ดำเนินการตามขั้นตอนที่ ๑๕
๑๑	ดำเนินการทำ Re-image และ Hardening ระบบ	ดำเนินการ Re-image และ Hardening ระบบ เช่น การอัปเดต patches การตรวจสอบและปิด port ที่ไม่ใช้งาน เป็นต้น เพื่อเป็นการป้องกันระบบและลดความเสี่ยงจากการถูกโจมตี
๑๒	ตรวจสอบผลการ Re-image และ Hardening	สอบทานผลการ Re-image และ Hardening ระบบ เพื่อให้แน่ใจว่าไม่พบ Malware หรือสิ่งแปลกปลอมอื่น ๆ คงเหลืออยู่

ลำดับ ที่	ขั้นตอน	คำอธิบาย
๑๓	ดำเนินการกู้คืนระบบ	ดำเนินการกู้คืนระบบ (Restore) กลับสู่การ ดำเนินงานปกติ ตรวจสอบผลการดำเนินงาน และบันทึกผล
๑๔	กำหนดระยะเวลาในการเฝ้าระวัง ระบบ	กำหนดระยะเวลาในการเฝ้าระวังระบบ เพื่อให้มั่นใจว่า ระบบสามารถทำงานได้ตามปกติ ไม่ถูกโจมตีซ้ำด้วยวิธีเดิม
๑๕	รายงานผลการดำเนินงาน	สรุปผลการดำเนินงานรายต่อผู้บังคับบัญชาตามลำดับ และผู้ที่เกี่ยวข้อง

๙.๔ รายละเอียดขั้นตอนปฏิบัติสำหรับกรณีถูกโจมตีแบบ Ransomware

ลำดับ ที่	ขั้นตอน	คำอธิบาย
๑	ตรวจสอบที่จัดเก็บข้อมูล	ปิดการเข้าถึง (Off-line) ตรวจสอบที่จัดเก็บข้อมูล โดยพิจารณาว่าข้อมูลที่ถูกโจมตีจัดเก็บอยู่ในระบบเครือข่าย ที่มีการแชร์ไฟล์หรือไม่
๒	ตรวจสอบข้อมูลที่ถูกโจมตีว่าได้จัดเก็บ อยู่ในเครือข่ายที่มีการแชร์ไฟล์หรือไม่	- กรณีที่ข้อมูลที่ถูกโจมตีจัดเก็บอยู่ในระบบเครือข่าย ให้ดำเนินการตามขั้นตอนที่ ๓ - กรณีที่ข้อมูลที่ถูกโจมตีไม่จัดเก็บอยู่ในระบบเครือข่าย ให้ดำเนินการตามขั้นตอนที่ ๔
๓	แยกเครื่องที่ถูกโจมตีออกจากระบบ เครือข่าย	แยกเครื่องที่ถูกโจมตีออกจากระบบ เครือข่ายทั้งหมด เพื่อจำกัดขอบเขตของระบบที่ถูกโจมตี และกักกันขอบเขต ของระบบที่ได้รับผลกระทบ
๔	ตรวจสอบสถานะการเข้ารหัสไฟล์ข้อมูล	ตรวจสอบสถานะการเข้ารหัสไฟล์ข้อมูลเพื่อตรวจสอบว่า ข้อมูลถูกเข้ารหัสจนเสร็จสิ้นแล้วหรือไม่
๕	สถานะการเข้ารหัสไฟล์	- กรณีที่ไฟล์ถูกเข้ารหัสเสร็จสิ้นแล้ว ให้ดำเนินการ ตามขั้นตอนที่ ๑๑ - กรณีที่ไฟล์ยังเข้ารหัสไม่แล้วเสร็จ ให้ดำเนินการตามขั้นตอนที่ ๖
๖	ตรวจสอบการทำงานของโปรแกรม Task Manager	ตรวจสอบการทำงานของโปรแกรม Task manager เพื่อพิจารณาว่ายังสามารถทำงานได้อยู่หรือไม่
๗	การตรวจสอบการทำงานของ โปรแกรม Task Manager	- กรณีที่โปรแกรม Task manager ยังสามารถทำงานได้ ให้ ดำเนินการตามขั้นตอนที่ ๘ - กรณีที่โปรแกรม Task manager ไม่สามารถทำงานได้ ให้ดำเนินการตามขั้นตอนที่ ๑๘
๘	ตรวจสอบและปิดการทำงานของระบบ ที่ ผิดปกติ	ตรวจสอบและปิดการทำงานของระบบ หรือ Process ที่ผิดปกติ
๙	ตรวจสอบความเสียหายของข้อมูล	ตรวจสอบความเสียหายของข้อมูลเพื่อพิจารณาว่ามีไฟล์ ที่ถูกเข้ารหัสหรือไม่
๑๐	การตรวจสอบไฟล์ที่ถูกเข้ารหัส	- กรณีพบไฟล์ที่ถูกเข้ารหัส ให้ดำเนินการตามขั้นตอนที่ ๑๑ - กรณีไม่พบไฟล์ที่ถูกเข้ารหัส ให้ดำเนินการตามขั้นตอนที่ ๑๙
๑๑	ตรวจสอบการสำรองข้อมูล	ตรวจสอบว่าข้อมูลที่ถูกเข้ารหัสมีการ สำรองข้อมูลไว้หรือไม่
๑๒	มีการสำรองข้อมูลไฟล์ที่ถูกเข้ารหัสหรือไม่	- กรณีที่ไม่มีการสำรองข้อมูลไว้ ให้ดำเนินการตาม ขั้นตอนที่ ๑๓ - กรณีที่มีการสำรองข้อมูลไว้ ให้ดำเนินการตามขั้นตอนที่ ๑๙
๑๓	ตรวจสอบประเภท Malware เรียกค่าไถ่	ตรวจสอบประเภท Malware ที่ใช้ในการเข้ารหัสข้อมูลเรียกค่าไถ่ เพื่อใช้เป็นข้อมูลในการค้นหา เครื่องมือในการถอดรหัส
๑๔	ค้นหาข้อมูลเครื่องมือที่ช่วยในการถอดรหัส ข้อมูลจาก Malware ที่พบ	ค้นหาข้อมูลเครื่องมือ ที่ใช้ในการถอดรหัสข้อมูล อ้างอิงประเภท Malware ที่ใช้ในการเข้ารหัสข้อมูลเทียบกับข้อมูลจาก การแลกเปลี่ยนข้อมูลและอุปกรณ์ในการถอดรหัสจากสถาบัน ที่มีความน่าเชื่อถือ
๑๕	มีเครื่องมือที่ถอดรหัสแล้วหรือไม่	- กรณีที่มีเครื่องมือที่ถอดรหัสได้ ให้ดำเนินการตามขั้นตอนที่ ๑๖ - กรณีที่ไม่มีเครื่องมือที่ถอดรหัสได้ ให้ดำเนินการตามขั้นตอนที่ ๑๘
๑๖	ดำเนินการถอดรหัสไฟล์ข้อมูล	ดำเนินการถอดรหัสข้อมูล

ลำดับ ที่	ขั้นตอน	คำอธิบาย
๑๗	ถอดรหัสสำเร็จหรือไม่	- กรณีที่ถอดรหัสไม่สำเร็จ ให้ดำเนินการตามขั้นตอนที่ ๑๘ - กรณีที่ถอดรหัสสำเร็จ ให้ดำเนินการตามขั้นตอนที่ ๑๙
๑๘	บันทึกข้อมูลตั้งแต่เกิดเหตุจนถึงปัจจุบัน และนำข้อมูลปรึกษาผู้เชี่ยวชาญ เพื่อดำเนินการแก้ไข	เก็บรวบรวมข้อมูลตั้งแต่เกิดเหตุจนถึงปัจจุบัน เพื่อนำข้อมูลต่าง ๆ เป็นหลักฐานอ้างอิงและนำข้อมูลไป ปรึกษาผู้เชี่ยวชาญ เพื่อดำเนินการแก้ไขปัญหา
๑๙	ตรวจสอบระบบ เพื่อลบ Malware หรือสิ่งแปลกปลอมอื่น ๆ ออกจากระบบ	ตรวจสอบระบบ เพื่อทำการกำจัด Malware หรือสิ่งแปลกปลอม ในระบบทั้งหมด
๒๐	กู้คืนข้อมูลที่สำรองไว้	ทำการกู้คืนข้อมูลที่สำรองไว้ และตรวจสอบผลการกู้คืนข้อมูล เพื่อให้แน่ใจว่าสามารถดำเนินการกู้คืนข้อมูลได้แล้วเสร็จ
๒๑	รายงานผลการดำเนินงาน	สรุปผลการดำเนินงานรายต่อผู้บังคับบัญชาตามลำดับ และผู้ที่เกี่ยวข้อง