

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ
(IT Business Continuity Plan: IT-BCP)

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

ชื่อเรื่อง	แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (IT Business Continuity Plan: IT-BCP)
เอกสารหมายเลข	ITBCP-๐๑
รุ่นเอกสาร	๑.๐
วันที่ปรับปรุงล่าสุด	๒๑ ตุลาคม ๒๕๖๙
หน่วยงานผู้รับผิดชอบ	กองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้ กลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี

สารบัญ

	หน้า
หลักการและเหตุผล	๑
วัตถุประสงค์	๑
การวิเคราะห์ความเสี่ยง	๑
การเตรียมการเบื้องต้นระบบเทคโนโลยีสารสนเทศ	๒
ขอบเขตการดำเนินงาน	๓
ขั้นตอนการปฏิบัติการตามขอบเขตการดำเนินงาน	๔
ผู้รับผิดชอบและช่องทางประสานงาน	๑๓
แบบบันทึกเหตุการณ์ฉุกเฉิน (สำหรับเจ้าหน้าที่เทคโนโลยีและสารสนเทศ)	๑๔
หลังควบคุมเหตุการณ์ได้แล้ว	๑๖

คำนำ

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (IT Business Continuity Plan: IT-BCP) จัดทำขึ้นเพื่อให้กองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้ กลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี มีแนวทางในการรองรับ การดำเนินงานด้านเทคโนโลยีสารสนเทศภายใต้สภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ ทั้งที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือการก่อความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ให้เป็นไปอย่างราบรื่นและต่อเนื่อง โดยไม่ให้สภาวะวิกฤติหรือเหตุการณ์ฉุกเฉินเหล่านี้ส่งผลทำให้การดำเนินงานด้านเทคโนโลยีสารสนเทศต้องหยุดชะงัก ไม่สามารถให้บริการได้อย่างต่อเนื่อง หรือสามารถกู้คืนสถานะการดำเนินงานด้านเทคโนโลยีสารสนเทศให้กลับมาได้ภายในระยะเวลาการหยุดทำงานที่ยอมรับได้

หากไม่มีแผนในการรับมือกับสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ แล้ว อาจส่งผลกระทบต่อการดำเนินงานด้านเทคโนโลยีสารสนเทศในหลาย ๆ ด้าน อาทิ ไม่สามารถใช้งานระบบสารสนเทศในการปฏิบัติงานได้ ไม่สามารถรับ-ส่งข้อมูลผ่านระบบเครือข่ายภายในและระบบเครือข่ายอินเทอร์เน็ตได้ ไม่สามารถกู้คืนข้อมูลที่มีความสำคัญกลับคืนมาได้ ผู้มีส่วนได้ส่วนเสียขาดความเชื่อมั่นในกาดำเนินงานของ ศอ.บต. ดังนั้น แผน BCP จึงเป็นสิ่งสำคัญที่จะช่วยให้กองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้ กลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี มีแนวทางในการรับมือกับสภาวะวิกฤตหรือเหตุการณ์ฉุกเฉินต่าง ๆ ได้อย่างมีประสิทธิภาพ การดำเนินงานด้านเทคโนโลยีสารสนเทศเป็นไปอย่างต่อเนื่องหรือสามารถกู้คืนการดำเนินงานด้านเทคโนโลยีสารสนเทศให้กลับมาได้ภายในระยะเวลาการหยุดทำงานที่ยอมรับได้ ซึ่งจะช่วยลดระดับความรุนแรงของผลกระทบที่เกิดขึ้นต่อ ศอ.บต. ได้

กองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้
กลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี

แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ
(IT Business Continuity Plan: IT-BCP)
ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

๑. หลักการและเหตุผล

ปัจจุบันระบบเทคโนโลยีสารสนเทศ ถือเป็นทรัพยากรที่มีความสำคัญต่อหน่วยงาน โดยเหตุการณ์และปัจจัยภายนอกที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งมีความรุนแรงและความเสี่ยงที่ไม่สามารถคาดเดาได้ล่วงหน้า จึงจำเป็นต้องได้รับการดูแลรักษาให้มีความถูกต้องและปลอดภัย เพื่อให้มั่นใจว่าระบบเครือข่ายคอมพิวเตอร์และระบบข้อมูลสารสนเทศ สามารถใช้ได้งานได้ตามปกติส่งเสริมสนับสนุนการปฏิบัติงานตามภารกิจหน่วยงานได้

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ได้ตระหนักถึงภัยคุกคามทุกรูปแบบทั้งในรูปแบบไวรัสคอมพิวเตอร์ การโจมตีระบบความปลอดภัย การทำงานของระบบเครือข่าย การทำงานของระบบป้องกันความปลอดภัยของระบบดับเพลิง และการสำรองข้อมูล ศอ.บต. จึงได้จัดทำแผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ (IT Business Continuity Plan: IT-BCP) ของ ศอ.บต. เพื่อเป็นกรอบแนวทางในการป้องกันและแก้ไขปัญหาเมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและข้อมูลให้สามารถใช้งานได้ตามปกติหรือจำกัดความเสียหายให้น้อยที่สุด ตลอดจนการดูแลรักษาระบบต่าง ๆ ให้มีเสถียรภาพ พร้อมใช้งานได้อย่างมีประสิทธิภาพต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากภัยคุกคาม

๒.๒ เพื่อป้องกันและลดความเสียหายที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้การปฏิบัติราชการดำเนินไปได้อย่างมีเสถียรภาพ

๒.๔ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหาร และผู้ปฏิบัติในการดูแลรักษาระบบความปลอดภัยด้านเทคโนโลยีสารสนเทศของ ศอ.บต.

๓. การวิเคราะห์ความเสี่ยง

ศอ.บต. มีการใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านเทคโนโลยีสารสนเทศ รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศมีประสทธิภาพ มีความมั่นคงปลอดภัย เพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงาน การควบคุม กำกับ ให้เกิดประโยชนสูงสุด จากการวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศพบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๓.๑ ความเสี่ยงด้านเทคนิค

เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์เครื่องมือและอุปกรณ์ขัดข้อง จากการถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดีถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ กระแสไฟฟ้าหลักดับ ระบบดับเพลิงไม่ทำงาน ระบบเครือข่ายหลักไม่สามารถใช้งานได้เครื่องคอมพิวเตอร์แม่ข่าย (Server) และอุปกรณ์เครือข่าย (Network Devices) ไม่สามารถทำงานได้เป็นต้น

๓.๒ ความเสี่ยงด้านผู้ปฏิบัติงาน

เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่าง ๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓.๓ ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน

เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น เกิดไฟไหม้ แผ่นดินไหว อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบในพื้นที่จังหวัดชายแดนภาคใต้ เป็นต้น

๔. การเตรียมการเบื้องต้นระบบเทคโนโลยีสารสนเทศ

๔.๑ การประกาศแผน (Activation)

ศอ.บต. มีการประกาศใช้แผนบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศอย่างเป็นทางการเพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด รวมทั้งมีการซ้อมแผนเพื่อสามารถปฏิบัติตามแผนจำนวน ๒ ครั้ง/ปีงบประมาณ โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ศอ.บต. จะทำการแจ้งให้ผู้บังคับบัญชาทราบตามลำดับ

๔.๒ กระบวนการดำเนินงาน (Procedure)

ศอ.บต. จัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในหน่วยงาน โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมข้อมูล หลักฐานเพื่อหาช่องโหว่วิธีการที่ถูกโจมตีหรือระบุตัวผู้โจมตี เพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างถูกต้อง ทันเวลา และสามารถป้องกันการโจมตีในลักษณะเดิม ระบบงานต่าง ๆ ที่มีความสำคัญต้องมีการสำรองข้อมูล เพื่อความพร้อมในการกู้คืนข้อมูลหากข้อมูลความเสียหายจากการถูกโจมตี

๔.๓ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยคุกคามที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ ศอ.บต. หน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้โดยเตรียมอุปกรณ์ ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ ระบบปฏิบัติการระบบเครือข่าย/ แผ่นติดตั้งระบบงานที่สำคัญ
- แผ่นไดร์เวอร์ (Driver Disc) อุปกรณ์ต่าง ๆ
- ระบบสำรองไฟ (UPS) ฉุกเฉิน
- อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์
- อุปกรณ์เครือข่าย (Network Devices)

๔.๔ การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นกับข้อมูลหรือระบบงานจากภัยคุกคามระบบเทคโนโลยีสารสนเทศ ให้สามารถกู้คืนข้อมูลที่เสียหายหรือถูกทำลายกลับมาได้ให้มากที่สุดให้การดำเนินงานของหน่วยงานมีความต่อเนื่อง โดยหน่วยงานมีนโยบายการสำรองข้อมูลและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๔.๕ การป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการป้องกันและสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายของ ศอ.บต. จึงมีแนวทาง ดังนี้

๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบเครือข่าย หากกรณีจำเป็นให้มีเจ้าหน้าที่ได้รับมอบหมายเป็นผู้รับผิดชอบนำพาเข้าไป เจ้าหน้าที่ทุกคนต้องสแกนลายนิ้วมือ เพื่อใช้ในการเข้าออกห้องแม่ข่าย

๒) มีการติดตั้งระบบไฟร์วอลล์ (Firewall) เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยจะเปิดใช้งาน Firewall ตลอดเวลา และมีการเฝ้าระวัง (Monitor) เป็นประจำวัน

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของหน่วยงาน และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดการตั้งค่า (Configuration) ความปลอดภัยต่อระบบสารสนเทศ และเครือข่ายคอมพิวเตอร์

๔) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๕) มีการทำระบบยืนยันตัวตน (Authentication) โดยมีการ Login ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย

๖) มีเจ้าหน้าที่ระบบเครือข่ายทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของหน่วยงาน เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๗) การดำเนินการตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๕. ขอบเขตการดำเนินงาน

การบริหารความต่อเนื่องระบบเทคโนโลยีสารสนเทศ จัดทำขึ้นสำหรับ ศอ.บต. เพื่อใช้กู้คืนระบบงานให้กลับคืนสู่สภาพปกติ (Recovery) และบริหารหลัก (Critical Service) แผนบริหารความต่อเนื่อง (BCP) ฉบับนี้ใช้รองรับสถานการณ์ กรณีเกิดสภาวะวิฤต หรือเหตุการณ์ฉุกเฉินทางด้านระบบเทคโนโลยีสารสนเทศของ ศอ.บต. ประกอบด้วยเหตุการณ์ต่อไปนี้

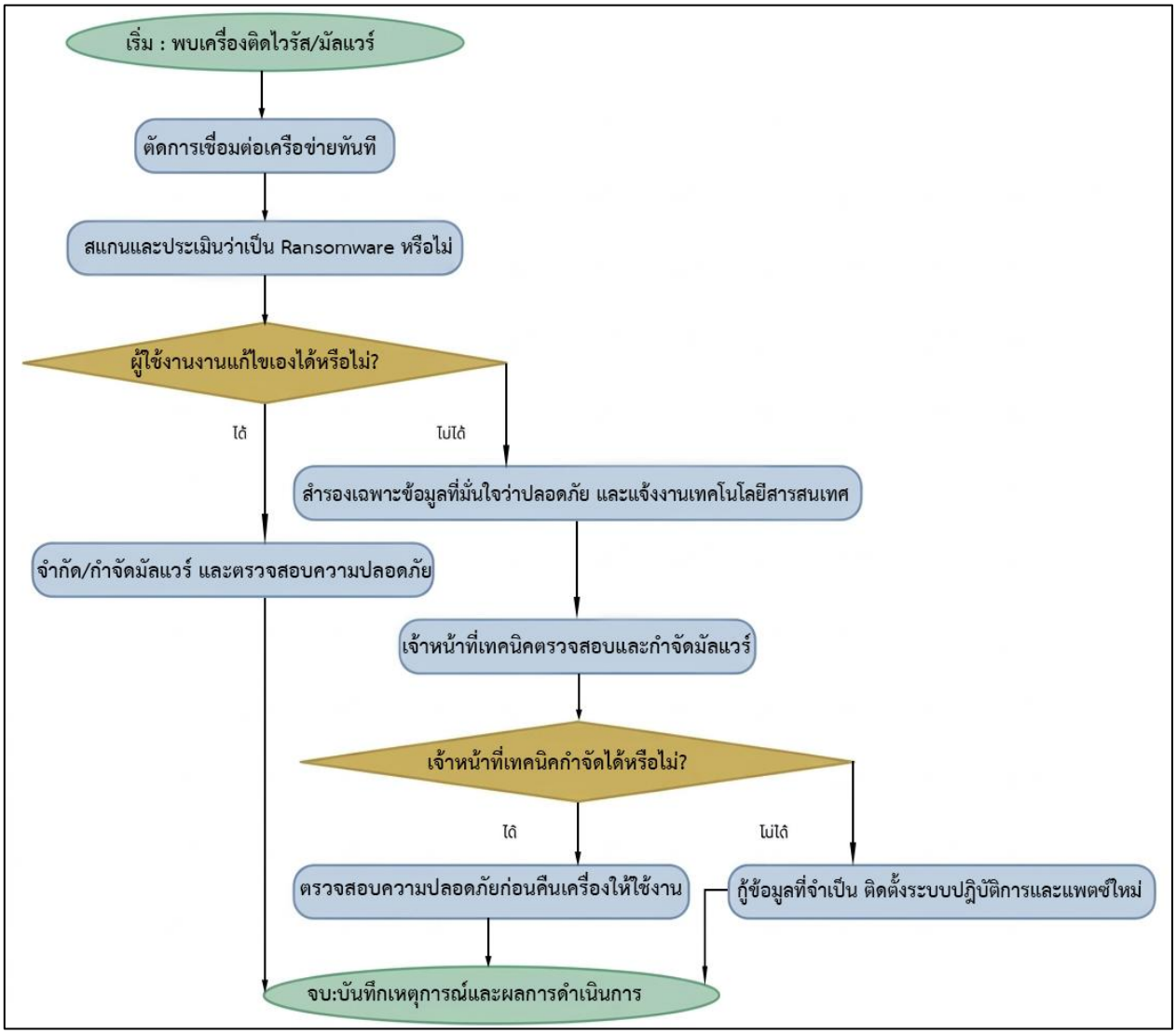
๑) เหตุการณ์เครื่องติดไวรัส/มัลแวร์
๒) เหตุการณ์เจาะระบบสารสนเทศหรือมีผู้บุกรุก
๓) เหตุการณ์ไฟฟ้าดับและเครื่องสำรองไฟ (UPS) ไม่ทำงาน
๔) เหตุการณ์ไฟไหม้ห้องเครื่องแม่ข่าย หรือมีสัญญาณเตือนไฟไหม้

๖. ขั้นตอนการปฏิบัติการตามขอบเขตการดำเนินงาน ดังนี้

๖.๑ เหตุการณ์เครื่องติดไวรัส/มัลแวร์

ผู้ใช้งานสังเกตจากเครื่องทำงานผิดปกติ มีหน้าต่างแสดงขึ้นมาผิดปกติ ไฟล์เอกสารเปิดไม่ได้ หรือมีข้อความเรียกเก็บเงิน

๖.๑.๑ <u>ขั้นตอนการปฏิบัติ (Flow Chart)</u>



ภาพที่ ๑ ขั้นตอนการปฏิบัติในเหตุการณ์เครื่องติดไวรัส/มัลแวร์

๖.๑.๒ <u>อธิบายขั้นตอนการปฏิบัติ</u>

๑) ผู้ใช้งานตัดการเชื่อมต่อระบบเครือข่ายของเครื่องทันที เช่น ถอดสาย LAN หรือปิด Wi-Fi เพื่อจำกัดการแพร่กระจ่าย หากไม่แน่ใจให้โทรแจ้งเจ้าหน้าที่เทคนิค

๒) สแกนและตรวจสอบชนิดมัลแวร์ โดยเฉพาะกรณีสงสัย Ransomware

๓) หากผู้ใช้งานจัดการไม่ได้ให้แจ้งงานเทคโนโลยีสารสนเทศ ศอ.บต.

๔) เจ้าหน้าที่เทคนิคทำการตรวจสอบและประเมินผลการใช้งานก่อนส่งมอบอีกครั้ง หากตรวจสอบแล้วยังไม่สามารถใช้งานได้ให้ทำการติดตั้งและประเมินผลใหม่ตามขั้นตอน

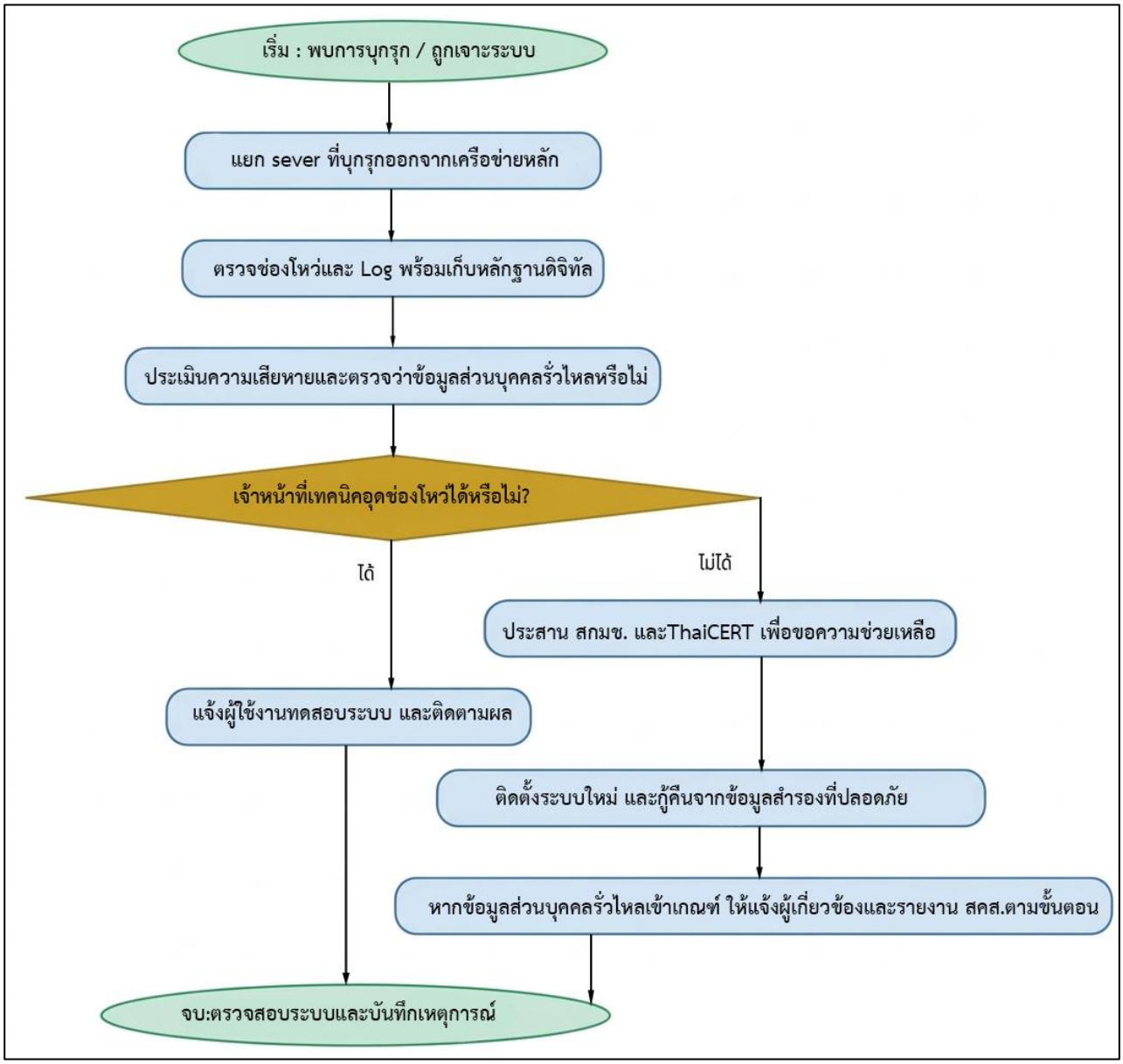
๕) บันทึกเหตุการณ์ผลการดำเนินการ

ข้อควรระวัง : อย่าเสียบ USB หรือคัดลอกไฟล์จากเครื่องที่สงสัยว่าติดไวรัสไปยังเครื่องคอมพิวเตอร์อื่น และอย่าลบไฟล์ที่ติดไวรัสด้วยตนเอง

๖.๒ เหตุการณ์เจาะระบบสารสนเทศหรือมีผู้บุกรุก

เจ้าหน้าที่เทคนิค หากสงสัยว่าถูกเจาะระบบหรือมีผู้บุกรุก เช่น พบการเข้าระบบที่ไม่รู้จักบัญชี ถูกเปลี่ยนรหัสโดยไม่ได้เกิดจากการกระทำเอง มีการตั้งค่าระบบเปลี่ยนไป หรือพบการเข้าถึงข้อมูลผิดปกติ

๖.๒.๑ ขั้นตอนการปฏิบัติ (Flow Chart)



ภาพที่ ๒ ขั้นตอนการปฏิบัติในเหตุการณ์เจาะระบบสารสนเทศหรือมีผู้บุกรุก

๖.๒.๒ <u>อธิบายขั้นตอนการปฏิบัติ</u>

๑) เจ้าหน้าที่ระบบเครือข่ายทำการแยกเครื่องแม่ข่ายที่ถูกบุกรุกออกจากเครือข่ายหลักทันที

๒) ตรวจสอบช่องโหว่ และ Log พร้อมเก็บสำเนาหลักฐานดิจิทัลไว้ หลีกเลี่ยงการลบหรือแก้ไขหลักฐาน

๓) ประเมินว่าระบบสารสนเทศใดได้รับผลกระทบ และตรวจสอบว่ามีข้อมูลส่วนบุคคลรั่วไหลหรือไม่

๔) เจ้าหน้าที่ระบบเครือข่ายดำเนินการแก้ไข ปิดช่องโหว่ แจ้งผู้ใช้งานที่ได้รับผลกระทบ และทดสอบระบบก่อนเปิดบริการ

๕) ถ้าแก้ไขไม่ได้ หัวหน้างานระบบเครือข่ายประสานสำศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (ThaiCERT)

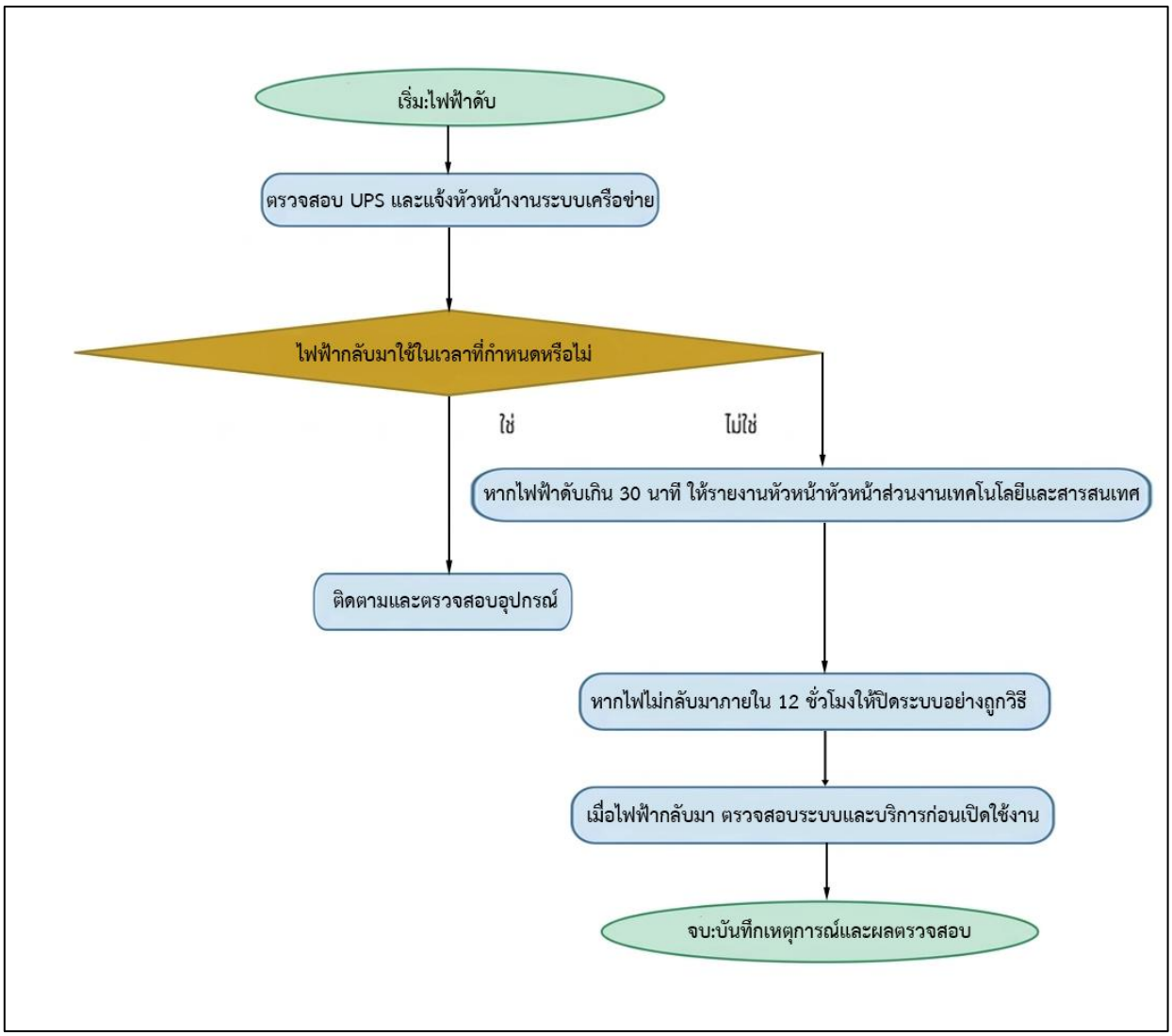
๖) ติดตั้งระบบใหม่ และกู้คืนจากข้อมูลสำรองที่ปลอดภัย หากข้อมูลส่วนบุคคลรั่วไหลเข้าเกณฑ์กฎหมาย หัวหน้างานระบบเครือข่ายรายงานสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (PDPC) ตามขั้นตอนที่เกี่ยวข้อง

ข้อควรละวัง : อย่ารีบลบ Log หรือรีบติดตั้งระบบใหม่ ให้ดำเนินการเก็บหลักฐานตามความเหมาะสม เพราะอาจทำให้ตรวจสอบสาเหตุได้ยาก

๖.๓ เหตุการณ์ไฟฟ้าดับและเครื่องสำรองไฟ (UPS) ไม่ทำงาน

หากได้รับประสานจากสำนักงานเลขาธิการ หรือผู้ใช้งาน มีกระแสไฟฟ้าดับภายใน ศอ.บต. เจ้าหน้าที่เทคนิค ตรวจสอบเครื่องสำรองไฟห้องแม่ข่าย (เครื่องสำรองไฟห้องแม่ข่าย สามารถสำรองไฟได้สูงสุดประมาณ ๑,๐๐๐ นาที (๑๖ ชั่วโมง ๔๐ นาที)) แต่กำหนดให้เริ่มพิจารณาปิดทุกระบบในห้องแม่ข่าย เช่น เครื่องแม่ข่าย ระบบเครือข่าย และเครื่องสำรองไฟ เป็นต้น เมื่อไฟฟ้าดับต่อเนื่องถึง ๑๒ ชั่วโมง เพื่อความปลอดภัยของอุปกรณ์ในห้องแม่ข่าย

๖.๓.๑ ขั้นตอนการปฏิบัติ (Flow Chart)



ภาพที่ ๓ ขั้นตอนการปฏิบัติในเหตุการณ์ไฟฟ้าดับและเครื่องสำรองไฟ (UPS)

๖.๓.๒ <u>อธิบายขั้นตอนการปฏิบัติ</u>

๑) เมื่อกระแสไฟฟ้าดับ เครื่องสำรองไฟห้องแม่ข่ายจะจ่ายไฟสำรองอัตโนมัติ ให้เจ้าหน้าที่เทคนิคตรวจสถานะของไฟบนเครื่องสำรองไฟ และแจ้งหัวหน้างานระบบเครือข่ายทันที

๒) หากกระแสไฟฟ้าดับดับเกิน ๓๐ นาที ให้รายงานหัวหน้าส่วนงานเทคโนโลยีและสารสนเทศและผู้บังคับบัญชาตามลำดับขั้น และแจ้งงานอาคารและสถานที่ สำนักงานเลขาธิการ ติดตามสถานการณ์กับเจ้าหน้าที่การไฟฟ้าในพื้นที่

๓) หากกระแสไฟฟ้าเข้าสู่สภาวะปกติภายใน ๑๒ ชั่วโมง ให้ตรวจเสถียรภาพของระบบและความเสียหายแล้วรายงานผลต่อหัวหน้าส่วนงานเทคโนโลยีและสารสนเทศ และผู้บังคับบัญชาตามลำดับขั้น

๔) หากกระแสไฟฟ้ายังไม่เข้าสู่สภาวะปกติภายใน ๑๒ ชั่วโมง ให้หัวหน้างานระบบเครือข่ายปิดระบบทุกระบบภายในห้องแม่ข่าย และอุปกรณ์เครือข่ายอย่างปลอดภัย

๕) หลักการทำงานของ Graceful Shutdown ในการปิดระบบตามคู่มือปฏิบัติงาน

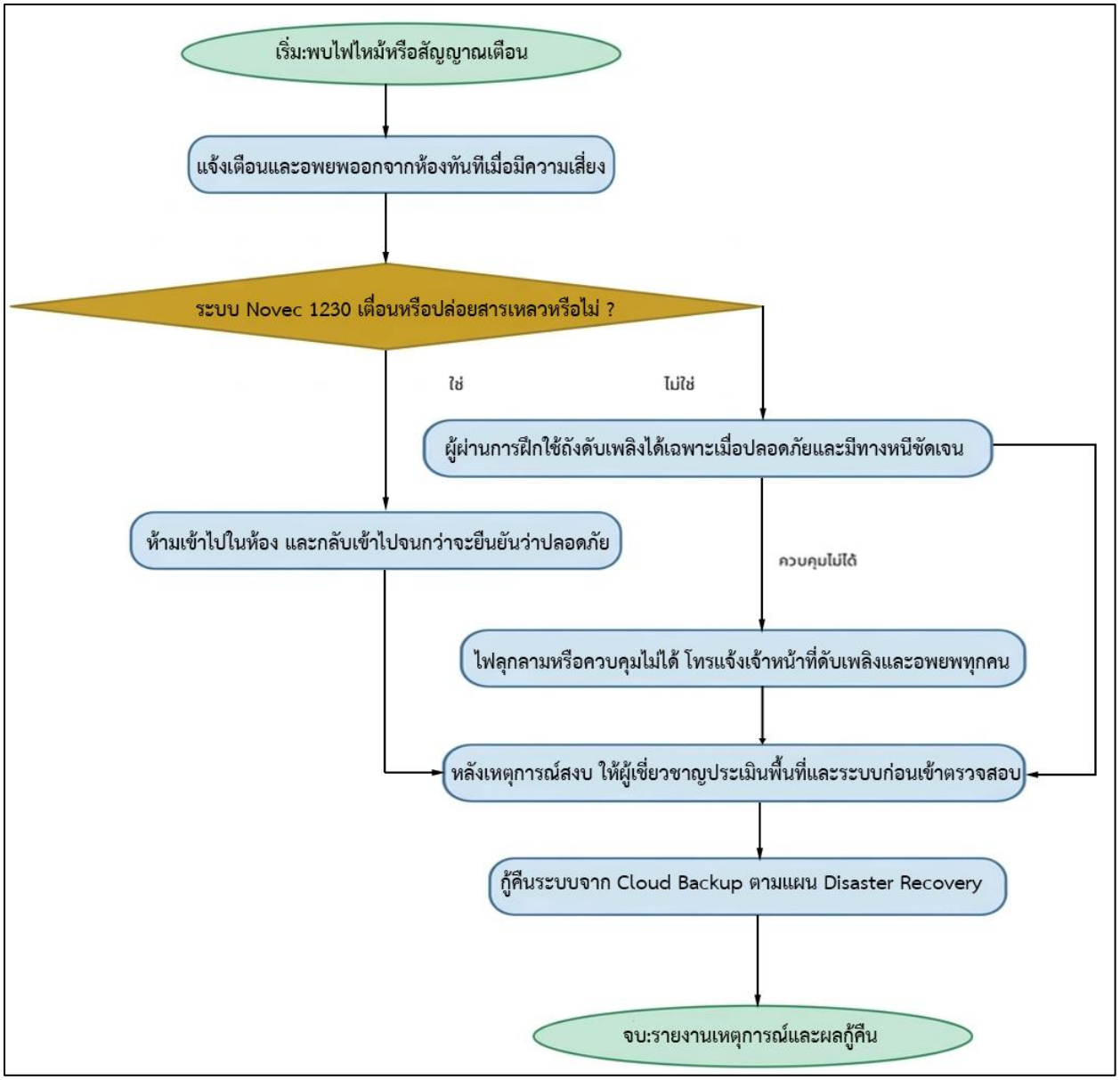
๖) รอจนกระแสไฟฟ้ากลับมาปกติ จากนั้นเปิดเครื่องสำรองไฟ และทยอยเปิดระบบตามหลักการการทำงานของอุปกรณ์ และเครือข่ายตามลำดับที่กำหนด ตรวจสอบการทำงานของระบบทุกระบบว่าทำงานอยู่ในสภาวะปกติ และสรุปรายงานเสนอต่อผู้บังคับบัญชาตามลำดับขั้นต่อไป

ข้อควรระวัง : อย่ารอจนเครื่องสำรองไฟใกล้หมดแล้วจึงค่อยปิดระบบในห้องแม่ข่าย และไม่ควรให้ผู้ที่ไม่มีความรู้และไม่ได้อยู่ในความรับผิดชอบในส่วนงานเทคโนโลยีและสารสนเทศเข้าไปปิดอุปกรณ์ภายในห้องแม่ข่าย

๖.๔ เหตุการณ์ไฟไหม้ห้องเครื่องแม่ข่าย หรือมีสัญญาณเตือนไฟไหม้

เมื่อเกิดไฟไหม้ห้องเครื่องแม่ข่าย หรือมีสัญญาณเตือนไฟไหม้ให้ถือว่าความปลอดภัยของชีวิตสำคัญกว่าเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายทุกชนิด

๖.๔.๑ <u>ขั้นตอนการปฏิบัติ (Flow Chart)</u>



ภาพที่ ๔ ขั้นตอนการปฏิบัติในเหตุการณ์ไฟไหม้ห้องเครื่องแม่ข่าย หรือมีสัญญาณเตือนไฟไหม้

๖.๔.๒ <u>อธิบายขั้นตอนการปฏิบัติ</u>

๑) เมื่อได้ยินเสียงสัญญาณเตือน/เริ่มอพยพตามแผนของอาคารทันที

๒) เจ้าหน้าที่ดับเพลิงอาจใช้เครื่องดับเพลิงเบื้องต้นได้เฉพาะเมื่อประเมินแล้วว่าปลอดภัยและมีทางหนีไฟที่ชัดเจน

๓) หากควบคุมเพลิงไม่ได้ทันทีหรือไฟลุกลาม ให้โทรแจ้งเจ้าหน้าที่ดับเพลิงและอพยพทุกคนไปยังพื้นที่ปลอดภัย

๔) ห้องแม่ข่ายมีระบบดับเพลิงอัตโนมัติ Novec ๑๒๓๐ เมื่อมีสัญญาณเตือนหรือระบบปล่อยสารให้อพยพทันที ห้ามกลับเข้าไปจนกว่าทีมฉุกเฉิน/ผู้รับผิดชอบจะยืนยันความปลอดภัย

๕) หลังเพลิงสงบและได้รับอนุญาตให้เข้าพื้นที่ เจ้าหน้าที่ที่เกี่ยวข้องประเมินความเสียหาย ประกาศใช้แผนกู้คืนระบบ และกู้คืนจากระบบสำรองข้อมูล (Dr-Site) พร้อมจัดหาอุปกรณ์ทดแทน

๖.๔.๓ ระบบดับเพลิงอัตโนมัติ Novec ๑๒๓๐

๑. <u>หลักการทำงานทั่วไป</u>

๑) เมื่อมีสัญญาณเตือนก่อนปล่อยสาร Novec ๑๒๓๐ ให้เจ้าหน้าที่ที่ทำงานในห้องแม่ข่ายหยุดปฏิบัติหน้าที่ทันที และอพยพออกจากห้องแม่ข่ายตามเส้นทางหนีไฟ อย่ารอให้เห็นควันหรือให้ระบบปล่อยสารก่อน

๒) หากได้ยินสัญญาณปล่อยสารหรือสงสัยว่าสารกำลังถูกปล่อย ให้รีบออกจากห้องและปิดประตูเมื่อทำได้ ห้ามกลับเข้าไปเพื่อหยิบอุปกรณ์หรือปิดระบบเอง

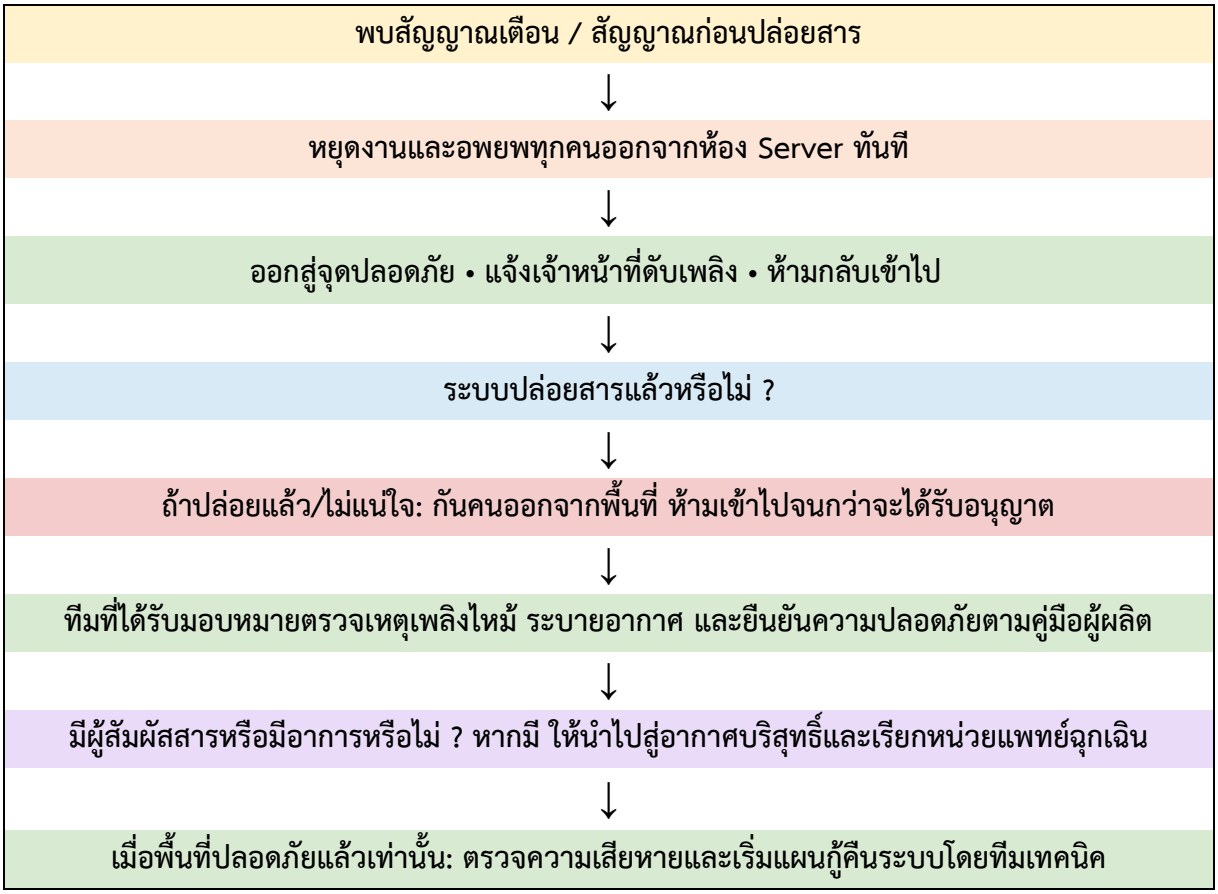
๓) ห้ามเข้าไปในห้องแม่ข่ายหลังการปล่อยสารจนกว่าเจ้าหน้าที่จะตรวจสอบและยืนยันว่าปลอดภัย รวมถึงระบายอากาศตามขั้นตอนของอาคารและผู้ผลิต

๔) อย่าพยายามช่วยผู้อื่นที่ยังอยู่ภายในห้องแม่ข่ายด้วยการเดินเข้าไป ผู้ช่วยเหลือต้องเป็นทีมที่ผ่านการฝึก และมีอุปกรณ์ป้องกันระบบทางเดินหายใจที่เหมาะสม

๕) Novec ๑๒๓๐ เป็นสารดับเพลิงชนิดสะอาด แต่ไม่ควรสรุปว่าขณะปล่อยสารปลอดภัยเสมอ ความปลอดภัยขึ้นกับความเข้มข้น การออกแบบระบบ ระยะเวลาสัมผัส และสภาพเหตุเพลิงไหม้

๖) หากมีอาการเสียงเปลี่ยน เสียงแหบ หายใจลำบาก เวียนศีรษะ หรือระคายเคืองหลังสัมผัส ให้ออกจากบริเวณไปสู่อากาศบริสุทธิ์และขอความช่วยเหลือทางการแพทย์ทันทีหากมีอาการ

๒. ขั้นตอนการปฏิบัติสำหรับเจ้าหน้าที่เทคนิค



ภาพที่ ๕ ขั้นตอนการทำงานของระบบดับเพลิงอัตโนมัติ Novec ๑๒๓๐ ปล่อยสาร

๓. ขั้นตอนการปฏิบัติสำหรับเจ้าหน้าที่ทั่วไป

๑) เมื่อได้ยินสัญญาณเตือน ให้แจ้งคนใกล้เคียง และออกตามทางหนีไฟไปยังจุดรวมพลทันที

๒) อย่ากดสวิตช์ หรือหยุดระบบดับเพลิง อย่าปลดล็อคถังหรือท่อ และอย่ากลับเข้าไปตรวจดูห้องแม่ข่ายด้วยตนเอง

๓) เจ้าหน้าที่เทคนิคแจ้งเจ้าหน้าที่ดับเพลิงว่าภายในห้องแม่ข่ายมีระบบดับเพลิง Novec ๑๒๓๐ ถังสารอยู่ด้านนอกห้อง และมีระบบท่อส่งสารเข้าห้องแม่ข่าย

๔) หากมีคนออกมาจากห้องแล้วมีอาการผิดปกติ ให้พาไปยังอากาศบริสุทธิ์โดยไม่ให้ผู้ช่วยเหลือเข้าไปในพื้นที่เสี่ยง และเรียกบริการแพทย์ฉุกเฉิน

๕) การกลับเข้าพื้นที่อาคาร ต้องได้รับอนุญาตจากผู้บังคับบัญชา/เจ้าหน้าที่ดับเพลิงหลังตรวจสอบพื้นที่แล้วเท่านั้น

๔. ขั้นตอนการปฏิบัติสำหรับผู้ดูแลอาคารและเจ้าหน้าที่ดูแลห้องแม่ข่าย

๑) ตรวจคู่มือของผู้ผลิตระบบ รุ่นถัง/แผงควบคุม และเอกสารข้อมูลความปลอดภัยของสารที่ใช้จริง

๒) ติดป้ายเตือนและแผนผังทางหนีไฟ รวมถึงป้ายระบุว่าเป็นห้องที่มีระบบดับเพลิงชนิดสารสะอาด

๓) กำหนดผู้รับผิดชอบในการยืนยันการปล่อยสาร การตัดระบบตามขั้นตอนของผู้ผลิต การระบายอากาศ และการอนุญาตให้กลับเข้าไป

๔) ทบทวนสัญญาณเตือนก่อนปล่อยสาร เวลาหน่วงก่อนปล่อย ปุ่มหยุด/ยกเลิกการปล่อย (ถ้ามี) และขั้นตอนฉุกเฉินกับผู้ติดตั้งระบบ ห้ามทดลองเองขณะระบบพร้อมทำงาน

๔) จัดทำรายชื่อผู้ติดต่อฉุกเฉิน และฝึกซ้อมอพยพเป็นระยะ

ข้อควรระวัง :

๑. ห้ามเข้าพื้นที่ที่ยังมีควัน ความร้อน หรือความเสี่ยง และอย่ากลับเข้าอาคารจนกว่าผู้มีอำนาจจะอนุญาต

๒. เนื้อหานี้เป็นแนวทางทั่วไปเพื่อการอพยพ ไม่ใช้แทนคู่มือของแผนฉุกเฉินของอาคาร หรือคำสั่งของเจ้าหน้าที่ดับเพลิง/ผู้เชี่ยวชาญระบบ

๗. ผู้รับผิดชอบและช่องทางประสานงาน

บทบาท/หน่วยงาน	ผู้รับผิดชอบ	ช่องทางติดต่อ/โทรศัพท์
ผู้มีอำนาจตามสายบังคับบัญชาสูงสุด	เลขาธิการ ศอ.บต.	๐๗๓-๒๗๔-๖๙๒
ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงระดับกระทรวง (Ministry Chief Information Officer : MCIO)	เลขาธิการ ศอ.บต. หรือผู้ที่ได้รับมอบหมาย	๐๗๓-๒๗๔-๖๙๒
กองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้	ผู้อำนวยการกองกองบริหารยุทธศาสตร์การพัฒนาจังหวัดชายแดนภาคใต้	๐๗๓-๒๐๓-๗๔๐
กลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี	ผู้อำนวยการกลุ่มงานบริหารยุทธศาสตร์การสื่อสารสร้างความเข้าใจที่ดี	๐๗๓-๒๗๔-๔๔๔
หัวหน้าส่วนงานเทคโนโลยีและสารสนเทศ	นางสาวสุภาพร กาญจนวงศ์ นักวิชาการคอมพิวเตอร์ชำนาญการพิเศษ	๐๖๔-๐๔๖-๒๒๕๖
หัวหน้างานระบบเครือข่าย	นายอับดุลฮาฟิต หะยีหะเต็ง นักวิชาการคอมพิวเตอร์ชำนาญการ	๐๘๘-๓๙๗-๓๖๑๘
เจ้าหน้าที่ดูแลห้องแม่ข่าย/ เจ้าหน้าที่ระบบเครือข่าย	นายธนาคม สมมาตร นักวิชาการคอมพิวเตอร์ปฏิบัติการ	๐๘๑-๔๑๘-๓๐๖๒
เจ้าหน้าที่เทคนิค	นายอภิชาติ จินดาวงษ์ พนักงานคอมพิวเตอร์ นางสาวรอฉีดา หัดขะแจ พนักงานคอมพิวเตอร์	๐๘๙-๐๐๘-๗๒๔๐ ๐๘๘-๗๙๒-๔๓๑๐
งานอาคารและสถานที่	นายกิตติพงศ์ สอดส่อง พนักงานช่างเทคนิค	๐๖๒-๓๖๐-๑๗๗๑

บทบาท/หน่วยงาน	ผู้รับผิดชอบ	ช่องทางติดต่อ/โทรศัพท์
งานป้องกันและบรรเทาสาธารณภัย เทศบาลนครยะลา	เจ้าหน้าที่ดับเพลิง	๐๗๓-๒๑๒-๓๔๕ หรือ สายด่วน ๑๙๙
การไฟฟ้าส่วนภูมิภาคจังหวัดยะลา (PEA)	เจ้าหน้าที่การไฟฟ้า	๐๗๓-๒๗๔-๘๘๐ หรือ สายด่วน ๑๑๒๙
สายด่วน อุ่นใจ ศอ.บต.	เจ้าหน้าที่สายด่วน ๑๘๘๐ ศอ.บต.	สายด่วน ๑๘๘๐
สำนักงานคณะกรรมการการรักษาความมั่นคงปลอดภัยไซเบอร์แห่งชาติ (สกมช.)	ศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์แห่งชาติ (Thailand Computer Emergency Response Team : ThaiCERT)	๐๒-๑๑๔-๓๕๓๑
สำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคล (สคส. หรือ PDPC)	ฝ่ายรับแจ้งเหตุละเมิดข้อมูลส่วนบุคคล	๐๒-๑๑๑-๘๘๐๐

๘. แบบบันทึกเหตุการณ์ฉุกเฉิน (สำหรับเจ้าหน้าที่เทคนิค)

เจ้าหน้าที่เทคนิค บันทึกข้อมูลเท่าที่ทราบในขณะเกิดเหตุ และอัปเดตเมื่อมีข้อมูลใหม่ ไม่จำเป็นต้องรอให้ทราบสาเหตุทั้งหมดก่อนจึงเริ่มบันทึก

รหัสเหตุการณ์	INC-..ปีงบประมาณ..-.....
ผู้รายงานเหตุการณ์	ชื่อ-สกุล..... ตำแหน่ง..... สังกัด..... เบอร์ติดต่อ.....
วันและเวลาที่พบเหตุการณ์	วันที่.....เวลา ..... น.
ประเภทเหตุการณ์	☐ ไวรัส/มัลแวร์ ☐ ถูกเจาะระบบ ☐ ไฟฟ้าดับ ☐ ไฟไหม้ ☐ อื่น ๆ .....
ระดับความรุนแรง	☐ สูงมาก: ระบบหลักหยุด/ปฏิบัติงานไม่ได้หรือข้อมูลรั่วไหล ☐ ปานกลาง: กระทบบางส่วน/มีระบบสำรอง ☐ ต่ำ: กระทบผู้ใช้รายบุคคล

ระบบ/อุปกรณ์ที่ได้รับผลกระทบ	☐ ชื่อเครื่อง/Server/IP: .... ☐ ระบบงาน/ฐานข้อมูล: .... ☐ อุปกรณ์ระบบเครือข่าย: .... ☐ อื่น ๆ : ....
ระบบ/อุปกรณ์ที่ได้รับผลกระทบ	
รายละเอียดที่พบ	....
สิ่งที่ดำเนินการแล้ว	....

สถานะล่าสุด	☐ อยู่ระหว่างควบคุม ☐ กำจัดภัยคุกคามแล้ว ☐ กู้คืนระบบแล้ว
การประสานงานภายนอก	☐ ไม่มี ☐ สกมช. วันที่..... เวลา..... ☐ ThaiCERT วันที่..... เวลา..... ☐ สคส. วันที่..... เวลา.....
ผู้รับผิดชอบ	ชื่อ-สกุล : ..... ตำแหน่ง : .....

๙. หลังควบคุมเหตุการณ์ได้แล้ว

๑) ตรวจสอบว่าระบบและข้อมูลกลับมาใช้งานได้อย่างปลอดภัยทุกระบบที่เกี่ยวข้อง ไม่ใช่เพียงเปิดเครื่องหรืออุปกรณ์ติดเท่านั้น

๒) บันทึกสาเหตุ ผลกระทบ เวลาที่เริ่มเหตุ เวลาที่ควบคุมเหตุ และวิธีแก้ไข

๓) เก็บ Log และหลักฐานที่จำเป็นตามแนวทางของเจ้าหน้าที่เทคนิค

๔) แจ้งผู้บังคับบัญชาและผู้ใช้งานที่เกี่ยวข้องถึงสถานะระบบและข้อควรปฏิบัติ

๕) ทบทวนเหตุการณ์และปรับปรุงแผน ผู้รับผิดชอบ เบอร์ติดต่อ และข้อมูลสำรองให้เป็นปัจจุบัน