แผนป้องกันภัยพิบัติ
ระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

อีเมล์ | contact@sbpac.go.th เว็บไซต์ | http://www.sbpac.go.th

คำนำ

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ และสอดคล้องกับแผนยุทธศาสตร์ของหน่วยงาน จำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่างๆอันอาจจะเกิดขึ้นกับระบบสารสนเทศ จึงได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษา ป้องกันและแก้ไขปัญหาอันอาจส่งผลกระทบต่อข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบฐานข้อมูล ระบบเครือข่ายของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)
กรกฎาคม ๒๕๕๕

สารบัญ

แผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้อง ได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศของ ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยจากภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการการพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศ รวมถึงการสื่อสารของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างต่อเนื่องเพื่อช่วยสนับสนุนการดำเนินงานตามพันธกิจให้บรรลุตามนโยบายและแผนงานของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ โดยมีศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานรับผิดชอบในการบริหารจัดการด้านเทคโนโลยีสารสนเทศภายในศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ในระยะเวลาที่ผ่านมาศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้พัฒนาระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีรวมทั้งบริการต่างๆ เป็นจำนวนมาก เพื่อให้บริการแก่บุคลากรของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ทั้งนี้ระบบเทคโนโลยีสารสนเทศหลักของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระบบเครือข่าย และอินเตอร์เน็ต อาจได้รับความเสียหายหรือหยุดชะงักการทำงาน เนื่องจากสาเหตุภายนอกที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ไม่สามารถควบคุมได้ ซึ่งอาจทำให้ส่งผลกระทบต่อการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันและแก้ไขปัญหาดังกล่าว ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจึงได้จัดทำแผนป้องกันภัยพิบัติด้านเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำหรับเป็นแนวทางในการดำเนินการป้องกันการกู้คืน และการบริหารในภาวะฉุกเฉินเพื่อลดผลกระทบจากความเสียหายที่อาจจะเกิดขึ้นได้ อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

๗. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

๘. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม

๙. การติดตามและรายงานผล

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) สามารถจำแนกได้เป็น สองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวมรวมข้อมูล

ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ **(Security Log Management System)** โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อนำมาสรุปเป็นข้อมูลต่อไป

ตารางแสดงโอกาสการเกิดภัยพิบัติ/เหตุการณ์ที่ทำให้เกิดการขัดข้องของระบบ

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)				
	ต่อ ระบบงาน	ต่อพันธกิจ ตามกฎหมาย	ต่อ ประชาชน	คะแนนรวม	จัด เรียงลำดับ
ไฟไหม้	๔	๔	๓	๔	๑
โดนเจาะระบบ	๕	๓	๓	๔	๑
ไฟฟ้าดับ	๓	๓	๓	๓	๒
น้ำท่วม / ถูกน้ำ / ความชื้น	๓	๓	๓	๓	๒
แผ่นดินไหว	๒	๒	๒	๒	๓
พายุ	๒	๒	๒	๒	๓
การก่อการร้าย / การจลาจล / การชุมนุม	๑	๑	๑	๑	๔
เหตุการณ์ความไม่สงบ	๒	๒	๒	๒	๓
สถานการณ์การเมือง	๒	๒	๒	๒	๓

๒. แนวทางการป้องกันและเตรียมการเบื้องต้น

๒.๑) การประกาศแผน (Activation)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการเพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะทำการแจ้งให้ CEO หรือ CIO ของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)ทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

๒.๒) กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติ ที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆที่มีความสำคัญ ต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๒.๓) การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า, สถานีดับเพลิง, สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

๒.๔) การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์ เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus/spyware
- แผ่น Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๕) การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๒.๖) การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สาหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) มีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

๒.๗) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่

อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๒.๘) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทาง ดังนี้

๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบแม่ข่าย (Server Room) หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์สารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๒.๙) การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

๑) เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

๓) ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า

๔) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๕) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๖) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๓. การเตรียมความพร้อม

๓.๑ การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก้ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑.๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อแปลงไฟฟ้าระเบิด

๑.๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๓๐ – ๖๐ นาที

๑.๓) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๑.๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๑.๕) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๒.๑) จัดทำแผนรองรับสถานการณฉุกเฉินอันเกิดจากไฟไหม้

๒.๒) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบแม่ข่ายคอมพิวเตอร์ (Server Room) เพื่อการควบคุมเพลิงในเบื้องต้น

๒.๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม /น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม/น้ำรั่ว

๒) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบแม่ข่ายคอมพิวเตอร์ (Server Room) เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเขาใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๓) อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย

๔) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๓.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุกและภัยคุกคามทางคอมพิวเตอร์โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบแม่ข่ายและการป้องกันความเสียหาย

๒) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเขาไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารผู้ดูแลระบบเครือข่าย เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงาน และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๖) มีการกรอกรายชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๓.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ

เจ้าหน้าที่แผนกต่างๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๓.๗ การเตรียมความพรอมรับสถานการณภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๓.๗.๑ ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัย จากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการปูองกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

๑.๑) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)

๑.๒) ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า (www.ndwc.thaigov.go.th)

๑.๓) กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม / แผ่นดินไหว (www.dmr.go.th)

๑.๔) หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์

แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)

๑.๕) กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการ และแนวทางปฏิบัติ (www.disaster.go.th)

๓.๗.๒ การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

๑) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

๒) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน

๓) หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

๔) ปลากระโดดขึ้นมาจากผิวน้ำ

๓.๗.๓ การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

๑) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

๒) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

๓) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่ม สำหรับบุคลากรของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

๔) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

๕) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๓.๗.๔ การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๑) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

๒) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไขหรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๓.๗.๕ การปฏิบัติขั้นเตรียมการ

๑) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

๒) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตาม

ความสำคัญ และกำหนดมาตรการในการเผชิญภัย

๓) อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่บุคลากรในองค์กร

๔) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๘ การเตรียมความพร้อมรับสถานการณภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

๑) ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๒) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสารยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓) ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

๔) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) จัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

- เลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (CEO)
- รองเลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (Director, Center for Information Technology)

๔.๒ ระดับปฏิบัติ

ก) ทีมบริหารจัดการการกู้คืนระบบ

ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ข) ทีมกู้คืนเครือข่าย

ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ตามปรกติ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ค) ทีมกู้คืนแอพลิเคชัน

ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ง) ทีมประเมินความเสียหาย

เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

จ) ทีมอาคารสถานที่

เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร แอร์ ให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ฉ) ทีมการจัดการทั่วไป

เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทางาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ

ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิงโดยใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศ (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ซ) ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อแปลงไฟฟ้าระเบิด

ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการ

สำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศ (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ฌ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ

ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์

ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ฎ) ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery)

ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ฏ) ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว

ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผน ที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกัน เหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล

ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่

เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

๕.๑ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์อำนวยการบริหารจังหวัดชายแดน
ภาคใต้ (ศอ.บต) ตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้ ให้แจ้งเหตุขัดข้องให้ผู้อำนวยการ ศูนย์เทคโนโลยีสารเทศทราบ เพื่อดำเนินการต่อไป

๕.๒ กรณีเครื่องแม่ข่ายบริการ (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปลดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปลดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

๖) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

๗) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๘) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๙) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยเร็ว

๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

กรณีจากไฟไหม้ห้องควบคุมระบบ

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ นางสาวรัตนา ไมสัน เบอร์โทรศัพท์ติดต่อ ๐๘-๙๔๘๐๗๒๔๘ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมแม่ข่ายระบบงานเสียหายน้อยที่สุด

๓. เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ดำเนินการดับเพลิงและจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัยได้แก่ อาคารอเนกประสงค์ แล้วแต่เหตุไฟไหม้และความเหมาะสม แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องดำเนินการในข้อ ๔ ต่อไป

๔. แจ้งสถานีดับเพลิงที่ใกล้ที่สุด ซึ่งในเขตที่ตั้งนี้คือสถานีตำรวจดับเพลิงเทศบาลนครยะลา เบอร์โทรศัพท์ ๐-๗๓๒๑-๒๓๔๕,๐-๗๓๒๑-๔๘๙๗ เพื่อดำเนินการต่อไป

๕. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ แก่ผู้อำนวยการเทคโนโลยีศูนย์สารสนเทศ เพื่อทราบและสั่งการต่อไป

๖. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

กรณีไฟดับ / หม้อแปลงไฟฟ้าระเบิด

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความ

เสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นายศิรวุฒิ กังวานเกียรติ เบอร์โทรศัพท์ติดต่อ ๐๘๘-๗๘๒๔๒๗๗

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบ งานเสียหายน้อยที่สุด

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทารายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

กรณีน้ำท่วมห้องควบคุมระบบ

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์สารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังอาคารอเนกประสงค์ พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายอาสลัน สะตาปอ เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๙

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

๑. ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการปูองกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบ ประกอบด้วย

- นายอาสลัน สะตาปอ เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๙
- นาย สุริยะ ดอเส็น เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๔

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้าควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุดพร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

๑) ควบคุมสถานการณ์

ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๒) วิเคราะห์การถูกโจมตี

ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่น ๆ

ข) วิเคราะห์ล็อกไฟล์ (Log file) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้

ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๓) กู้คืนระบบคอมพิวเตอร์

ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

ข) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานการถูกโจมตีผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

กรณีแผ่นดินไหว

๑. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางสาวกนกอร ไชยเทพ เบอร์โทรศัพท์ติดต่อ ๐๘๗-๒๙๐๒๓๗๑

๒. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือน เจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชาได้แก่

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๐๖๑๕๕๑
- หัวหน้าส่วนกลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๑๔๒๙๗๖

๓. เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้

๔. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

๑. **การปฏิบัติขณะเกิดแผ่นดินไหว**

๑) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน

๒) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

๓) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร

๔) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้

๕) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น

๗) ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า /สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๘) ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า

๙) ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด

๑๐) หลังจากการสั่นสะเทือนสิ้นสุด ให้รีบออกจากอาคาร

๑๑) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้อง โดยยึดหลัก

“หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๑๒) ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่

๑๓) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

๑๔) ห้ามใช้ลิฟต์โดยเด็ดขาด

๑๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

๑) ถ้าอาคารมั่นคงแข็งแรง ให้หลบอยู่ในอาคารนั้น

๒) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น

๓) หลังการสั่นสะเทือนสิ้นสุดลง ให้หาทางออกจากอาคารนั้น

๔) ถ้าไม่อยู่ใกล้ทางออก ให้ “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดชุลมุน

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

๑) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๒) หลีกเลี่ยงสิ่งของที่อาจโค่นล้มลงมาทาอันตราย เช่น ตู้ เสาไฟฟ้า ป้ายโฆษณาต้นไม้ใหญ่

๓) หลีกเลี่ยงอาคารสูง กาแพง ระวังเศษอิฐ กระจก ชิ้นส่วนของอาคารที่อาจหล่นลงมา

๔) วิ่งไปสู่ที่โล่ง

๕) รีบออกจากอาคารที่ชารุดเสียหายโดยเร็วที่สุด

กรณีอยู่ใกล้ชายฝั่ง

หากได้รับการแจ้งเตือน หรือรู้สึกได้ถึงแรงสั่นสะเทือน ให้รีบอพยพจากบริเวณชายฝั่งและริมแม่น้าลาคลองที่เชื่อมต่อกับทะเลโดยด่วน เพราะอาจเกิดคลื่นสึนามิได้

เมื่อแผ่นดินไหวสงบลง

๑) ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทาการปฐมพยาบาลเบื้องต้นและนาส่งโรงพยาบาล

๒) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ

๓) ตรวจสอบโครงสร้างอาคาร ท่อน้า ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบการทำงานทั้งหมดทันที

๔) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

๑) อยู่กับที่ ป้องกันศีรษะและหน้า จากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ

๒) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัสดุหล่นใส่

๓) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย

๔) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น

การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

๑) ระงับสติอารมณ์ ปฏิบัติตามแผนอพยพ

๒) เชื่อฟังคาแนะนาของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.

๓) เก็บทรัพย์สิน/เอกสารสำคัญ ไว้ในลิ้นชักโต๊ะและล๊อคกุญแจ

๔) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด

๕) ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ

๖) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า

๗) ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ ๒ คน

๘) ห้ามพูดคุย สายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง

๙) ห้ามใช้ลิฟต์ โดยเด็ดขาด

๑๐) เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที

๑๑) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้

๑๒) ตรวจสอบจานวนผู้อพยพ

เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ เพื่อทราบและสั่งการต่อไป

ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

๑. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้ง

ผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางสาวกนกอร ไชยเทพ เบอร์โทรศัพท์ติดต่อ ๐๘๗-๒๙๐๒๓๗๑

เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือน เจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชาได้แก่

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๐๖๑๕๕๑
- หัวหน้าส่วนกลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๑๔๒๙๗๖

๒. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดาเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจลาจล

๑) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของผู้ปฏิบัติงานและของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

๒) เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า

๓) ปิดประตูทั้ง ๒ ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาใน ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

๔) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของ ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ ให้แจ้งไปยังสถานีตำรวจ หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้อานวยการสำนักบริหารกลาง เพื่อทราบ

ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

๑) เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที

๒) รปภ. หรือเจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมทั้งติดต่อเจ้าหน้าที่ตำรวจในพื้นที่มาตรวจสอบวัตถุต้องสงสัย

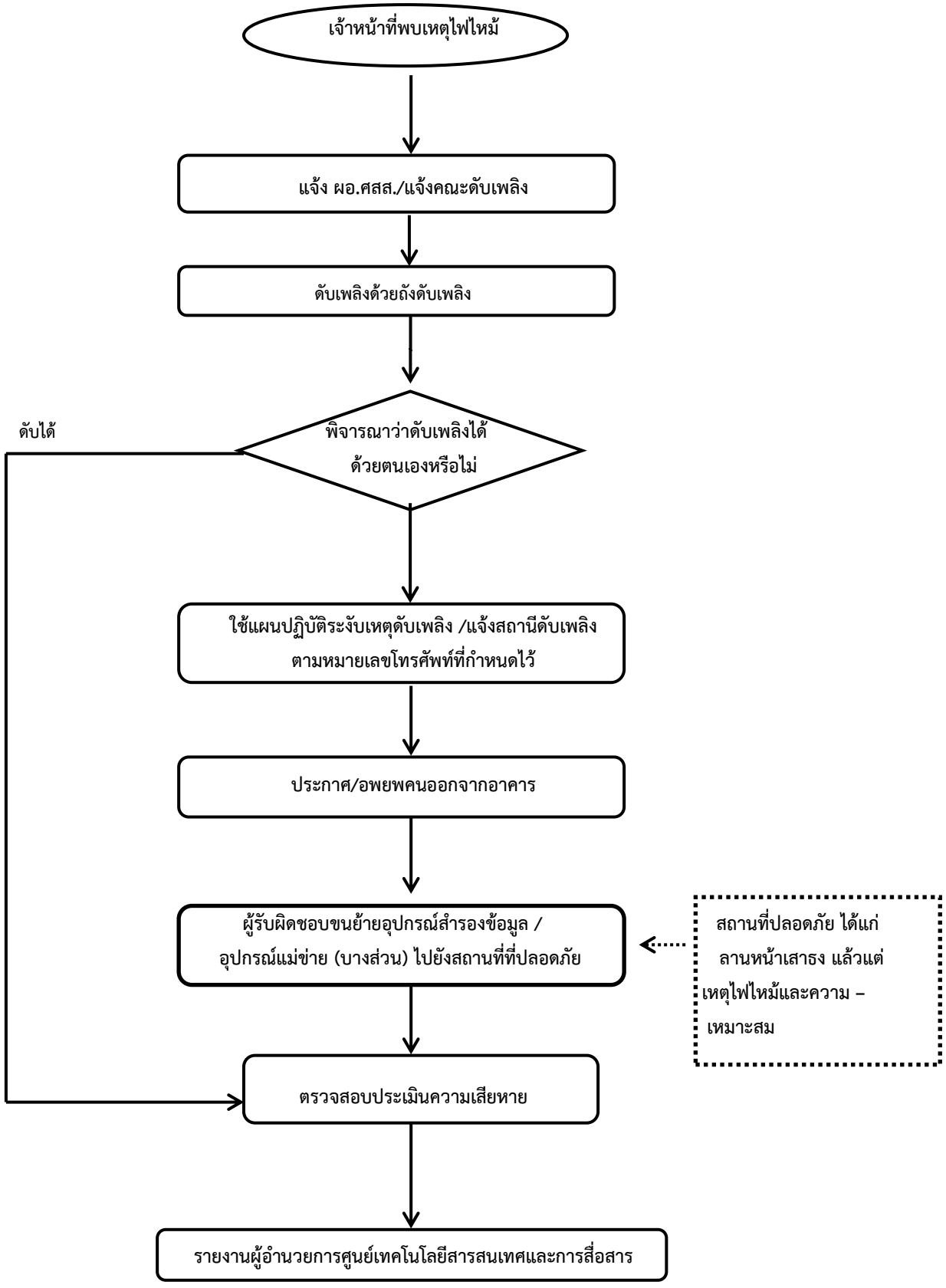
๓) ในกรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกั้นพื้นที่อันตรายที่พบวัตถุระเบิดกัน - บุคคลที่ไม่เกี่ยวข้องออกจากบริเวณที่พบวัตถุระเบิด และแจ้งอพยพผู้ปฏิบัติงานออกจากบริเวณหรือรัศมีของวัตถุระเบิด

๔) เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ เพื่อทราบและสั่งการต่อไป

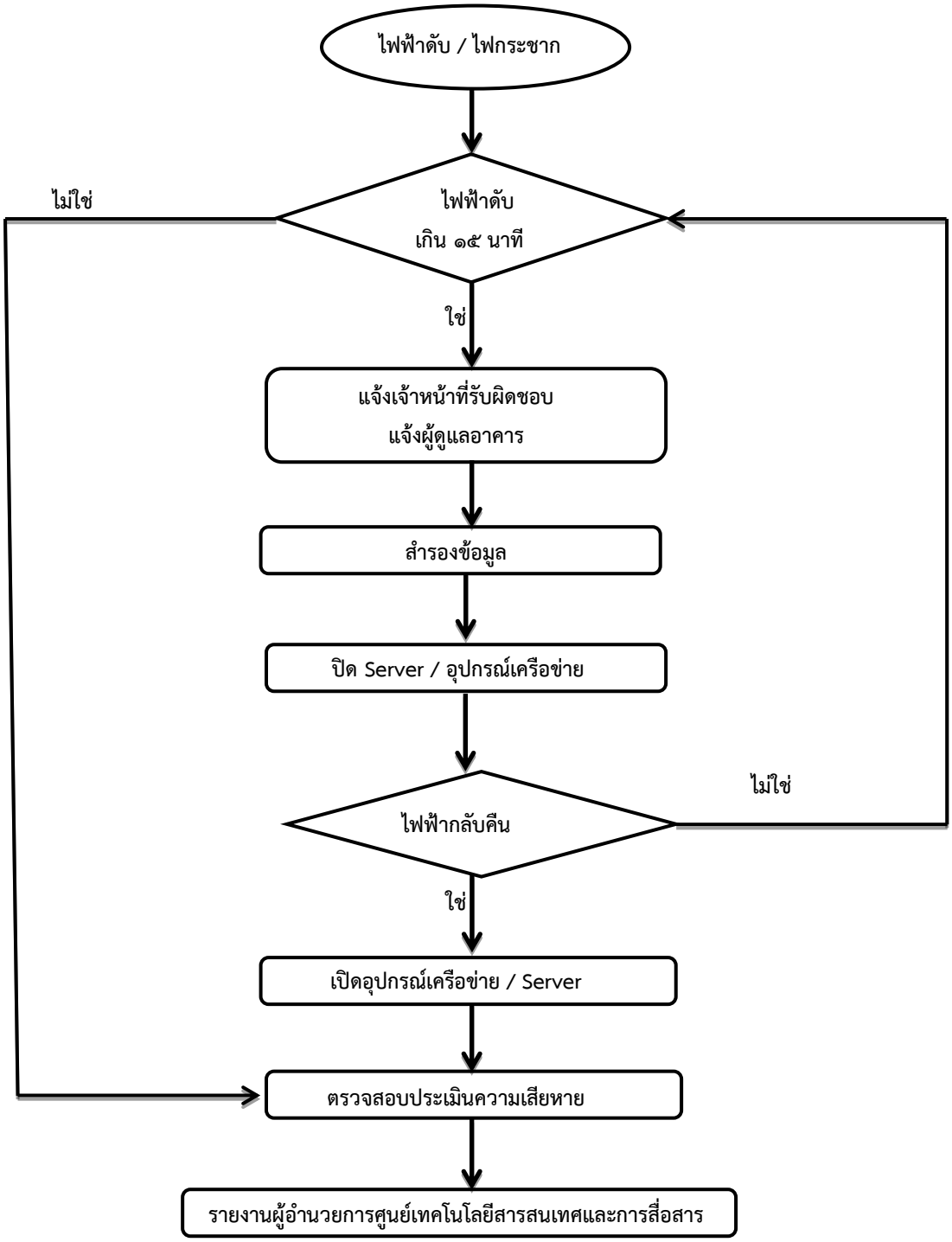
๕) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและ

ระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทารายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

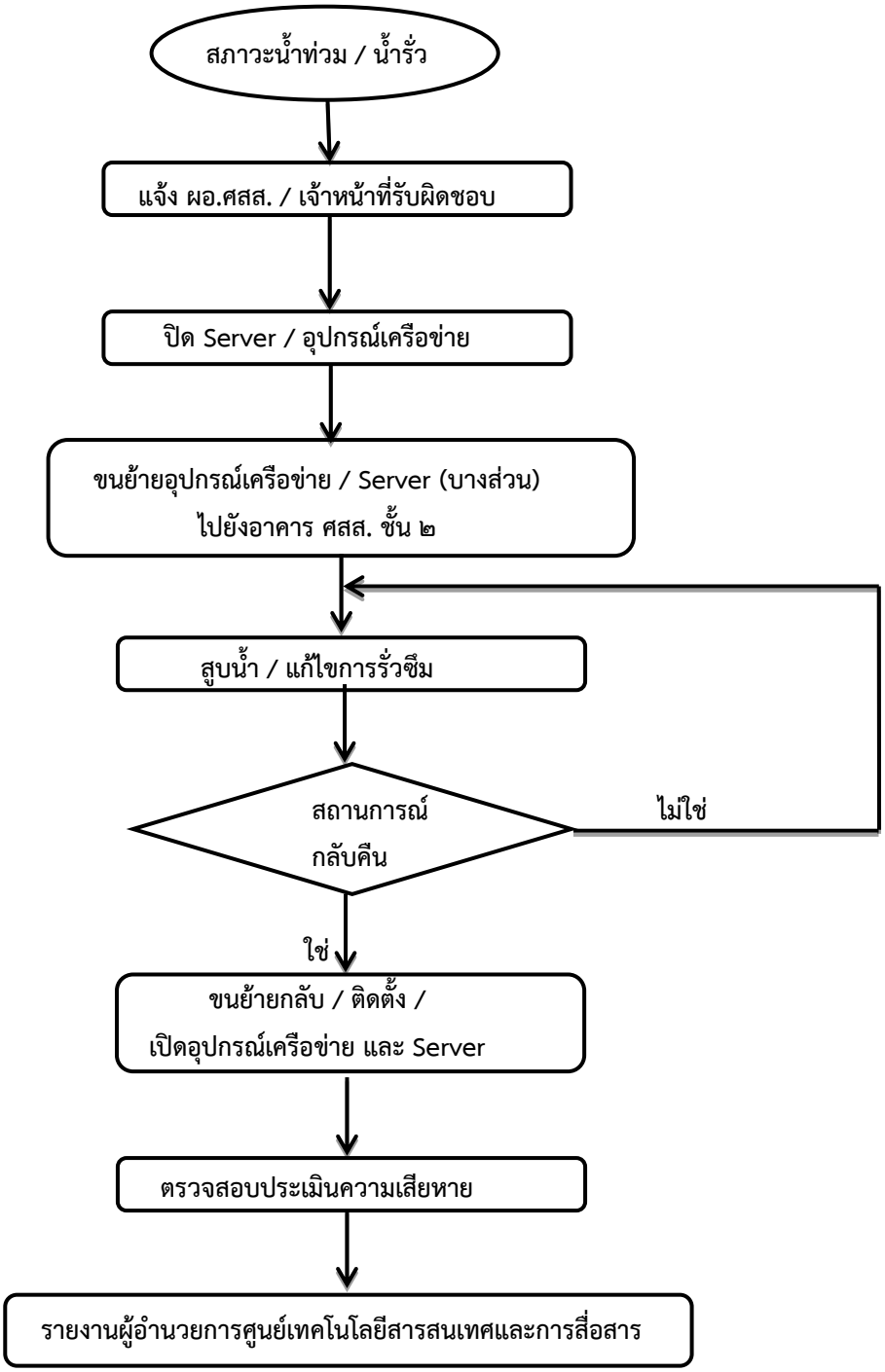
Flowchart กรณีไฟไหม้



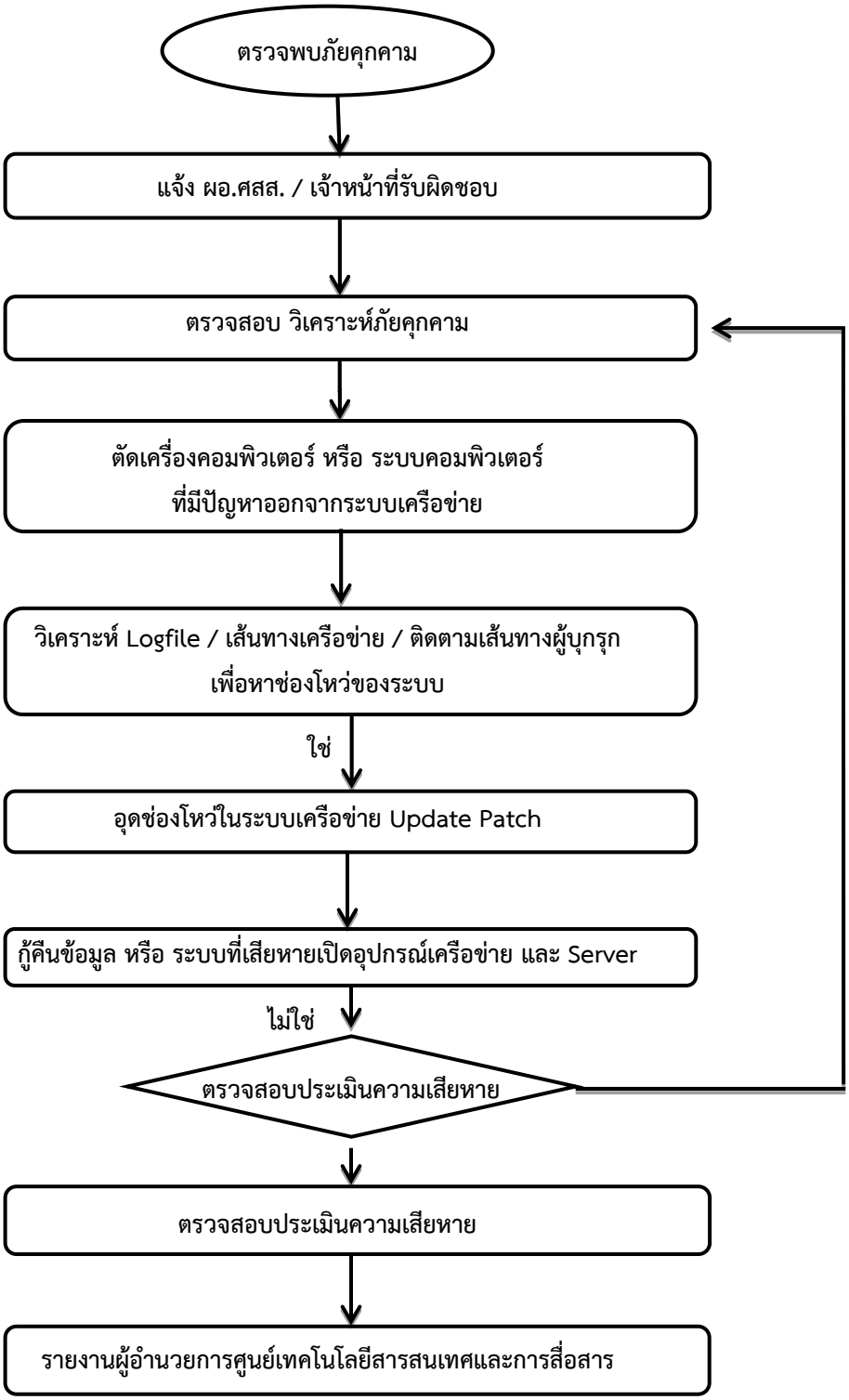
Flowchart กรณีไฟฟ้าดับ / ไฟฟ้ากระชาก / หม้อแปลงไฟฟ้าระเบิด



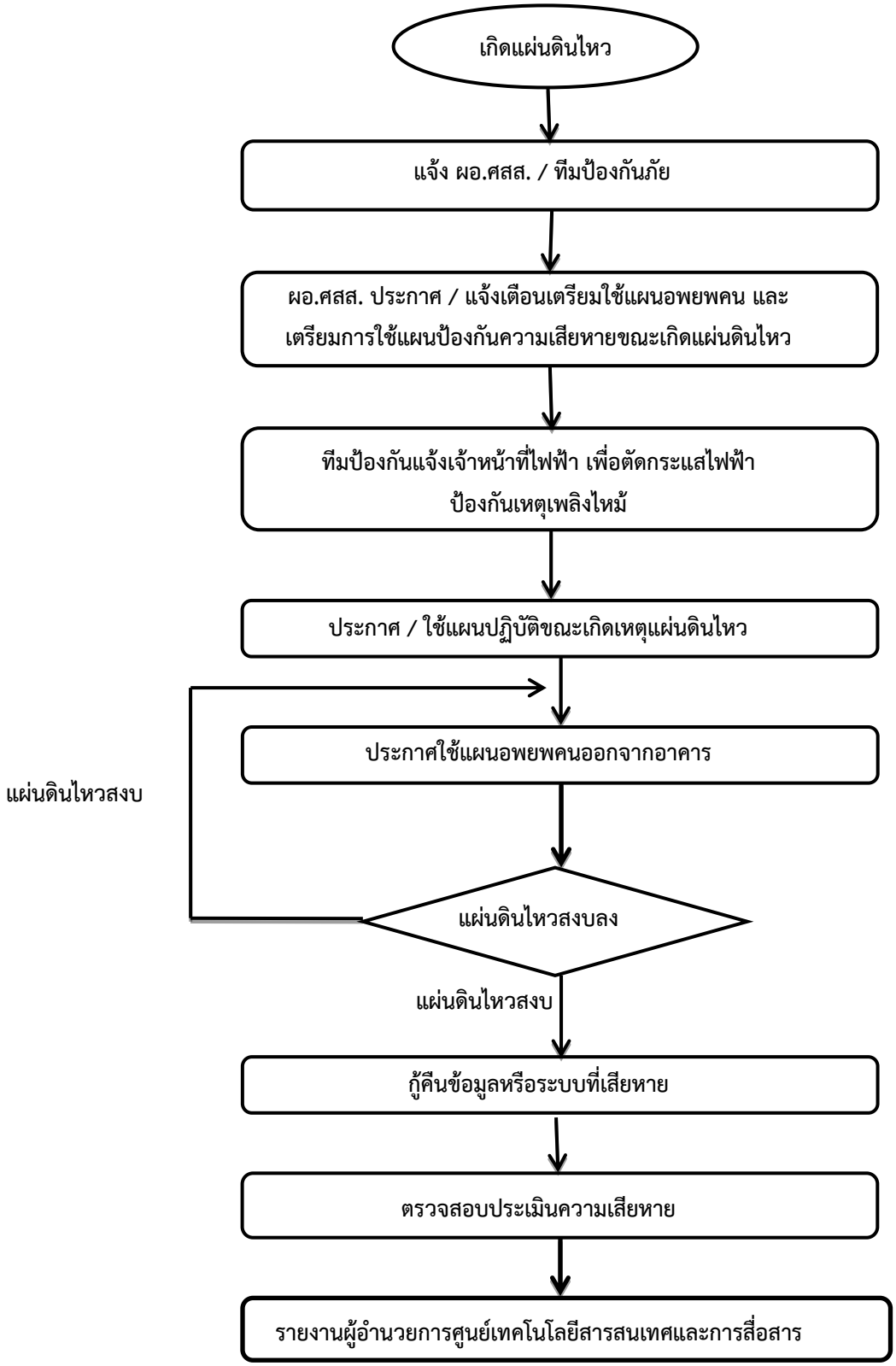
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีน้ำท่วม



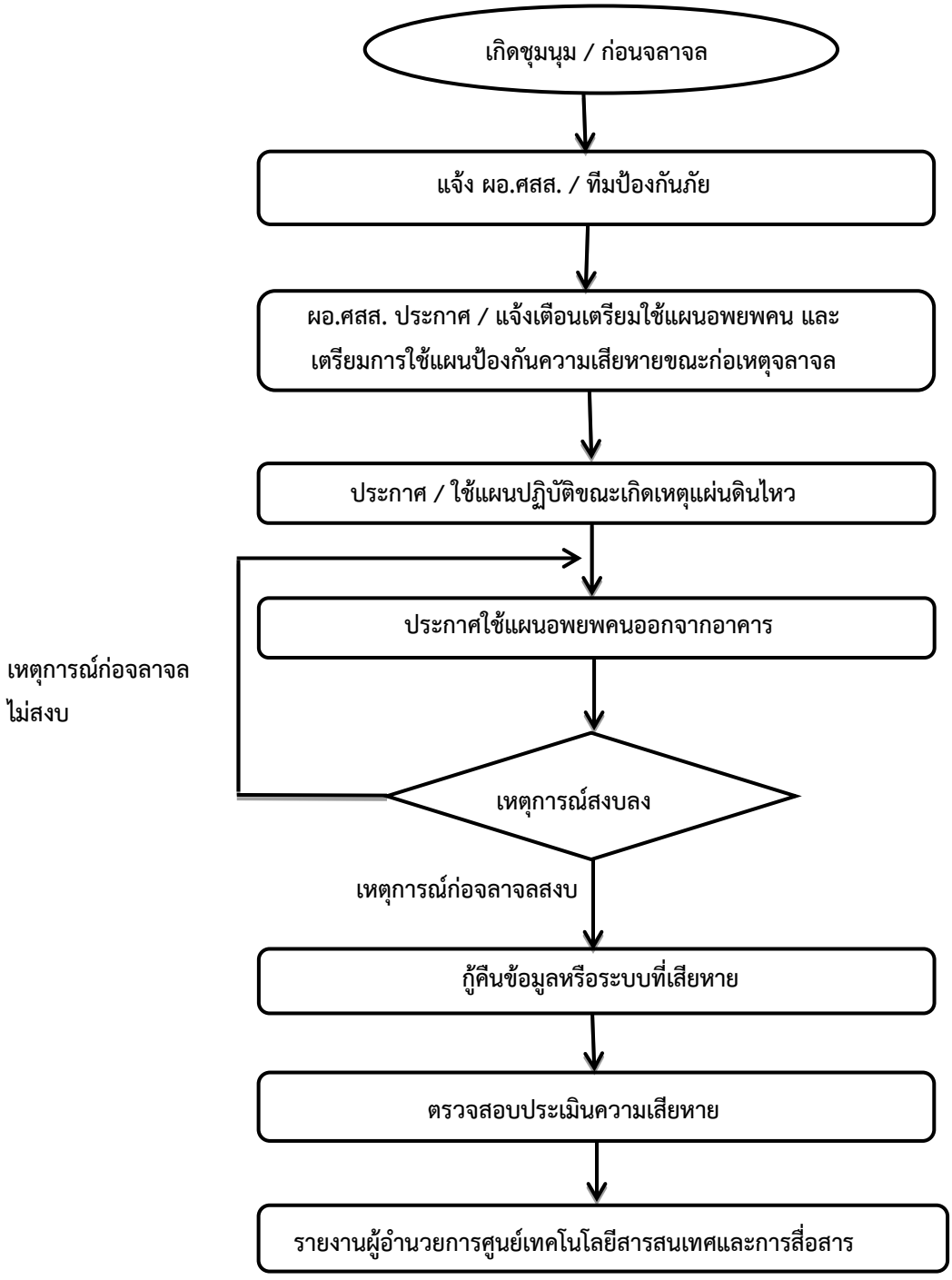
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือ ตรวจพบภัยคุกคาม



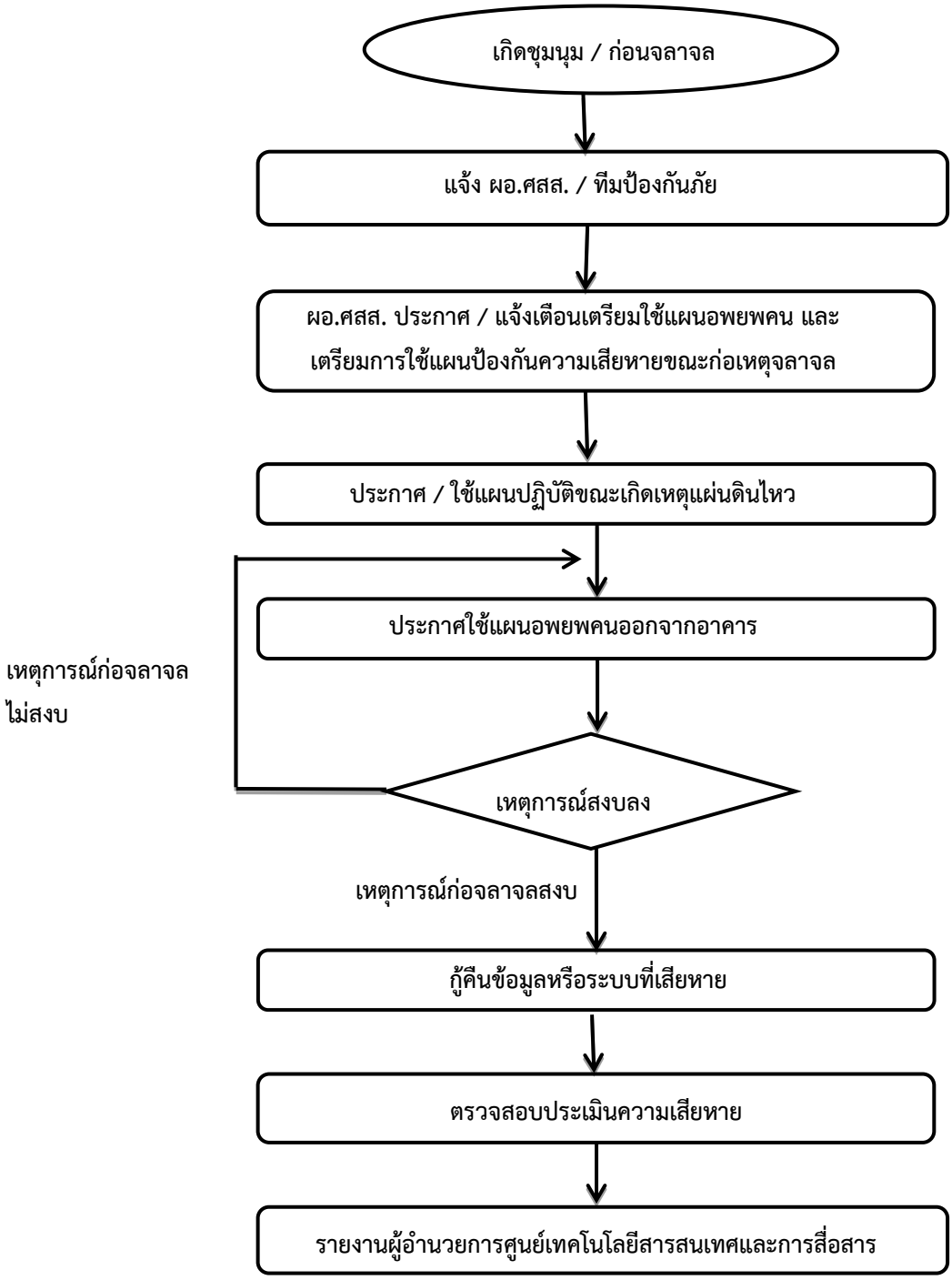
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีแผ่นดินไหว



Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



คำนำ

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ได้ตระหนักถึงความสำคัญของข้อมูลสารสนเทศที่มีความสำคัญยิ่งต่อการบริหารระบบราชการ และสอดคล้องกับแผนยุทธศาสตร์ของหน่วยงาน จำเป็นต้องได้รับการดูแลรักษาให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้งานได้อย่างเต็มประสิทธิภาพตลอดเวลา ดังนั้น เพื่อลดความเสี่ยงต่างๆอันอาจจะเกิดขึ้นกับระบบสารสนเทศ จึงได้จัดทำแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการบำรุงรักษา ป้องกันและแก้ไขปัญหาอันอาจส่งผลกระทบต่อข้อมูลและสารสนเทศ เครื่องคอมพิวเตอร์และอุปกรณ์ โปรแกรมระบบฐานข้อมูล ระบบเครือข่ายของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร
ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)
มิถุนายน ๒๕๕๘

สารบัญ

แผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศ
(IT Contingency Plan)

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินที่มีความสำคัญต่อการดำเนินงานขององค์กร จำเป็นต้อง ได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้ตระหนักถึงความสำคัญของระบบฐานข้อมูลและสารสนเทศของ ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยจากภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศ รวมทั้งระบบอุปกรณ์เสียหายได้

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ได้ดำเนินการพัฒนาและปรับปรุงระบบเทคโนโลยีสารสนเทศ รวมถึงการสื่อสารของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร อย่างต่อเนื่องเพื่อช่วยสนับสนุนการดำเนินงานตามพันธกิจให้บรรลุตามนโยบายและแผนงานของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ โดยมีศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเป็นหน่วยงานรับผิดชอบในการบริหารจัดการด้านเทคโนโลยีสารสนเทศภายในศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ในระยะเวลาที่ผ่านมาศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้พัฒนาระบบสารสนเทศและโครงสร้างพื้นฐานด้านเทคโนโลยีรวมทั้งบริการต่างๆ เป็นจำนวนมาก เพื่อให้บริการแก่บุคลากรของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ทั้งนี้ระบบเทคโนโลยีสารสนเทศหลักของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงระบบเครือข่าย และอินเตอร์เน็ต อาจได้รับความเสียหายหรือหยุดชะงักการทำงาน เนื่องจากสาเหตุภายนอกที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ไม่สามารถควบคุมได้ ซึ่งอาจทำให้ส่งผลกระทบต่อการดำเนินงานของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อป้องกันและแก้ไขปัญหาดังกล่าว ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจึงได้จัดทำแผนป้องกันภัยพิบัติด้านเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำหรับเป็นแนวทางในการดำเนินการป้องกันการกู้คืน และการบริหารในภาวะฉุกเฉินเพื่อลดผลกระทบจากความเสียหายที่อาจจะเกิดขึ้นได้ อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

ดังนั้นจึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาและแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) ดังนี้

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ
๒. แนวทางการป้องกันและเตรียมการเบื้องต้น
๓. การเตรียมความพร้อม
๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

๗. ผัง Flowchart กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติฯ

๘. แผนกู้คืนระบบกลับสู่สภาพปกติเดิม

๙. การติดตามและรายงานผล

๑. การวิเคราะห์และประเมินความรุนแรงของเหตุการณ์ภัยพิบัติ

๑.๑ วิเคราะห์เหตุการณ์ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) สามารถจำแนกได้เป็น สองกลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

ก) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แผ่นดินไหว ฯลฯ

ข) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวมรวมข้อมูล

ค) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

ง) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

จ) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

ฉ) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

ก) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

ข) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

ค) เจ้าหน้าที่หรือบุคลากรขององค์กรขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงาน

๑.๒ การประเมินสถานการณ์และกำหนดระดับความรุนแรง (Situation assessment)

เมื่อศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติ เพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ละเมิดความปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ **(Security Log Management System)** โดยเจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อนำมาสรุปเป็นข้อมูลต่อไป

ตารางแสดงโอกาสการเกิดภัยพิบัติ/เหตุการณ์ที่ทำให้เกิดการขัดข้องของระบบ

สถานการณ์หรือภาวะฉุกเฉิน	ระดับความรุนแรง (คะแนน 5 คะแนน)				
	ต่อ ระบบงาน	ต่อพันธกิจ ตามกฎหมาย	ต่อ ประชาชน	คะแนนรวม	จัด เรียงลำดับ
ไฟไหม้	๔	๔	๓	๔	๑
โดนเจาะระบบ	๕	๓	๓	๔	๑
ไฟฟ้าดับ	๓	๓	๓	๓	๒
น้ำท่วม / ถูกน้ำ / ความชื้น	๓	๓	๓	๓	๒
แผ่นดินไหว	๒	๒	๒	๒	๓
พายุ	๒	๒	๒	๒	๓
การก่อการร้าย / การจลาจล / การชุมนุม	๑	๑	๑	๑	๔
เหตุการณ์ความไม่สงบ	๒	๒	๒	๒	๓
สถานการณ์การเมือง	๒	๒	๒	๒	๓

๒. แนวทางการป้องกันและเตรียมการเบื้องต้น

๒.๑) การประกาศแผน (Activation)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารมีการประกาศใช้แผนการรักษาความปลอดภัยระบบสารสนเทศอย่างเป็นทางการเพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันที่แสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย โดยเมื่อเกิดเหตุการณ์ฉุกเฉิน ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจะทำการแจ้งให้ CEO หรือ CIO ของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)ทราบ เพื่อพิจารณาและประกาศใช้แผนต่อไป

๒.๒) กระบวนการดำเนินงาน (Procedure)

ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารจัดเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติในศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) โดยเมื่อเกิดเหตุการณ์ฉุกเฉินต้องมีการเลือกขั้นตอนปฏิบัติ ที่เหมาะสมกับสถานการณ์ต่างๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของผู้บุกรุกเพื่อยุติเหตุการณ์ที่เกิดขึ้นได้อย่างทันเวลาและถูกต้อง ระบบงานต่างๆที่มีความสำคัญ ต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหาขึ้น

๒.๓) การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกับหน่วยงานภายนอก เพื่อใช้สำหรับการติดต่อทางด้านความมั่นคงปลอดภัยกรณีที่มีความจำเป็นฉุกเฉิน เช่น การไฟฟ้า, สถานีดับเพลิง, สถานีตำรวจ เป็นต้น มีการเตรียมการประสานงานกับสถานีดับเพลิงเรื่องแผนที่อาคารและเส้นทางการเดินทาง

๒.๔) การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์ เกิดขัดข้องใช้งานไม่ได้ โดยเตรียมอุปกรณ์ดังนี้

- แผ่นติดตั้งระบบปฏิบัติการ/ระบบปฏิบัติการระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
- เทปสำรองข้อมูลและระบบงานที่สำคัญ
- แผ่นโปรแกรม Antivirus/spyware
- แผ่น Driver อุปกรณ์ต่างๆ
- ระบบสำรองไฟฉุกเฉิน
- อุปกรณ์สำรองต่างๆ ของเครื่องคอมพิวเตอร์

๒.๕) การสำรองข้อมูล (Backup)

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้ โดยศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan Policy)

๒.๖) การป้องกันไวรัสคอมพิวเตอร์

มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ สาหรับเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายที่เชื่อมต่อกับระบบเครือข่าย โดยผู้ใช้งานจำเป็นจะต้องระมัดระวังในการใช้งานระบบคอมพิวเตอร์โดยเฉพาะในการเชื่อมต่อกับอินเตอร์เน็ต เพื่อไม่ให้เป็นช่องทางให้ผู้ไม่หวังดีเข้ามาบุกรุกหรือทำลายระบบได้ โดยศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) มีนโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious software Protection Policy)

๒.๗) การป้องกันและแก้ไขปัญหาที่เกิดจากกระแสไฟฟ้าขัดข้อง

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์

๑) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่

อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะเวลาการสำรองไฟฟ้าได้ประมาณ ๓๐-๖๐ นาที

๒) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์ และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๓) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบบันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ

๒.๘) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่ายมีแนวทาง ดังนี้

๑) มาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้องควบคุมระบบแม่ข่าย (Server Room) หากจำเป็นให้มีเจ้าหน้าที่ของศูนย์สารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป และมีการติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๒) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕) การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทาความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์ได้เป็นอย่างดี

๒.๙) การจัดเตรียมวัสดุอุปกรณ์ที่จำเป็น กรณีเกิดแผ่นดินไหว

มีการจัดเตรียมวัสดุอุปกรณ์และเครื่องมือที่จำเป็นในกรณีเกิดแผ่นไหว โดยเตรียมอุปกรณ์ดังนี้

๑) เตรียมไฟฉาย อุปกรณ์ยังชีพ เช่น ยารักษาโรค ฯลฯ และแจ้งให้ทุกคนทราบถึงที่เก็บ

๒) ฝึกซ้อมการปฐมพยาบาลเบื้องต้น เพื่อปฏิบัติในยามฉุกเฉิน

๓) ควรทราบตำแหน่งวาล์วถังก๊าซ น้ำประปา และสะพานไฟฟ้า

๔) ไม่วางของหนักไว้บนชั้น หลังตู้ หรือที่สูง

๕) ผูกหรือยึดติดเครื่องใช้เฟอร์นิเจอร์ที่มีน้ำหนักมากไว้กับพื้นหรือผนัง

๖) ศึกษาแผน/ฝึกซ้อมแผนอพยพในภาวะฉุกเฉิน พร้อมกำหนดจุดรวมพลที่ชัดเจน และเป็นสัดส่วนของแต่ละชั้นหรือหน่วยงาน

๓. การเตรียมความพร้อม

๓.๑ การเตรียมความพรอมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อไฟฟ้าดับ และปัญหาไฟฟ้ากระชาก

เป็นการป้องกันและแก้ไขปัญหาจากกระแสไฟฟ้าซึ่งอาจสร้างความเสียหายแก้ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑.๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากไฟดับ หม้อแปลงไฟฟ้าระเบิด

๑.๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าและป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ หรือการประมวลผลของระบบคอมพิวเตอร์ในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ซึ่งมีระยะในเวลาในการสำรองไฟฟ้าโดยประมาณ ๓๐ – ๖๐ นาที

๑.๓) เปิดเครื่องสำรองไฟฟ้า ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๑.๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้รีบทำการบันทึกข้อมูลที่ยังค้างอยู่ทันทีและปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่าง ๆ

๑.๕) ให้มีการสำรองฐานข้อมูลทุก ๑ เดือนเป็นอย่างน้อย

๓.๒ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหายเมื่อเกิดเหตุไฟไหม้

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์ไฟไหม้ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่าง ๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๒.๑) จัดทำแผนรองรับสถานการณฉุกเฉินอันเกิดจากไฟไหม้

๒.๒) ติดตั้งเครื่องดับเพลิงแบบมือถือในทุกชั้นของอาคาร โดยเฉพาะห้องควบคุมระบบแม่ข่ายคอมพิวเตอร์ (Server Room) เพื่อการควบคุมเพลิงในเบื้องต้น

๒.๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๓ การเตรียมความพร้อมรับสถานการณ์ภัยพิบัติจากระบบคอมพิวเตอร์และข้อมูลเกิดความเสียหาย เมื่อเกิดเหตุน้ำท่วม /น้ำรั่ว

เป็นการป้องกันและแก้ไขปัญหาจากสถานการณ์น้ำท่วม/น้ำรั่ว ซึ่งอาจสร้างความเสียหายแก่ระบบสารสนเทศและอุปกรณ์คอมพิวเตอร์ต่างๆ กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบสารสนเทศ ดังนี้

๑) จัดทำแผนรองรับสถานการณ์ฉุกเฉินอันเกิดจากน้ำท่วม/น้ำรั่ว

๒) มีการตรวจสอบระบบท่อน้ำประปา ฝ้าเพดานห้องควบคุมระบบแม่ข่ายคอมพิวเตอร์ (Server Room) เพื่อให้ปลอดภัยต่อการรั่วซึมอย่างสม่ำเสมอ

๓) ให้มีการสำรองฐานข้อมูลเดือนละ ๑ ครั้งเป็นอย่างน้อย

๓.๔ การเตรียมความพร้อมรับสถานการณ์ภัยจากไวรัส

๑) ทำการติดตั้ง Firewall ซึ่งทำหน้าที่กำหนดสิทธิการเขาใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากบุคคลภายนอก

๒) มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสที่เครื่องแม่ข่าย (Server) และเครื่องลูกข่าย (Client)

๓) อัพเดตโปรแกรมกำจัดไวรัส ทุก ๑ เดือน เป็นอย่างน้อย

๔) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีแจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์อย่างต่อเนื่อง สม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดไวรัสในเบื้องต้น

๓.๕ การเตรียมความพร้อมรับสถานการณ์ภัยจากการบุกรุกและภัยคุกคามทางคอมพิวเตอร์โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๑) กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบแม่ข่ายและการป้องกันความเสียหาย

๒) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเขาไปในห้องควบคุมระบบเครือข่าย จะต้องให้เจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศและการสื่อสารผู้ดูแลระบบเครือข่าย เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก และคอยกำกับดูแลตลอดการปฏิบัติงาน และติดตั้งกล้องโทรทัศน์วงจรปิดเพื่อป้องกันการโจรกรรม

๓) มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งาน Firewall ตลอดเวลา

๔) มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตและกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมาก

ผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๖) มีการกรอกรายชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๓.๖ การเตรียมความพร้อมรับสถานการณ์จากเจ้าหน้าที่ผู้รับผิดชอบ

เจ้าหน้าที่แผนกต่างๆ ภายในองค์กรขาดทักษะความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ชี้แจงและอบรมเจ้าหน้าที่ให้มีความรู้ความเข้าใจในด้านฮาร์ดแวร์ (Hardware) และ ด้านซอฟต์แวร์ (Software) เบื้องต้น ตลอดจนวิธีการใช้ระบบเครือข่ายอย่างปลอดภัย เพื่อลดความเสี่ยงให้เกิดขึ้นน้อยที่สุด

๑) สร้างเครือข่ายด้านการรักษาความปลอดภัยระบบสารสนเทศ (Information Security) โดยเจ้าหน้าที่ของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เพื่อช่วยกำกับดูแลและถ่ายทอดความรู้ให้เพื่อนร่วมงาน

๒) วางกฎระเบียบให้เจ้าหน้าที่ปฏิบัติ เพื่อรักษาความปลอดภัยในการใช้งานระบบเครือข่ายคอมพิวเตอร์จัดทำคู่มือบริหารความเสี่ยงระบบสารสนเทศ เป็นแนวทางให้เจ้าหน้าที่ปฏิบัติ

๓.๗ การเตรียมความพรอมรับสถานการณภัยจากแผ่นดินไหว

การเตรียมความพร้อมในขั้นนี้ ให้เริ่มตั้งแต่ปัจจุบันเพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากแผ่นดินไหวที่เกิดขึ้น เตรียมการต่างๆ ที่จำเป็นเพื่อให้สามารถเผชิญกับภัย

๓.๗.๑ ติดตามข้อมูลข่าวเตือนภัยแผ่นดินไหว ข้อมูลพื้นที่เสี่ยงภัย ข้อมูลสถานการณ์สาธารณภัย จากหน่วยงานที่เกี่ยวข้อง และข้อมูลการพยากรณ์อากาศจากหน่วยงานอุตุนิยมวิทยาทั่วโลก มาตรการ/แนวทางปฏิบัติในการปูองกันและแก้ไขปัญหาสาธารณภัย ติดตามระเบียบ/กฎหมายที่เกี่ยวข้อง เชื่อมโยงไปถึงเว็บไซต์ของหน่วยงานต่างๆ ทั้งหน่วยงานภายในและต่างประเทศ ได้แก่

๑.๑) กรมอุตุนิยมวิทยา : ข้อมูลพยากรณ์อากาศ ข้อมูลอุณหภูมิ ข่าวเตือนภัย (www.tmd.go.th)

๑.๒) ศูนย์เตือนภัยพิบัติแห่งชาติ : การแจ้งเตือนล่วงหน้า(www.ndwc.thaigov.go.th)

๑.๓) กรมทรัพยากรธรณี : ข้อมูลพื้นที่เสี่ยงภัยจากดินถล่ม / แผ่นดินไหว (www.dmr.go.th)

๑.๔) หน่วยงานสำรวจเชิงภูมิศาสตร์ ประเทศสหรัฐอเมริกา : ข้อมูลสถานการณ์แผ่นดินไหวทั่วโลก (www.earthquake.usgs.gov)

๑.๕) กรมป้องกันและบรรเทาสาธารณภัย : การแจ้งเตือนภัย ข้อมูลพื้นที่เสี่ยงภัย มาตรการ และแนวทางปฏิบัติ (www.disaster.go.th)

๓.๗.๒ การสังเกตพฤติกรรมของสัตว์

สัตว์หลายชนิดมีการรับรู้และมักแสดงท่าทางออกมาก่อนเกิดแผ่นดินไหว อาจจะรู้ล่วงหน้าเป็นชั่วโมงหรือเป็นวันก็ได้ เช่น

๑) สัตว์เลี้ยง สัตว์บ้านทั่วไปตื่นตกใจ เช่น สุนัข เป็ด ไก่ หมู

๒) แมลงสาบจำนวนมากวิ่งเพ่นพ่าน

๓) หนู งู วิ่งออกมาจากที่อาศัย ถึงแม้ในบางครั้งจะเป็นช่วงฤดูจำศีลของพวกมัน

๔) ปลากระโดดขึ้นมาจากผิวน้ำ

๓.๗.๓ การเตรียมคน สถานที่อพยพและวัสดุอุปกรณ์

๑) ประสานการเตรียมงานกับหน่วยกู้ภัยเพื่อเตรียมการในการป้องกันและบรรเทาภัยจากแผ่นดินไหวและอาคารถล่ม และกำหนดวิธีการปฏิบัติทุกขั้นตอน

๒) ประสานการเตรียมการกับส่วนราชการที่เกี่ยวข้องในการจัดเตรียมกำลังคน วัสดุ อุปกรณ์ต่าง ๆ ตามความจำเป็นและเหมาะสม

๓) สำรวจสถานที่อพยพที่ปลอดภัยพร้อมอำนวยความสะดวก อาหาร และน้ำดื่มสำหรับบุคลากรของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.)

๔) สำรวจ จัดทำบัญชียานพาหนะและเครื่องมือเครื่องใช้ให้สามารถตรวจสอบและใช้ประโยชน์ได้อย่างมีประสิทธิภาพเมื่อเกิดภัย

๕) จัดเตรียมยานพาหนะเพื่อการอพยพผู้ประสบภัยและการขนส่งสิ่งของที่จำเป็นต่าง ๆ

๓.๗.๔ การจัดเตรียมมาตรการเพื่อความปลอดภัยของอาคาร

๑) สำรวจอาคารสูง อาคารขนาดใหญ่ที่อยู่ในพื้นที่ที่รับผิดชอบเพื่อประโยชน์ในการตรวจสอบของเจ้าหน้าที่ผู้รับผิดชอบ พร้อมทั้งกำหนดให้ปรับปรุงแก้ไขให้การใช้ประโยชน์ในอาคารให้ถูกต้องตามระเบียบกฎหมาย สามารถป้องกันแรงสั่นสะเทือนที่มีผลต่ออาคารตามความเหมาะสม

๒) เมื่อมีอาคารที่มีการก่อสร้าง ดัดแปลง โดยไม่ถูกต้องตามแบบแปลนแผนผัง เจ้าหน้าที่ผู้รับผิดชอบฝ่ายอาคารต้องดำเนินการตามระเบียบของทางราชการ เพื่อให้เจ้าของหรือผู้ครอบครองอาคารดำเนินการแก้ไขหรือรื้อถอนเพื่อความปลอดภัยต่อชีวิตและทรัพย์สินของประชาชน

๓.๗.๕ การปฏิบัติขั้นเตรียมการ

๑) การซักซ้อมแผนการป้องกันและบรรเทาภัยจากแผ่นดินไหว และอาคารถล่ม

๒) การสำรวจและจัดทำบัญชีเป้าหมาย พื้นที่เสี่ยงภัย โดยแยกประเภทเป้าหมายตามความสำคัญ และกำหนดมาตรการในการเผชิญภัย

๓) อบรม ให้ความรู้การปฏิบัติเมื่อเกิดแผ่นดินไหวและอาคารถล่ม แก่เจ้าหน้าที่บุคลากรในองค์กร

๔) รายงานสรุปผลการปฏิบัติการขั้นเตรียมการ

๓.๘ การเตรียมความพร้อมรับสถานการณภัยจากการชุมนุมประท้วงและก่อจลาจล

เพื่อติดตามสถานการณ์ รวบรวมข่าวสารข้อมูล ประเมินสถานการณ์จากการชุมนุมประท้วงและก่อจลาจล เตรียมการต่าง ๆ ที่จำเป็นเพื่อให้ สามารถเผชิญกับภัย

๑) ดำเนินการหาข่าวจากแหล่งต่าง ๆ เช่น ตำรวจ นักข่าว โทรทัศน์ วิทยุ และหน่วยงานที่เกี่ยวข้อง

๒) จัดเตรียมกำลังเจ้าหน้าที่ วัสดุ อุปกรณ์ เครื่องมือเครื่องใช้ ระบบการสื่อสารยานพาหนะ เป็นต้น และมอบหมายหน้าที่ความรับผิดชอบในการปฏิบัติไว้ให้พร้อม

๓) ตรวจสอบระบบไฟฟ้า ระบบปั๊มน้ำ ให้อยู่ในสภาพที่พร้อมใช้งาน

๔) ติดตั้งกล้องวงจรปิดเพื่อรักษาความปลอดภัย

๔. การจัดองค์กรและกำหนดผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) จัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๔.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

- เลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (CEO)
- รองเลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (CIO)
- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (Director, Center for Information Technology)

๔.๒ ระดับปฏิบัติ

ก) ทีมบริหารจัดการการกู้คืนระบบ

ซึ่งมีหน้าที่หลักในการจัดการและประสานงานการกู้คืนต่างๆ ผู้รับผิดชอบได้แก่

เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ข) ทีมกู้คืนเครือข่าย

ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ตามปรกติ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ค) ทีมกู้คืนแอพลิเคชัน

ทำหน้าที่ติดตั้ง กู้คืนระบบงานและฐานข้อมูลให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ง) ทีมประเมินความเสียหาย

เป็นทีมให้ข้อมูลความเสียหายทั้งด้าน Hardware และ Software เพื่อเตรียมจัดหาอุปกรณ์มาทดแทน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

จ) ทีมอาคารสถานที่

เป็นทีมที่จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบการสื่อสาร แอร์ ให้พร้อมใช้งาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ฉ) ทีมการจัดการทั่วไป

เป็นทีมประสานงานช่วยเหลือทีมอื่นๆ ให้บรรลุวัตถุประสงค์ในการทางาน ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ช) ทีมแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ห้องควบคุมระบบ

ทำหน้าที่ดำเนินการแก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิงโดยใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศ (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ซ) ทีมแก้ไขปัญหาเบื้องต้น กรณีไฟดับ / หม้อแปลงไฟฟ้าระเบิด

ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการ

สำรองข้อมูลที่สำคัญ จากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคนิคและการสื่อสาร ศูนย์เทคโนโลยีสารสนเทศ (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ฌ) ทีมแก้ไขปัญหาเบื้องต้น กรณีน้ำท่วมห้องควบคุมระบบ

ทำหน้าที่ในการป้องกันมิให้เกิดความเสียหายต่อระบบเครือข่าย โดยต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ สูบน้ำออกจากห้องควบคุมระบบและตรวจสอบการรั่วซึม ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ญ) ทีมแก้ไขปัญหา เนื่องจากโดนเจาะระบบ หรือภัยคุกคามทางคอมพิวเตอร์

ทำหน้าที่กู้คืนระบบให้ทำงานได้ปกติ รวมทั้งหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ฎ) ทีมสำรองและกู้คืนข้อมูล (Backup & Recovery)

ทำหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์ ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานเทคโนโลยีสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.). เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ฏ) ทีมแก้ไขปัญหา เนื่องจากแผ่นดินไหว

ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศสั่งการตามแผน ที่เตรียมไว้ และแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกัน เหตุเพลิงไหม้ และหลังจากเหตุแผ่นดินไหวสงบลงให้ตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

ฐ) ทีมแก้ไขปัญหา เนื่องจากเกิดการชุมนุมประท้วงและก่อจลาจล

ทำหน้าที่แจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง ให้เจ้าหน้าที่รับผิดชอบสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุมและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป ผู้รับผิดชอบ ได้แก่

เจ้าหน้าที่กลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

๕. มาตรการในการป้องกันและแก้ไขปัญหาภัยพิบัติ

มาตรการในการป้องกันและแก้ไขปัญหาจากภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ กำหนดแนวทางให้บุคลากรปฏิบัติดังนี้

๕.๑ กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งเหตุนั้นให้ผู้ดูแลระบบเครือข่ายหรือฐานข้อมูลสารสนเทศ ของหน่วยงานทราบ หรือในกรณีเกิดจากศูนย์เทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารต้องประกาศให้ทุกหน่วยงานในองค์กรทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่อหน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

๓) ให้เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต) ตรวจสอบและแก้ไขปัญหาเบื้องต้น ถ้าหากไม่สามารถแก้ไขปัญหาได้ ให้แจ้งเหตุขัดข้องให้ผู้อำนวยการ ศูนย์เทคโนโลยีสารเทศทราบ เพื่อดำเนินการต่อไป

๕.๒ กรณีเครื่องแม่ข่ายบริการ (Server)

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปลดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปลดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีที่ไม่ปลอดภัยให้รีบขนย้ายไปไว้ที่ปลอดภัย

๕) กรณีไฟไหม้ให้ใช้น้ำยาดับเพลิง ฉีดควบคุมเพลิงโดยเร็ว

๖) รีบขนย้ายเครื่องไว้ในที่ปลอดภัย

๗) ประสานขอความช่วยเหลือกับหน่วยงานภายนอกที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายหรือผู้เชี่ยวชาญระบบเครือข่ายโดยเร็วที่สุด

๘) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

๙) ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบโดยเร็ว

๖. กระบวนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ ที่อาจจะเกิดกับระบบฐานข้อมูลและสารสนเทศ

กรณีจากไฟไหม้ห้องควบคุมระบบ

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้น พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

เจ้าหน้าที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ (ศอ.บต.) เบอร์โทรศัพท์ติดต่อ ๐๗๓-๒๗๔๑๐๐ หรือ สายด่วน ๑๘๘๐

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ นางสาวรัตนา ไมสัน เบอร์โทรศัพท์ติดต่อ ๐๘-๙๔๘๐๗๒๔๘ หรือ สายด่วน ๑๘๘๐ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมแม่ข่ายระบบงานเสียหายน้อยที่สุด

๓. เจ้าหน้าที่รับผิดชอบต้องใช้อุปกรณ์ที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสารได้จัดหาไว้ดำเนินการดับเพลิงและจัดการขนย้ายอุปกรณ์ที่สามารถขนย้ายได้ (บางส่วน) ไปยังสถานที่ที่ปลอดภัยได้แก่ อาคารอเนกประสงค์ แล้วแต่เหตุไฟไหม้และความเหมาะสม แต่ถ้าไม่สามารถแก้ไขหรือควบคุมเพลิงได้ต้องดำเนินการในข้อ ๔ ต่อไป

๔. แจ้งสถานีดับเพลิงที่ใกล้ที่สุด ซึ่งในเขตที่ตั้งนี้คือสถานีตำรวจดับเพลิงเทศบาลนครยะลา เบอร์โทรศัพท์ ๐-๗๓๒๑-๒๓๔๕,๐-๗๓๒๑-๔๘๙๗ หรือ สายด่วน ๑๘๘๐ เพื่อดำเนินการต่อไป

๕. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ แก่ผู้อำนวยการเทคโนโลยีศูนย์สารสนเทศ เพื่อทราบและสั่งการต่อไป

๖. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุม

ระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารทราบ

กรณีไฟดับ / หม้อแปลงไฟฟ้าระเบิด

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการป้องกันมิให้เกิดความเสียหายกับระบบงาน โดยจะต้องดำเนินการสำรองข้อมูลที่สำคัญจากเครื่องสำรองไฟที่ยังสามารถให้พลังงานอยู่ จากนั้นผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบในห้องควบคุม พร้อมทั้งแจ้งผู้รับผิดชอบห้องคุมระบบ ประกอบด้วย

นายศิรวุฒิ กังวานเกียรติ เบอร์โทรศัพท์ติดต่อ ๐๘๘-๗๘๒๔๒๗๗ หรือ สายด่วน ๑๘๘๐

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทารายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสารเพื่อทราบและสั่งการต่อไป

กรณีน้ำท่วมห้องควบคุมระบบ

๑. ผู้ที่อยู่เวรรักษาการณ์ต้องนำอุปกรณ์ที่ศูนย์สารสนเทศจัดหาไว้มาดำเนินการป้องกันมิให้เกิดความเสียหายในเบื้องต้น โดยผู้ที่อยู่เวรรักษาการณ์จะต้องปิดระบบที่จะเกิดผลกระทบจากการเกิดน้ำท่วมลงทุกระบบ จากนั้นติดตั้งอุปกรณ์เครื่องสูบน้ำ ทำการสูบน้ำออกจากห้องควบคุมระบบ ตรวจสอบการรั่วซึม และดำเนินการเคลื่อนย้ายอุปกรณ์ที่สำคัญให้พ้นจากภัยน้ำท่วม (บางส่วน) ไปยังอาคารอเนกประสงค์ พร้อมทั้งแจ้งผู้รับผิดชอบห้องควบคุมระบบ ประกอบด้วย

นายอาสลัน สะตาปอ เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๙ หรือ สายด่วน ๑๘๘๐

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่เข้าปฏิบัติงาน เพื่อให้ห้องควบคุมระบบงานเสียหายน้อยที่สุด

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบและอุปกรณ์ภายในห้องควบคุมระบบ พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งหัวหน้ากลุ่มคอมพิวเตอร์และเทคโนโลยีเครือข่ายและผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์

๑. ผู้ที่อยู่เวรรักษาการณ์ ต้องดำเนินการแก้ไขปัญหาเบื้องต้นในการปูองกันมิให้เกิดความเสียหายแก่ระบบเครือข่าย โดยจะต้องแจ้งผู้รับผิดชอบห้องควบคุมระบบทราบโดยด่วนเพื่อเข้าควบคุมสถานการณ์ ผู้รับผิดชอบ ประกอบด้วย

- นายอาสลัน สะตาปอ เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๙ หรือ สายด่วน ๑๘๘๐
- นาย สุริยะ ดอเส็น เบอร์โทรศัพท์ติดต่อ ๐๘-๘๗๙๒-๔๓๐๔ หรือ สายด่วน ๑๘๘๐

๒. แจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ เพื่อทราบ และดำเนินการสั่งการแก่เจ้าหน้าที่ที่ได้รับมอบหมายให้เข้าควบคุมสถานการณ์ เพื่อระบบงานและเครือข่ายได้รับความเสียหายน้อยที่สุดพร้อมทั้งทำให้ระบบรักษาความปลอดภัยกลับมาใช้งานได้โดยเร็วที่สุด

ขั้นตอนในการกู้คืนระบบความปลอดภัย กรณีโดนเจาะระบบ และภัยคุกคามทางคอมพิวเตอร์ มีดังนี้

๑) ควบคุมสถานการณ์

ก) ตรวจสอบภัยคุกคาม เพื่อแก้ไขปัญหา

ข) ตัดเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีปัญหาออกจากระบบเครือข่าย

ค) เตรียมการสำหรับการกู้คืนระบบโดยพิจารณาถึงการส่งผลกระทบต่อองค์กรเป็นหลัก

๒) วิเคราะห์การถูกโจมตี

ก) ตรวจสอบการเปลี่ยนแปลงของไฟล์ในระบบปฏิบัติการ (System file) และไฟล์อื่น ๆ

ข) วิเคราะห์ล็อกไฟล์ (Log file) ตรวจสอบโปรแกรมหรือ ข้อมูลที่ผู้บุกรุกทิ้งไว้

ค) ตรวจสอบระบบเครือข่าย และระบบที่เกี่ยวข้องกับการ Remote System

ง) ตรวจสอบติดตามเส้นทางผู้บุกรุก สแกนเพื่อหาช่องโหว่ของระบบ

๓) กู้คืนระบบคอมพิวเตอร์

ก) กู้คืนข้อมูลหรือสารสนเทศที่เสียหาย หรือติดตั้งระบบปฏิบัติการทั้งหมดใหม่

ข) งดใช้เซอร์วิสที่ไม่จำเป็น

ค) ติดตั้งข้อแก้ไขเพิ่มเติมเพื่อความปลอดภัยของข้อมูล (Update Patch)

ง) อุดช่องโหว่ในระบบเครือข่าย

จ) เปลี่ยนแปลงพาสเวิร์ดใหม่ หลังจากได้แก้ไขช่องโหว่ของระบบแล้ว

๓. ผู้รับผิดชอบในข้อ ๒ ดำเนินการรายงานการถูกโจมตีผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ แก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

๔. ผู้ควบคุมในกรณีนี้ จะต้องดำเนินการเข้าตรวจสอบระบบงานและระบบเครือข่าย พร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เพื่อทราบและสั่งการต่อไป

กรณีแผ่นดินไหว

๑. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบหรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางสาวกนกอร ไชยเทพ เบอร์โทรศัพท์ติดต่อ ๐๘๗-๒๙๐๒๓๗๑ หรือ สายด่วน ๑๘๘๐

๒. เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำแจ้งเตือน เจ้าหน้าที่ในองค์กรให้หลบภัยบริเวณนอกอาคาร หรือเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชาได้แก่

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐
- หัวหน้าส่วนกลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๑๔๒๙๗๖ หรือ สายด่วน ๑๘๘๐

๓. เจ้าหน้าที่รับผิดชอบแจ้งเจ้าหน้าที่ไฟฟ้าในพื้นที่ดำเนินการหยุดปล่อยกระแสไฟฟ้าเพื่อป้องกันเหตุเพลิงไหม้

๔. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดำเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

ขั้นตอนการปฏิบัติกรณีเกิดแผ่นดินไหว

๑. **การปฏิบัติขณะเกิดแผ่นดินไหว**

๑) ควบคุมสติ อย่าตื่นตกใจ อยู่อย่างสงบ รอฟังประกาศฉุกเฉิน

๒) ถ้าอยู่ในอาคารให้อยู่ในอาคารที่แข็งแรง อยู่ห่างจากหน้าต่าง/ประตู/กำแพงด้านนอก/ชั้นวางของ/สิ่งที่อาจล้มหรือหล่นได้

๓) อย่ารีบออกจากอาคาร อาจได้รับบาดเจ็บจากฝูงชนที่ตื่นตกใจและแย่งกันออกจากอาคาร

๔) ห้ามใช้เทียนไข ไม้ขีดไฟ หรือสิ่งที่ทำให้เกิดเปลวไฟ อาจเกิดอันตรายจากก๊าซรั่วได้

๕) อย่าตื่นตกใจหากไฟฟ้าดับหรือสัญญาณเตือนภัยดังขึ้น

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด หากต้องอพยพให้ใช้บันไดหนีไฟที่ปลอดภัยตามแผนอพยพเท่านั้น

๗) ถ้าอยู่นอกอาคาร ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า /สิ่งห้อยแขวน/ป้ายโฆษณา โดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๘) ถ้ากำลังขับรถยนต์ให้จอดรถยนต์ในที่ที่ปลอดภัยโดยเร็วเท่าที่จะทำได้และอยู่ในรถยนต์ หลีกเลี่ยงการจอดรถยนต์ใกล้หรือใต้ต้นไม้/อาคาร/สะพาน/ทางต่างระดับ/เสาไฟฟ้า

๙) ถ้าอาคารเก่าหรือไม่มั่นคง ให้หาทางออกจากอาคารให้เร็วที่สุด

๑๐) หลังจากการสั่นสะเทือนสิ้นสุด ให้รีบออกจากอาคาร

๑๑) ถ้าไม่อยู่ใกล้ทางออกให้รีบมุดลงไปอยู่ใต้โต๊ะที่แข็งแรง หรือมุมห้อง โดยยึดหลัก “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๑๒) ให้อยู่ห่างจากประตู หน้าต่าง โดยเฉพาะที่เป็นกระจกและอยู่ห่างจากบริเวณที่อาจมีวัสดุหล่นใส่

๑๓) ให้อยู่ห่างจากสายไฟฟ้า สิ่งห้อยแขวน

๑๔) ห้ามใช้ลิฟต์โดยเด็ดขาด

๑๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็วตามแผนอพยพหนีไฟของแต่ละอาคาร

กรณีอยู่ตึกสูง

๑) ถ้าอาคารมั่นคงแข็งแรง ให้หลบอยู่ในอาคารนั้น

๒) ถ้าอาคารเก่าและไม่มั่นคง ให้หาทางออกจากอาคารนั้น

๓) หลังการสั่นสะเทือนสิ้นสุดลง ให้หาทางออกจากอาคารนั้น

๔) ถ้าไม่อยู่ใกล้ทางออก ให้ “หมอบ” “ป้อง” “เกาะ”จนกว่าจะมีผู้เข้าไปช่วยเหลือ

๕) ถ้าอยู่ใกล้ทางออกให้ออกจากอาคารโดยเร็ว อย่าแย่งกันจนเกิดชุลมุน

๖) ห้ามใช้ลิฟท์โดยเด็ดขาด

กรณีอยู่ภายนอกอาคาร

๑) ให้อยู่ห่างจากอาคาร/เสาไฟฟ้า/สิ่งห้อยแขวน/ป้ายโฆษณาโดยให้อยู่ในที่โล่งจนกว่าการสั่นไหวจะหยุด

๒) หลีกเลี่ยงสิ่งของที่อาจโค่นล้มลงมาทาอันตราย เช่น ตู้ เสาไฟฟ้า ป้ายโฆษณาต้นไม้ใหญ่

๓) หลีกเลี่ยงอาคารสูง กาแพง ระวังเศษอิฐ กระจก ชิ้นส่วนของอาคารที่อาจหล่นลงมา

๔) วิ่งไปสู่ที่โล่ง

๕) รีบออกจากอาคารที่ชารุดเสียหายโดยเร็วที่สุด

กรณีอยู่ใกล้ชายฝั่ง

หากได้รับการแจ้งเตือน หรือรู้สึกได้ถึงแรงสั่นสะเทือน ให้รีบอพยพจากบริเวณชายฝั่งและริมแม่น้าลาคลองที่เชื่อมต่อกับทะเลโดยด่วน เพราะอาจเกิดคลื่นสึนามิได้

เมื่อแผ่นดินไหวสงบลง

๑) ตรวจดูอาการบาดเจ็บของตัวเองและคนใกล้เคียงหากได้รับบาดเจ็บให้ทาการปฐมพยาบาลเบื้องต้นและนาส่งโรงพยาบาล

๒) รีบออกจากอาคารที่เสียหาย เพราะอาจเกิดการถล่มซ้ำ

๓) ตรวจสอบโครงสร้างอาคาร ท่อน้า ก๊าซ กระแสไฟฟ้าและหากพบความเสียหายให้ปิดระบบการทำงานทั้งหมดทันที

๔) หากพบก๊าซรั่ว ให้เปิดหน้าต่างและประตูทุกบานโดยรีบออกจากอาคารแล้วแจ้งเจ้าหน้าที่ทันที

ข้อปฏิบัติหากติดอยู่ภายใต้ซากปรักหักพัง

๑) อยู่กับที่ ป้องกันศีรษะและหน้า จากกระจกที่แตกหรือวัสดุที่หล่นโดยใช้เสื้อ ผ้าห่ม หนังสือพิมพ์ กล่องกระดาษ ฯลฯ คลุมศีรษะ

๒) พิงตัวเองกับผนังห้องที่ไม่มีหน้าต่างกระจก/ชั้นวางของ หรือคลานไปหลบใต้โต๊ะเพื่อป้องกันวัสดุหล่นใส่

๓) หากติดอยู่ในที่ปลอดภัย ให้อยู่กับที่ อย่าเคลื่อนย้ายเพราะอาจได้รับอันตรายจากสิ่งของแตกหักพังทลาย

๔) ห้ามก่อให้เกิดเปลวไฟใดๆ ทั้งสิ้น

การปฏิบัติตนในการอพยพหนีภัยจากแผ่นดินไหว

๑) ระงับสติอารมณ์ ปฏิบัติตามแผนอพยพ

๒) เชื่อฟังคาแนะนาของผู้ที่เกี่ยวข้อง ผู้บังคับบัญชา พนักงานดับเพลิง อาสาสมัคร รปภ.

๓) เก็บทรัพย์สิน/เอกสารสำคัญ ไว้ในลิ้นชักโต๊ะและล๊อคกุญแจ

๔) เมื่อออกมาภายนอกแล้ว ห้ามกลับเข้าไปอีกเด็ดขาด

๕) ห้ามขนสัมภาระใดๆ ติดตัวขณะอพยพ

๖) ใช้วิธีเดินเร็ว ห้ามวิ่งหรือเดินช้า

๗) ใช้ช่องทางหนีไฟ เรียงแถว ขั้นบันไดละ ๒ คน

๘) ห้ามพูดคุย สายตามองขั้นบันได มือจับราวบันได ห้ามส่งเสียงเอะอะ หรือเร่งผู้อื่น ห้ามดันหรือแซง

๙) ห้ามใช้ลิฟต์ โดยเด็ดขาด

๑๐) เมื่ออพยพถึงชั้นล่างสุดให้ออกจากอาคารทันที

๑๑) ไปรวมพล ณ จุดนัดพบที่กำหนดไว้

๑๒) ตรวจสอบจานวนผู้อพยพ

เจ้าหน้าที่รับผิดชอบดำเนินการตรวจสอบผู้ประสบภัย อาคารที่เสียหาย แจ้งความเสียหายแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ เพื่อทราบและสั่งการต่อไป

ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทำรายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

กรณีเกิดการชุมนุมประท้วงและก่อจลาจล

๑. ผู้ที่อยู่เวรรักษาการณ์เมื่อได้รับสิ่งแจ้งเหตุ ให้แจ้งเจ้าหน้าที่รับผิดชอบ หรือแจ้งผู้บังคับบัญชาตามลำดับชั้นทีมอาคารสถานที่ ผู้รับผิดชอบ ได้แก่

นางสาวกนกอร ไชยเทพ เบอร์โทรศัพท์ติดต่อ ๐๘๗-๒๙๐๒๓๗๑ หรือ สายด่วน ๑๘๘๐

เจ้าหน้าที่รับผิดชอบแจ้งเหตุต่อผู้บังคับบัญชา เพื่อผู้บังคับบัญชาดำเนินการประกาศแนะนำ แจ้งเตือน เจ้าหน้าที่ในองค์กร และเตรียมการป้องกันเพื่อลดอันตรายและความเสียหายผู้บังคับบัญชาได้แก่

- ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐
- หัวหน้าส่วนกลุ่มงานอำนวยการและปฏิบัติการ Call Center ๑๘๘๐ เบอร์โทรศัพท์ติดต่อ ๐๘๐-๗๑๔๒๙๗๖ หรือ สายด่วน ๑๘๘๐

๒. หากจำเป็นและเห็นสมควร ผู้บังคับบัญชาสั่งการให้ดาเนินการป้องกันภัยตามแผนที่เตรียมไว้ล่วงหน้าตามควรแก่กรณีดังนี้

ขั้นตอนการปฏิบัติเมื่อเกิดการชุมนุมประท้วงและก่อจลาจล

๑) แต่งตั้งเจ้าหน้าที่เฝ้าสังเกตการณ์ดูแลความเรียบร้อยและความปลอดภัยต่อชีวิตและทรัพย์สินของผู้ปฏิบัติงานและของศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

๒) เพิ่มจำนวนยามรักษาความปลอดภัยเป็นสองเท่า

๓) ปิดประตูทั้ง ๒ ด้าน ควบคุมพื้นที่มิให้บุคคลภายนอกเข้ามาใน ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้

๔) กรณีเกิดเหตุความไม่ปลอดภัยจนเจ้าหน้าที่ไม่สามารถควบคุมได้ หรือมีการทำลายทรัพย์สินของ ศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้ ให้แจ้งไปยังสถานีตำรวจ หรือหน่วยงานรับแจ้งเหตุฉุกเฉินต่าง ๆ และรายงานให้ผู้อานวยการสำนักบริหารกลาง เพื่อทราบ

ขั้นตอนการปฏิบัติกรณีพบวัตถุต้องสงสัยภายในตึกหรือรอบบริเวณตึก

๑) เมื่อพบวัตถุต้องสงสัย ให้แจ้ง รปภ. หรือเจ้าหน้าที่รับผิดชอบทราบทันที

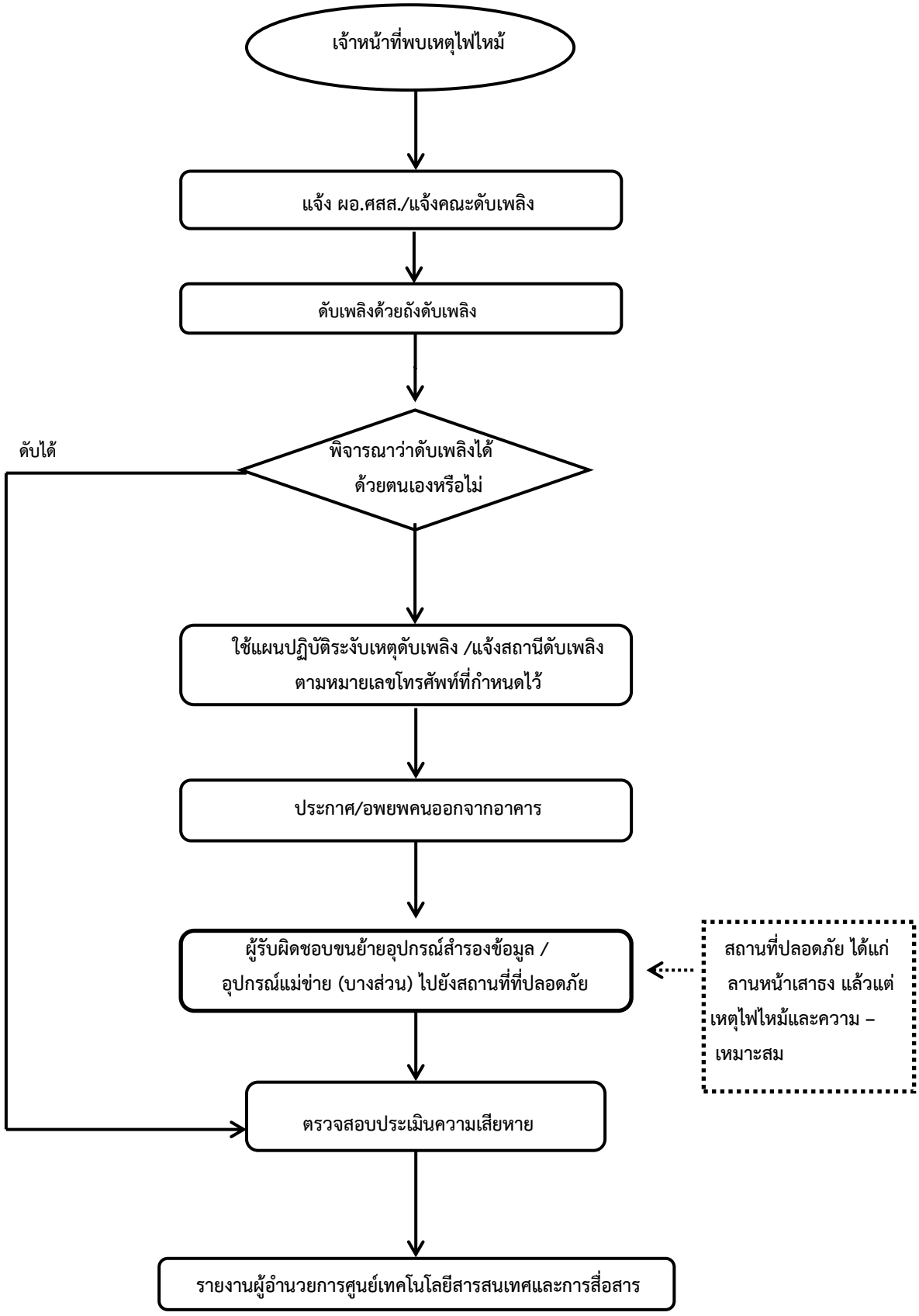
๒) รปภ. หรือเจ้าหน้าที่รับผิดชอบรายงานผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร พร้อมทั้งติดต่อเจ้าหน้าที่ตำรวจในพื้นที่มาตรวจสอบวัตถุต้องสงสัย

๓) ในกรณีตรวจสอบเป็นวัตถุระเบิดให้ดำเนินการกั้นพื้นที่อันตรายที่พบวัตถุระเบิดกัน - บุคคลที่ไม่เกี่ยวข้องออกจากบริเวณที่พบวัตถุระเบิด และแจ้งอพยพผู้ปฏิบัติงานออกจากบริเวณหรือรัศมีของวัตถุระเบิด

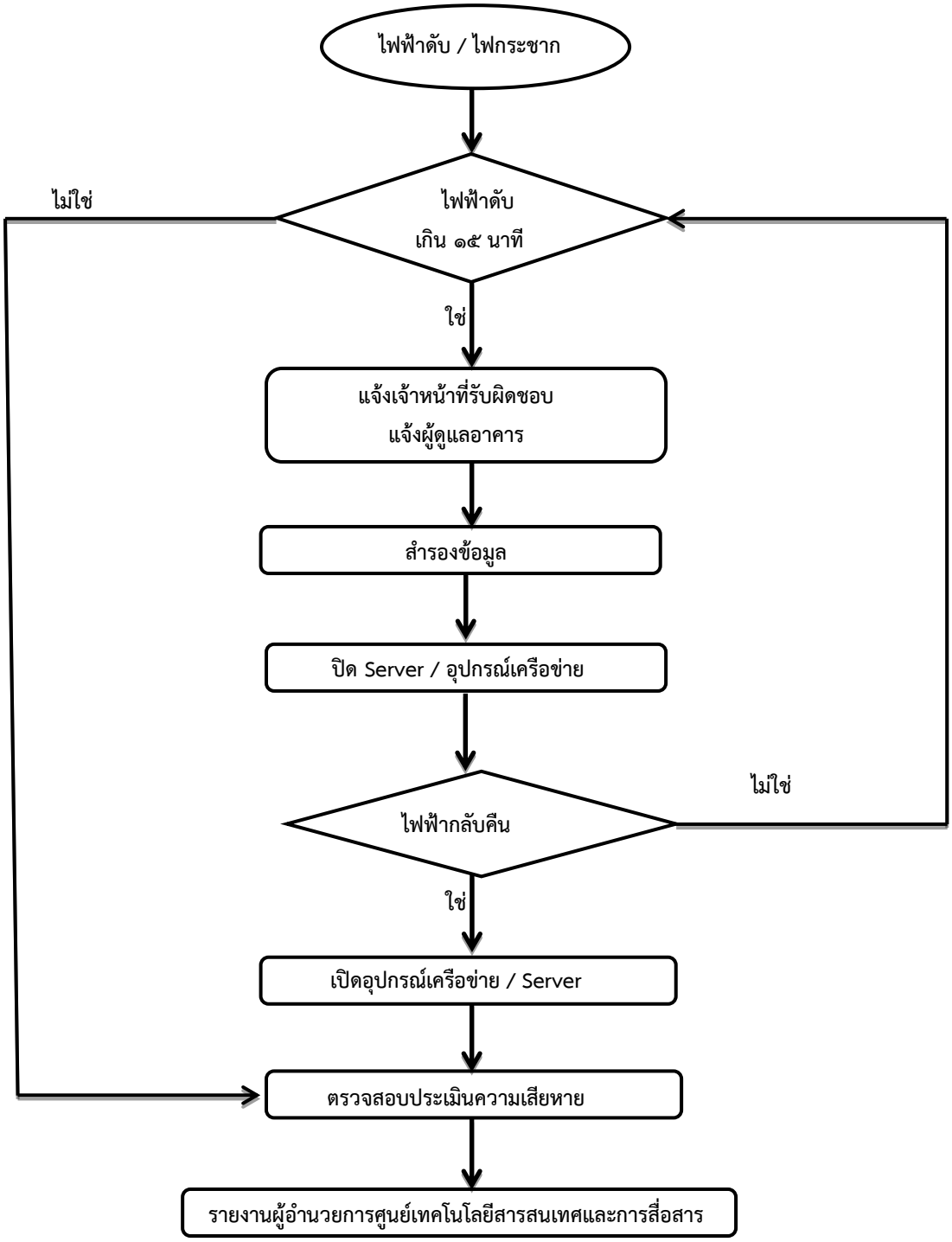
๔) เมื่อการชุมนุมประท้วงและก่อจลาจลสิ้นสุดลง เจ้าหน้าที่รับผิดชอบดำเนินการสำรวจความเสียหายทุกด้านอย่างละเอียด แล้วรายงานแก่ผู้ควบคุม และผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ผ่านทางโทรศัพท์ ๐๘๐-๗๐๖๑๕๕๑ หรือ สายด่วน ๑๘๘๐ เพื่อทราบและสั่งการต่อไป

๕) ผู้ควบคุมและทีมประเมินความเสียหาย ดำเนินการเข้าตรวจสอบระบบเครือข่ายและระบบเทคโนโลยีสารสนเทศ ประเมินความเสียหายพร้อมทั้งจัดทารายงานความเสียหาย เพื่อแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร ทราบ

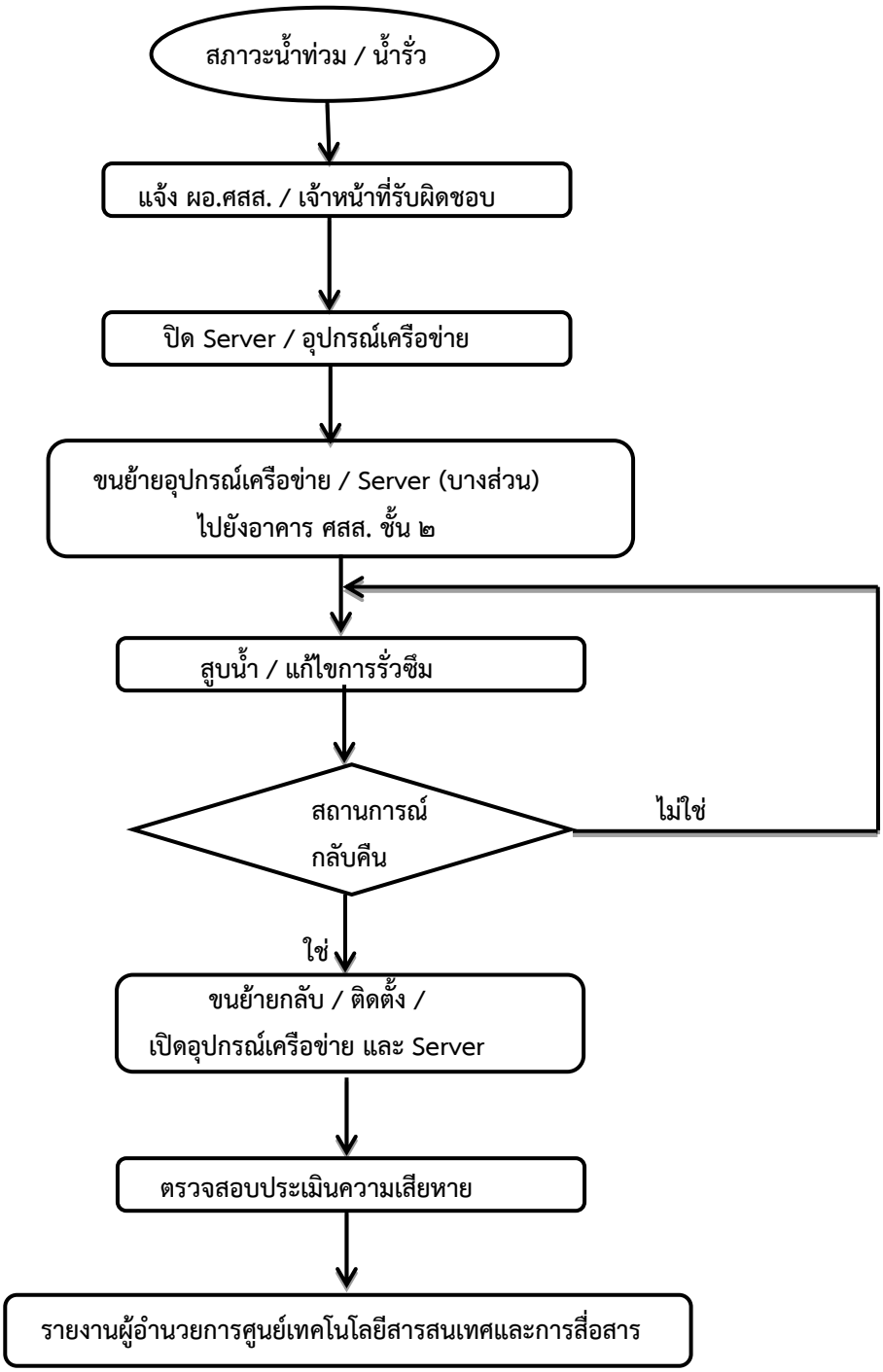
Flowchart กรณีไฟไหม้



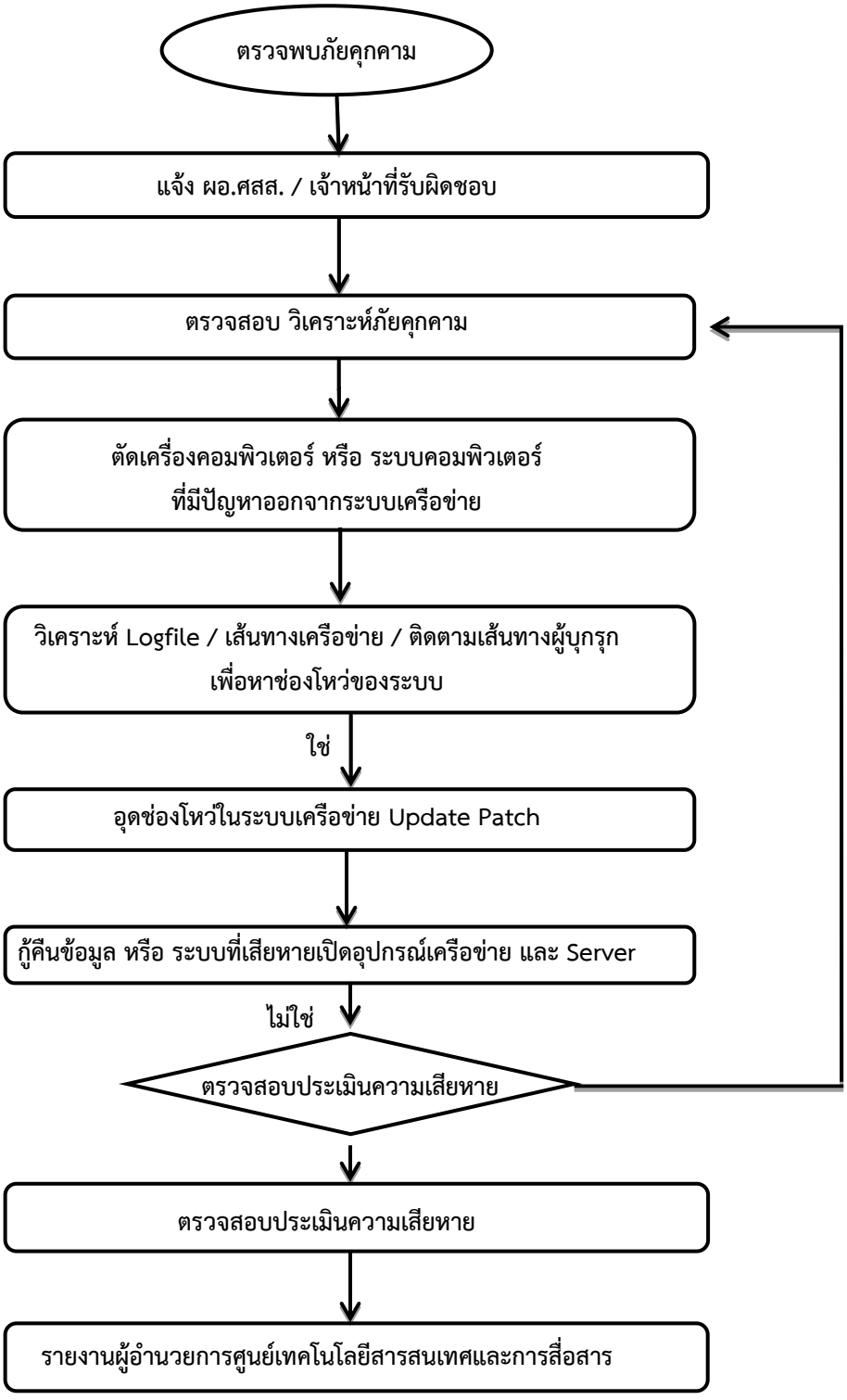
Flowchart กรณีไฟฟ้าดับ / ไฟฟ้ากระชาก / หม้อแปลงไฟฟ้าระเบิด



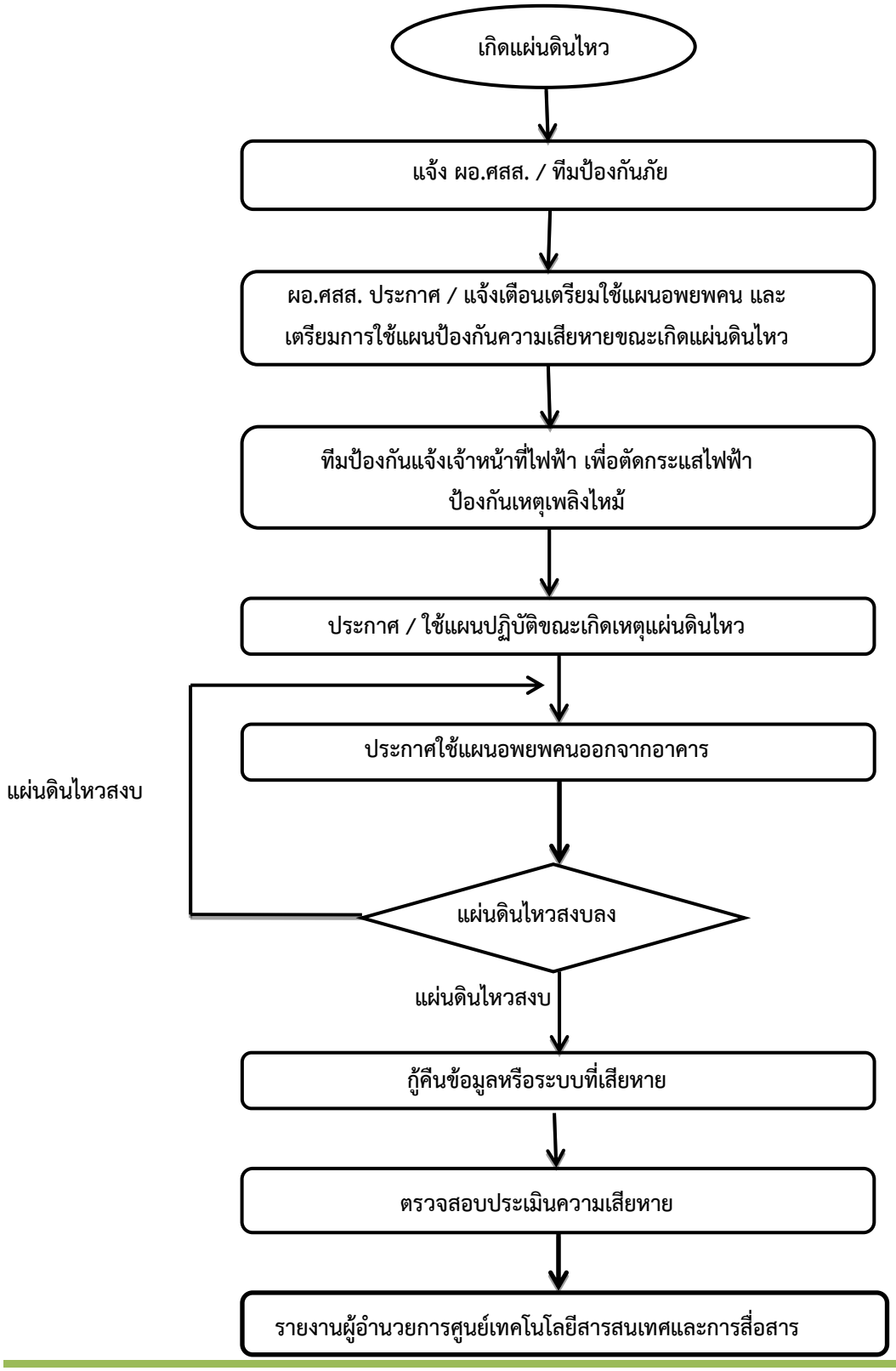
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีน้ำท่วม



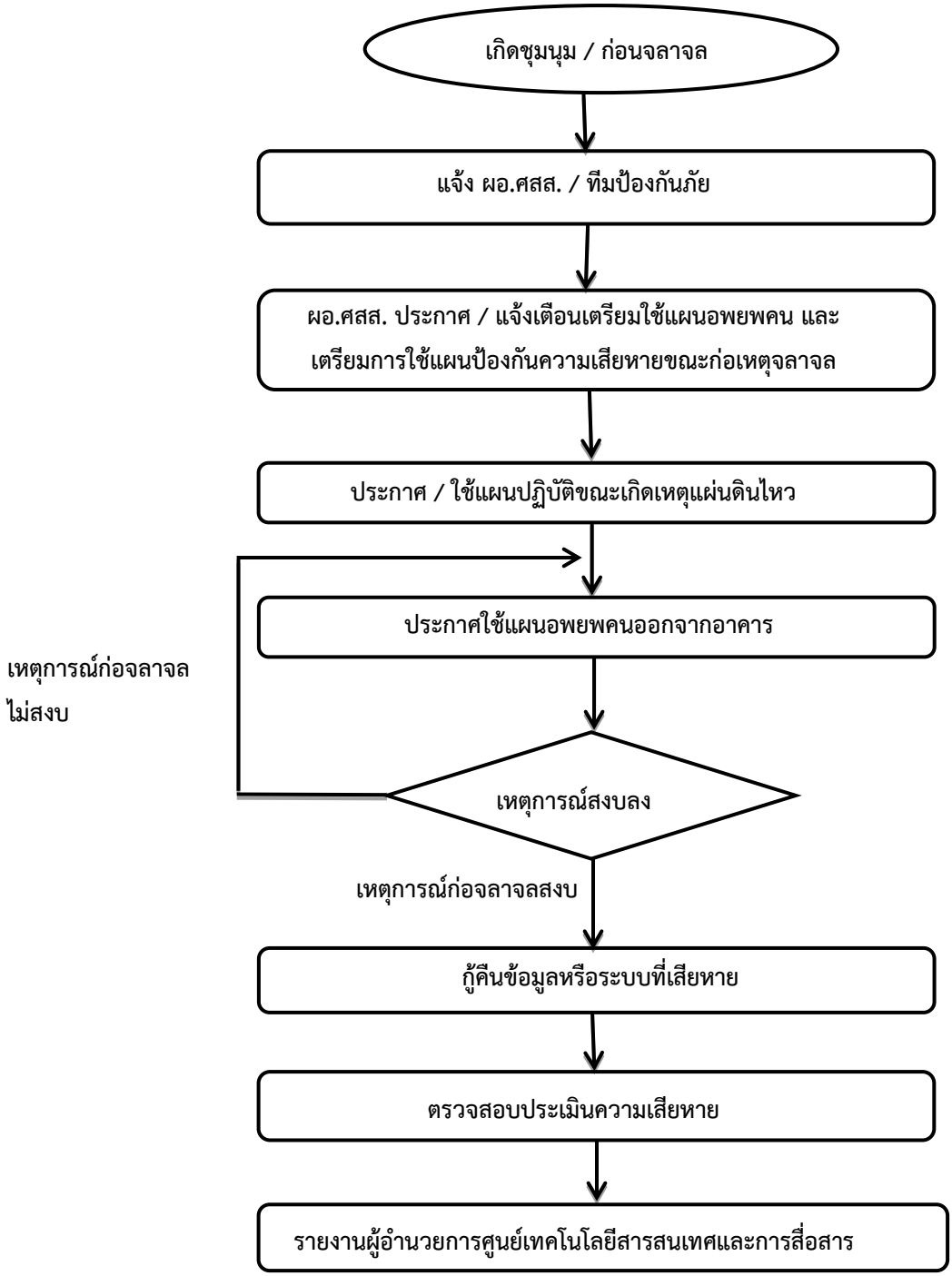
Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีโดนเจาะระบบ หรือ ตรวจพบภัยคุกคาม



Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีแผ่นดินไหว



Flowchart แสดงขั้นตอนการปฏิบัติงาน กรณีเกิดการชุมนุมประท้วงและก่อจลาจล



บทสรุปผู้บริหาร

ความสำคัญของแผนป้องกันภัยพิบัติ

จากแผนป้องกันภัยพิบัติที่ศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร (ศสส.) ได้จัดทำขึ้น เพื่อป้องกันผลกระทบที่อาจเกิดขึ้นจากปัจจัยภายในและภายนอก ซึ่งเป็นนโยบายและแนวทางเพื่อป้องกันและบริหารความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศและการสื่อสารให้มีการทำงานได้โดยไม่หยุดชะงัก

คู่มือฉบับนี้ เป็นแนวทางการดำเนินงานของแผนป้องกันภัยพิบัติระบบเทคโนโลยีสารสนเทศและการสื่อสารที่มีความสำคัญ ตั้งแต่การวิเคราะห์ การเกิดเหตุ การป้องกัน การดำเนินงาน รวมถึงการแก้ปัญหาที่ถูกจุด จึงเน้นย้ำให้มีการจัดเตรียม วางแผนปฏิบัติตามแนวทางโดยเคร่งครัด

ลงชื่อ.....

(ผศ. ปิยะ กิจถาวร)

ตำแหน่ง ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

ลงชื่อ.....

(นายภาณุ อุทัยรัตน์)

เลขาธิการศูนย์อำนวยการบริหารจังหวัดชายแดนภาคใต้