กรมการขนส่งทางราง
Department Of Rail Transport

แผนบริหารความต่อเนื่อง ทางด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) ประจำปี ๒๕๖๗

www.drt.go.th

DRT.OfficialFanpage

สารบัญ

หน้า

แผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
กรมการขนส่งทางราง

๑. หลักการและเหตุผล

ระบบข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการทำงานได้อย่างมีประสิทธิภาพ กรมการขนส่งทางราง (ขร.) ได้ตระหนักถึงความสำคัญต่อระบบฐานข้อมูลและสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลและสารสนเทศรวมทั้งระบบอุปกรณ์เสียหายได้

ดังนั้น ขร. จึงได้จัดทำแผนบริหารความต่อเนื่องทางด้านเทคโนโลยีสารสนเทศ อันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดำเนินการตามแผน ซึ่งจะช่วยให้ ขร. สามารถจัดการกับสถานการณ์ฉุกเฉินได้อย่างมีประสิทธิภาพลดผลกระทบที่อาจเกิดขึ้น และรักษาความเชื่อมั่นของบุคลากรใน ขร. และผู้มีส่วนได้ส่วนเสียในระยะยาว

๒. วัตถุประสงค์

๒.๑ เพื่อกำหนดกระบวนการขั้นตอนในการปฏิบัติเพื่อแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๒ เพื่อลดความเสียหายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒.๓ เพื่อให้การปฏิบัติงาน ดำเนินไปได้อย่างมีเสถียรภาพ และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ และสามารถรองรับการเกิดโรคระบาดต่อเนื่อง

๓. เป้าหมาย

๓.๑ ระบบเทคโนโลยีสารสนเทศและโปรแกรมปฏิบัติการที่ให้บริการประชาชน ได้แก่ เว็บไซต์กรมการขนส่งทางราง ฐานข้อมูลจุดตัดทางรถไฟและระบบแผนที่สารสนเทศออนไลน์ของจุดตัดทางรถไฟทั่วประเทศ ฐานข้อมูลรถขนส่งทางรางในประเทศไทย ระบบภาพรวมสถิติการขนส่งทางรางในประเทศไทย ระบบฐานข้อมูลผู้ประกอบการและการออกใบอนุญาตด้านการขนส่งทางรางผ่านระบบดิจิทัล e-License R

๓.๒ ระบบสารสนเทศภายใน (Back Office) ได้แก่ ระบบสำนักงานอัตโนมัติ (e-office) ระบบสำนักงานอัตโนมัติ (e-office) ระยะที่ ๒ ระบบ DPIS ของสำนักงาน ก.พ. เป็นต้น

๔. คำนิยาม

๑) หน่วยงาน หรือ องค์กร หมายถึง กรมการขนส่งทางราง หรือ ขร.

๒) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของกรมการขนส่งทางราง (ขร.)

๓) ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานบริหารหรือดูแลรักษา ระบบเทคโนโลยีสารสนเทศของกรมการขนส่งทางราง (ขร.) โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาทข้าราชการ พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างตามสัญญาจ้างในหน่วยงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของ ขร.

๔) บุคคลภายนอก หมายถึง บุคคลจากหน่วยภายนอกที่เข้ามาประชุมหรือปฏิบัติงานร่วมกับ ขร.

๕) หน่วยงานภายนอก หมายถึง หน่วยงานภายนอกที่ ขร. อนุญาต ให้มีสิทธิในการเข้าถึงและใช้งานข้อมูล หรือทรัพย์สินต่าง ๆ ของสำนักงาน โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๖) สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๗) ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบงาน

๘) สินทรัพย์ หมายถึง ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน อันมีมูลค่าคุณค่าสำหรับหน่วยงาน

๙) การเข้าถึงหรือควบคุม หมายถึง การขออนุญาต การกำหนดสิทธิ หรือการใช้งานสารสนเทศมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๑๐) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๑๑) รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๒) ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๓) ระบบเครือข่าย (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของ ขร. ได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเตอร์เน็ต (Internet)

ระบบแลน (LAN) และระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อ ระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเตอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

๑๔) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผนบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูล และสารสนเทศ เป็นต้น

๕. แนวทางปฏิบัติเพื่อป้องกันและการรักษาความปลอดภัยด้านกายภาพ สถานที่ และสภาพแวดล้อมด้านระบบเทคโนโลยีสารสนเทศ

๕.๑ อาคาร สถานที่

อาคาร สถานที่ และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่น ๆ พื้นที่เตรียมข้อมูล จัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์ รวมทั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๕.๒ ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ต้องมีลักษณะดังนี้

๑. กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

๒. ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า-ออก ของบุคคลเป็นจำนวนมาก

๓. จะต้องไม่มีป้ายหรือสัญลักษณ์แสดงถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

๔. จะต้องปิดล็อก หรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

๕. หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

๖. ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

๗. จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศ จัดตั้งไว้เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๕.๓ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๑. มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

๒. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๕.๔ การควบคุมการเข้าออก อาคารสถานที่

๑. กำหนดสิทธิผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๒. การเข้าถึงอาคารของหน่วยงาน ของบุคคลภายนอก หรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๓. ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitor)

๔. ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในหน่วยงาน

๕. บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

๖. จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น Data Center เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๗. ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

๘. มีการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

๙. สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๐. มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๑. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญเว้นแต่ได้รับการอนุญาต

๑๒. มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

๑๓. จัดให้มีการดูแลเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๔. จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

๕.๕ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๑. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

๒. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีหรือภายใน ๑-๒ วันทำการ เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๓. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๔. ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับเทคโนโลยีสารสนเทศ

๕. ผู้ดูแลระบบต้องมอบหมายสิทธิที่มีความสอดคล้องกับนโยบายควบคุมการเข้าถึง

๖. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๗. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๘. ผู้ดูแลระบบดำเนินการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้งและทบทวนสำหรับผู้ที่มีสิทธิในระดับสูงด้วยความถี่มากกว่าผู้ใช้งาน

๙. ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน

๕.๖ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

การใช้รหัสผ่าน (Password Use)

๑. ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น

๒. ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

๓. ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๔. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๕. ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๖. ผู้ใช้งานควรเปลี่ยนรหัสผ่านไม่เกิน ๙๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่านหรือตามรอบระยะเวลาที่กำหนด

๗. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๘. ผู้ใช้งานควรตั้งรหัสที่มีความซับซ้อนไม่น้อยกว่า ๘ ตัวอักษร ประกอบด้วย ตัวอักษรเล็ก ตัวอักษรใหญ่ ตัวเลข และอักขระพิเศษ (! @ $ #)

๙. ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

๑๐. ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อคอินในภายหลัง

๑๑. ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๑๒. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

๕.๗ ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

๑. มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังต่อไปนี้

- ระบบสำรองกระแสไฟฟ้า (UPS)
- ระบบปรับอากาศ และควบคุมความชื้น
- ระบบตรวจจับควันไฟ
- ระบบตรวจจับน้ำรั่วซึม
- ระบบดับเพลิงชนิดก๊าซอัตโนมัติ

๒. ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๕.๘ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

๑. หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

๒. ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

๓. ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

๔. ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

๕. จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๖. ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๗. พิจารณาใช้งานไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม

๘. ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๕.๙ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑. ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาตามคำแนะนำของผู้ผลิต

๒. ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามคำแนะนำของผู้ผลิต

๓. จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

๔. จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์

๕. ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

๖. จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕.๑๐ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๑. มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๒. กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๓. กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๔. เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์

๕. บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๕.๑๑ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

๑. กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

๒. ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓. เจ้าหน้าที่ที่รับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของหน่วยงานให้เสมือนเป็นทรัพย์สินของตนเอง

๕.๑๒ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-Use of Equipment)

๑. ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

๒. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูล ก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๕.๑๓ การสำรองข้อมูล (Back up)

๑.พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยเรียงลำดับความจำเป็นจากมากไปน้อย

๑.๑ การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะทำการสำรองข้อมูลไว้ในฮาร์ดดิสก์ ๑ ชุดในเวลาเที่ยงคืนของทุกวัน

๑.๒. การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่ทำการสำรองข้อมูล (Back up) ตามระยะเวลาที่กำหนด รวมทั้งจัดให้มีระบบการบำรุงรักษา (Restructure/Reformat) ระบบฐานข้อมูลประกอบด้วย

๑.๒.๑ การสำรองข้อมูลประจำวัน จะทำการสำรองข้อมูลและโครงสร้างข้อมูล

๑.๒.๒ การสำรองข้อมูลประจำสัปดาห์ จะทำการสำรองข้อมูล โครงการข้อมูล และ Source Code โดยบันทึกข้อมูลลงใน External Hard disk

๑.๒.๓ การสำรองข้อมูล Source Code โปรแกรมประจำเครื่อง

๑.๒.๔ การสำรองข้อมูลประจำปี

๒.กำหนดให้มีการสำรวจข้อมูลของสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล

๕.๑๔ การกู้ข้อมูล (Recovery)

๑. ทำการทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูลที่ได้ทำการสำรองไว้ใน External Hard disk ทุกวันศุกร์ของสัปดาห์

๒. ทำการทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้ทำการสำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

๓. ข้อมูลที่ต้องทำการ Recovery ทันที เช่น ระบบสำนักงานอัตโนมัติ (E-office) ระบบสำนักงานอัตโนมัติ (E-office) ระยะที่ ๒ ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น

๔. ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนของข้อมูลอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้งหรือตามความเหมาะสมโดยคำนึงถึงความเสี่ยงต่าง ๆ ที่จะเกิดขึ้น

๕.๑๕ การป้องกันไวรัส

๑. ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดตข้อมูลไวรัสอยู่เสมอ

๒. มีการตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูล นอกจากนี้ควรมีการตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๓. ใช้ความระมัดระวังในการเปิด e-mail ที่ไม่ทราบแหล่งที่มา เช่น spam mail

๔. ระมัดระวังในการดาวน์โหลดไฟล์ต่าง ๆ จากอินเตอร์เน็ต เช่น เว็บไซต์ดาวน์โหลดหนังต่าง ๆ

๕.๑๖ การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์

เพื่อเป็นการสร้างความปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ มีแนวทางการควบคุมดังนี้

๑. มาตรการควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้องเข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของกลุ่มเทคโนโลยีและสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไปที่ประตูเข้าออก มีการติดตั้งรหัส/Keycard ในการเข้าออก

๒. มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครื่อข่ายคอมพิวเตอร์ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

๓. มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตของ ขร. เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบเทคโนโลยีสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๔. มีการติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเตอร์เน็ตของ ขร. และกลั่นกรองข้อมูลที่มาทางเว็บไซต์ ซึ่งจะมีการกำหนดค่า Configuration ให้ปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

๕. มีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

๖. การดำเนินการตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ จะช่วยเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามทางคอมพิวเตอร์ได้เป็นอย่างดี

๗. กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก Log และตรวจสอบการตั้งค่า Firewall ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้และแจ้งให้ DCIO และผู้ช่วย DCIO ให้ทรบโดยด่วน

๘. กรณีการเชื่อมโยงเครือข่ายล้มเหลว ผู้ดูแลระบบต้องรีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

๕.๑๗ การจัดเตรียมอุปกรณ์ที่จำเป็น

การเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของ ขร .ซึ่งได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

๑. แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

๒. แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

๓. แผ่นโปรแกรม Antivirus/Antispyware

๔. แผ่น driver อุปกรณ์ต่าง ๆ

๕. ระบบสำรองไฟฉุกเฉิน

๖. อุปกรณ์สำรองต่าง ๆ ของเครื่องคอมพิวเตอร์

๗. เครื่องแม่ข่ายสำรอง

๕.๑๘ อุปกรณ์อื่น ๆ ที่เกี่ยวข้อง ได้แก่

๑. อุปกรณ์ควบคุมการเข้าสู่เครือข่ายที่เรียกว่า Firewall ติดตั้งอยู่ที่เครื่อง Server หลักที่ทำหน้าที่เป็น Web Server สำหรับป้องกันการบุกรุกจากบุคคลภายนอกที่ต้องการเจาะเข้าสู่ระบบประมวลผลของ ขร. คือ ระบบ Internet จำนวน ๒ เครื่อง

๒. อุปกรณ์ดับเพลิงอัตโนมัติด้วยสารเคมี สำหรับอุปกรณ์ IT ติดตั้งอยู่ที่ห้อง Data Center กองยุทธศาสตร์และแผนงาน สำหรับกรณีเกิดไฟไหม้ในห้อง Server

๓. จัดให้มีระบบทำความเย็นเปิดสลับภายในห้อง Data Center เพื่อรักษาสมรรถนะเครื่อง Server ให้สามารถทำงานได้ตลอด ๒๔ ชั่วโมง

๔. จัดให้มีโปรแกรมสำหรับตรวจสอบ และป้องกันการบุกรุกเข้าสู่ระบบประมวลผลฐานข้อมูลเครื่องแม่ข่ายหลัก จำนวน ๑ โปรแกรม

๕. จัดให้มีโปรแกรมสำหรับป้องกันการถูกโปรแกรมไวรัสเข้าทำลายโปรแกรมระบบปฏิบัติการและระบบฐานข้อมูล (Antivirus) โดยกำหนดให้ Server ตรวจสอบและ update โปรแกรมอัตโนมัติ

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑ กรณีเกิดเหตุไฟไหม้ (อัคคีภัย)

๖.๒ กรณีไฟฟ้าดับ

๖.๓ กรณีแผ่นดินไหว

๖.๔ กรณีโจรกรรม

๖.๕ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

๖.๖ กรณีสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

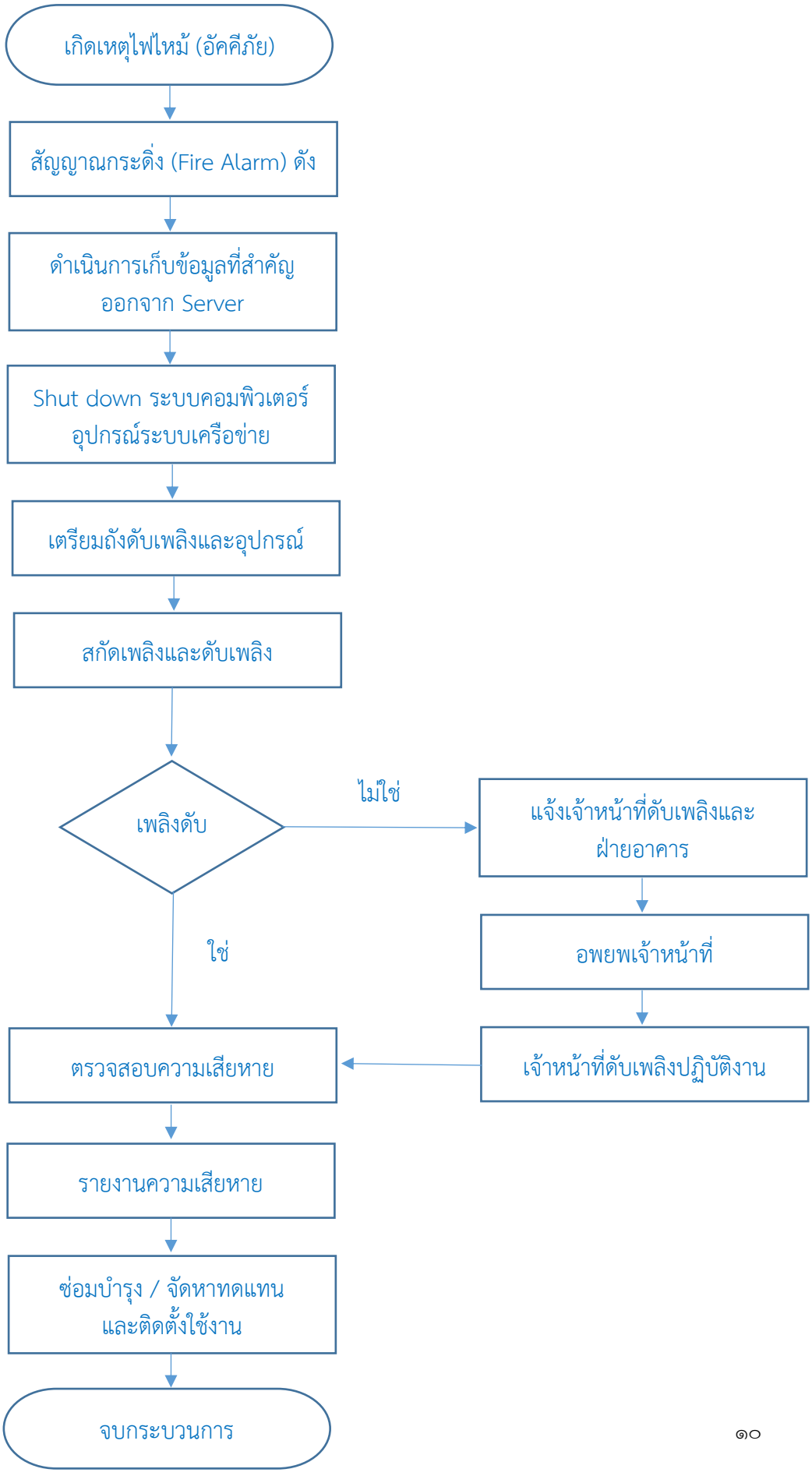
๖.๗ กรณีระบบเครือข่ายล้มเหลว

๖.๘ กรณีระบบป้องกันผู้บุกรุกล้มเหลว

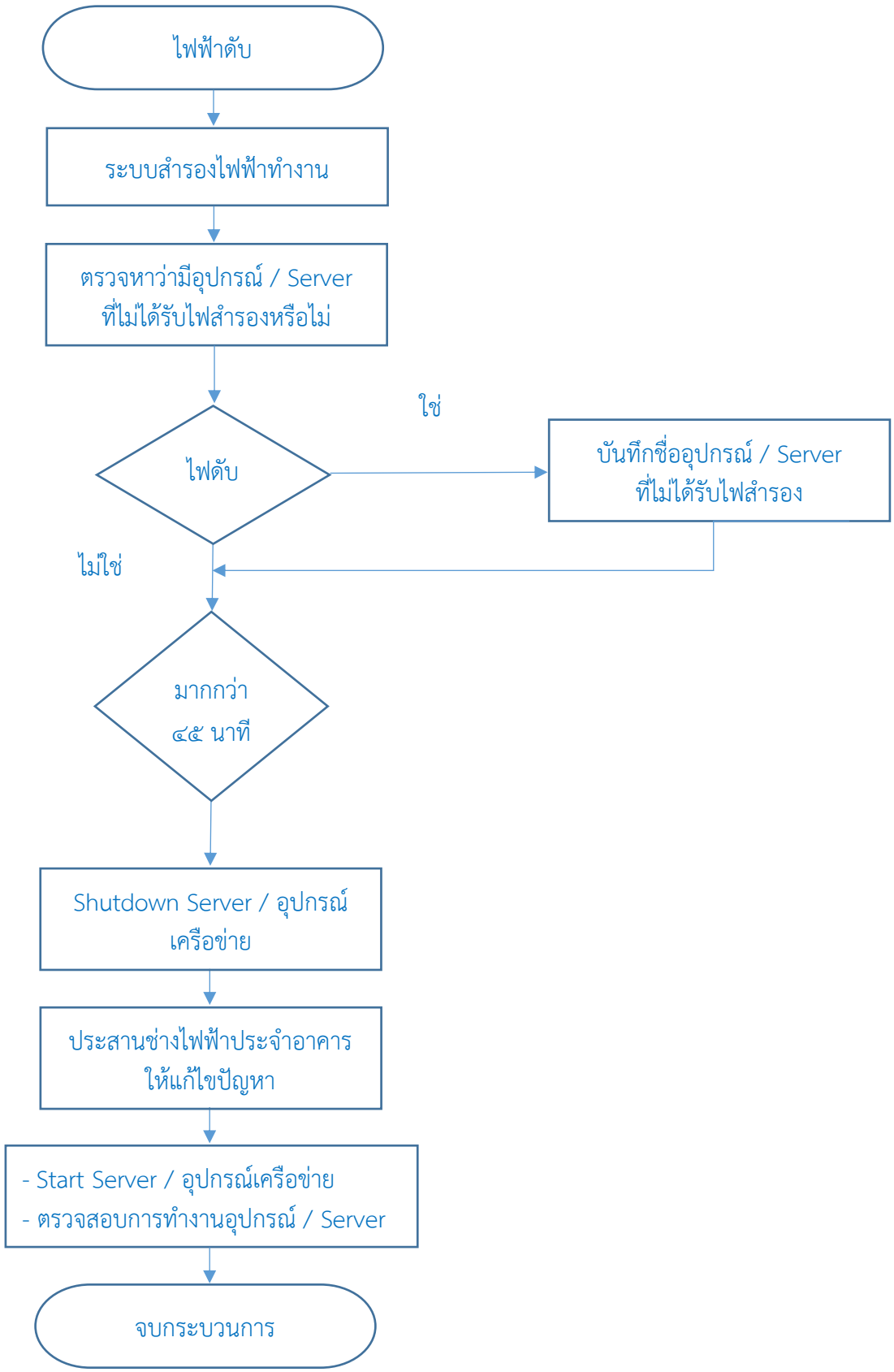
๖.๙ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากภัยพิบัติทางธรรมชาติ

๖.๑๐ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดโรคระบาด

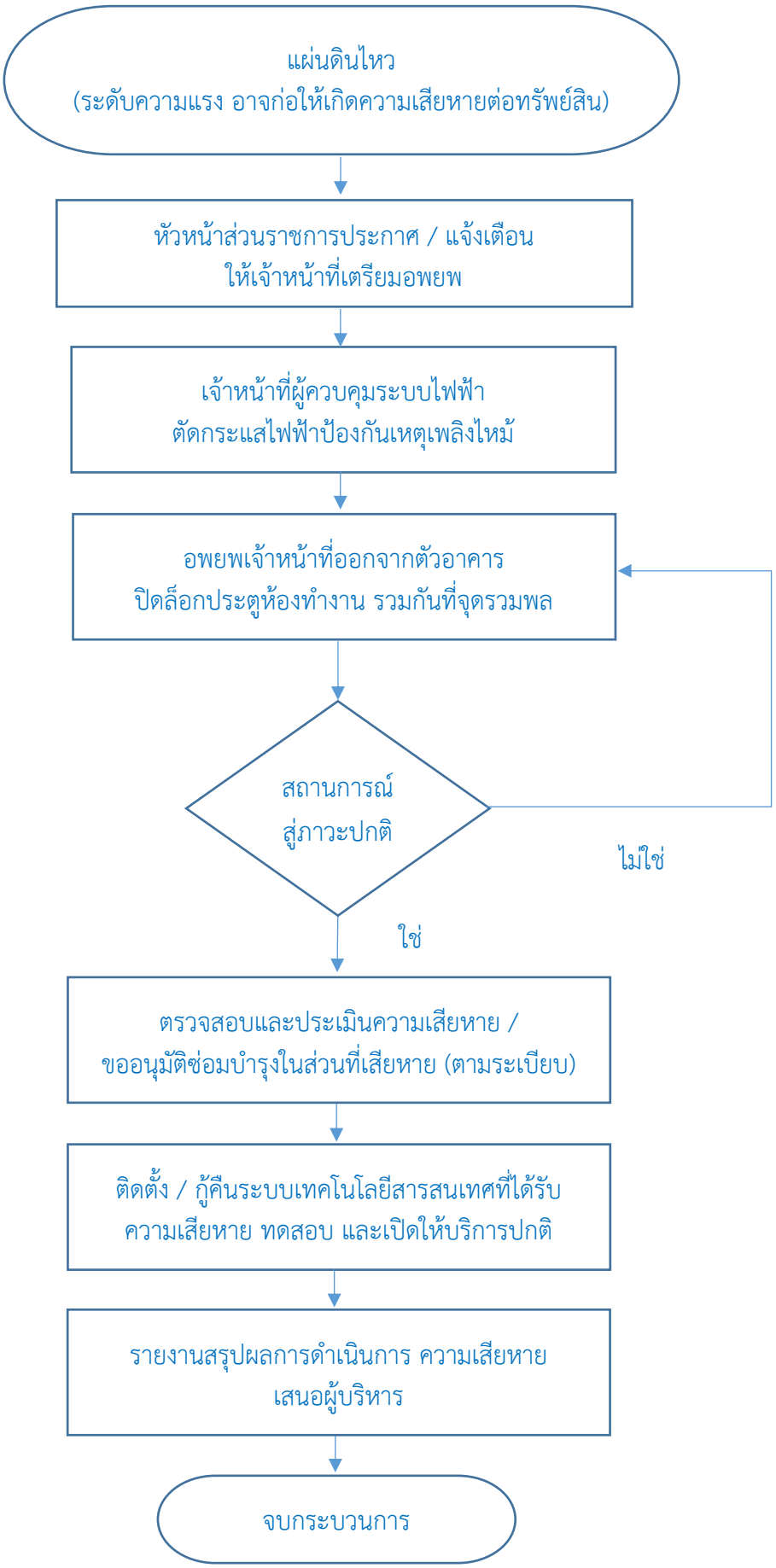
๖.๑ กรณีเกิดเหตุไฟไหม้ (อัคคีภัย) มีขั้นตอนการปฏิบัติดังนี้



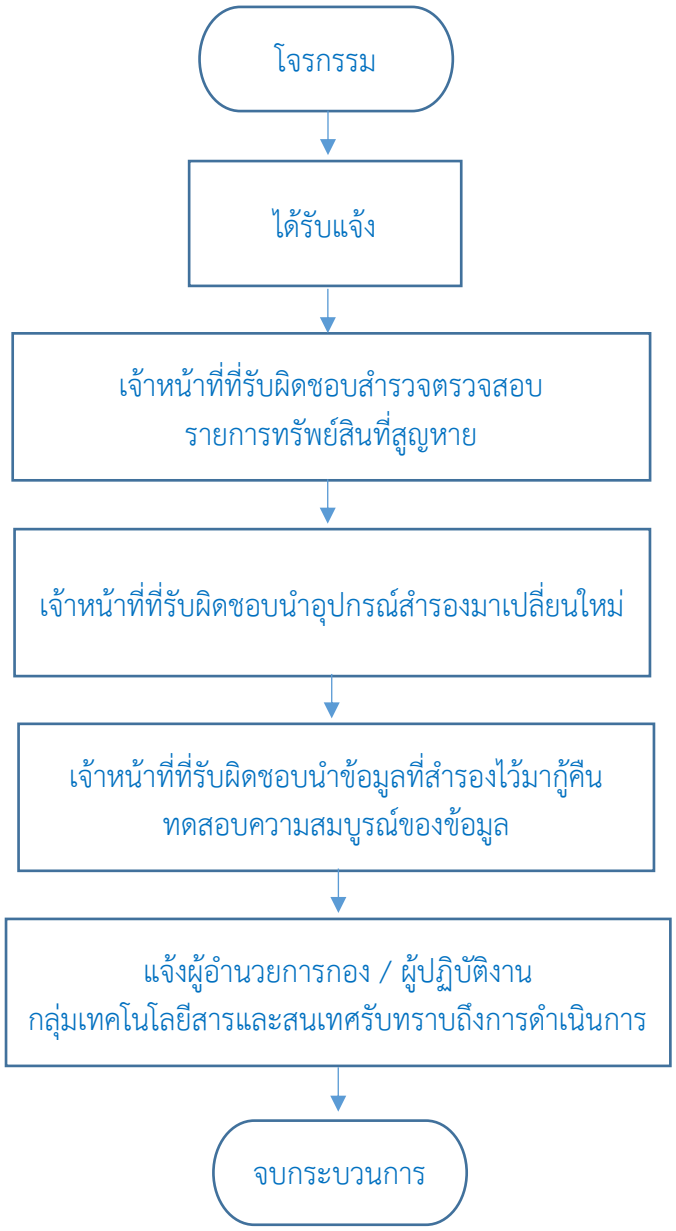
๖.๒ กรณีไฟฟ้าดับ มีขั้นตอนการปฏิบัติดังนี้



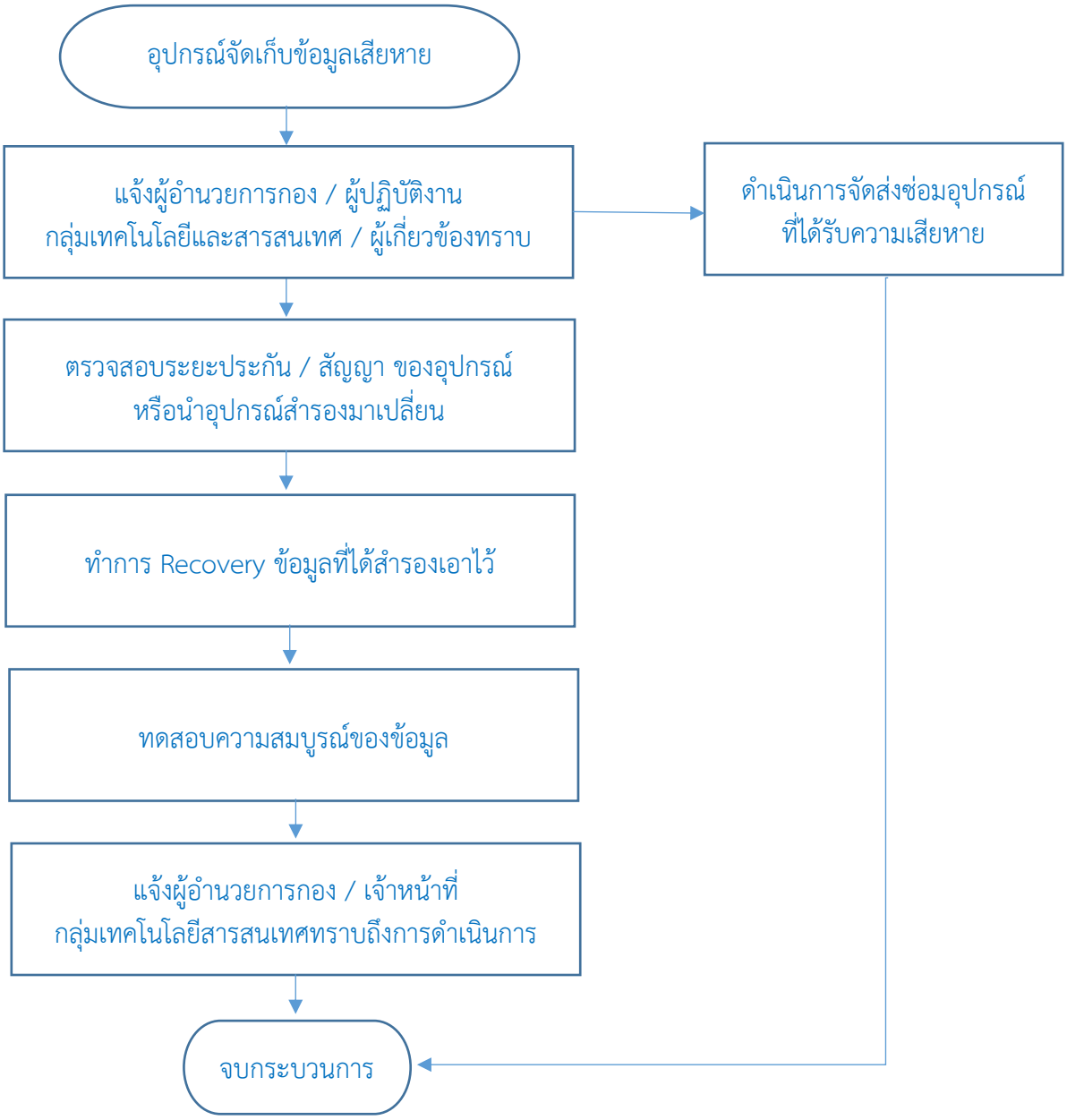
๖.๓ กรณีแผ่นดินไหว มีขั้นตอนการปฏิบัติดังนี้



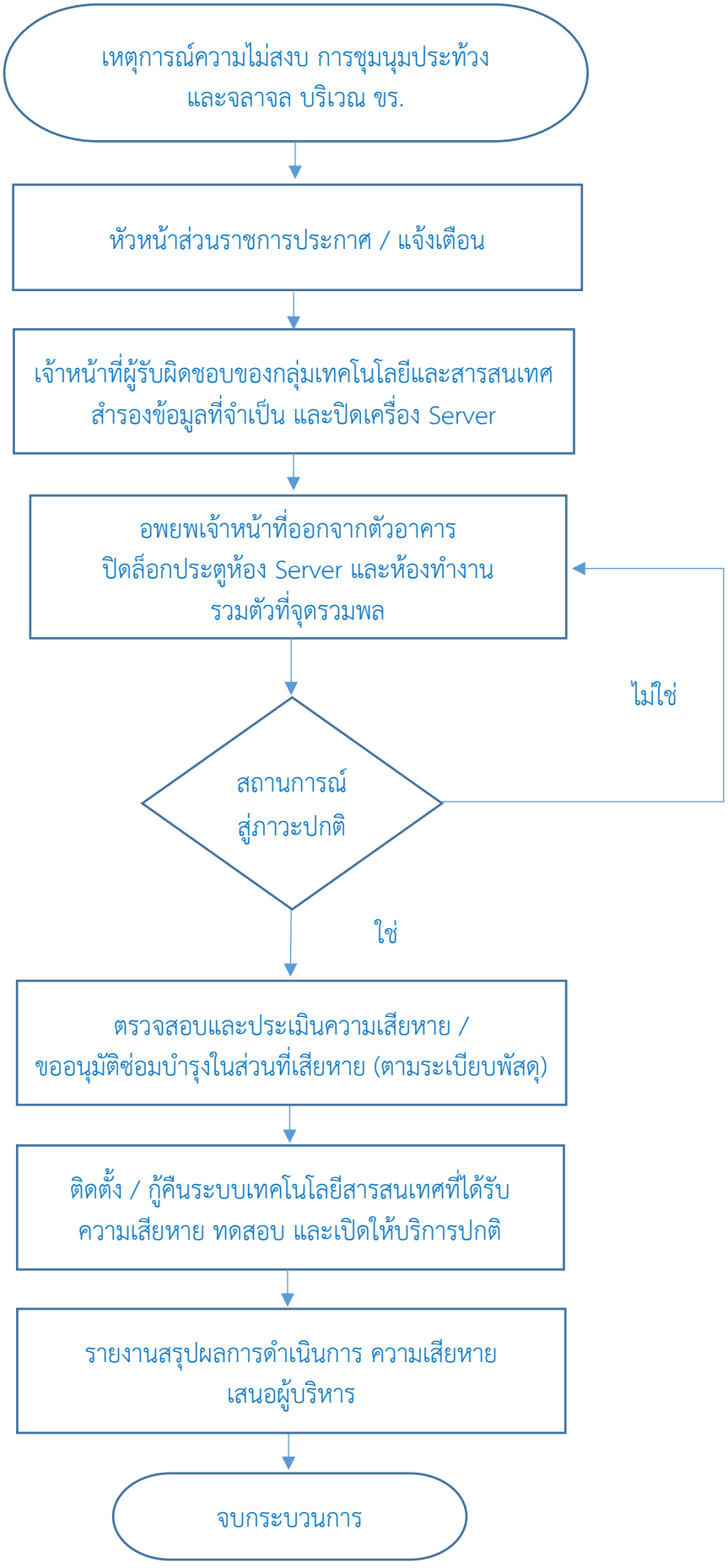
๖.๔ กรณีโจรกรรม มีขั้นตอนการปฏิบัติดังนี้



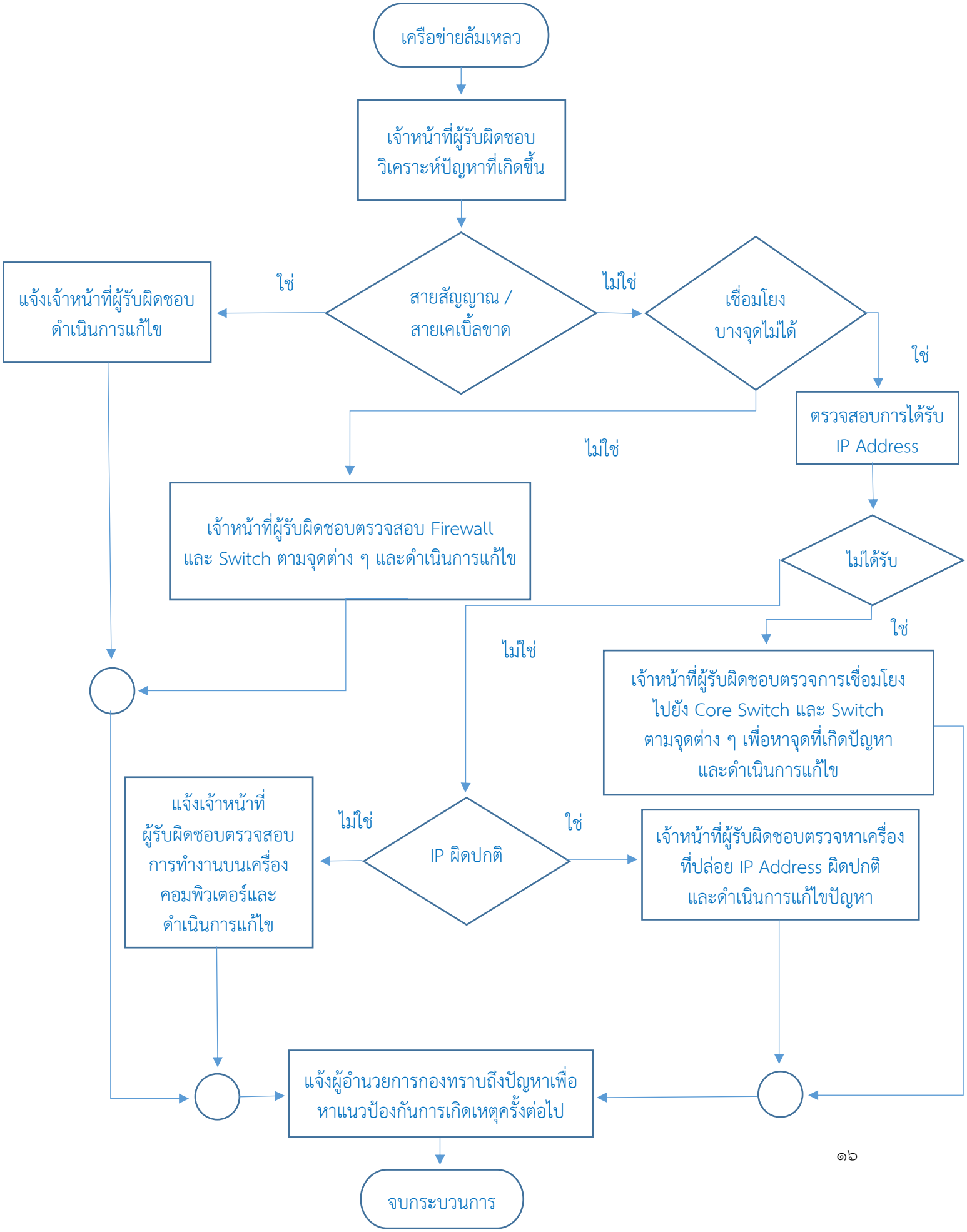
๖.๕ กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย มีขั้นตอนการปฏิบัติดังนี้



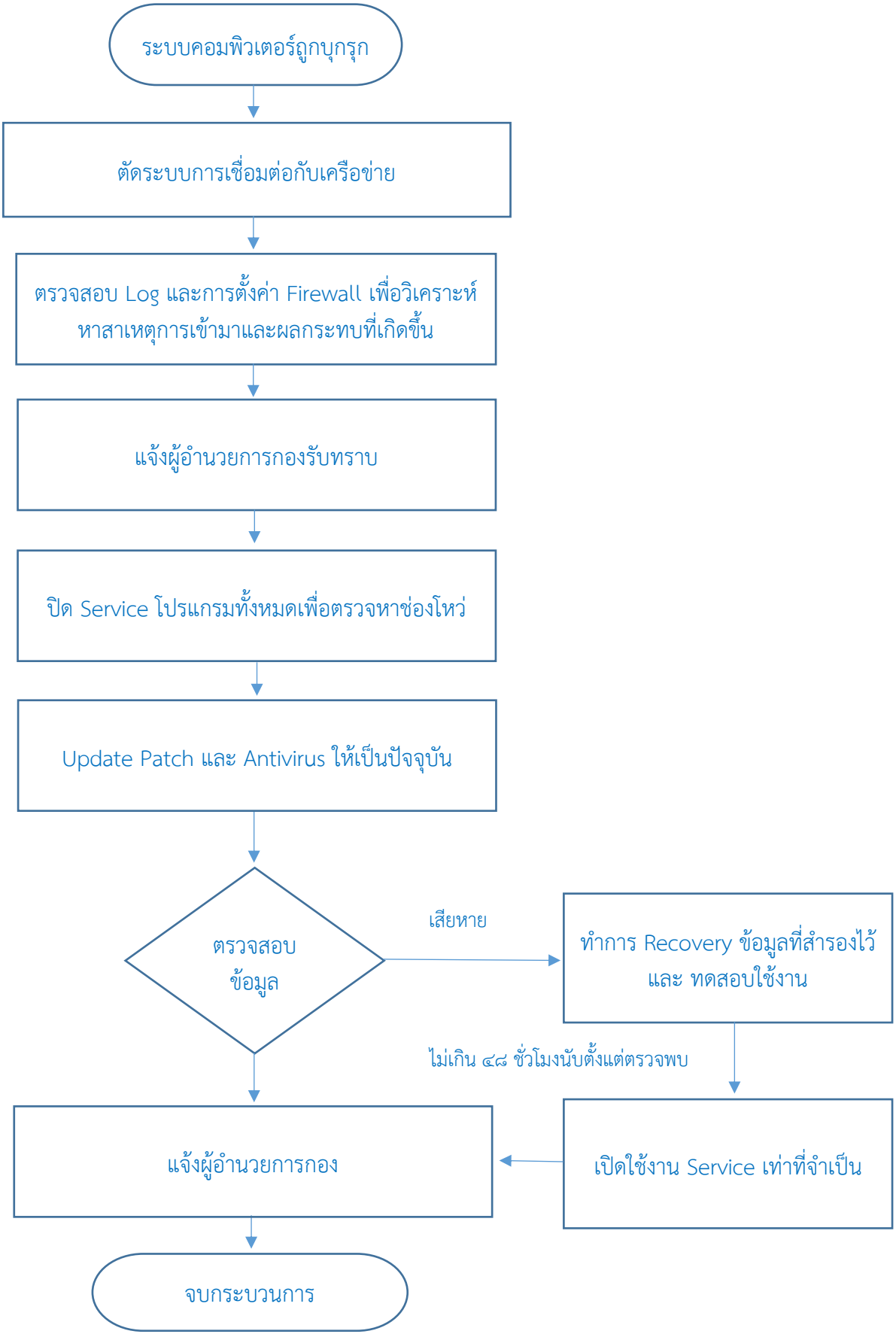
๖.๖ กรณีสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง มีขั้นตอนการปฏิบัติดังนี้



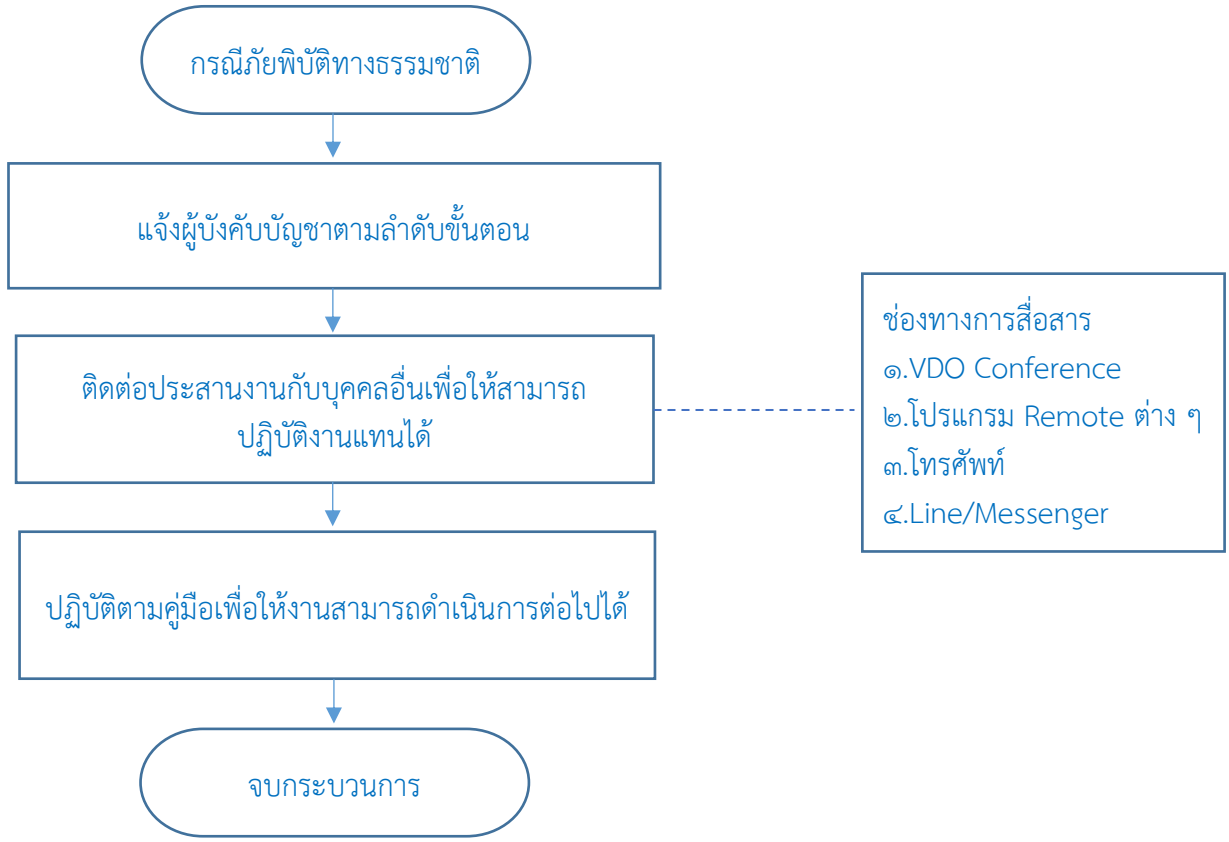
๖.๗ กรณีระบบเครือข่ายล้มเหลว มีขั้นตอนการปฏิบัติดังนี้



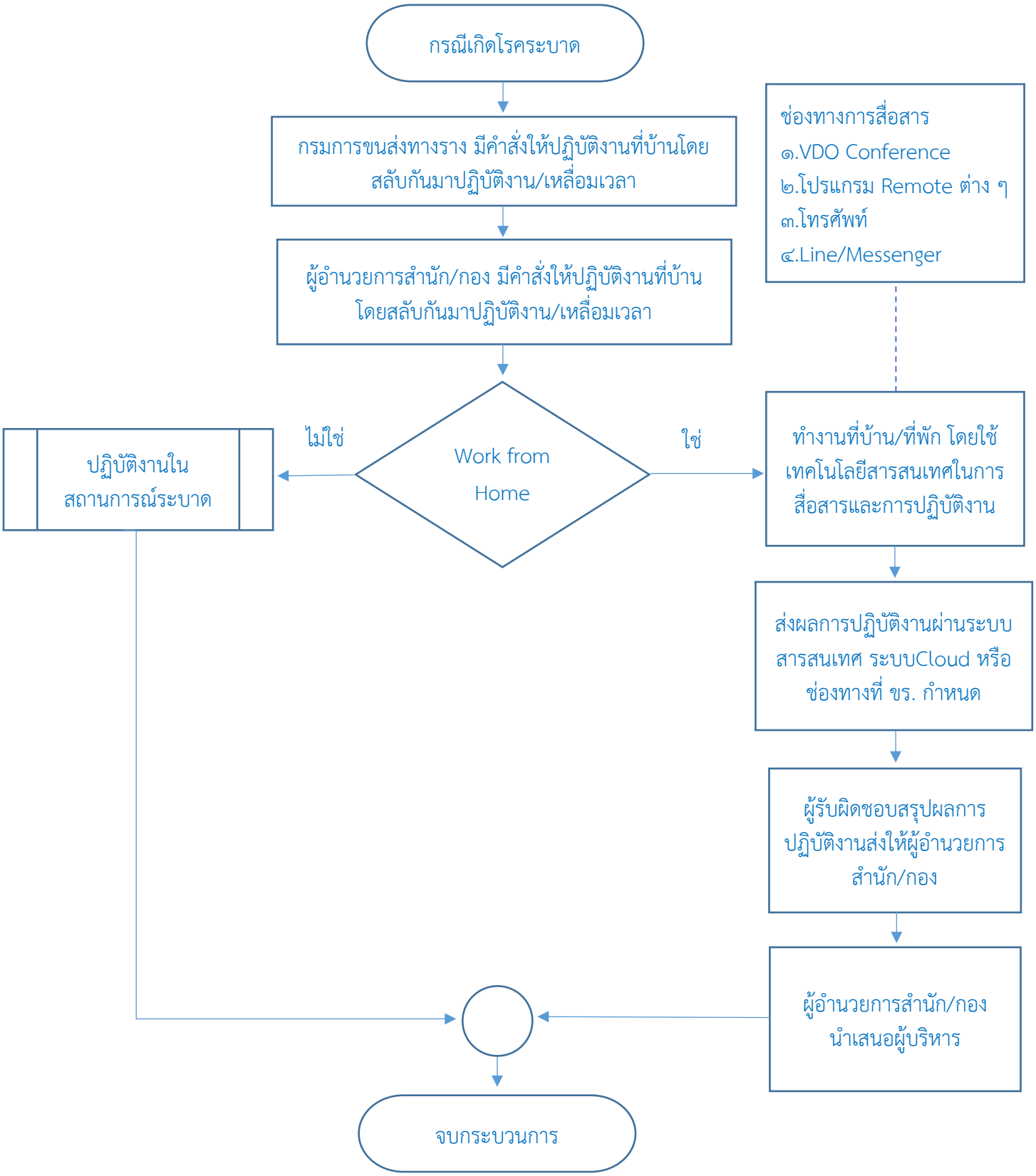
๖.๘ กรณีระบบป้องกันผู้บุกรุกล้มเหลว มีขั้นตอนการปฏิบัติดังนี้



๖.๙ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดเหตุภัยพิบัติทางธรรมชาติ มีขั้นตอนการปฏิบัติดังนี้



๖.๑๐ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้เนื่องจากเกิดโรคระบาด มีขั้นตอนการปฏิบัติดังนี้



ภาคผนวก

รายชื่อผู้รับผิดชอบและเบอร์โทรศัพท์ติดต่อ ดังต่อไปนี้

๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

๑) อธิบดีกรมการขนส่งทางราง (Department Chief Information Office : DCIO)

๒) รองอธิบดีกรมการขนส่งทางราง (ผู้ช่วย DCIO)

๒. ระดับอำนวยการ

รับผิดชอบในการอำนวยการ วิเคราะห์ปัจจัย ประเมินสถานการณ์ ให้ข้อสังเกตและแนวทางในการดำเนินการ ตลอดจนกำชับติดตามสถานการณ์อย่างใกล้ชิด และรายงานต่อ DCIO และผู้ช่วย DCIO ให้รับทราบ

๓. ระดับปฏิบัติ

หัวหน้ากลุ่มเทคโนโลยีสารสนเทศ รับผิดชอบประสานงานกับผู้ปฏิบัติและทีมงานด้านเทคโนโลยีสารสนเทศของ ขร. ให้ความเห็น เสนอแนะวิธีการ แนวทางแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติต่อระบบเทคโนโลยีสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการปฏิบัติตามแผนการป้องกันและแก้ไขปัญหา และตรวจสอบระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศพร้อมรายงานผลการดำเนินการ

เจ้าหน้าที่ผู้ดูแลระบบหน่วยงาน รับผิดชอบการปฏิบัติงาน การบริหารจัดการ ศึกษา ทบทวน วางแผน ติดตาม และรักษาความปลอดภัยระบบฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ ดังนี้

๒.๑ คณะแก้ไขปัญหาเบื้องต้น กรณีจากไฟไหม้ ไฟฟ้าดับ

มีหน้าที่แก้ไขปัญหาเบื้องต้น ควบคุมการดำเนินงานในการดับเพลิง ผู้รับผิดชอบ ได้แก่

นายภูวิศ รักษาแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๒-๗๙๑-[redacted]

นายณัฐวีร์ พูลสมบัติภิญโญ เบอร์โทรศัพท์ติดต่อ ๐๙๑-๗๗๑-[redacted]

๒.๒ คณะกู้คืนระบบ

มีหน้าที่ประสานงานการกู้คืนระบบต่าง ๆ ให้สามารถกลับมาใช้งานได้ตามปกติ ผู้รับผิดชอบ ได้แก่

<u>ผู้รับผิดชอบหลัก</u>

นายณัฐวีร์ พูลสมบัติภิญโญ เบอร์โทรศัพท์ติดต่อ ๐๙๑-๗๗๑-[redacted]

นายภูวิศ รักษาแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๒-๗๙๑-[redacted]

<u>ผู้รับผิดชอบสนับสนุน</u>

นายมนตรี สุดสาย เบอร์โทรศัพท์ติดต่อ ๐๘๕-๑๑๘-[redacted]

นายศรัทธา พันธ์พุทธ เบอร์โทรศัพท์ติดต่อ ๐๖๓-๖๙๑-[redacted]

๒.๓ คณะกู้คืนเครือข่าย

มีหน้าที่ดูแลกู้คืนให้เครือข่ายกลับมาใช้งานได้ปกติ ผู้รับผิดชอบ ได้แก่

<u>ผู้รับผิดชอบหลัก</u>

นายภูวิศ รักษาแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๒-๗๙๑-[redacted]

นายณัฐวีร์ พูลสมบัติภิญโญ เบอร์โทรศัพท์ติดต่อ ๐๙๑-๗๗๑-[redacted]

<u>ผู้รับผิดชอบสนับสนุน</u>

นายมนตรี สุดสาย เบอร์โทรศัพท์ติดต่อ ๐๘๕-๑๑๘-[redacted]

นายศรัทธา พันธ์พุทธ เบอร์โทรศัพท์ติดต่อ ๐๖๓-๖๙๑-[redacted]

๒.๔ คณะสำรองและกู้คืนข้อมูล (Backup & Recovery)

มีหน้าที่สำรองและกู้คืนข้อมูล เพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูล และฟื้นฟูระบบ/ข้อมูลจากความเสียหายให้กลับมาใช้งานใหม่ได้ทันทีและครบถ้วนสมบูรณ์ ผู้รับผิดชอบ ได้แก่

ผู้รับผิดชอบหลัก

นายภูวิศ รักษาแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๒-๗๙๑-

นายณัฐวีร์ พูลสมบัติภิญโญ เบอร์โทรศัพท์ติดต่อ ๐๙๑-๗๗๑-

ผู้รับผิดชอบสนับสนุน

นายมนตรี สุดสาย เบอร์โทรศัพท์ติดต่อ ๐๘๕-๑๑๘-

นายศรัทธา พันธ์พุทธ เบอร์โทรศัพท์ติดต่อ ๐๖๓-๖๙๑-

๒.๕ คณะแก้ไขปัญหาเนื่องจากสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

มีหน้าที่แก้ไขปัญหาเบื้องต้นเนื่องจากเกิดการความไม่สงบเรียบร้อยในบ้านเมือง แจ้งเหตุต่อผู้บังคับบัญชาเพื่อผู้บังคับบัญชาดำเนินการสั่งการตามแผนที่เตรียมไว้ ผู้รับผิดชอบ ได้แก่

นายภูวิศ รักษาแก้ว เบอร์โทรศัพท์ติดต่อ ๐๘๒-๗๙๑-

นายณัฐวีร์ พูลสมบัติภิญโญ เบอร์โทรศัพท์ติดต่อ ๐๙๑-๗๗๑-

นายสุกฤษฎ์ คำหอมกุล เบอร์โทรศัพท์ติดต่อ ๐๘๘-๖๓๘-

นายธีรพัฒน์ ยิ้มเจริญ เบอร์โทรศัพท์ติดต่อ ๐๘๖-๖๘๑-

นายมนตรี สุดสาย เบอร์โทรศัพท์ติดต่อ ๐๘๕-๑๑๘-

นายศรัทธา พันธ์พุทธ เบอร์โทรศัพท์ติดต่อ ๐๖๓-๖๙๑-

นายธรรมสรณ์ อยู่ไพศาล เบอร์โทรศัพท์ติดต่อ ๐๘๒-๔๘๙-