แผนรองรับสถานการณ์ฉุกเฉิน ปรับปรุงปี ๒๕๖๖

(IT Contingency Plan: Revised 2023)

งานพัฒนาเทคโนโลยีเครือข่ายและบริการคอมพิวเตอร์ และ
งานพัฒนาระบบสารสนเทศ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยราชภัฏสกลนคร

สารบัญ

หน้า

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

๑. บทนำ

ปัจจุบัน มหาวิทยาลัยราชภัฏสกลนคร ได้มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการ การเรียนการสอน การศึกษา ค้นคว้า และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการเรียนการสอน การวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ มีจำนวนเพิ่มมากขึ้นทุกๆปี ดังนั้นจำเป็นต้องมีการบริหารจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศเพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

งานพัฒนาเทคโนโลยีเครือข่ายและบริการคอมพิวเตอร์ และงานพัฒนาระบบสารสนเทศมหาวิทยาลัยราชภัฏสกลนคร ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการนักศึกษาตลอดจนบุคลากรได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย จากอุทกภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๒. วัตถุประสงค์

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและเทคโนโลยีสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

๓. การวิเคราะห์ความเสี่ยง

มหาวิทยาลัยราชภัฏสกลนคร มีการใช้เทคโนโลยีสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการเรียนการสอนและการปฏิบัติงานให้เกิดประโยชน์สูงสุด

การวิเคราะห์และตรวจสอบความเสี่ยงด้านสารสนเทศ ของมหาวิทยาลัยมหาวิทยาลัยราชภัฏสกลนคร พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

๑. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง การถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ ถูกก่อกวนจาก Hacker ถูกเจาะทำลายระบบจาก Cracker ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ไฟฟ้าขัดข้อง เป็นต้น

๒. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้

๓. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟไหม้ น้ำท่วม อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น

๔. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏสกลนคร ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนั้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ มหาวิทยาลัยราชภัฏสกลนคร มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศ

๔. แผนรองรับสถานการณ์ฉุกเฉิน

๔.๑ สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

๔.๑.๑ กรณีการป้องกันไวรัสล้มเหลว

☐ กรณีถูกไวรัสหรือผู้บุกรุก เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

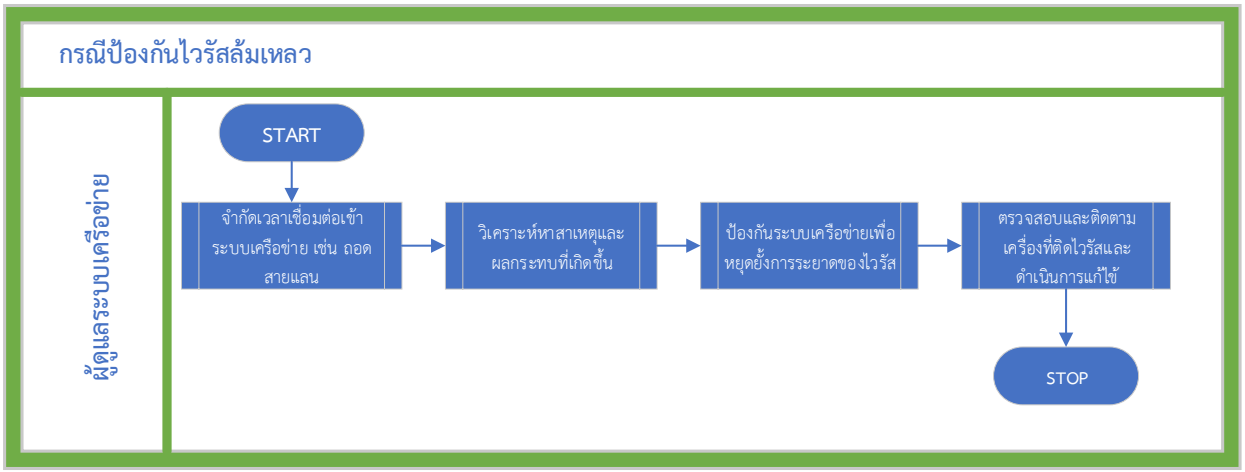
☐ วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสที่ระบาด

☐ ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

☐ ตรวจสอบและติดตามเครื่องที่ติดไวรัสและดำเนินการแก้ไข

☐ กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่งานพัฒนาเทคโนโลยีเครือข่ายและบริกาคอมพิวเตอร์ทราบ หรือกรณีมีเหตุอันทำให้งานพัฒนาเทคโนโลยีเครือข่ายและบริกาคอมพิวเตอร์ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ งานพัฒนาเทคโนโลยีเครือข่ายและบริกาคอมพิวเตอร์จะต้องประกาศให้ทุก คณะและหน่วยงาน ทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



๔.๑.๒ กรณีการป้องกันผู้บุกรุกล้มเหลว

☐ กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

☐ ผู้ดูแลระบบแจ้งหัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและบริกาคอมพิวเตอร์ให้ทราบโดยด่วน

☐ ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

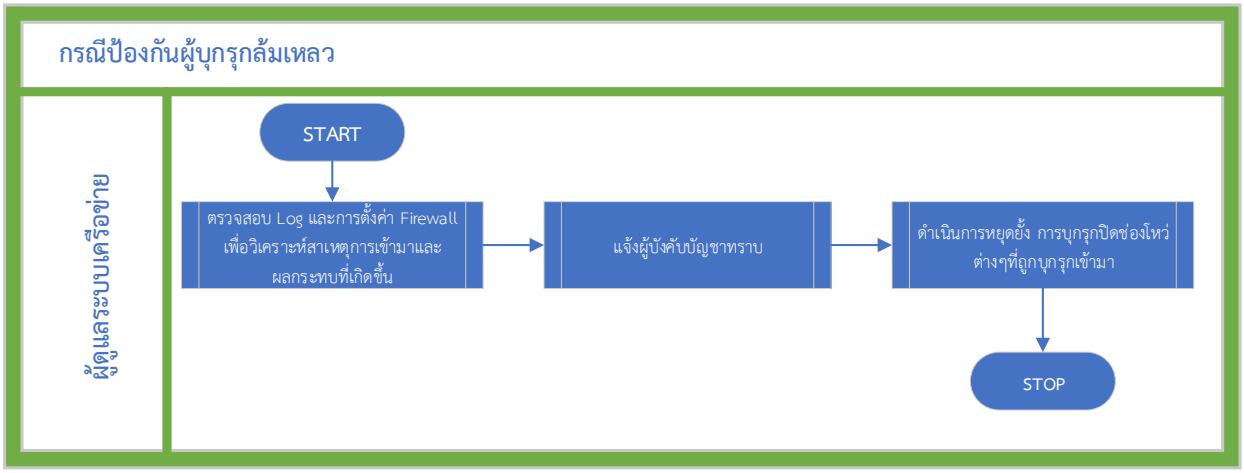
☐ ในกรณีที่ตรวจพบว่าเครื่องแม่ข่ายถูกบุกรุก ให้ดำเนินการตามกระบวนการต่อไปนี้

☐ เบื้องต้น ให้หยุดการเชื่อมต่อกับเครือข่ายทั้งหมดของเครื่องแม่ข่าย เช่น การไม่เชื่อมต่อสายสัญญาณอินเทอร์เน็ตหรือปิดเครื่องแม่ข่ายเพื่อลดความเสียหายที่อาจจะเกิดขึ้น ถ้าเป็น เว็บไซต์ให้บริการ ให้ทำการขึ้นหน้าแจ้งปิดบริการชั่วคราว พร้อมให้รายละเอียดในการติดต่อสื่อสาร

☐ ในกรณีเป็นเครื่องแม่ข่ายหรือเซอร์วิสที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศดูแล ให้ดำเนินการตรวจสอบแก้ไข โดยการตรวจสอบ log file ของไฟร์วอลล์ และเซอร์วิสที่ให้บริการของเครื่องแม่ข่าย เพื่อหาต้นทางที่ทำการบุกรุก พร้อมทั้งทำการ Patch software ทั้งในส่วนของระบบปฏิบัติการณ์ ซอฟต์แวร์เซอร์วิสที่ให้บริการ และแพลตฟอร์มที่ใช้ในการพัฒนา ที่เกี่ยวข้องทั้งหมด

☐ ในกรณีเป็นเครื่องแม่ข่ายหรือเซอร์วิสที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศไม่ได้ดูแล ให้ทำหนังสือแจ้งให้ทางหน่วยงานที่รับผิดชอบดูแลเครื่องแม่ข่ายหรือเซอร์วิสดังกล่าว เพื่อให้รับทราบและดำเนินการตรวจสอบแก้ไขภายในระยะเวลาที่กำหนด

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



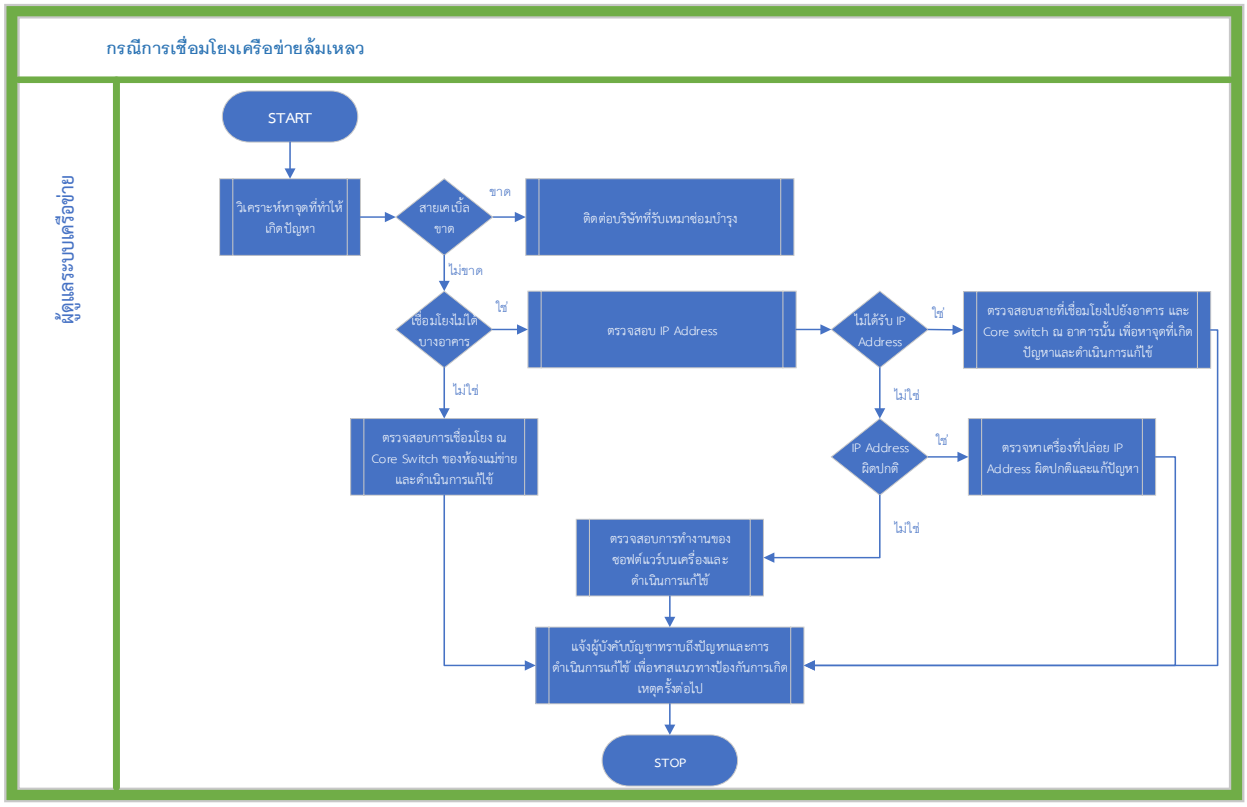
๔.๑.๓ กรณีการเชื่อมโยงเครือข่ายล้มเหลว

☐ รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

☐ หากสายเคเบิ้ลขาด ให้รีบแจ้งผู้บริหารพร้อมติดต่อบริษัทฯ เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

☐ หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ core switch ที่ติดตั้งอยู่ ณ อาคารนั้นๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



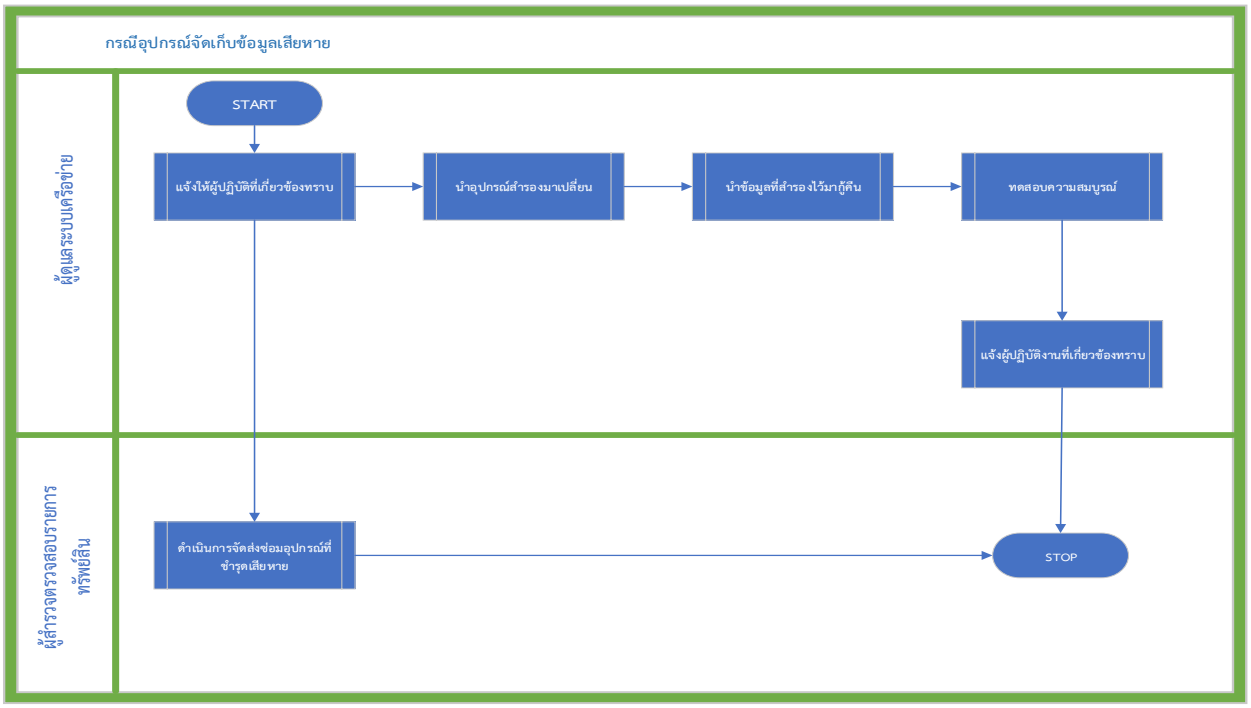
๔.๑.๔ กรณีอุปกรณ์หรือคอมพิวเตอร์ขัดข้อง

☐ แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

☐ รีบดำเนินการจัดหาอุปกรณ์มาเปลี่ยนใหม่และนำข้อมูลที่ได้สำรองไว้ มาทำการกู้คืนข้อมูลโดยเร็ว

☐ ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

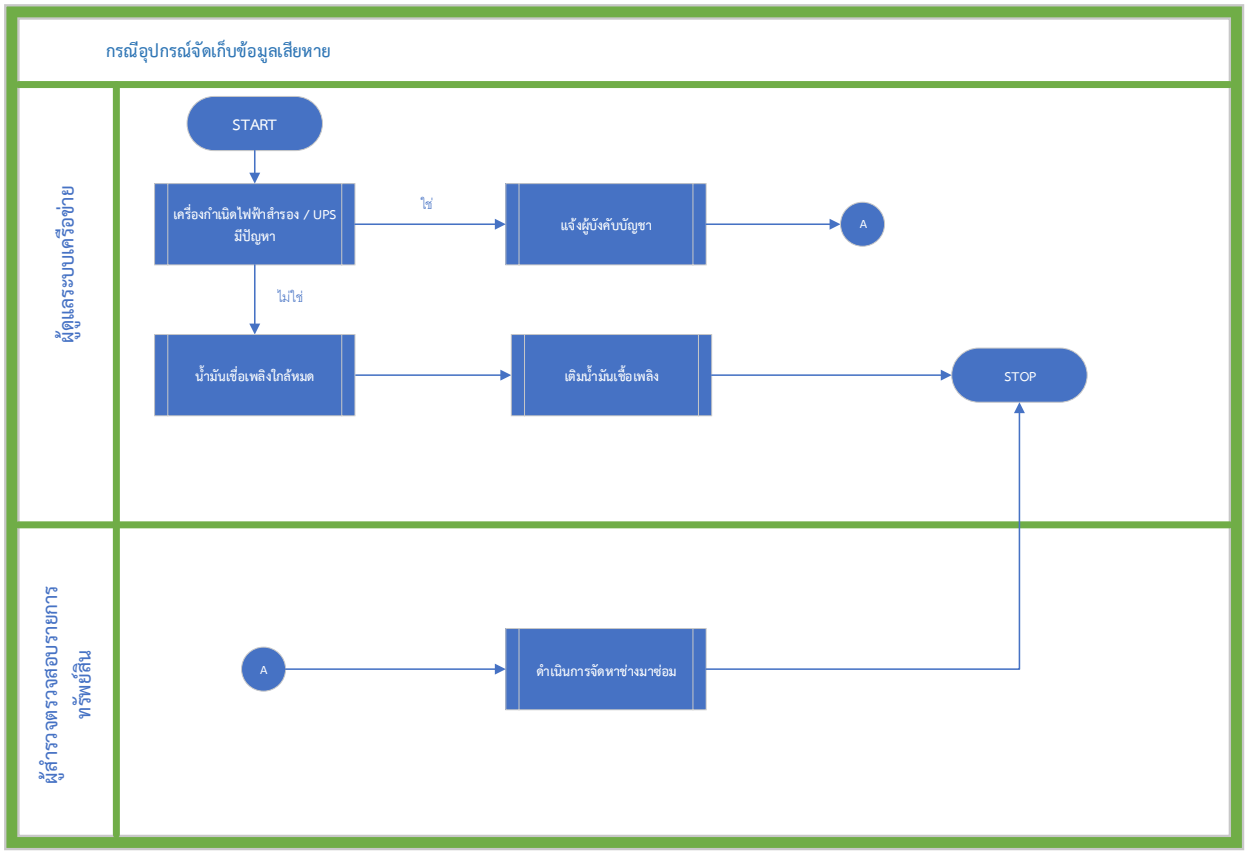


๔.๑.๕ กรณีไฟฟ้าขัดข้อง

☐ ระบบสารสนเทศมีเครื่องปั่นไฟฟ้าสำรองพร้อม UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ ๔๘ ชั่วโมง และ UPS สามารถสำรองกระไฟฟ้าได้ ๔ ชั่วโมง

☐ หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง



๔.๒ สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

๔.๒.๑ กรณีไฟไหม้

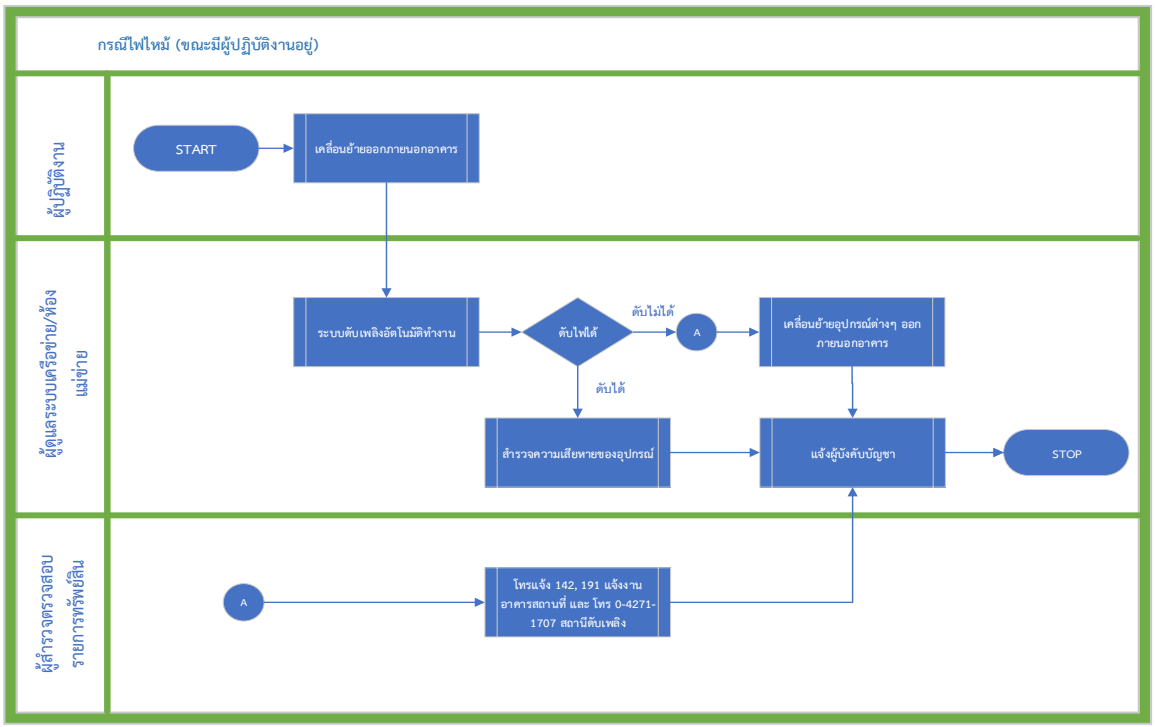
☐ หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่ความสามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

☐ หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้งงานอาคารและสถานที่และยานพาหนะทันที ที่ โทร. **๑๔๒** หรือหัวหน้างานอาคาร โทร. **๐๘-๑๙๗๔-๔๙๒๙** และสถานีดับเพลิงเทศบาลสกลนคร **โทร. ๐-๔๒๗๑-๑๗๐๗**

☐ หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆมาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และ/หรือ ระบบดับไฟอัตโนมัติ

☐ อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑-๒ ครั้ง

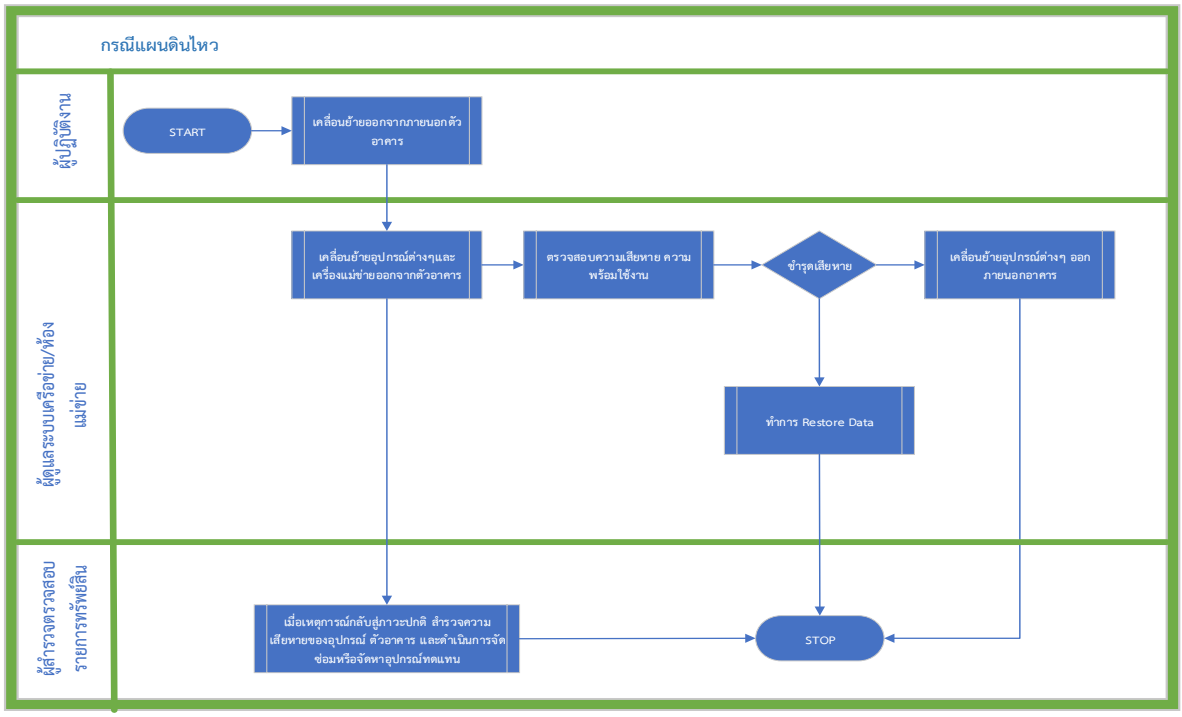
แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



๔.๒.๒ กรณีแผ่นดินไหว/อาคารถล่ม

- ☐ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร
- ☐ ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- ☐ เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



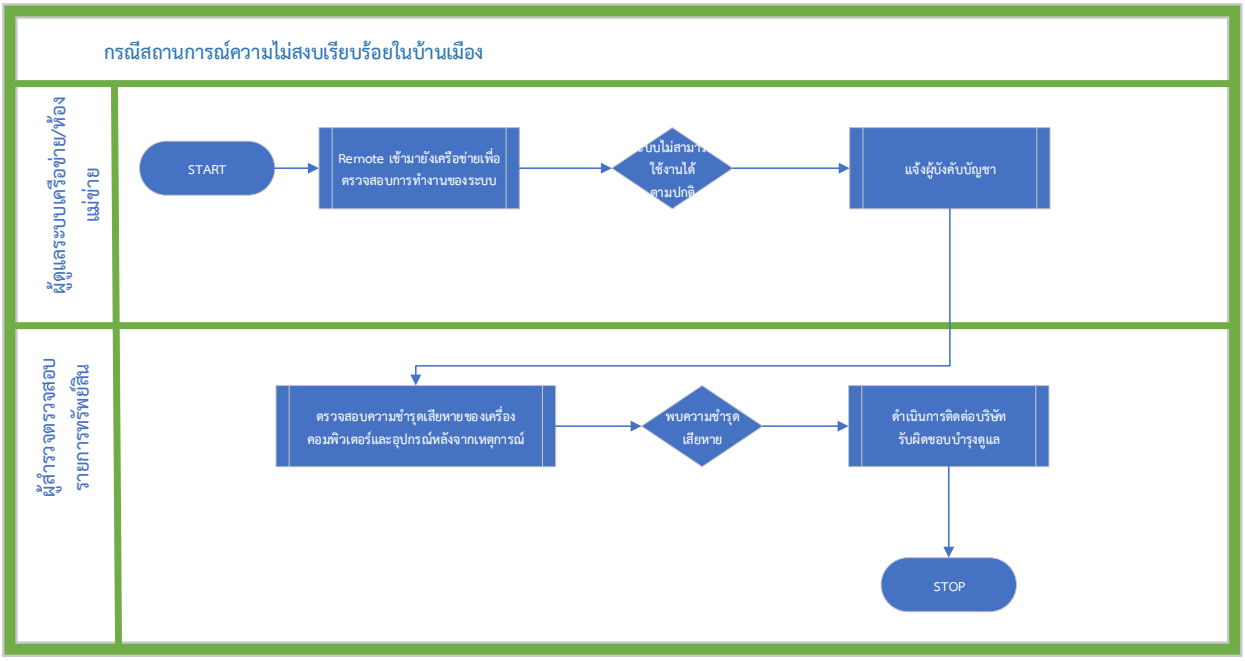
๔.๓ สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

๔.๓.๑ กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

☐ กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งหัวหน้างานพัฒนาเทคโนโลยีเครือข่ายและบริกาคอมพิวเตอร์ทราบ

☐ หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้แจ้งผู้บริหารทราบพร้อมดำเนินการติดต่อบริษัทภายนอกดำเนินการซ่อมแซมแก้ไขหากจำเป็น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



๔.๔ สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

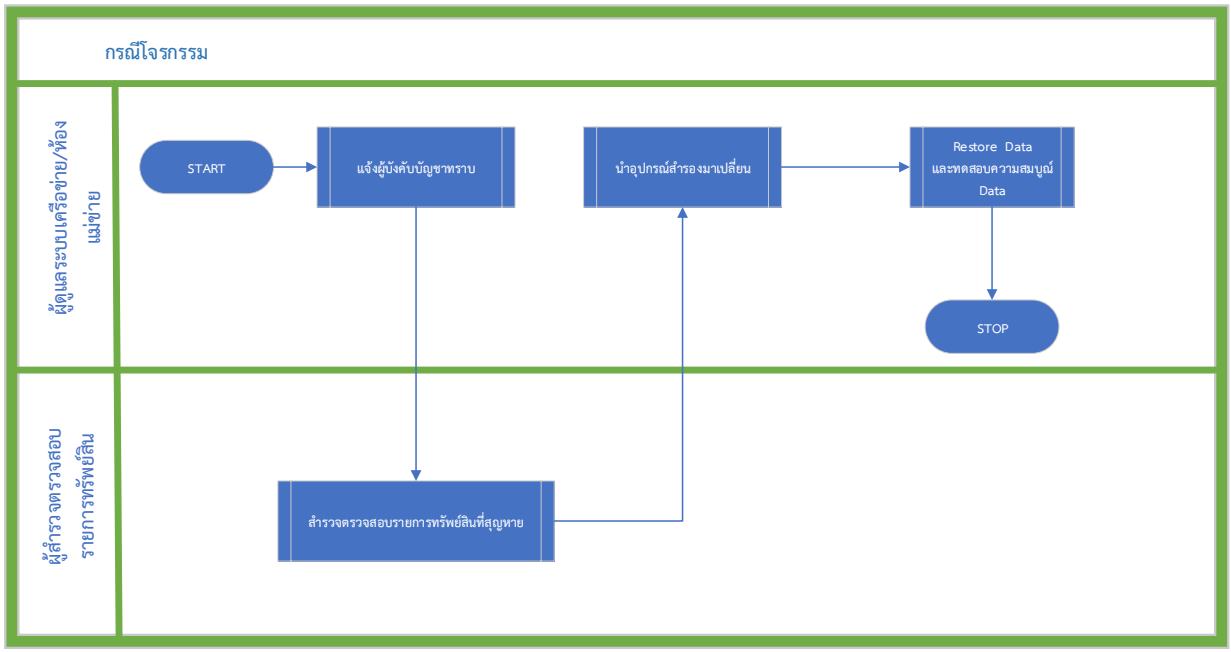
๔.๔.๑ กรณีโจรกรรม

☐ ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

☐ สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

☐ ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่างๆได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

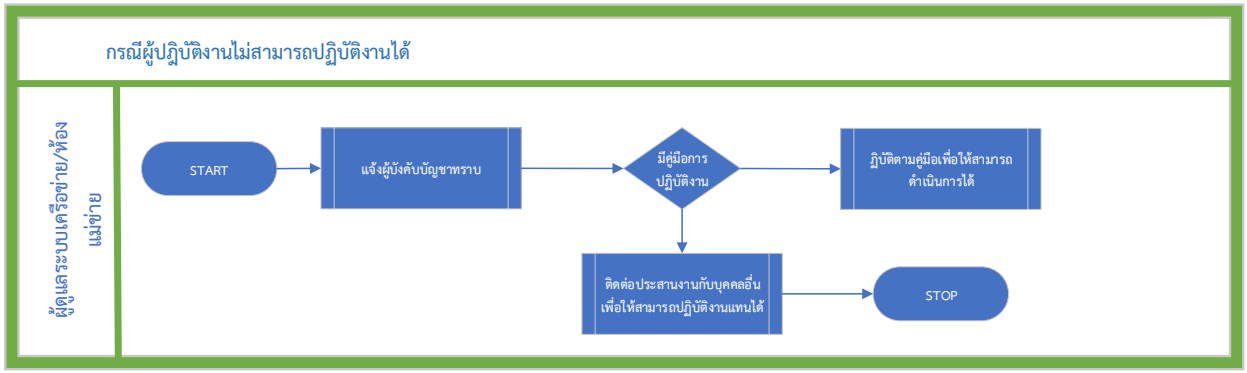


๔.๔.๒ กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

☐ แจ้งผู้บังคับบัญชาทราบ

☐ ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



๕. แผนการสำรองระบบและกู้คืนระบบสารสนเทศในสถานการณ์ฉุกเฉิน

บทนำ

ในปัจจุบัน ทุกหน่วยงานราชการต้องนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์การและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศและฐานข้อมูลต่างๆ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร

ดังนั้น ข้อมูลสารสนเทศต่างๆ จึงมีจำนวนเพิ่มมากขึ้นอย่างต่อเนื่อง และนับเป็นสิ่งจำเป็นที่จะต้องมีการจัดการฐานข้อมูลการเฝ้าระวัง การจัดเก็บ และการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้รวดเร็ว แม่นยำ เต็มประสิทธิภาพตลอดเวลาและต่อเนื่อง

มหาวิทยาลัย ได้นำเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงานและให้บริการประชาชนให้ได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบเทคโนโลยีสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของหน่วยงาน ดังนั้น เพื่อป้องกันและแก้ไขปัญหา

จึงมีความจำเป็นที่จะต้องมีแผนการสำรองข้อมูล เพื่อป้องกันเหตุการณ์ที่ผิดปกติ ซึ่งอาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยเฉพาะที่อาจจะเกิดต่อชุดข้อมูลต่างๆ ที่สำคัญในฐานข้อมูลและระบบงานต่างๆ ของมหาวิทยาลัย

วัตถุประสงค์

๑ เพื่อเพิ่มประสิทธิภาพในการสำรองข้อมูล และสามารถนำข้อมูลมาใช้งานได้อย่างต่อเนื่องและเพิ่มความน่าเชื่อถือในการใช้งานระบบอีกทั้งระบบการสำรองข้อมูลนี้จะช่วย ให้ระบบสารสนเทศสามารถนำข้อมูลสำรองมาใช้งานทดแทนข้อมูลที่ถูกทำให้สูญหาย หรือเสียหายได้อย่างต่อเนื่องและรวดเร็ว

๒. เพื่อให้ข้อมูลสำคัญมีความปลอดภัยจากการถูกทำลาย หรือสูญหาย

๓. เพื่อให้ระบบสารสนเทศมีเสถียรภาพ โดยมีระบบจัดเก็บสำรองข้อมูลที่สามารถทำงานทดแทนกันได้ตลอดเวลา

๔ เพื่อให้การฟื้นคืนสภาพของระบบสารสนเทศเป็นไปตามระยะเวลาและเป้าหมาย

การดำเนินการ

แผนสำรองข้อมูลพร้อมกู้คืนระบบ จะต้องทำการปรับปรุงให้เป็นปัจจุบัน ตามรอบระยะเวลาอยู่เสมอ เพื่อให้แน่ใจว่าแผนนั้น ยังสามารถนำไปใช้งานได้อย่างมีประสิทธิผลและประสิทธิภาพตามที่คาดหมายไว้

๕.๑ แผนการสำรองข้อมูล

๕.๑.๑ การสำรองข้อมูลเครื่องแม่ข่าย

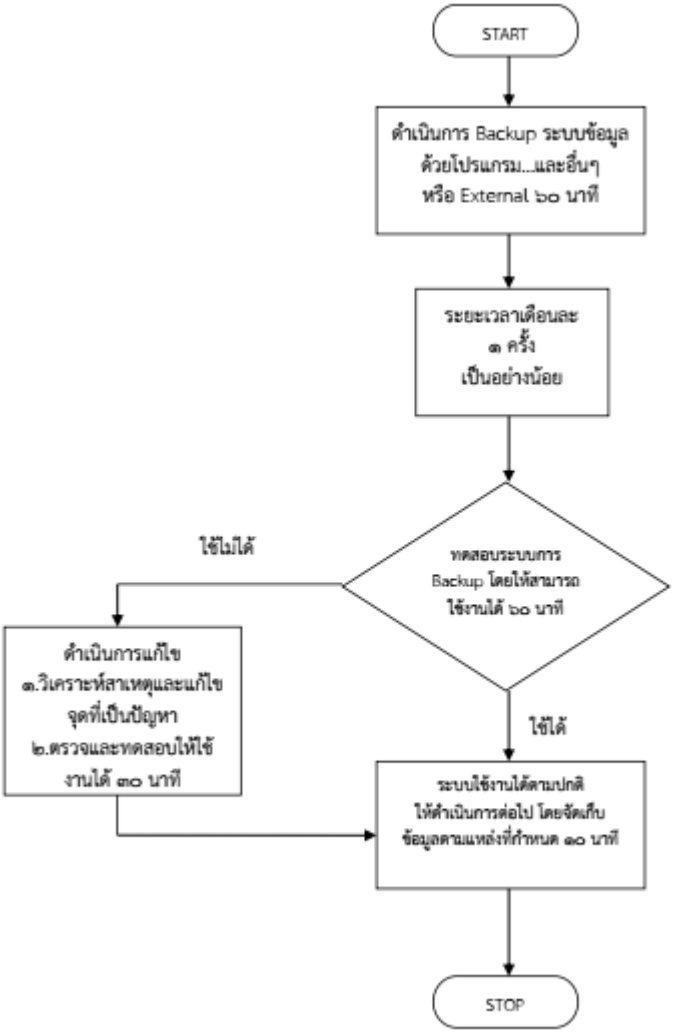
☐ การสำรองข้อมูลต้องใช้โปรแกรมตามที่กำหนดหรือเห็นสมควร

☐ ระยะเวลาในการสำรองข้อมูลจะต้อง Backup เดือนละ ๑ ครั้ง เป็นอย่างน้อย

☐ หลังจาก Backup ในครั้งแรกต้องตรวจสอบด้วยว่าระบบและข้อมูลที่นำมานั้นสามารถใช้งานได้เป็นปกติหรือไม่ ถ้าไม่สามารถใช้งานได้ให้ดำเนินการแก้ไข

☐ ดำเนินการจัดเก็บข้อมูลไว้ใน Server ที่กำหนด

แผนผังแสดงขั้นตอนการสำรองข้อมูลเครื่องแม่ข่าย



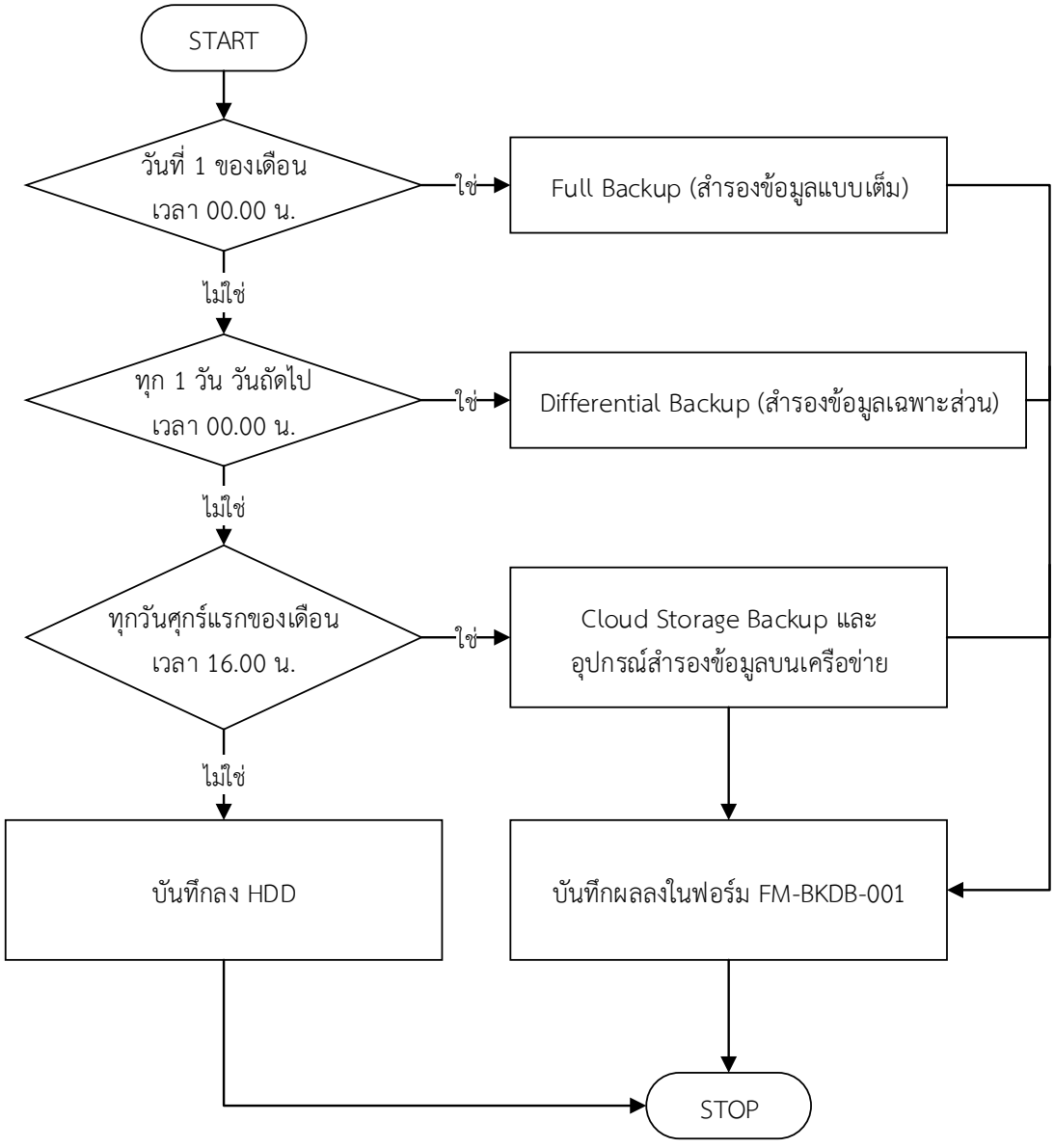
๕.๑.๒ การสำรองฐานข้อมูลและแอพพลิเคชั่นระบบฐานข้อมูลสารสนเทศ

☐ ฐานข้อมูลกลางที่เกิดจากการบูรณาการฐานข้อมูล

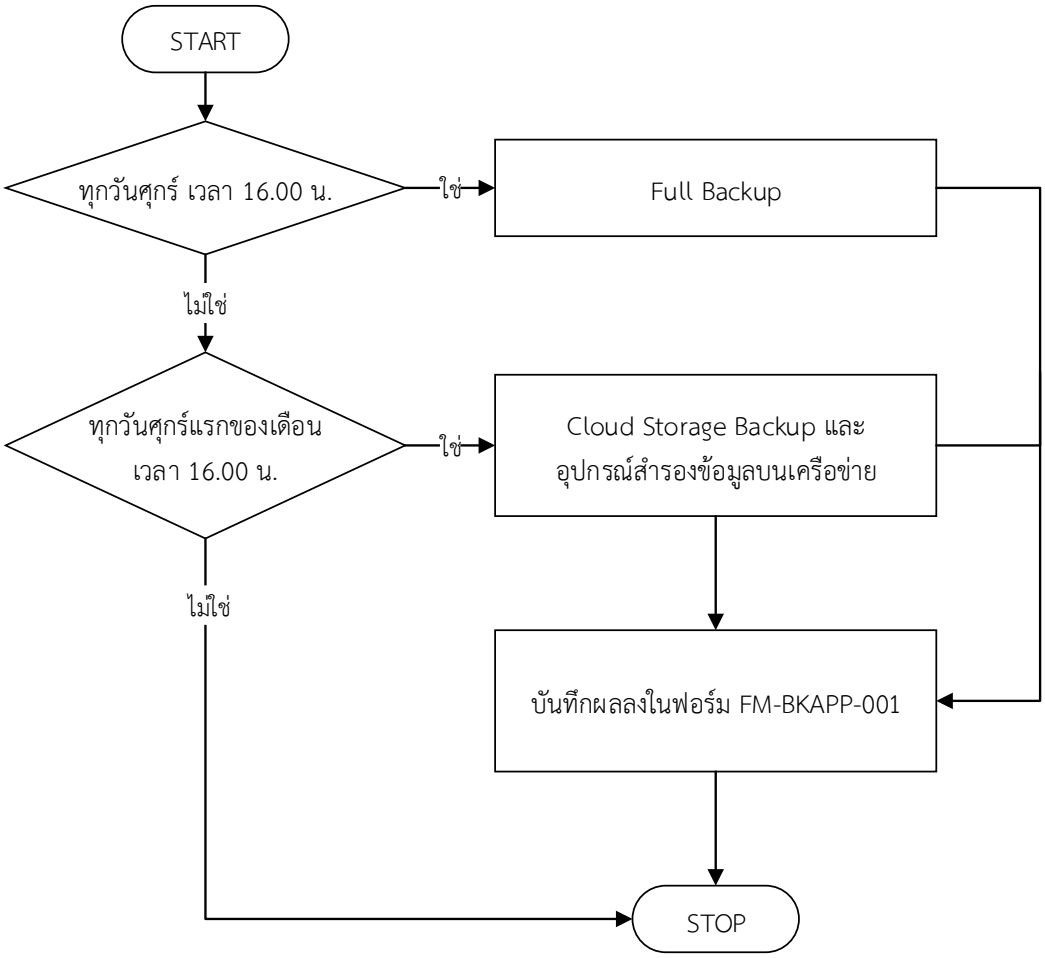
☐ ฐานข้อมูลที่งานพัฒนาระบบสารสนเทศดำเนินการพัฒนา

☐ แอพพลิเคชั่น ระบบฐานข้อมูลสารสนเทศที่งานพัฒนาระบบสารสนเทศดำเนินการพัฒนา

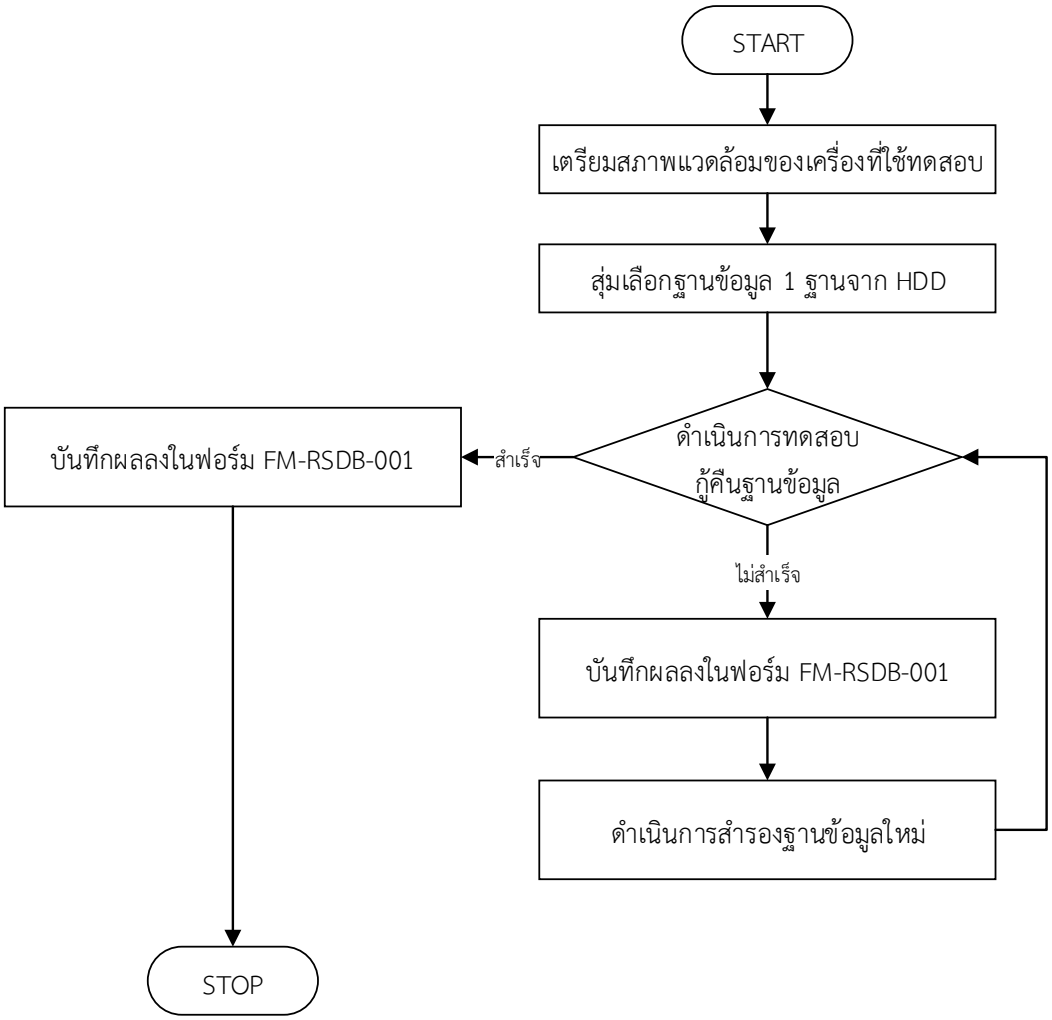
แผนผังขั้นตอนการสำรองฐานข้อมูล



แผนผังแสดงขั้นตอนการสำรองแอพพลิเคชั่น ระบบฐานข้อมูลสารสนเทศ



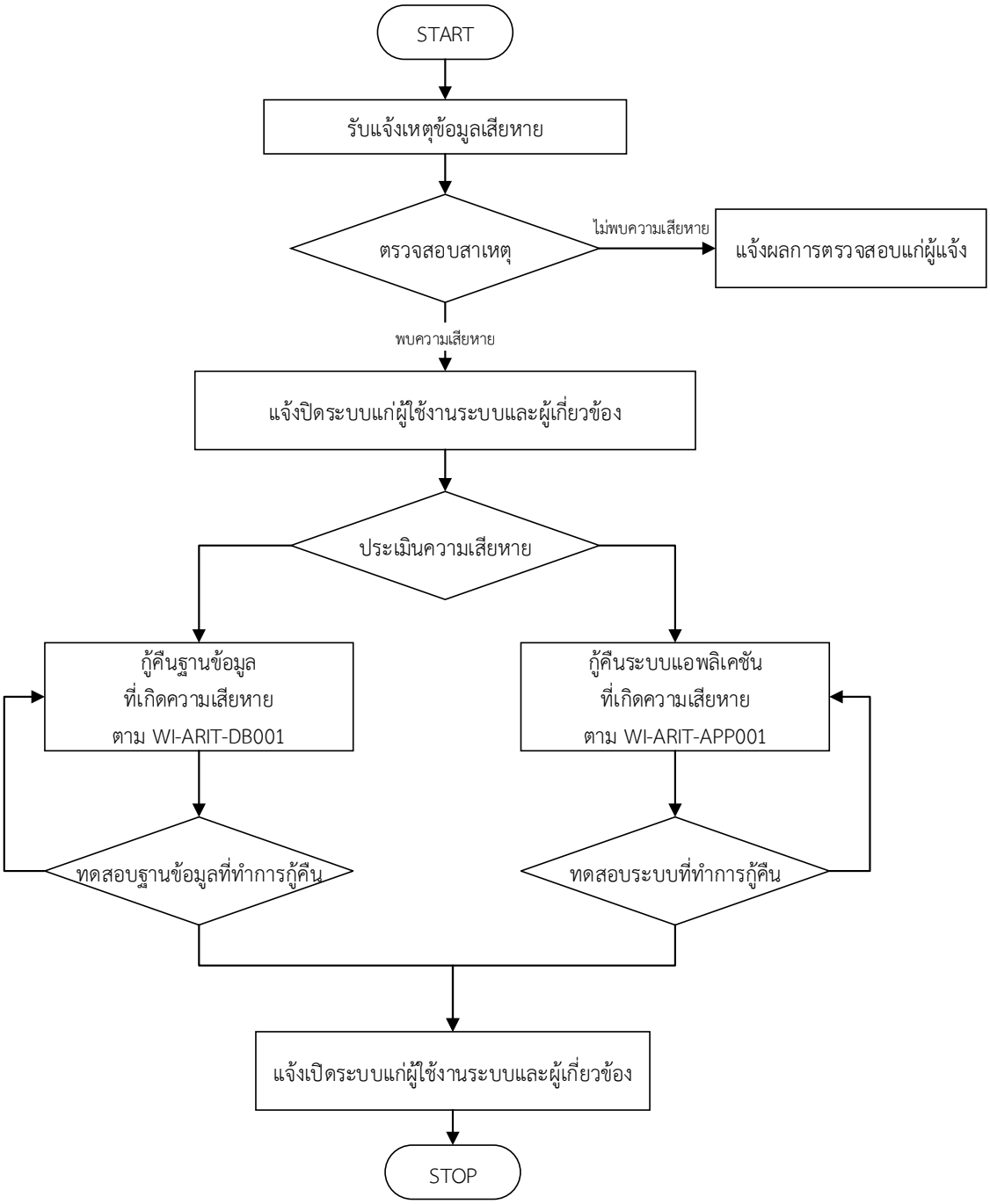
แผนผังแสดงขั้นตอนการทดสอบกู้คืนฐานข้อมูล



๕.๒ แผนการกู้คืนข้อมูล

ขั้นตอนการปฏิบัติตามแผนฉุกเฉินการกู้คืนข้อมูลเพื่อให้บุลากรผู้ปฏิบัติงานเข้าใจขั้นตอนการปฏิบัติได้ถูกต้อง และลดความเสียหายของข้อมูลและระบบสารสนเทศเมื่อเกิดเหตุ

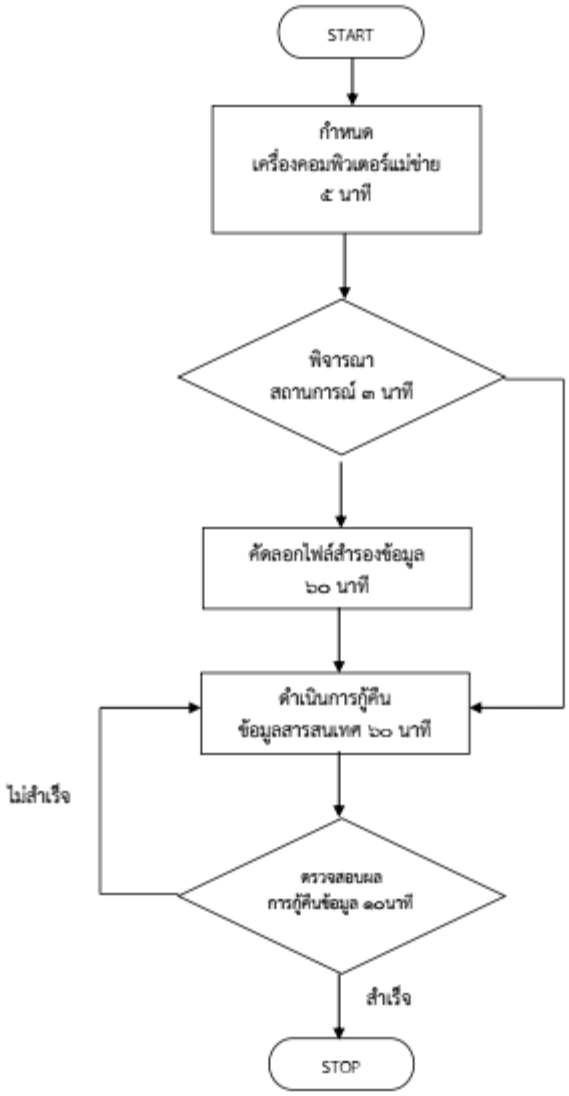
แผนผังแสดงขั้นตอนการปฏิบัติตามแผนฉุกเฉิน



๕.๒.๑ การกู้คืนข้อมูลเครื่องแม่ข่าย

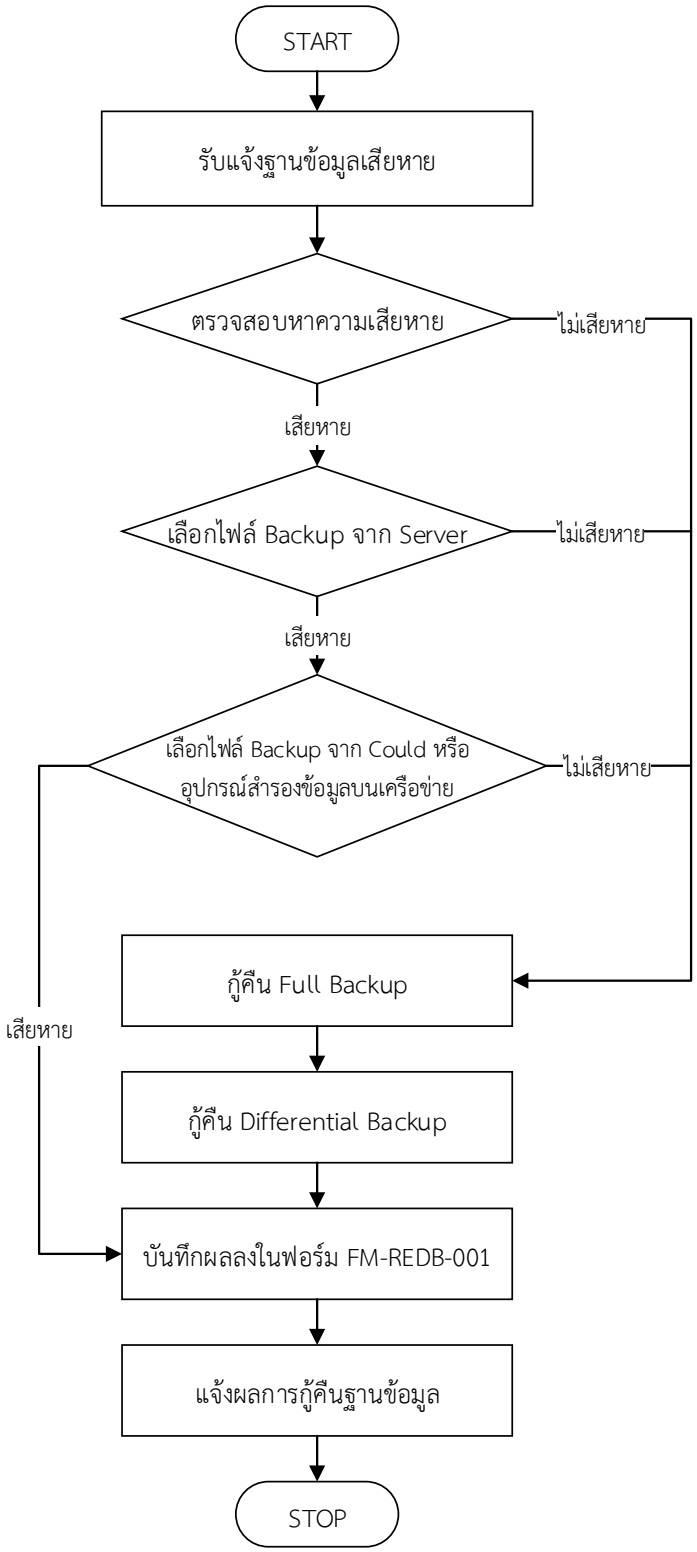
กระบวนการปฏิบัตินี้ครอบคลุมการกู้คืนข้อมูล สำหรับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ต่อพ่วง เพื่อให้การฟื้นคืนสภาพของระบบสารสนเทศเป็นไปตามระยะเวลาและเป้าหมาย และระยะเวลาที่กำหนดตามแผนการกู้คืนระบบของ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

แผนผังแสดงขั้นตอนการกู้คืนข้อมูลเครื่องแม่ข่าย

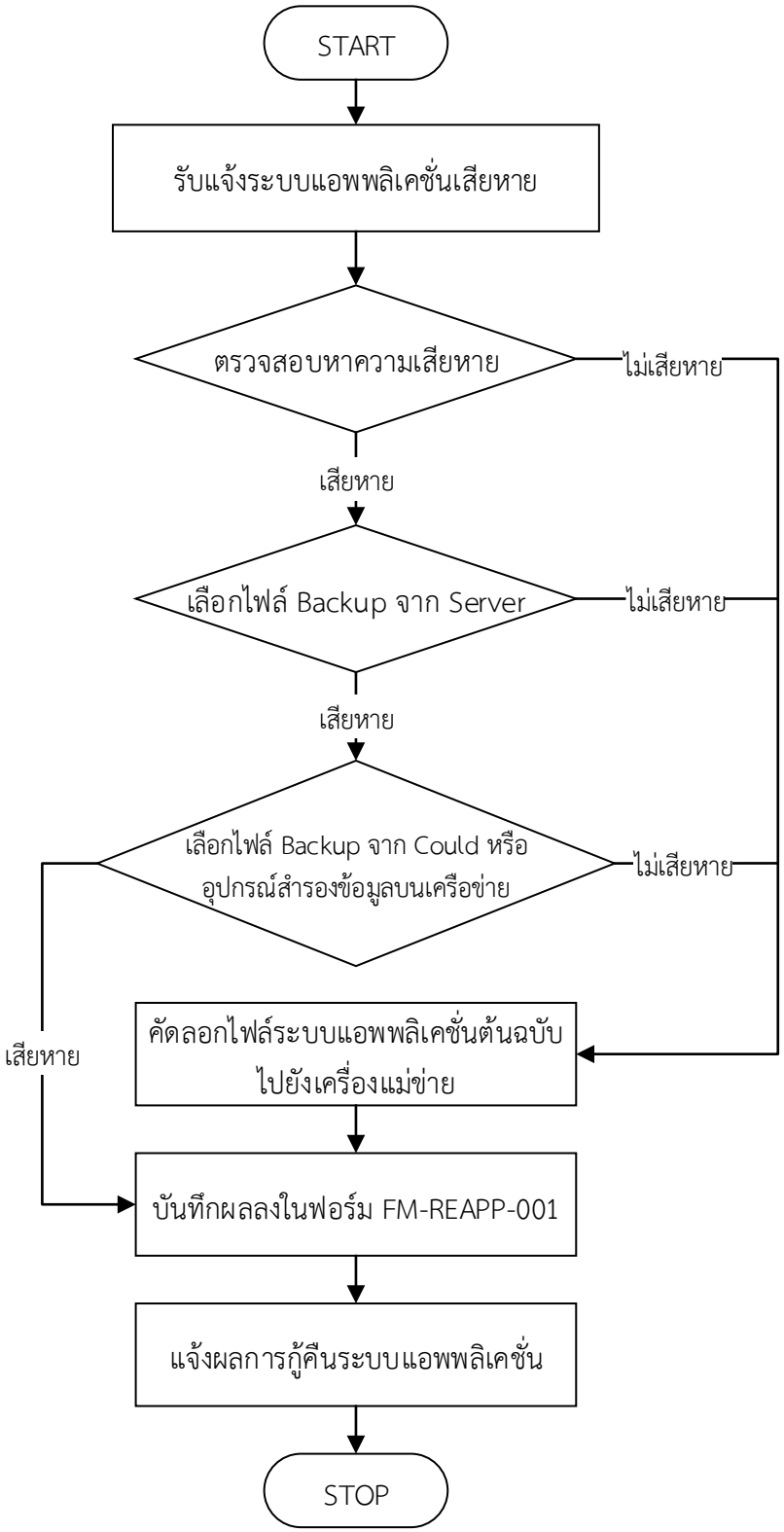


๕.๒.๒ การกู้คืนฐานข้อมูลและแอพพลิเคชั่น ระบบฐานข้อมูลสารสนเทศ

แผนผังแสดงขั้นตอนการกู้คืนฐานข้อมูล (WI-ARIT-DB001)



แผนผังแสดงการกู้คืนแอพพลิเคชั่น ระบบฐานข้อมูลสารสนเทศ (WI-ARIT-APP001)



๕.๓ ระบบที่ต้องสำรองข้อมูล

ระบบงาน เว็บไซต์ และฐานข้อมูล เป็นชุดข้อมูลที่มีความสำคัญและมีค่ามากสำหรับการดำเนินงานของหน่วยงาน ดังนั้น จึงได้คัดเลือกระบบงาน ในเครื่องคอมพิวเตอร์แม่ข่ายที่สำคัญ ไว้ดังนี้

ลำดับที่	รายการ	รายละเอียด	ความถี่ / จำนวนการสำรองข้อมูล
1	เครื่องแม่ข่ายระบบเว็บไซต์	ค่าพารามิเตอร์การติดตั้ง / ข้อมูลระบบเว็บไซต์ที่เกี่ยวข้อง	๑ ครั้ง ต่อ ๑ วัน
2	เครื่องแม่ข่ายระบบฐานข้อมูล	ค่าพารามิเตอร์การติดตั้ง / ข้อมูลระบบฐานข้อมูล	๑ ครั้ง ต่อ ๑ วัน
3	เครื่องแม่ข่ายระบบไฟล์ / งานบริการภายใน	ค่าพารามิเตอร์การติดตั้ง / ข้อมูลระบบไฟล์ เอกสาร	๑ ครั้ง ต่อ ๑ เดือน
4	เครื่องแม่ข่ายหน่วยงานภายในมหาวิทยาลัย	ค่าพารามิเตอร์การติดตั้ง / ข้อมูลระบบไฟล์ เอกสาร	๑ ครั้ง ต่อ ๑ เดือน
5	ฐานข้อมูลที่งานพัฒนาระบบสารสนเทศพัฒนา	ฐานข้อมูล MSSQL, Mysql	สำรองข้อมูลแบบเต็ม จำนวน ๑ ครั้ง ต่อ ๑ เดือน สำรองข้อมูลเฉพาะส่วนเป็นประจำทุกวัน
6	แอพพลิเคชั่น ระบบฐานข้อมูลสารสนเทศที่งานพัฒนาระบบสารสนเทศพัฒนา	ระบบสารสนเทศที่ได้พัฒนา แลกำกับดูแลทั้งหมด	๑ ครั้ง ต่อ ๑ สัปดาห์

๖. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

๑. ผู้บริหาร รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา จัดหาและสนับสนุนงบประมาณสำหรับค่าใช้จ่าย ตลอดจน ติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแลรับผิดชอบการปฏิบัติงาน ได้แก่

๑.๑. อธิการบดีมหาวิทยาลัยราชภัฏสกลนคร

๑.๒. รองอธิการบดีฝ่ายบริหารมหาวิทยาลัยราชภัฏสกลนคร

๑.๓. ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒. ผู้รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ได้แก่

๒.๑. นายจยุตย์ พูลเพิ่ม นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓-๔๗๕๓

๒.๒. นายอรรณพ อรังศรี นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓-๔๗๕๓

๒.๓. นายธีระยุทธ โคธิเวทย์ นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓-๔๗๕๓2.5. นาย

๒.๔. วิทวัส จักรคม นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๖๔๕๙-๘๓๖๑

๓. ผู้รับผิดชอบระบบสารสนเทศและฐานข้อมูล รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

๓.๑ นายกิตติภูมิ คำศรี นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓-๔๗๕๓

๓.๒. นายดนุชา บัวพินธุ นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓-๔๗๕๓

๓.๓. นางสาวสิริวรรณ ยะไชยศรี นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓- ๔๗๕๓

๓.๔. นางพินิดดา ธงษาราษฎร์ นักวิชาการคอมพิวเตอร์ เบอร์ติดต่อ ๐๘-๓๓๕๓- ๔๗๕๓

๔. ผู้รับการบริการเทคนิคและการประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

๔.๑. นายประไพ ศรีสมัย นักเทคโนโลยี

๔.๒. นางเจริญพร บาทชารี เจ้าหน้าที่บริหารงานทั่วไป

๕. ผู้รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน ได้แก่

๕.๑. นางอังคณา ศิริกุล หัวหน้าสำนักงาน

๕.๒. นางสาวอุ่นเรือน แสนเสน

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการพัฒนาระบบเทคโนโลยีดิจิทัลเพื่อการพัฒนามหาวิทยาลัยราชภัฏสกลนคร เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

คณะกรรมการพัฒนาระบบเทคโนโลยีดิจิทัล
เพื่อการพัฒนามหาวิทยาลัยราชภัฏสกลนคร
ปรับปรุง ๒๙ ตุลาคม ๒๕๖๖