ประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
เรื่อง แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศ

ตามที่มหาวิทยาลัยราชภัฏราชนครินทร์ ได้นำระบบเทคโนโลยีสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการนักศึกษาตลอดจนบุคลากรได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบข้อมูลสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคคล จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ อาจก่อให้เกิดความเสียหายต่อระบบข้อมูลสารสนเทศ และส่งผลกระทบต่อการดำเนินงาน ดังนั้น เพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ จึงกำหนดแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติอันอาจมีผลกระทบต่อระบบข้อมูลสารสนเทศ ดังนี้

๑. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้มีเสถียรภาพ และมีความพร้อมสำหรับการใช้งาน

๒. เพื่อลดความเสียหายที่อาจเกิดขึ้นแก่ระบบสารสนเทศ

๓. เพื่อให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

๕. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูและรักษาระบบความปลอดภัยของฐานข้อมูลและสารสนเทศ

จึงประกาศมาให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๒๒ เมษายน พ.ศ. ๒๕๖๕

(ผู้ช่วยศาสตราจารย์ ดร.สายฝน เสกขุนทด)
รักษาราชการแทน ผู้อำนวยการ
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ที่ ๐๐๓ /๒๕๖๕

แผนรองรับสถานการณ์ฉุกเฉิน

มหาวิทยาลัยราชภัฏราชนครินทร์

สารบัญ

หน้า

แผนรองรับสถานการณ์ฉุกเฉิน
ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
(IT Contingency plan)

1. บทนำ

ปัจจุบัน มีการนำระบบสารสนเทศมาใช้ในการบริหารจัดการการเรียนการสอน และสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการเรียนการสอน การวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลาการ ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นจำเป็นจะต้องมีการจัดการฐานข้อมูล การเฝ้าระวัง การจัดเก็บและการดูแลรักษาข้อมูลสารสนเทศ เพื่อให้ เกิดความมั่นคงปลอดภัย และมีความพร้อมในการที่จะนำข้อมูลสารสนเทศดังกล่าวไปใช้งานได้ อย่างเต็มประสิทธิภาพตลอดเวลา

มหาวิทยาลัยราชภัฏราชนครินทร์ ได้นำระบบสารสนเทศมาใช้เพื่อช่วยเพิ่มประสิทธิภาพในการดำเนินงานของหน่วยงาน และให้บริการนักศึกษาตลอดจนบุคลากรได้รับความสะดวกมากยิ่งขึ้น ในขณะเดียวกันระบบสารสนเทศอาจได้รับความเสียหายจากการถูกโจมตี จากไวรัสคอมพิวเตอร์ จากบุคลากร จากปัญหาไฟฟ้า จากอัคคีภัย หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศ และส่งผลกระทบต่อการดำเนินงาน ดังนั้นเพื่อป้องกันและแก้ไขปัญหา จึงมีความจำเป็นที่จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบสารสนเทศ

2. วัตถุประสงค์

1. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน
2. เพื่อลดความเสียหายที่จะอาจเกิดแก่ระบบสารสนเทศ
3. เพื่อให้ระบบสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบสารสนเทศ
5. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบ ความปลอดภัยของฐานข้อมูลและสารสนเทศ

3. การวิเคราะห์ความเสี่ยง

มหาวิทยาลัยราชภัฏราชนครินทร์ มีการนำระบบสารสนเทศเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการความเสี่ยงด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น รวมไปถึงแนวทางในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ อันจะส่งผลกระทบต่อระบบสารสนเทศ เพื่อให้ระบบสารสนเทศทำงานได้อย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้สามารถนำเทคโนโลยีสารสนเทศมาใช้สนับสนุนการเรียนการสอน และการปฏิบัติงานให้เกิดประโยชน์สูงสุด

การวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏราชนครินทร์ พบประเภทความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ ดังนี้

1. ความเสี่ยงด้านเทคนิค เป็นความเสี่ยงที่อาจเกิดขึ้นจากระบบคอมพิวเตอร์ เครื่องมือและอุปกรณ์ขัดข้อง การถูกโจมตีจากไวรัสหรือโปรแกรมไม่ประสงค์ดี ถูกก่อกวนและโจมตีแฮกเกอร์ ถูกเจาะทำลายระบบจากแครกเกอร์ทั้งที่เกิดจากความตั้งใจและไม่ตั้งใจ ระบบไฟฟ้าขัดข้อง เป็นต้น
2. ความเสี่ยงด้านผู้ปฏิบัติงาน เป็นความเสี่ยงที่อาจเกิดขึ้นจากการดำเนินการ การจัดความสำคัญในการเข้าถึงข้อมูลไม่เหมาะสมกับการใช้งานหรือการให้บริการ โดยผู้ใช้อาจเข้าสู่ระบบสารสนเทศ หรือใช้ข้อมูลต่างๆ เกินกว่าอำนาจหน้าที่ของตนเองที่มีอยู่ และอาจทำให้เกิดความเสียหายต่อข้อมูลสารสนเทศได้
3. ความเสี่ยงด้านภัยหรือสถานการณ์ฉุกเฉิน เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น ไฟไหม้ อาคารถล่ม การชุมนุมประท้วง หรือความไม่สงบเรียบร้อยในบ้านเมือง เป็นต้น
4. ความเสี่ยงด้านการบริหารจัดการ เป็นความเสี่ยงจากการแนวนโยบายในการบริหารจัดการที่อาจส่งผลกระทบต่อการดำเนินการด้านเทคโนโลยีสารสนเทศ

จากผลการวิเคราะห์และตรวจสอบความเสี่ยงด้านเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยราชภัฏราชนครินทร์ ดังที่กล่าวมาแล้ว พบว่ามีความเสี่ยงที่อาจเป็นอันตรายต่อระบบสารสนเทศ ดังนั้น เพื่อให้ระบบสารสนเทศของ มหาวิทยาลัยราชภัฏราชนครินทร์ สามารถใช้งานได้อย่างประสิทธิภาพ มีความมั่นคงปลอดภัย และสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบสารสนเทศ

4. การวิเคราะห์ปัญหาความรุนแรงของเหตุการณ์ภัยพิบัติ

4.1 วิเคราะห์เหตุการณ์ภัยพิบัติ ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบสนเทศของมหาวิทยาลัย จำแนกเป็น 2 กลุ่มหลักๆ ได้แก่

ภัยพิบัติจากภายนอก

1) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทบต่อสถานที่ตั้งของเครื่องคอมพิวเตอร์แม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย การจลาจล ชุมนุมประท้วง แผ่นดินไหว ฯลฯ

2) ระบบเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเตอร์เน็ตเกิดความขัดข้อง

3) การบุกรุกหรือโจมตีระบบควบคุมสารสนเทศจากภายนอก เพื่อสร้างความเสียหายหรือทำลายระบบข้อมูล

4) ระบบกระแสไฟฟ้าขัดข้อง /ไฟฟ้าดับ /ไฟกระชาก

5) ไวรัสคอมพิวเตอร์

ภัยพิบัติจากภายใน

1) ระบบเครื่องคอมพิวเตอร์แม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย ถูกทำลาย

2) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในมหาวิทยาลัย

3) เจ้าหน้าที่หรือบุคลากรของมหาวิทยาลัย ขาดความรู้ความเข้าใจในการใช้อุปกรณ์คอมพิวเตอร์ ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อาจทำให้ระบบสารสนเทศเสียหาย

4.2 การประเมินสถานการณ์และกำหนดระดับความรุนแรง

เมื่อทำการวิเคราะห์เหตุการณ์ภัยพิบัติแล้ว จะทำการประเมินและกำหนดระดับความรุนแรง ภัยพิบัติเพื่อเตรียมการตอบสนองต่อเหตุการณ์ที่ไม่ปลอดภัย จัดเตรียมระบบบันทึกและวิเคราะห์เหตุการณ์ต่างๆ ซึ่งสรุปเป็นข้อมูล ดังนี้

สถานการณ์หรือภาวะฉุกเฉิน	**ระดับความรุนแรง (คะแนน 5 คะแนน)**			**จัดเรียงลำดับ**	
	ต่อระบบงาน	**ต่อพันธกิจ**	**ต่อประชาชน**	**รวม**	**จัดลำดับ**
กรณีไฟไหม้	5	5	5	15	1
กรณีโดนแทรกแซงระบบ	5	4	3	12	2
กรณีไฟฟ้าดับ	5	3	2	10	3
กรณีแผ่นดินไหว	3	2	3	8	4
กรณีจลาจล การชุมนุม / เหตุการณ์ความไม่สงบ	2	2	3	7	5

5. แผนรองรับสถานการณ์ฉุกเฉิน

5.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

5.1.1 กรณีการป้องกันไวรัสล้มเหลว

1) จำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

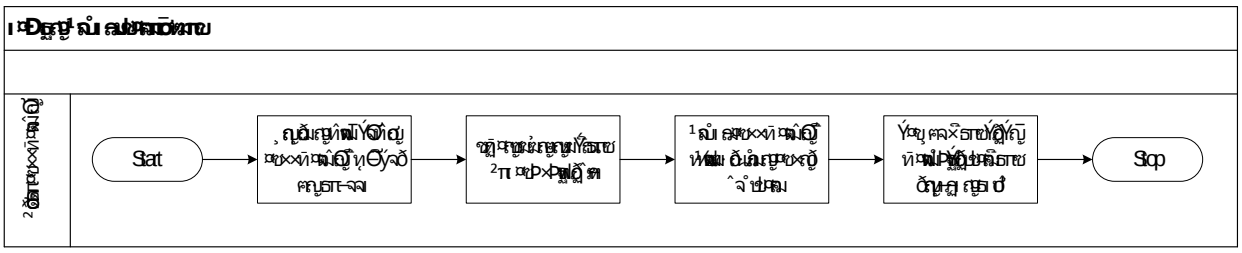
2) วิเคราะห์หาสาเหตุ และผลกระทบที่เกิดจากไวรัสที่ระบาด

3) ดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัส

4) ตรวจสอบ ติดตามเครื่องที่ติดไวรัส และดำเนินการแก้ไข

5) กรณีที่เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่หน่วยงานเทคโนโลยีสารสนเทศและการสื่อสาร สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทราบ หรือกรณีมีเหตุอันทำให้หน่วยงานเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ หน่วยงานเทคโนโลยีสารสนเทศและการสื่อสารจะต้องประกาศให้ทุก คณะฯ/หน่วยงาน ทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสล้มเหลว



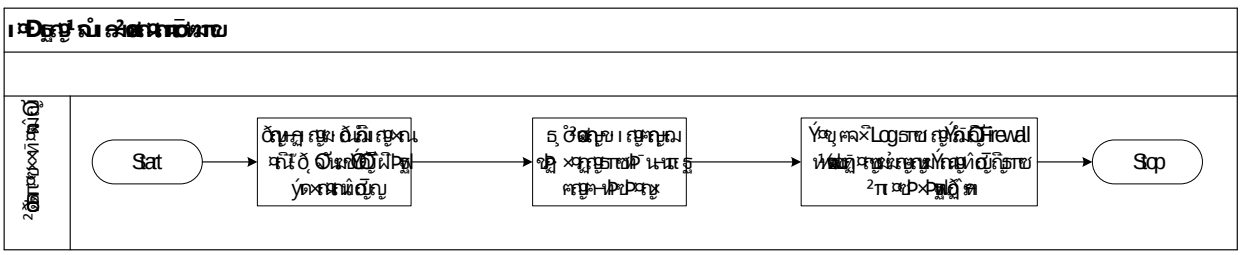
5.1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

1) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบเครือข่ายและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

2) ผู้ดูแลระบบแจ้งหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศและการสื่อสารให้ทราบโดยด่วน

3) ดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่าง ๆ ที่ทำให้ผู้บุกรุกเข้ามาได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว



5.1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

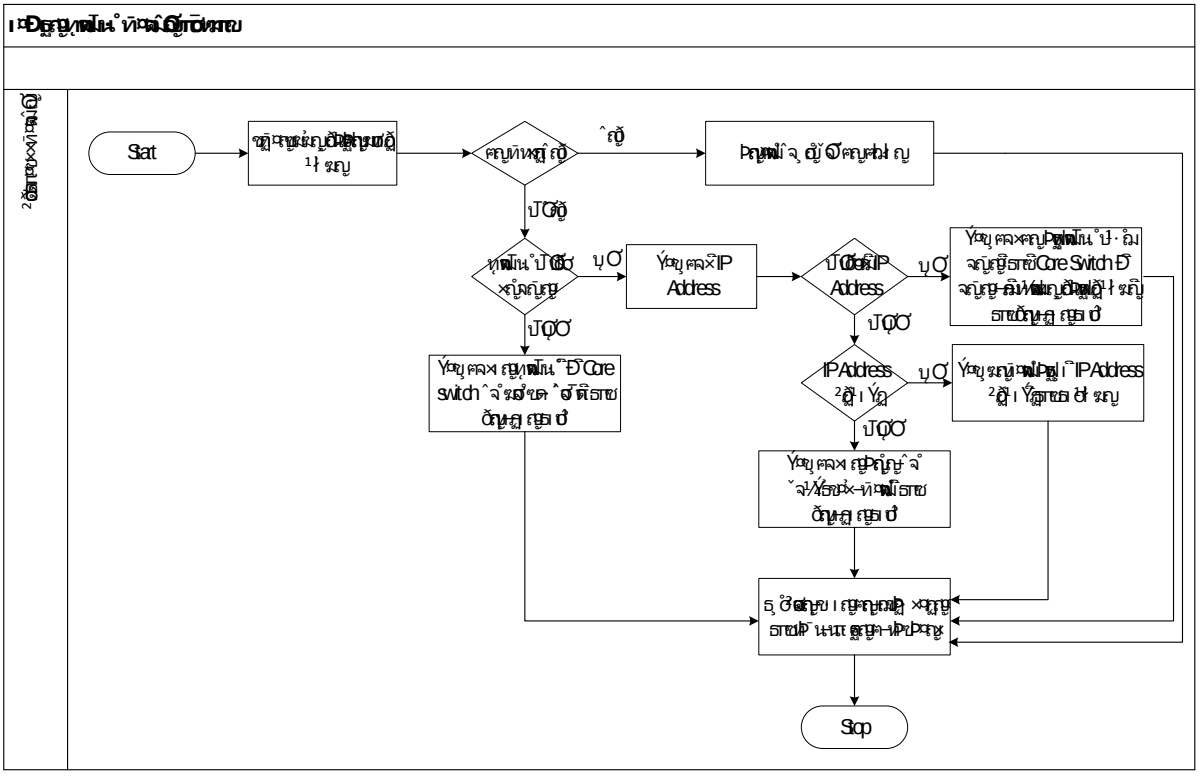
1) รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

2) หากสายเคเบิ้ลขาด ให้รีบแจ้งผู้บริหารทราบ พร้อมทั้งติดต่อบริษัทเพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

3) หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคารและ อุปกรณ์กระจายสัญญาณเครือข่ายที่ติดตั้งอยู่ ณ อาคารนั้นๆ

4) หากอุปกรณ์กระจายสัญญาณเครือข่ายเสีย ให้รีบแจ้งผู้บริหารทราบ และดำเนินการจัดหาทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



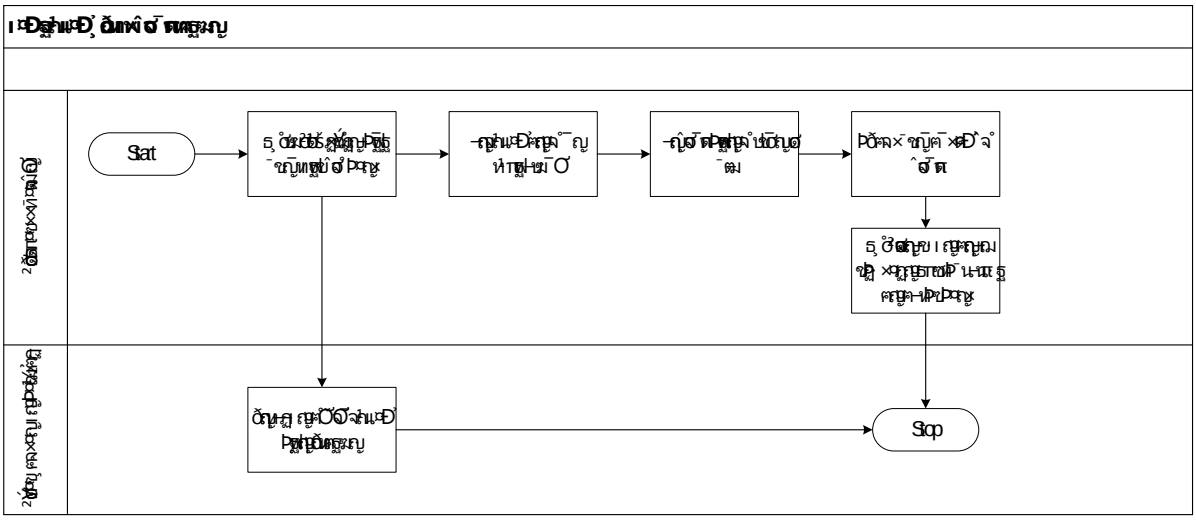
5.1.4 กรณีอุปกรณ์จัดเก็บข้อมูล หรือคอมพิวเตอร์เสียหาย

1) แจ้งผู้ปฏิบัติงานที่เกี่ยวข้องทราบ และดำเนินการสำรองข้อมูล

2) ดำเนินการจัดหาอุปกรณ์มาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูล

3) ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



5.1.5 กรณีไฟฟ้าขัดข้อง หรือไฟฟ้าดับ

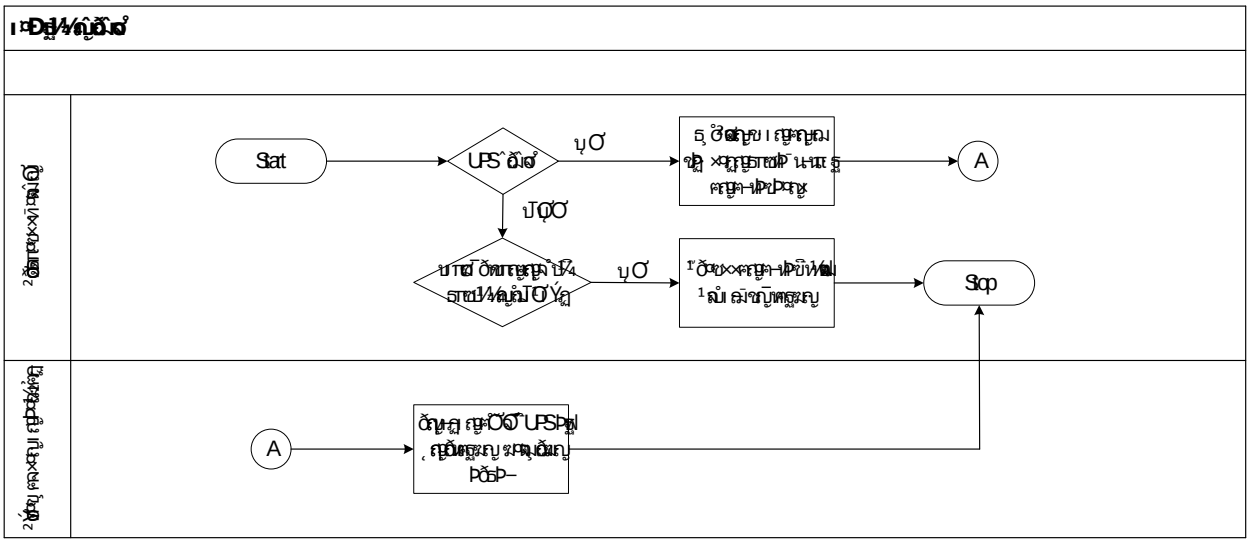
1) ระบบสนเทศสารสนเทศมีเครื่องสำรองไฟฟ้าซึ่งสามารถสำรองกระแสไฟฟ้าได้ประมาณ 2 ชั่วโมง

2) หากใกล้ครบ 2 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังหัวหน้างานเทคโนโลยีสารสนเทศและการสื่อสาร

3) ผู้ดูแลดำเนินการปิดระบบสารสนเทศเพื่อป้องกันความเสียหาย

4) หากเครื่องสำรองไฟฟ้าเกิดความเสียหาย แจ้งผู้บริหารทราบ เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง



5.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่างๆ

5.2.1 กรณีไฟไหม้

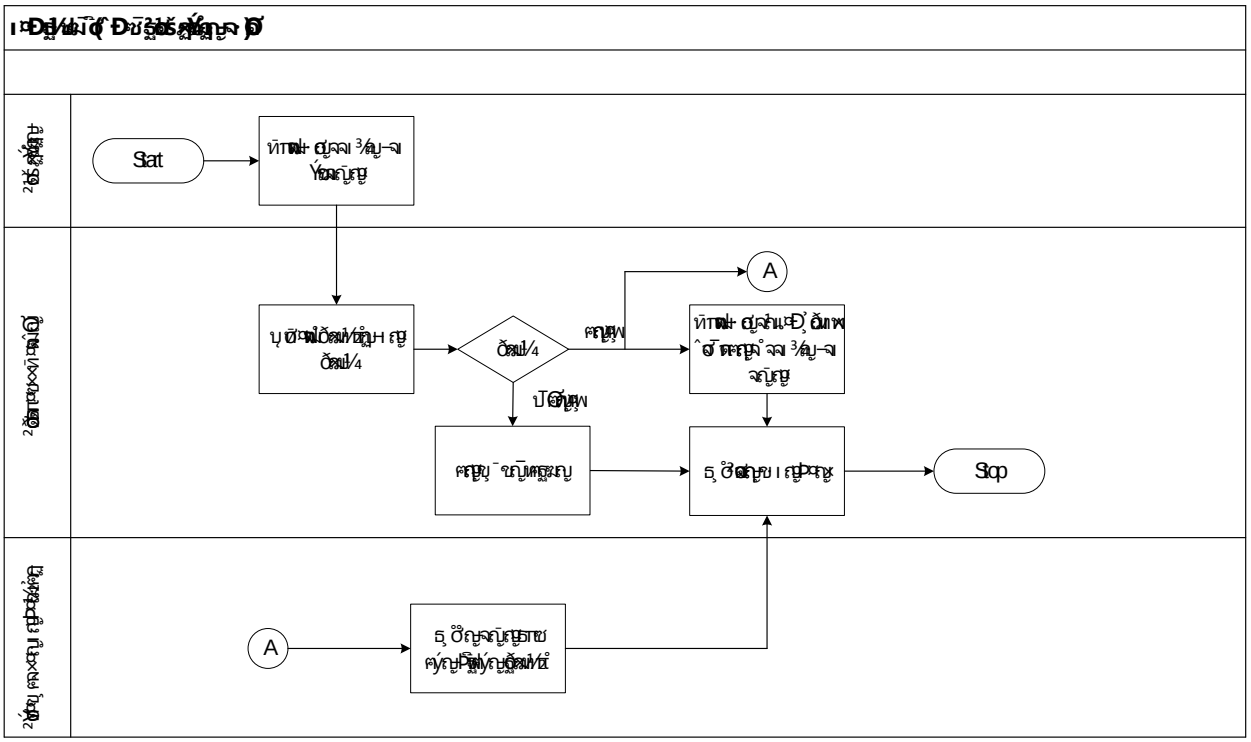
1) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับเพลิง

2) หากไม่สามารถควบคุมเพลิงได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานโทรแจ้งงานอาคารและสถานที่ทันที โทร. 6073 หรือหัวหน้างานอาคารและสถานที่ โทร. 038-500000 และโทรแจ้งสถานีดับเพลิง อำเภอเมืองฉะเชิงเทรา โทร. 038511061

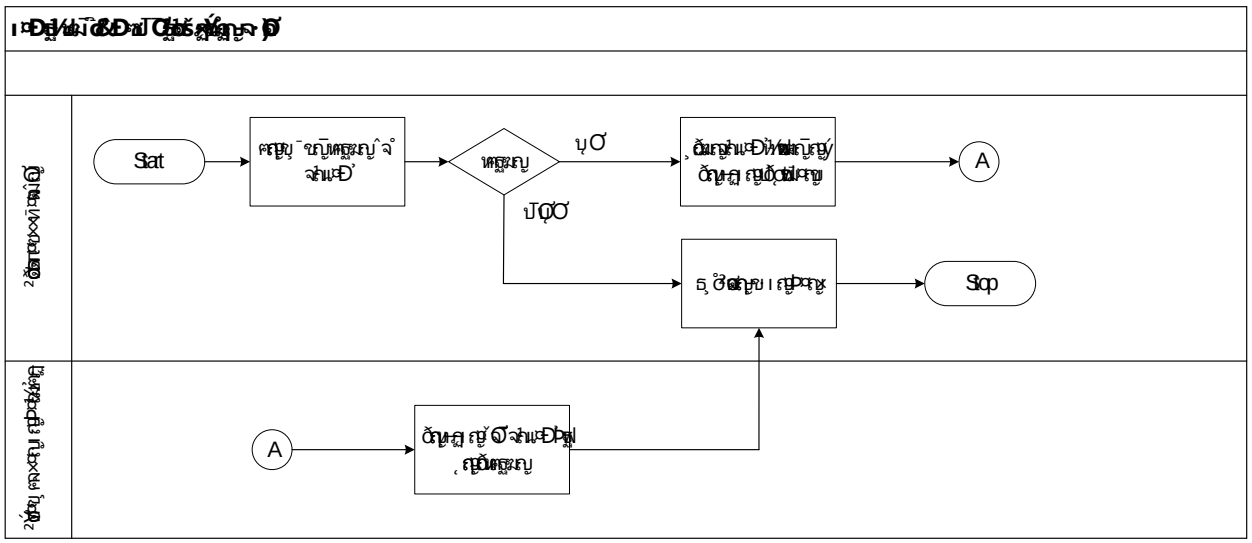
3) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และ/หรือ ระบบดับไฟอัตโนมัติ

4) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 1-2 ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะมีผู้ปฏิบัติงานอยู่)



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้ (ขณะไม่มีผู้ปฏิบัติงานอยู่)



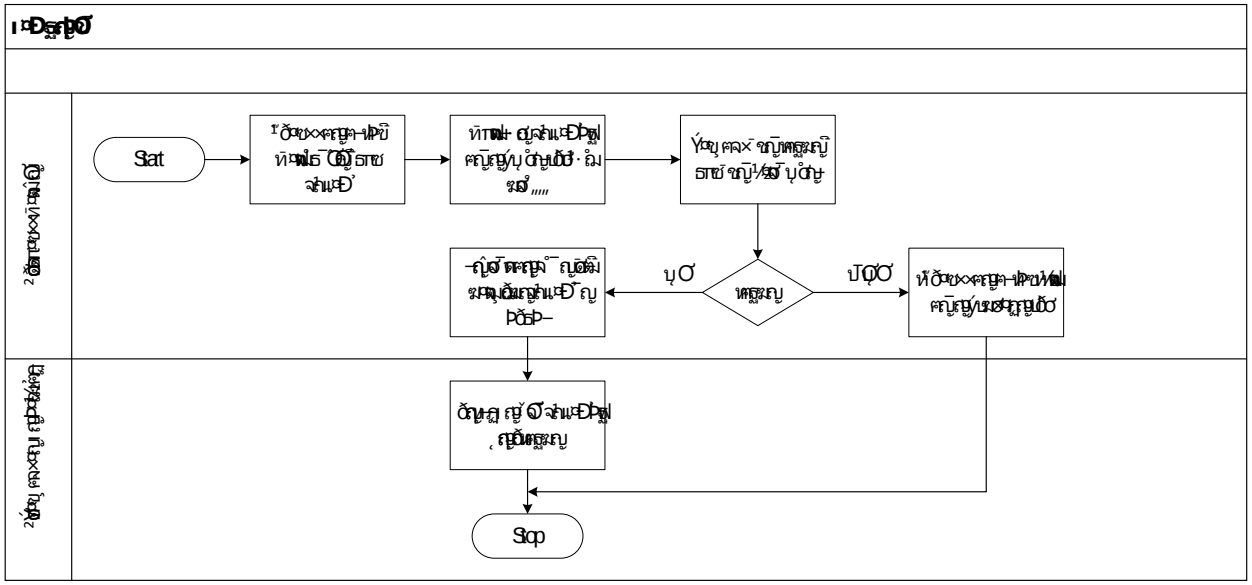
5.2.2 กรณีน้ำท่วม

1) ผู้ดูแลระบบปิดระบบ และทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ ที่ยังสามารถใช้งานได้ไปติดตั้ง ณ ชั้น 5 อาคาร อาคารราชนครินทร์

2) ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

3) ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถระบบสารสนเทศทำงานได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีน้ำท่วม



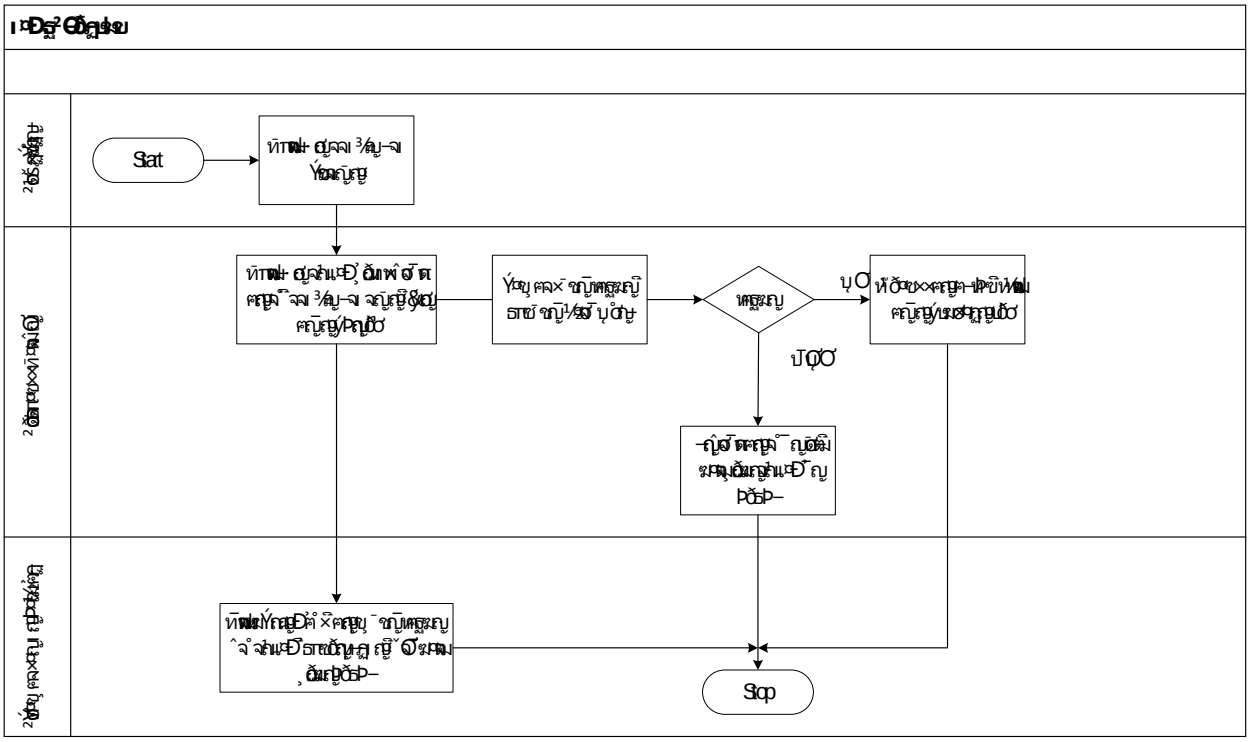
5.2.3 กรณีแผ่นดินไหว/อาคารถล่ม

1) ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร

2) ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้

3) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีแผ่นดินไหว



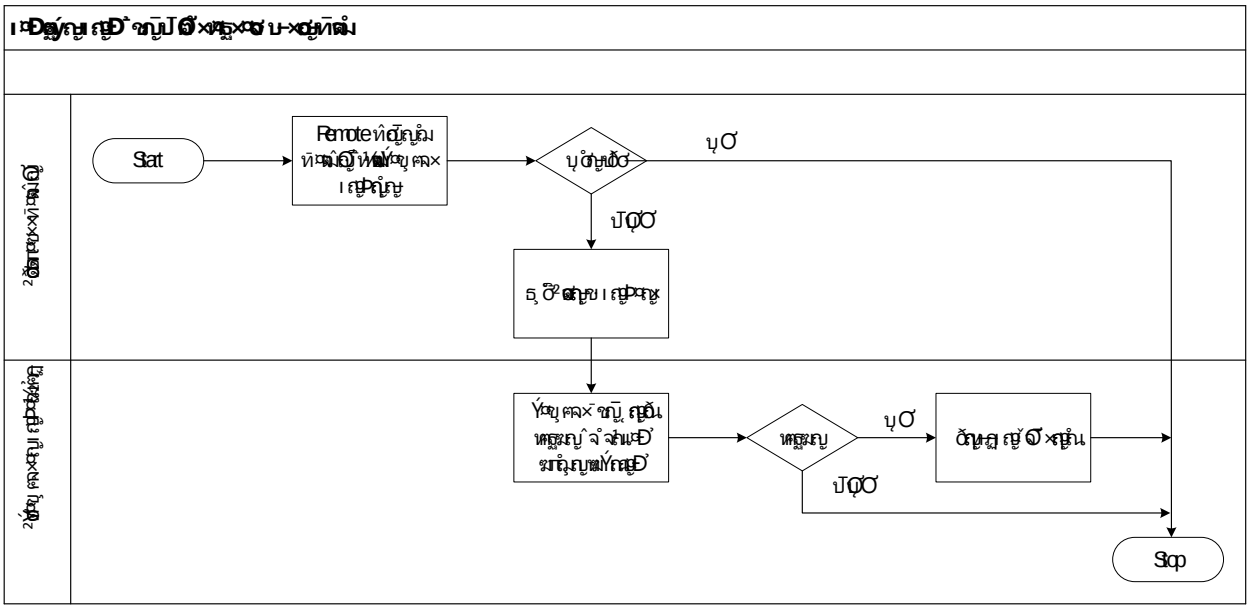
5.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

5.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง เป็นต้น

1) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบต้อง Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งหัวหน้าหน่วยงานเทคโนโลยีสารสนเทศและการสื่อสารทราบ

2) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สิน ตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้แจ้งผู้บริหารทราบ พร้อมดำเนินการติดต่อบริษัทดำเนินการซ่อมแซมแก้ไขหากจำเป็น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



5.4 สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

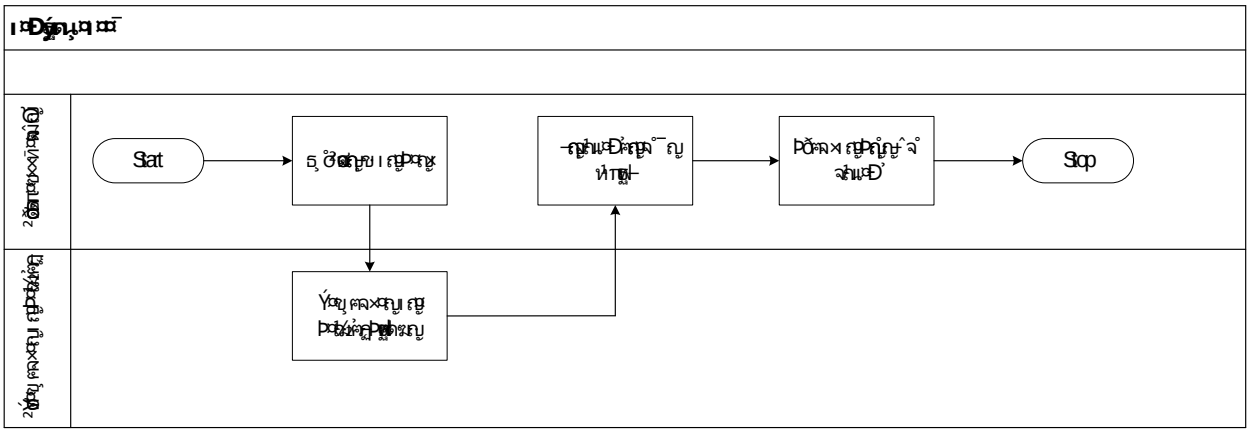
5.4.1 กรณีโจรกรรม

1) ผู้ปฏิบัติงานแจ้งผู้บริหารให้ทราบโดยด่วน

2) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

3) ผู้ดูแลระบบบริบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีโจรกรรม

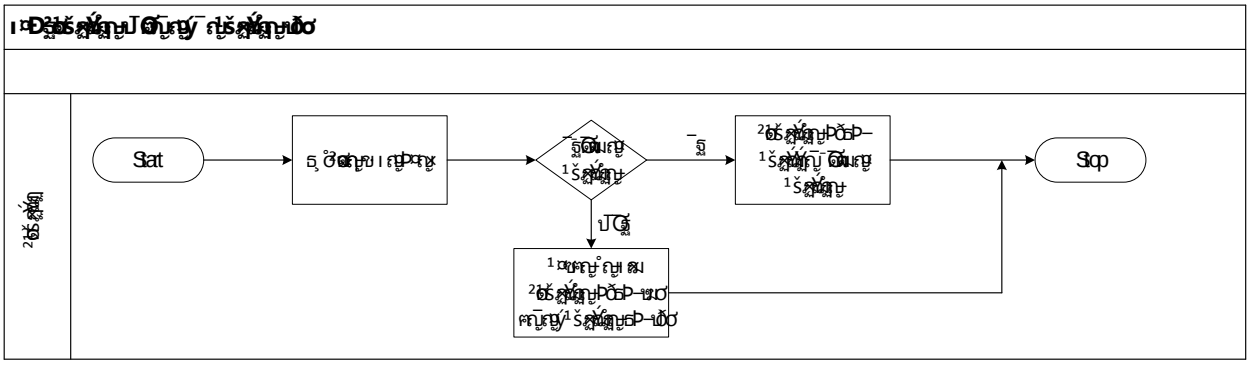


5.4.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

1) แจ้งผู้บังคับบัญชาทราบ

2) ปฏิบัติตามคู่มือการปฏิบัติงาน (Workflow) หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



6. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบสารสนเทศเป็น ดังนี้

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

1.1 รองอธิการบดีกิจการพิเศษ

1.2 ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

1.3 รองผู้อำนวยการเทคโนโลยีสารสนเทศและการสื่อสาร

1.4 หัวหน้าหน่วยงานเทคโนโลยีสารสนเทศและการสื่อสาร

2. ผู้รับผิดชอบการปฏิบัติงานระบบเครือข่าย ห้องแม่ข่ายและศูนย์ข้อมูล ได้แก่

2.1 นายบุญญา วาสี นักวิชาการคอมพิวเตอร์

2.2 นายนภดล เวศวงศ์ษาทิพย์ นักวิชาการคอมพิวเตอร์

2.3 นายภิญโญ สารนาถ วิศวกร

3. ผู้รับผิดชอบการปฏิบัติงานระบบสารสนเทศและฐานข้อมูล ได้แก่

3.1 นายบุญญา วาสี นักวิชาการคอมพิวเตอร์

4. ผู้รับผิดชอบประสานงานหน่วยงานที่เกี่ยวข้อง ได้แก่

4.1 นางสาวพิไลพร วงษา นักวิชาการคอมพิวเตอร์

5. ผู้รรับผิดชอบตรวจสอบรายการทรัพย์สิน ได้แก่

5.1 นางสาวพิไลพร วงษา นักวิชาการคอมพิวเตอร์

แผนรองรับสถานการณ์ฉุกเฉินฉบับนี้ ได้ผ่านการพิจารณาจากคณะกรรมการบริหารเทคโนโลยีดิจิทัล มหาวิทยาลัยราชภัฏราชนครินทร์ เพื่อให้เจ้าหน้าที่ใช้เป็นแนวทางในการดำเนินการรับมือกับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง
พฤษภาคม 2564