แผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

(IT Contingency Plan)

1. หลักการและเหตุผล

ระบบข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ โดยมีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานมากขึ้น ประกอบกับการพัฒนาเทคโนโลยีสารสนเทศเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศ อันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากร ซึ่งข้อมูลสารสนเทศต่างๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้นจำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการบริหารราชการได้อย่างมีประสิทธิภาพ แม้ว่าด้วยการปฏิบัติการจะมีข้อกำหนดที่จัดทำไว้เพื่อเป็นคู่มือปฏิบัติงานของเจ้าหน้าที่ แต่ก็ยังมีข้อจำกัดด้านความรู้และทักษะของเจ้าหน้าที่ อุปกรณ์ เครือข่ายการสื่อสาร ระบบไฟฟ้าที่อาจเกิดความขัดข้องและภัยจากธรรมชาติ จนเป็นเหตุให้การทำงานหยุดชะงักและเกิดความเสียหาย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศตระหนักถึงความสำคัญของระบบฐานข้อมูลสารสนเทศ ซึ่งอาจมีทั้งปัจจัยภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลสารสนเทศรวมทั้งอุปกรณ์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลสารสนเทศที่ใช้ในการบริหารจัดการ ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ ขึ้นเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

2. วัตถุประสงค์

2.1 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

2.2 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.4 เพื่อเป็นการลดความเสียหายและเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ

3. คำนิยาม

“ระบบสารสนเทศ” หมายความว่า ระบบข้อมูลข่าวสารของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาช่วยในการสร้างระบบสารสนเทศที่มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิสามารถนำมาใช้ในการบริหาร การพัฒนาและการควบคุม มีองค์ประกอบดังนี้

1. ระบบคอมพิวเตอร์ (Computer System)
2. ระบบสื่อสาร (Communication System)
3. ระบบสารสนเทศ (Information System)

“ภัยคุกคาม” หมายความว่า อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยคน สิ่งต่างๆ หรือเหตุการณ์อื่น ๆ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูล ข่าวสารของระบบสารสนเทศเสียหาย ถูกทำลาย ปฏิเสธการทำงาน หรือ ถูกโจรกรรมข้อมูล

“ระบบสื่อสาร” หมายความว่า ระบบที่ใช้ในการรับ - ส่ง และเป็นสื่อกลางในระบบสื่อสารที่ใช้การส่งผ่านข้อมูล ทั้งระบบทางสาย และระบบไร้สาย รวมทั้งอุปกรณ์อื่นๆ เช่น ฮับ สวิชชิ่ง เราท์เตอร์ เป็นต้น

“ระบบคอมพิวเตอร์” หมายความว่า ระบบที่ประกอบด้วย Hardware, Software และ People ware ที่ใช้ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ

“สารสนเทศ” หมายความว่า ข้อเท็จจริงที่ได้จากการวิเคราะห์ข้อมูล ให้มีความหมาย โดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของ ตัวเลข ข้อความหรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ

“พื้นที่ใช้งานระบบสารสนเทศ” หมายความว่า พื้นที่ที่ใช้ติดตั้งระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสารสนเทศอื่นๆ หรือเตรียมข้อมูล เก็บอุปกรณ์คอมพิวเตอร์ ในที่นี้หมายถึง ห้องปฏิบัติการคอมพิวเตอร์เครือข่ายสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ศูนย์นนทบุรี (Network Operation Center: NOC)

“เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสารหรือการส่งข้อมูลกันระหว่างระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

4. วิเคราะห์ปัจจัยความเสี่ยง

ปัจจัยที่อาจเกิดและทำให้เสียหายกับระบบฐานข้อมูลสารสนเทศ ของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ได้แก่

4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

1. กรณีเกิดภัยคุกคามทางไซเบอร์
2. กรณีการเชื่อมโยงเครือข่ายล้มเหลว
3. กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)
4. กรณีไฟฟ้าขัดข้อง

4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

1. กรณีไฟไหม้
2. กรณีน้ำท่วม
3. กรณีแผ่นดินไหว

4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาด

1. กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้
2. กรณีหลังเหตุการณ์ความไม่สงบ

4.4 สถานการณ์ฉุกเฉินที่เกิดจากบุคคล

1. กรณีโจรกรรม
2 .กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

5. แนวทางการป้องกันและการเตรียมการเบื้องต้น

5.1 การประกาศแผน (Activation)

มีการประกาศใช้แผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ ขึ้นเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันแสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย

5.2 กระบวนการดำเนินงาน (Procedure)

มีการเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติ โดยเมื่อเกิดเหตุการณ์ฉุกเฉินจะต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของปัญหา ระบบงานต่าง ๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหา

5.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกรณีที่มีความจำเป็นฉุกเฉิน

5.4 การจัดเตรียมอุปกรณ์ที่จำเป็น (Preparation)

มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์ขัดข้องไม่สามารถใช้งานได้โดยมีการติดตั้งอุปกรณ์ที่ปลายทางเพื่อรองรับและทดแทนอุปกรณ์หลักได้

5.5 การสำรองข้อมูล (Backup)

มีนโยบายการสำรองข้อมูลระบบคอมพิวเตอร์สำรองและแผนฉุกเฉิน (Backup and IT Continuity Plan) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นเมื่อข้อมูลเสียหาย ถูกทำลาย หรือการเปลี่ยนแปลงข้อมูลจากผู้บุกรุก การสำรองข้อมูลในส่วนของข้อมูล (Data Backup) เป็นประจำทุกวัน และสำรองข้อมูลทั้งระบบ (System Backup) เป็นประจำทุกเดือนเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายโดยไวรัสคอมพิวเตอร์ หรือผู้บุกรุก หรือมีการเปลี่ยนแปลงข้อมูล เป็นต้น

5.6 การเสริมสร้างความปลอดภัย (Enhancing)

5.6.1 มีมาตรการควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากมีความจำเป็นให้มีเจ้าหน้าที่ที่รับผิดชอบนำเข้าไป

5.6.2 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

5.6.3 มีการติดตั้งอุปกรณ์เพื่อใช้ในการตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี ซึ่งจะทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้า-ออกภายในเครือข่ายที่มีลักษณะการทำงานเป็นความเสี่ยงเพื่อป้องกันการบุกรุกผ่านเครือข่าย

5.6.4 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

5.6.5 การเรียกใช้ระบบสารสนเทศผู้ใช้ระบบจะต้องมีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ ตามอำนาจหน้าที่และความรับผิดชอบ

5.6.6 มีการปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และพรบ. การรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562 เพื่อเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์

6. มาตรการในการป้องกันและแก้ไขปัญหา

6.1 กรณีเครื่องลูกข่าย

6.1.1 ในกรณีที่เครื่องคอมพิวเตอร์ไม่สามารถใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่แจ้งเหตุแก่ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลฐานข้อมูลสารสนเทศ หรือในกรณีเกิดจากไม่สามารถให้บริการด้านเครือข่ายหรือระบบสารนเทศได้ ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศประกาศให้ทุกหน่วยงานในมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิทราบ

6.1.2 กรณีเกิดการขัดข้องเนื่องจากไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ตัดการเชื่อมต่อระบบเครือข่าย

6.2 กรณีเครื่องแม่ข่ายบริการ (Server)

6.2.1 ตัดการเชื่อมต่อระบบเครือข่าย จากนั้นให้ปฏิบัติตามแผนรับมือภัยคุกคามทางไซเบอร์

6.2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ทั้งนี้การปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ให้พิจารณาจากระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองกระแสไฟฟ้า

6.2.3 กรณีไฟไหม้ ให้ตัดระบบจ่ายไฟและใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

6.2.4 ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีสถานการณ์ยังไม่ปลอดภัยให้ขนย้ายเครื่องและอุปกรณ์ไปไว้ในที่ปลอดภัย

7. แผนรองรับสถานการณ์ฉุกเฉิน

7.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

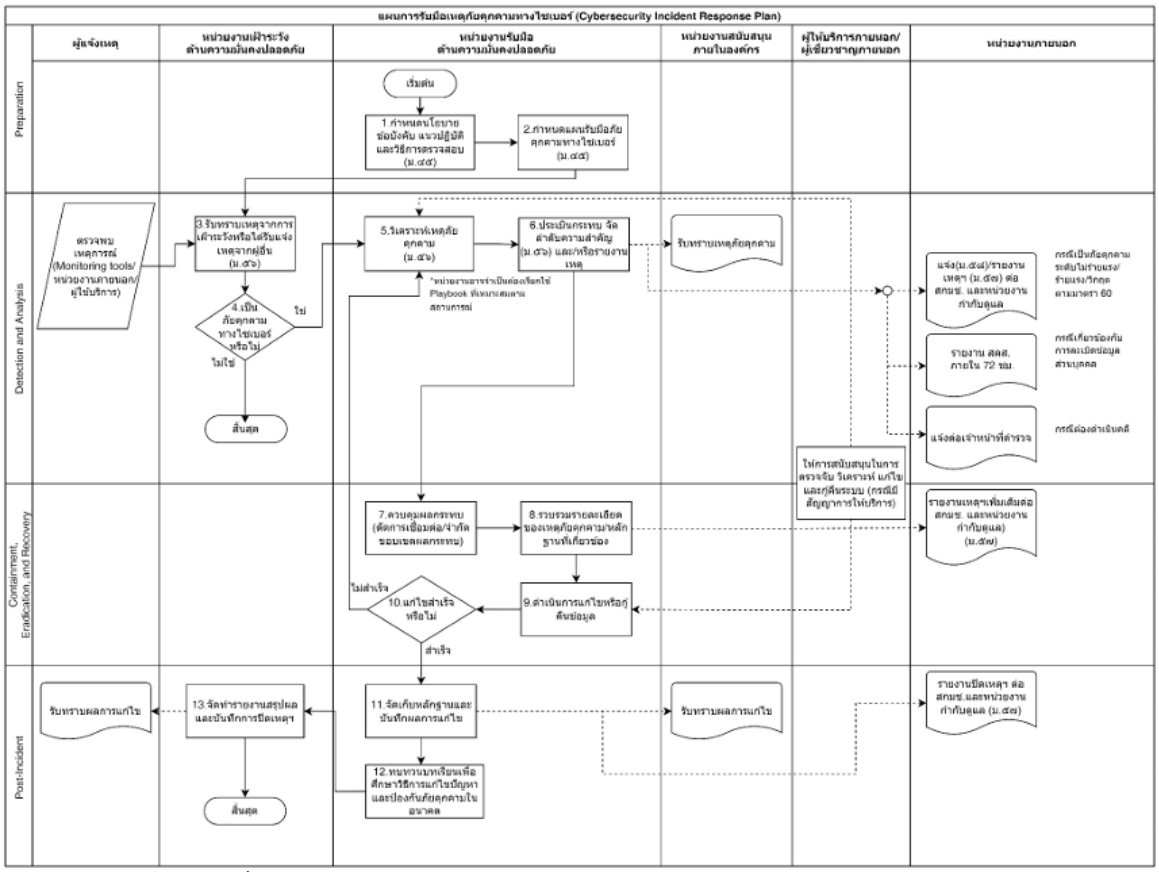
1) กรณีเกิดภัยคุกคามทางไซเบอร์

- เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

- ปฏิบัติตามแผนรับมือภัยคุกคามทางไซเบอร์

- กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุ ให้เจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ สำนักวิทยบริการและเทคโนโลยีสารสนเทศจะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

แผนผังแสดงขั้นตอนการรับมือภัยคุกคามทางไซเบอร์



2) กรณีการเชื่อมโยงเครือข่ายล้มเหลว

- รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

- ตรวจสอบเครื่องแม่ข่ายให้บริการทางด้านอินเตอร์เน็ต(DNS และ DHCP) ว่าทำงานปกติหรือไม่ หากพบปัญหาให้รีบแก้ไขทันทีหรือประสานงานผู้ที่เกี่ยวข้อง

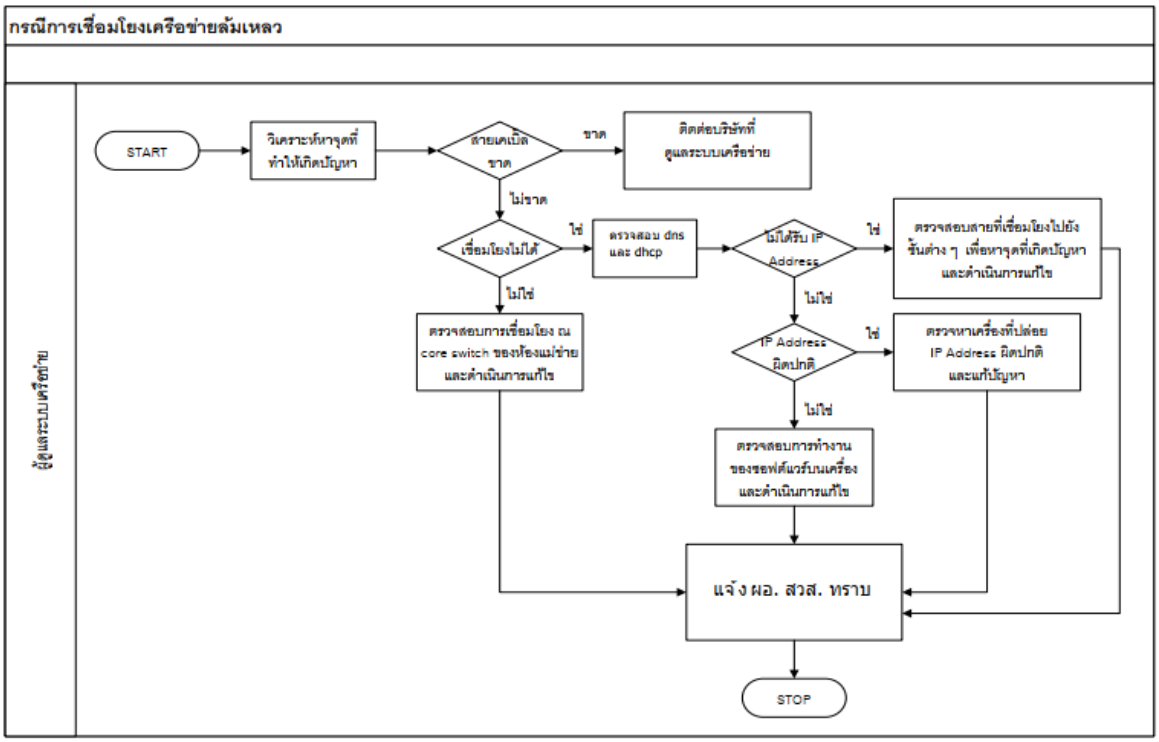
- ตรวจสอบอุปกรณ์เครือข่าย ว่าทำงานปกติหรือไม่ หากพบปัญหาให้รีบแก้ไขทันทีหรือประสานงานผู้ที่เกี่ยวข้อง

- หากพบปัญหาในส่วนผู้ให้บริการเครือข่าย ให้รีบประสานงานแก้ไขทันที

- หากสายคเบิลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

- หากเชื่อมโยงเครือข่ายไม่ได้ ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อของแต่ละชั้นภายในอาคาร

แผนผังแสดงขั้นตอนการรับมือกรณีการเชื่อมโยงเครือข่ายล้มเหลว



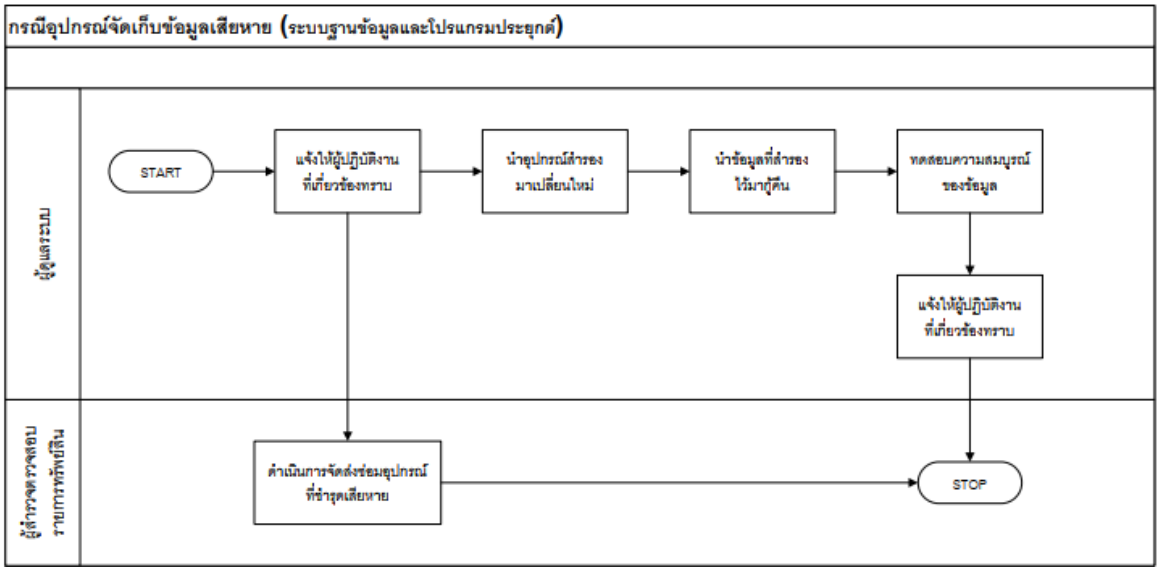
3) กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย (ระบบฐานข้อมูลและโปรแกรมประยุกต์)

- แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

- รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้ มากู้คืนข้อมูลโดยเร็ว

- ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

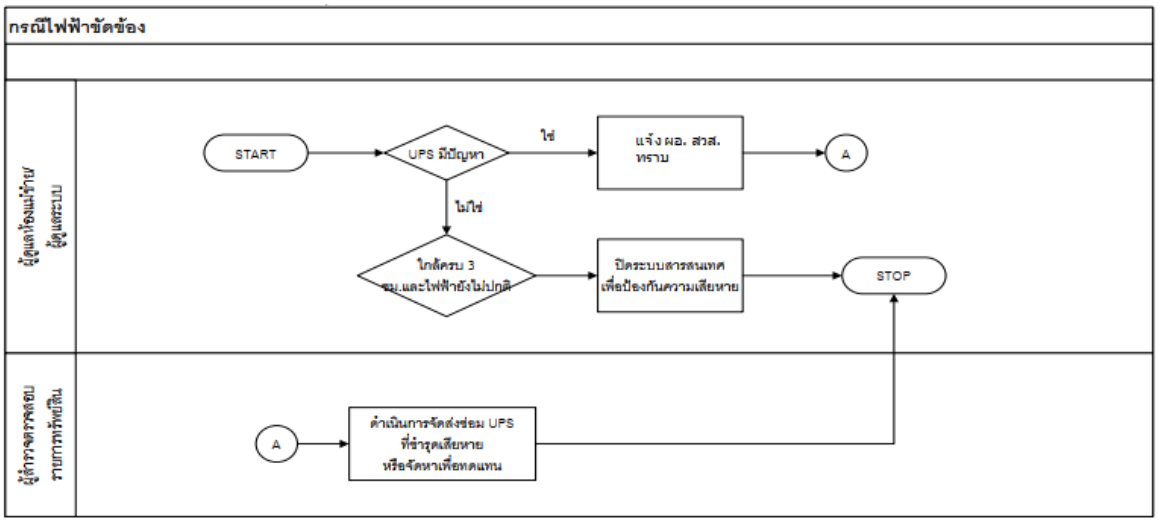
แผนผังแสดงขั้นตอนการรับมือกรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



4) กรณีไฟฟ้าขัดข้อง

- ระบบฐานข้อมูลสารสนเทศมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 3 ชั่วโมง
- หากใกล้ครบ 3 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการแจ้งเตือนไปยังบังคับบัญชา
- ผู้ดูแลดำเนินการปิดระบบเพื่อป้องกันความเสียหาย
- หากเครื่องสำรองไฟฟ้ามีปัญหา แจ้งผู้บังคับบัญชา เพื่อดำเนินการแก้ไขปัญหาที่เกิดขึ้น หรือจัดหาเครื่องสำรองไฟฟ้าทดแทน

แผนผังแสดงขั้นตอนการรับมือกรณีไฟฟ้าขัดข้อง

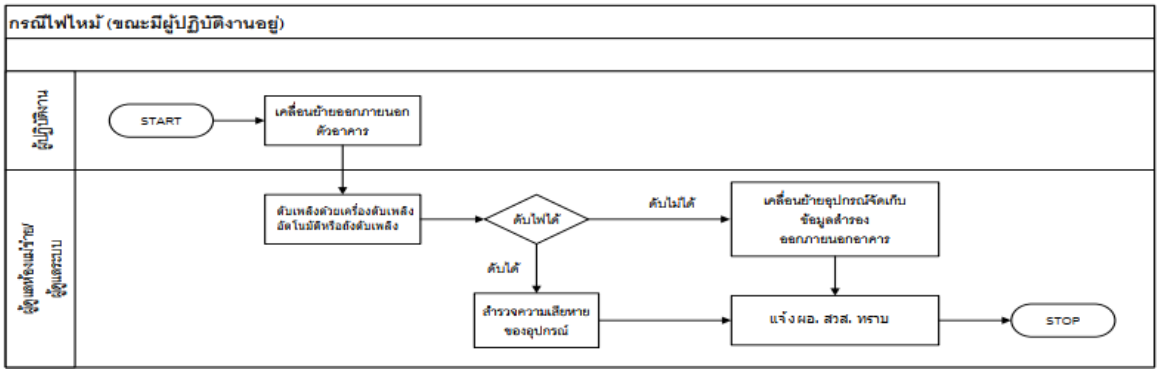


7.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยต่าง ๆ

1) กรณีฟไหม้ แยกเป็น ๒ กรณี กรณีไฟไหม้ขณะมีผู้ปฏิบัติงานอยู่ และกรณีไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงานอยู่

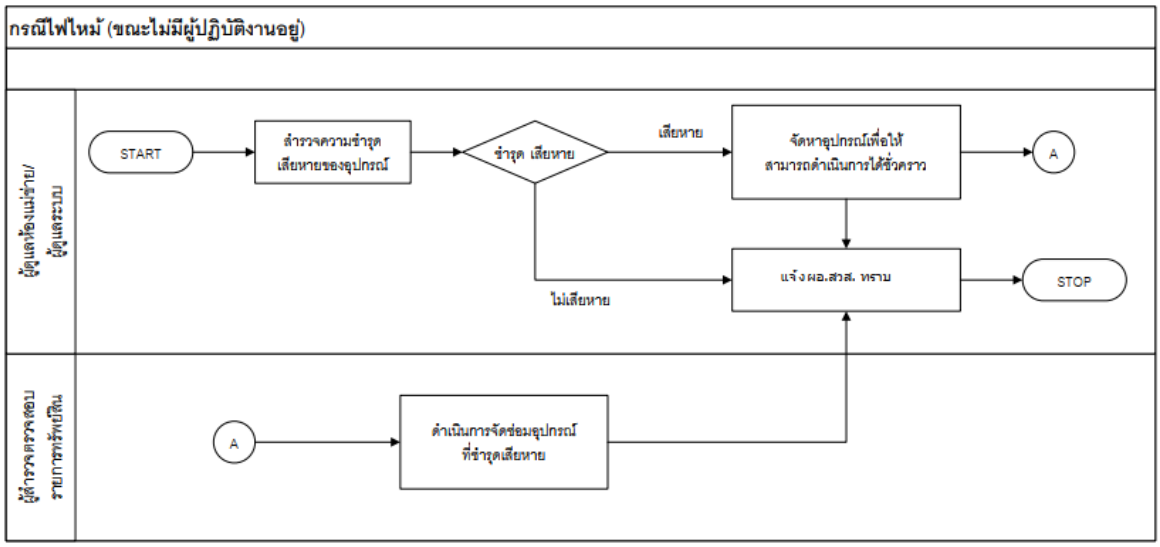
- หากเกิดไฟไหมัขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ
- หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ติดต่อประสานงานกับผู้ที่เกี่ยวข้องให้รีบดำเนินการแก้ไขอย่างเร่งด่วน

แผนผังแสดงขั้นตอนการรับมือกรณีไฟไหม้(มีผู้ปฏิบัติงาน)



- หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่าง ๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่าง ๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

แผนผังแสดงขั้นตอนการรับมือกรณีไฟไหม้(ไม่มีผู้ปฏิบัติงาน)

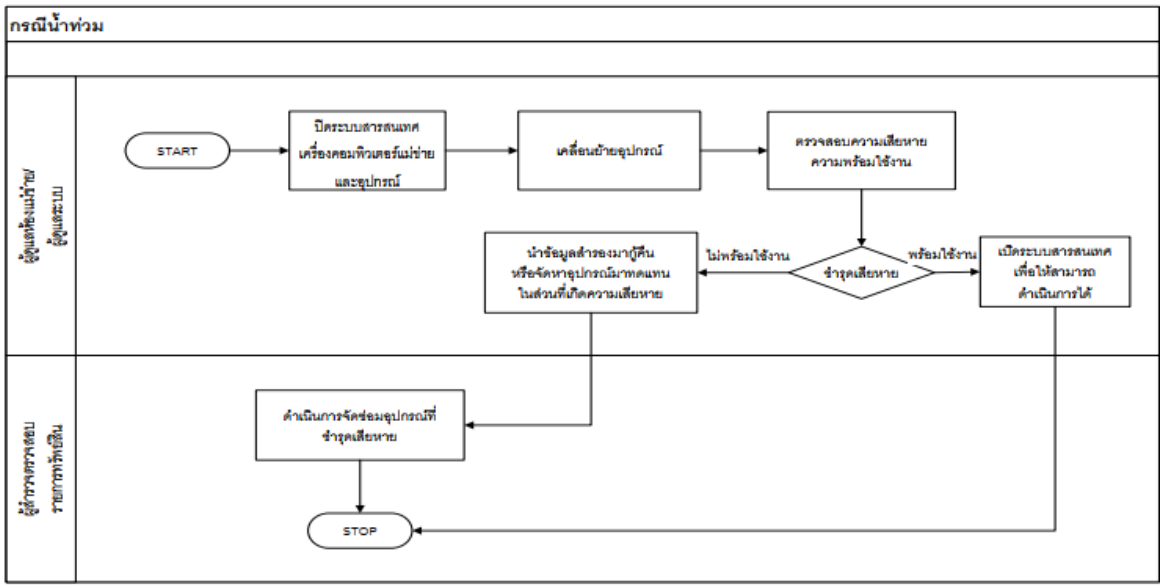


- อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

2) กรณีน้ำท่วม

- ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ
- ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย
- ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้ สามารถดำเนินการได้

แผนผังแสดงขั้นตอนการรับมือกรณีน้ำท่วม

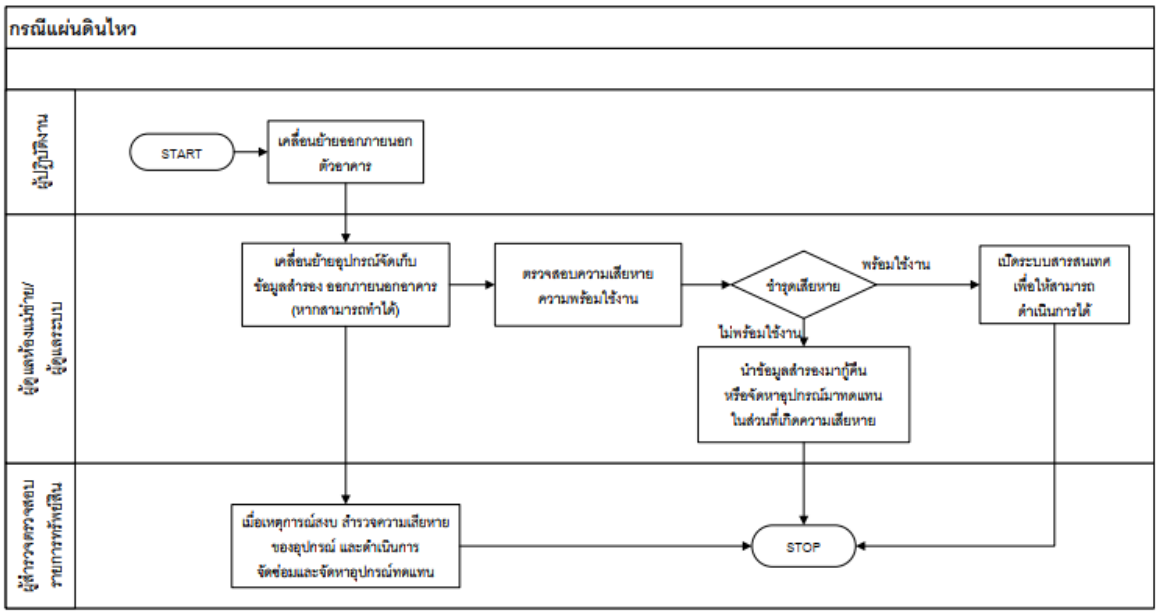


๓) กรณีแผ่นดินไหว

- ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร

- ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้
- เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุด เสียหาย และดำเนินการแก้ไขเพื่อให้ระบบ สามารถดำเนินการต่อไปได้

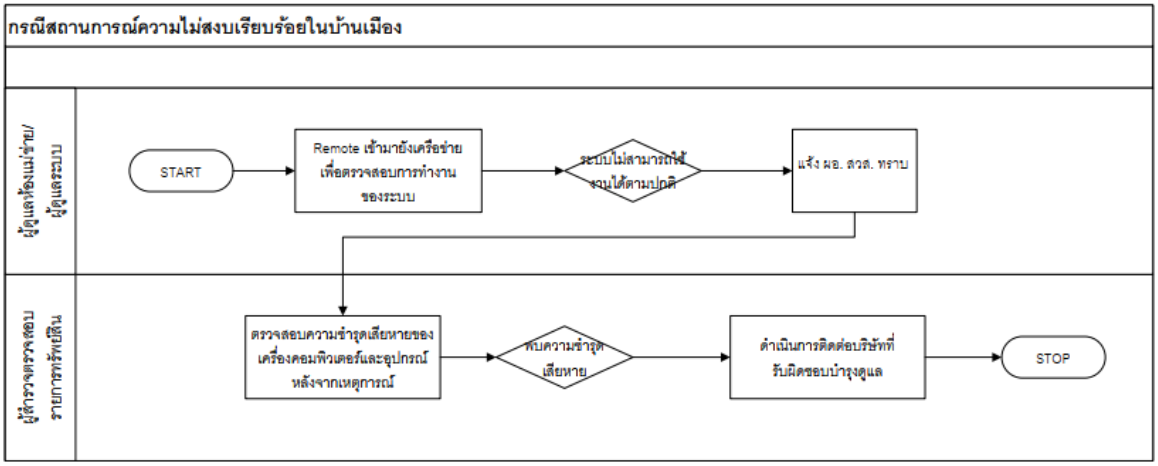
แผนผังแสดงขั้นตอนการรับมือกรณีแผ่นดินไหว



7.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมืองหรือโรคระบาดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

- กรณีที่ไม่สามารถข้ามาปฏิบัติงานได้ ผู้ดูแสระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ แจ้งบังคับบัญชาทราบ
- กรณีหลังเหตุการณ์ความไม่ส่งบ ให้ผู้ดูแสระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือกรณีสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

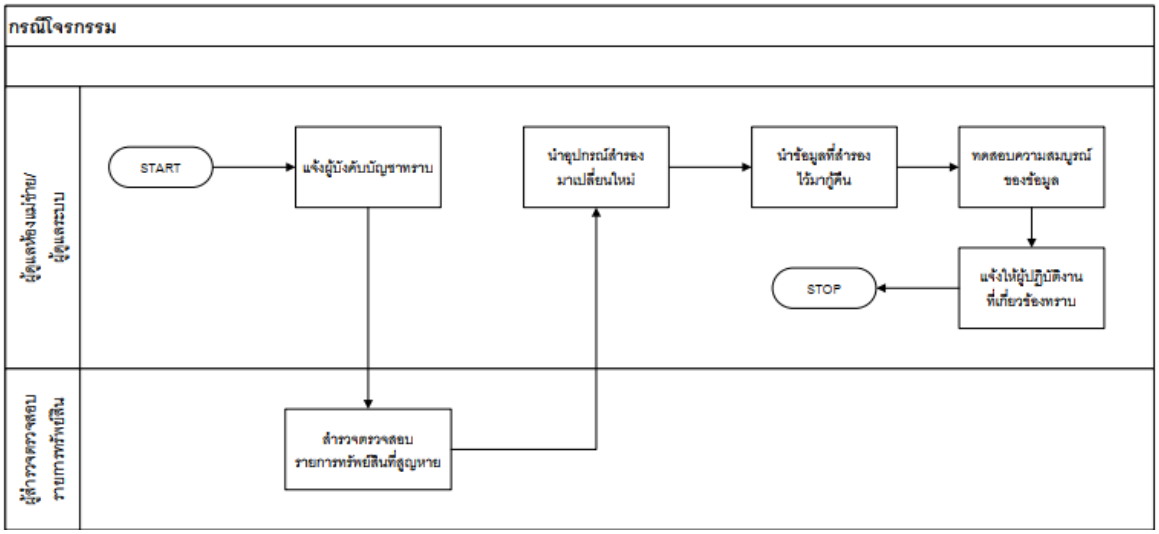


7.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

1) กรณีโจรกรรม

- ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน
- สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย
- ผู้ดูแลระบบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้กู้คืน ให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้โดยเร็ว

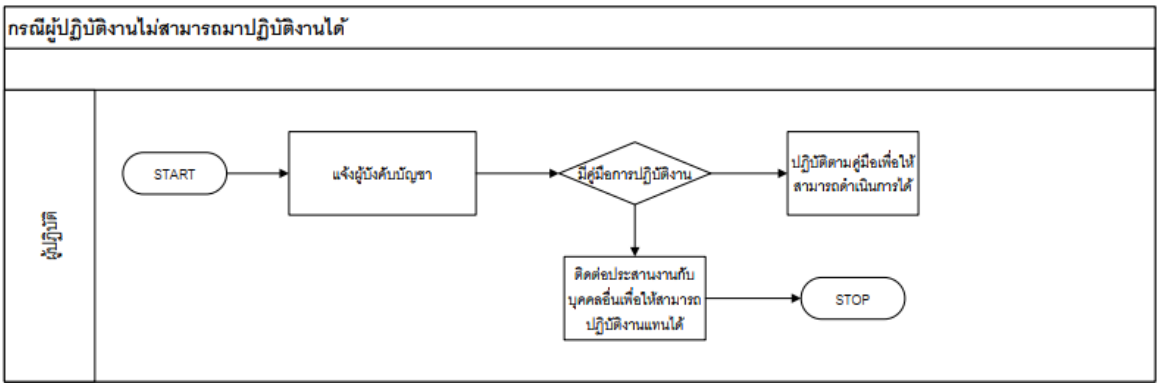
แผนผังแสดงขั้นตอนการรับมือกรณีโจรกรรม



2) กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

- แจ้งผู้บังคับบัญชาทราบ
- ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือกรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



8. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศเป็น ดังนี้

8.1.ผู้รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุมตรวจสอบ เจ้าหน้าที่ผู้ดูแสรับผิดชอบปฏิบัติงาน ได้แก่

- รองอธิการบดี ที่ดำรงตำแหน่งผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)
- ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

8.2 ผู้รับผิดชอบการปฏิบัติงาน ดูแลระบบ ดูแลห้องปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่าย คือ

- นายจตุพร ระเวงจิตร์ นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่วาสุกรี
- นายพันธฤทธิ์ พุ่มจำปา นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่หันตรา
- นายฐิตินันท์ ภู่พันธ์ นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่นนทบุรี
- นายสิริพงษ์ เกียรติพิทักษ์สุข นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่นนทบุรี
- นายจิรวัฒน์ พงษ์วิเชียร นักวิชาการคอมพิวเตอร์ ดูแลศูนย์พื้นที่หันตรา
- นายสุวิชัย แช่มชื่น นักวิชาการคอมพิวเตอร์ ดูแลศูนย์พื้นที่วาสุกรี
- นายวิทยา ปานเพชร นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่สุพรรณบุรี
- นายณัฐวัฒน์ เขาแก้ว นักวิชาการคอมพิวเตอร์ ดูแลศูนย์พื้นที่สุพรรณบุรี

8.3 ผู้รับผิดชอบการสำรวจตรวจสอบรายการทรัพย์สิน คือ

- นายพันธฤทธิ์ พุ่มจำปา นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่หันตรา
- นายจตุพร ระเวงจิตร์ นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่วาสุกรี
- นายฐิตินันท์ ภู่พันธ์ นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่นนทบุรี
- นายวิทยา ปานเพชร นักวิชาการคอมพิวเตอร์ชำนาญการ ดูแลศูนย์พื้นที่สุพรรณบุรี

8.4 หน่วยงานที่เกี่ยวข้อง

- กองกลาง (หันตรา) 035-709101
- กองบริหารทรัพยากร วาสุกรี 035-324180
- กองบริหารทรัพยากร นนทบุรี 0-2969-1369
- กองบริหารทรัพยากร สุพรรณบุรี 035-5544301
- แจ้งไฟฟ้าขัดข้องการไฟฟ้าส่วนภูมิภาค 24 ชั่วโมง 1129