ระเบียบวาระที่ 5.11 **ขอเสนอแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ**

เสนอที่ประชุม คณะกรรมการประจำคณะสังคมศาสตร์
ครั้งที่ 6/2569 วันพฤหัสบดีที่ 25 มิถุนายน พ.ศ. 2569
โดยใช้ห้องประชุมราชพฤกษ์ 1 อาคารคณะสังคมศาสตร์

มติที่ประชุม **ที่ประชุมพิจารณาแล้วมีมติ ดังนี้**

1. เห็นชอบแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ
2. มอบหน่วยประชาสัมพันธ์ งานยุทธศาสตร์และบุคคล และหน่วยเทคโนโลยีสารสนเทศ งานอำนวยการ ดำเนินการในส่วนที่เกี่ยวข้องต่อไป
3. รับรองรายงานการประชุมคณะกรรมการประจำคณะสังคมศาสตร์ ระเบียบวาระพิจารณาที่ 5.11 ในการประชุมครั้งที่ 6/2569 วันพฤหัสบดีที่ 25 มิถุนายน 2569

(นางวนมาลินทร์ มหะพันธ์)
กรรมการและเลขานุการคณะกรรมการประจำคณะ

เห็นชอบและดำเนินการตามมติ

(ผู้ช่วยศาสตราจารย์ ดร.นภิสา ไวฑูรเกียรติ)
ประธานคณะกรรมการประจำคณะสังคมศาสตร์

บันทึกข้อความ

ส่วนราชการ สำนักงานเลขานุการคณะสังคมศาสตร์ งานยุทธศาสตร์และบุคคล หน่วยประชาสัมพันธ์ โทร.1923

ที่ อว 0603.21.01(3)/465 **วันที่** 15 มิถุนายน 2569

เรื่อง ขอเสนอแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

เรียน คณบดีคณะสังคมศาสตร์

ตามที่ หน่วยประชาสัมพันธ์ งานยุทธศาสตร์และบุคคล คณะสังคมศาสตร์ ได้จัดประชุมคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ครั้งที่ 1/2569 เมื่อวันพฤหัสบดีที่ 21 พฤษภาคม 2569 ณ ห้องประชุมราชพฤกษ์ 3 อาคารคณะสังคมศาสตร์ โดยในวาระที่ 4.2 เรื่อง การทบทวนและปรับปรุงแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ที่ประชุมมีมติเห็นชอบในหลักการ และมอบหมายให้หน่วยประชาสัมพันธ์ งานยุทธศาสตร์และบุคคล ร่วมกับหน่วยเทคโนโลยีสารสนเทศ งานอำนวยการ ดำเนินการปรับปรุงรายละเอียดของแผนให้ครบถ้วน โดยให้เพิ่มเติมกิตติกรรมประกาศแก่ ผู้ช่วยศาสตราจารย์ ดร.วัชรพล ศุภจักรวัฒนา ซึ่งได้ให้ข้อเสนอแนะทางวิชาการและสนับสนุนข้อมูลด้านการบริหารจัดการภัยพิบัติและการรับมือสถานการณ์ฉุกเฉิน รวมทั้งปรับปรุงภาคผนวกให้มีรายชื่อคณะกรรมการและผู้มีส่วนร่วมให้ครบถ้วน ตลอดจนปรับปรุงขั้นตอนการบริหารจัดการกรณีเกิดเหตุขัดข้องด้านเทคนิคให้มีความชัดเจน ครอบคลุมการประเมินผลกระทบ การรายงานต่อผู้บริหาร การแจ้งผู้มีส่วนเกี่ยวข้องตามกฎหมายและระเบียบที่เกี่ยวข้อง ตลอดจนแนวทางการดำเนินการตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล รวมถึงการจัดทำรายงานเหตุการณ์ในกรณีเกิดเหตุผิดปกติ หรือข้อมูลรั่วไหล นั้น

บัดนี้ หน่วยประชาสัมพันธ์ งานยุทธศาสตร์และบุคคล ร่วมกับหน่วยเทคโนโลยีสารสนเทศ งานอำนวยการ ได้ดำเนินการปรับปรุงแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ตามข้อเสนอแนะของคณะกรรมการแล้วเสร็จ และได้ดำเนินการเวียนรับรองแผนดังกล่าวเป็นที่เรียบร้อยแล้ว ในการนี้ จึงขอเสนอแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เพื่อนำเสนอเข้าที่ประชุมคณะกรรมการประจำคณะสังคมศาสตร์ ในวาระเพื่อพิจารณา รายละเอียดตามเอกสารที่แนบมาพร้อมนี้

จึงเรียนมาเพื่อโปรดพิจารณา

(ดร.พุธิธาดา เดชพิทักษ์)
ประธานกรรมการ
คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์

เรียน คณบดีคณะสังคมศาสตร์

- เพื่อโปรดพิจารณา

- หน่วยประชาสัมพันธ์ งานยุทธศาสตร์และบุคคล ร่วมกับหน่วยเทคโนโลยีสารสนเทศ งานอำนวยการ แจ้งว่าได้ดำเนินการปรับปรุงและเวียนรับรองแผนบริหารความมั่นคงปลอดภัย และความต่อเนื่องของระบบเทคโนโลยีสารสนเทศตามข้อเสนอแนะของคณะกรรมการแล้วเสร็จ จึงขอเสนอแผนดังกล่าวเพื่อนำเข้าพิจารณาในการประชุมคณะกรรมการประจำคณะสังคมศาสตร์ รายละเอียดตามเอกสารแนบ (1)

(นายสุทธิศักดิ์กิติคุณภิวัฒน์)

นักวิชาการโสตทัศนศึกษา

16 มิถุนายน 2569

– เสนอไปยังที่ประชุม เพื่อขอความเห็นชอบ (1)

(นางพชรวรรธน์ นลินรัตนกุล)

รักษาการในตำแหน่งหัวหน้างานยุทธศาสตร์และบุคคล

16 มิถุนายน 2569

(นางวนมาลินทร์มหะพันธ์)

รักษาการในตำแหน่งหัวหน้าสำนักงานเลขานุการคณะสังคมศาสตร์

16 มิถุนายน 2569

(อาจารย์พงศ์ศิร คงแถวทอง)

ผู้ช่วยคณบดีคณะสังคมศาสตร์

17 มิถุนายน 2569

(ดร.พุธิธาดาเดชพิทักษ์)

รองคณบดีฝ่ายบริหาร

18 มิถุนายน 2569

– ให้เข้าที่ประชุมคณะฯ นี้

– มอบรองคณบดีฝ่ายบริหารนำเสนอสาระสำคัญในที่ประชุม

(ผู้ช่วยศาสตราจารย์ดร.นภิสาไวฑูรเกียรติ)

คณบดีคณะสังคมศาสตร์

18 มิถุนายน 2569

แผนบริหารความมั่นคงปลอดภัย
และความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

Information Technology Security

and Continuity Management Plan

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

Faculty of Social Sciences, Naresuan University

ปีงบประมาณ พ.ศ.2569 - 2571

ประวัติการควบคุมเอกสาร

รายการ	รายละเอียด
ชื่อเอกสาร	แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ
หน่วยงานเจ้าของแผน	หน่วยเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์
ฉบับที่	1/2569-2571
วันที่มีผลบังคับใช้	xx/xx/xxxx
ผู้จัดทำ	หน่วยเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ (นายสุทธิศักดิ์ กิติคุณภิวัฒน์)
ผู้ตรวจทาน	คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์
ผู้อนุมัติ	คณะกรรมการประจำคณะสังคมศาสตร์
รอบการทบทวน	อย่างน้อยปีละ 1 ครั้ง หรือหลังเกิดเหตุสำคัญ

ประวัติการแก้ไข

ครั้งที่	วันที่แก้ไข	รายละเอียดที่แก้ไข	ผู้แก้ไข	ผู้อนุมัติ
1.	25 พ.ย. 2564	จัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติฉบับแรก	คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์	คณะกรรมการประจำคณะสังคมศาสตร์
2.	24 ก.ค. 2566	ปรับปรุงแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ	คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์	คณะกรรมการประจำคณะสังคมศาสตร์
3.	21 พ.ค. 2569	ปรับปรุงและยกร่างให้เป็นแผนบริหารความมั่นคงปลอดภัย และความต่อเนื่องของระบบเทคโนโลยีสารสนเทศที่สามารถปฏิบัติตามได้จริง	คณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์	คณะกรรมการประจำคณะสังคมศาสตร์

คำนำ

แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร จัดทำขึ้นเพื่อเป็นกรอบแนวทางในการบริหารจัดการด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบและสอดคล้องกับนโยบาย กฎหมาย และมาตรฐานสากลที่เกี่ยวข้อง โดยมีความจำเป็นเพื่อให้มั่นใจว่าระบบงานและสถานที่ปฏิบัติงานมีความพร้อมต่อภัยพิบัติหรือภาวะฉุกเฉิน ทั้งในด้านการป้องกัน การจัดการความต่อเนื่อง และการฟื้นฟูสู่สภาพเดิม โดยได้มีการวิเคราะห์สถานการณ์หรือภาวะฉุกเฉินที่อาจส่งผลกระทบต่อกระบวนการทำงานที่สำคัญของคณะ อันเป็นการเตรียมความพร้อมเพื่อให้สามารถบริหารจัดการด้านเทคโนโลยีสารสนเทศและสนับสนุนภารกิจหลักได้อย่างมีประสิทธิภาพ

แผนฉบับนี้ได้กำหนดมาตรการด้านการป้องกัน การตรวจสอบ การตอบสนอง และการฟื้นฟูระบบ เพื่อรักษาความมั่นคงปลอดภัยและความต่อเนื่องทางการดำเนินงาน โดยเน้นให้เกิดการพัฒนาเชิงรุกและการปรับปรุงอย่างต่อเนื่อง ทั้งนี้ หน่วยเทคโนโลยีสารสนเทศจะดำเนินการทดสอบ ซักซ้อม และปรับปรุงแผนอย่างสม่ำเสมอ เพื่อให้สามารถรองรับสถานการณ์วิกฤตได้อย่างมีประสิทธิภาพและรักษาความต่อเนื่องในการให้บริการแก่นิสิต อาจารย์ และบุคลากร ตลอดจนผู้มีส่วนได้ส่วนเสียทุกฝ่าย อันจะเป็นการสร้างความเชื่อมั่นต่อคุณภาพและความมั่นคงของระบบสารสนเทศของคณะสังคมศาสตร์อย่างยั่งยืน

หน่วยเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

กิตติกรรมประกาศ

แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ฉบับนี้ จัดทำขึ้นเพื่อใช้เป็นแนวทางในการบริหารจัดการและรองรับสถานการณ์ฉุกเฉิน ภัยพิบัติ และเหตุการณ์ที่อาจส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ข้อมูลสารสนเทศ และการดำเนินงานของคณะฯ ให้สามารถดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความมั่นคงปลอดภัย

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ขอขอบคุณ ผู้ช่วยศาสตราจารย์ ดร. วัชรพล ศุภจักรวัฒนา อาจารย์ประจำภาควิชารัฐศาสตร์และรัฐประศาสนศาสตร์ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ผู้เชี่ยวชาญด้านการบริหารจัดการภัยพิบัติและการรับมือสถานการณ์ฉุกเฉิน ที่ได้กรุณาให้คำปรึกษา ข้อเสนอแนะ และข้อมูลอันเป็นประโยชน์ต่อการทบทวนและพัฒนาแผนฉบับนี้ ให้มีความเหมาะสม สอดคล้องกับสถานการณ์ปัจจุบัน และสามารถนำไปใช้ในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ขอขอบคุณคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศ หน่วยเทคโนโลยีสารสนเทศ บุคลากร และผู้มีส่วนเกี่ยวข้องทุกท่าน ที่ได้ร่วมสนับสนุนข้อมูล ข้อคิดเห็น และการดำเนินงานในการจัดทำและปรับปรุงแผนฉบับนี้จนสำเร็จลุล่วงด้วยดี

หน่วยเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

สารบัญ

แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่อง ของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

บทนำ

ปัจจุบัน ระบบเทคโนโลยีสารสนเทศมีบทบาทสำคัญยิ่งต่อการดำเนินงานขององค์กร โดยเฉพาะในสถาบันการศึกษา ที่ระบบสารสนเทศเป็นกลไกหลักในการสนับสนุนการบริหารจัดการ การเรียนการสอน การวิจัย และการบริการวิชาการแก่สังคม อย่างไรก็ดี ความก้าวหน้าทางเทคโนโลยีได้นำมาซึ่งความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีความหลากหลายและทวีความซับซ้อนมากขึ้น อาทิ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การโจมตีทางไซเบอร์ ความเสียหายของอุปกรณ์หรือระบบ ตลอดจนความผิดพลาดจากการปฏิบัติงานของบุคลากร

มาตรฐานและกรอบแนวทางการจัดทำแผน

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ให้ความสำคัญกับการบริหารความมั่นคงปลอดภัยสารสนเทศและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ เพื่อรองรับความเสี่ยง ภัยคุกคาม และเหตุการณ์ที่อาจกระทบต่อข้อมูล ระบบ เครือข่าย และการให้บริการของคณะ แผนฉบับนี้จัดทำขึ้นตามแนวทาง ISO 22301 ด้านการบริหารความต่อเนื่อง และ ISO/IEC 27001 ด้านการบริหารความมั่นคงปลอดภัยสารสนเทศ โดยครอบคลุมการ ป้องกัน ตรวจจับ ตอบสนอง ฟื้นฟู และปรับปรุงแผนอย่างต่อเนื่อง

แนวทางดำเนินงานประกอบด้วย 4 ขั้นตอนหลัก ได้แก่

1. การสร้างความรู้และความตระหนักแก่บุคลากร
2. การเตรียมความพร้อมและจัดทำแผนรองรับภารกิจสำคัญ
3. การทดสอบ ซักซ้อมแผน และประเมินผล (After Action Review)
4. การบริหารจัดการและฟื้นฟูหลังเกิดเหตุการณ์

แนวทางดังกล่าวมีเป้าหมายเพื่อให้คณะสามารถลดผลกระทบ ฟื้นฟูระบบ และดำเนินงานได้อย่างต่อเนื่อง มีประสิทธิภาพ และสอดคล้องกับมาตรฐานสากล

การประกาศใช้แผน

แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ จะประกาศใช้เมื่อเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ข้อมูลสำคัญ เครือข่ายคอมพิวเตอร์ สถานที่ปฏิบัติงาน บุคลากรหลัก หรือการให้บริการของคณะ ในระดับที่ไม่สามารถดำเนินงานได้ตามปกติ ทั้งนี้ การประกาศใช้แผนต้องได้รับความเห็นชอบจากผู้บริหาร หรือผู้ที่ได้รับมอบหมาย และมีการบันทึกวัน เวลา เหตุการณ์ ผู้มีอำนาจตัดสินใจ และรายละเอียดการดำเนินการไว้ใน Log Book ทุกครั้ง

ด้วยเหตุนี้ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร จึงได้จัดทำ แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ขึ้น โดยยึดหลักการสำคัญ 5 ประการ คือ

1. การป้องกัน (Prevention): มาตรการและกลไกป้องกันความเสี่ยงด้านสารสนเทศ
2. การตรวจสอบ (Detection): ระบบติดตามและประเมินเหตุการณ์ด้านความมั่นคงปลอดภัย
3. การตอบสนอง (Response): ขั้นตอนการแก้ไขปัญหาและลดผลกระทบจากเหตุการณ์
4. การฟื้นฟู (Recovery): แนวทางกู้คืนระบบและข้อมูลสู่สภาวะปกติ
5. การพัฒนาอย่างต่อเนื่อง (Continuous Improvement): การปรับปรุงมาตรการให้สอดคล้องกับภัยคุกคามใหม่ ๆ

หน่วยเทคโนโลยีสารสนเทศ ซึ่งเป็นหน่วยงานหลักในการดูแลระบบและบริการด้านสารสนเทศ ได้จัดทำ คู่มือการปฏิบัติตามแผน เพื่อให้การดำเนินงานมีความมั่นคงปลอดภัย และสอดคล้องกับกฎระเบียบที่เกี่ยวข้อง โดยต้องอาศัยความร่วมมือจากผู้ดูแลระบบ ผู้ใช้งาน และผู้ที่เกี่ยวข้องทุกฝ่ายในการปฏิบัติตามอย่างเคร่งครัด

คณะสังคมศาสตร์คาดหวังว่า แผนและคู่มือฉบับนี้จะช่วยเสริมสร้างความมั่นใจ ความน่าเชื่อถือ และความยั่งยืนในการดำเนินงานด้านสารสนเทศ เพื่อสนับสนุนการบรรลุพันธกิจและเป้าหมายเชิงกลยุทธ์ของมหาวิทยาลัยนเรศวรต่อไป

วัตถุประสงค์

1. เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวรในภาษาที่ง่ายต่อความเข้าใจ โดยสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง สำหรับผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง ใช้เป็นคู่มือและถือปฏิบัติอย่างเคร่งครัด ตามหลักจริยธรรม

2. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

3. เพื่อสร้างความตระหนักและความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่ผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง

4. ช่วยลดความสูญเสียหรือความเสียหายจากภัยคุกคามด้านความมั่นคงปลอดภัย ที่อาจเกิดขึ้นกับข้อมูลสารสนเทศขององค์กร

5. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

นิยามศัพท์

มหาวิทยาลัย	มหาวิทยาลัยนเรศวร
คณะ	คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร
ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีภาระหน้าที่รับผิดชอบในการดูแล รักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
ผู้พัฒนาระบบ (Programmer)	ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ
เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย ซึ่งหมายถึงข้อมูลส่วนบุคคล และข้อมูลของหน่วยงาน
เจ้าของระบบ	ผู้ได้รับมอบหมายให้เป็นหน่วยงานเจ้าภาพ ในการรับผิดชอบดูแลระบบสารสนเทศ โดยมีหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลในระดับหน่วยงาน
ผู้ใช้งาน	บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของคณะสังคมศาสตร์ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของคณะสังคมศาสตร์ได้แก่ **ผู้บริหาร** หมายถึง คณบดี รองคณบดี ผู้ช่วยคณบดี หัวหน้าสำนักฯ หัวหน้างาน **ผู้ดูแลระบบ** (System Administrator) หมายถึง ผู้ที่ได้รับมอบหมาย จากผู้บริหารให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ **นิสิต** หมายถึง นิสิตคณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ระดับปริญญาตรีปริญญาโท ปริญญาเอก **บุคคลภายนอก** หมายถึง เจ้าหน้าที่จากหน่วยงานภายนอกที่ปฏิบัติการร่วมกับคณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร
DPO	**เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล** (Data Protection Officer) ซึ่งมีหน้าที่กำกับดูแล และให้คำแนะนำเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลให้เป็นไปตามกฎหมาย PDPA และมาตรฐานที่เกี่ยวข้อง
BIA	การวิเคราะห์ผลกระทบต่อภารกิจหรือบริการสำคัญเมื่อระบบหยุดชะงัก
RTO	ระยะเวลาสูงสุดที่ต้องกู้คืนระบบให้กลับมาใช้งานได้
RPO	ระยะเวลาสูงสุดของข้อมูลย้อนหลังที่ยอมให้สูญหายได้
MTPD	ระยะเวลาสูงสุดที่กระบวนการสำคัญหยุดชะงักได้ก่อนเกิดผลกระทบรุนแรง
Incident	เหตุการณ์ที่กระทบต่อระบบ ข้อมูล หรือบริการ
Crisis	เหตุการณ์ที่มีผลกระทบรุนแรง เกินขีดความสามารถของการแก้ไขปกติ
Disaster Recovery	กระบวนการกู้คืนระบบเทคโนโลยีสารสนเทศหลังเกิดเหตุ
Data Breach	เหตุการณ์ข้อมูลรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต
After Action Review	การทบทวนบทเรียนหลังเหตุการณ์หรือหลังการซักซ้อม

สมมติฐาน

เอกสารฉบับนี้จัดทำขึ้นภายใต้สมมติฐานดังต่อไปนี้

1) เหตุการณ์ฉุกเฉินที่เกิดขึ้นอาจส่งผลกระทบต่อการปฏิบัติงานปกติของคณะ แต่ไม่ส่งผลกระทบต่อสถานที่ปฏิบัติงานสำรองที่ได้มีการกำหนดและจัดเตรียมไว้ล่วงหน้า

2) ทีมงานหลัก กลุ่มงาน/ฝ่าย ที่รับผิดชอบตามบทบาทหน้าที่ รวมถึงการบริหารจัดการและการสำรองระบบสารสนเทศที่เกี่ยวข้อง ยังคงสามารถดำเนินงานได้โดยไม่ถูกกระทบจากเหตุการณ์ฉุกเฉินโดยตรง

3) สถานที่ปฏิบัติงานสำรอง ตลอดจนระบบคอมพิวเตอร์ ระบบเครือข่าย และระบบสารสนเทศสำคัญที่ใช้ในการสำรองข้อมูลของคณะ ยังคงสามารถทำงานได้ตามปกติและไม่ถูกกระทบจากเหตุการณ์ฉุกเฉิน

4) ระบบสารสนเทศหลักของแต่ละหน่วยงานภายในคณะสังคมศาสตร์มีผู้ประสานงานด้านระบบคอมพิวเตอร์รับผิดชอบดูแล พร้อมทั้งมีการดำเนินการสำรองข้อมูลของระบบงานที่เกี่ยวข้องอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าสามารถกู้คืนข้อมูลและดำเนินการต่อได้ในกรณีเกิดเหตุฉุกเฉิน

เกณฑ์การประกาศใช้แผนและการยกระดับเหตุการณ์

ระดับ	ลักษณะเหตุการณ์	ผู้มีอำนาจตัดสินใจ
ระดับ 1	เหตุขัดข้องเล็กน้อย กระทบผู้ใช้งานบางราย	หัวหน้าหน่วยเทคโนโลยีสารสนเทศ
ระดับ 2	กระทบหลายระบบ หรือหลายหน่วยงาน	คณบดีหรือผู้ได้รับมอบหมาย
ระดับ 3	ระบบสำคัญหยุดชะงัก กระทบการเรียน การสอน การบริหาร	คณบดีหรือผู้ได้รับมอบหมาย
ระดับ 4	ข้อมูลรั่วไหล Ransomware หรือภัยไซเบอร์ร้ายแรง	คณบดีหรือผู้ได้รับมอบหมาย

การวิเคราะห์ทรัพยากรสำคัญ

เพื่อให้การดำเนินงานของหน่วยเทคโนโลยีสารสนเทศเป็นไปอย่างต่อเนื่องในสภาวะวิกฤต หน่วยงานต้องระบุและจัดเตรียมทรัพยากรสำคัญ โดยพิจารณาผลกระทบหลัก 5 ด้าน:

1. **อาคาร/สถานที่ปฏิบัติงานหลัก:** ความเสียหายหรือไม่สามารถใช้งานได้ของสถานที่ทำงาน ส่งผลต่อความพร้อมของบุคลากร

2. **วัสดุอุปกรณ์สำคัญ:** ความเสียหายหรือขาดแคลนอุปกรณ์ที่จำเป็นต่อการปฏิบัติงาน

3. **เทคโนโลยีสารสนเทศและข้อมูลสำคัญ:** การใช้งานระบบคอมพิวเตอร์ เครือข่าย หรือข้อมูลสำคัญถูกขัดข้อง

4. **บุคลากรหลัก:** การขาดความพร้อมของบุคลากรที่สำคัญต่อการปฏิบัติงาน

5. **คู่ค้า/ผู้ให้บริการ/ผู้มีส่วนได้ส่วนเสีย:** การไม่สามารถให้บริการหรือรับบริการจากผู้มีส่วนเกี่ยวข้อง

การวิเคราะห์เชิงระบบนี้ช่วยเพิ่มความมั่นคง ลดความเสี่ยง และรับประกันความต่อเนื่องของการปฏิบัติงานและระบบสารสนเทศของหน่วยงาน

การวิเคราะห์ผลกระทบต่อภารกิจและระบบสำคัญ (BIA)

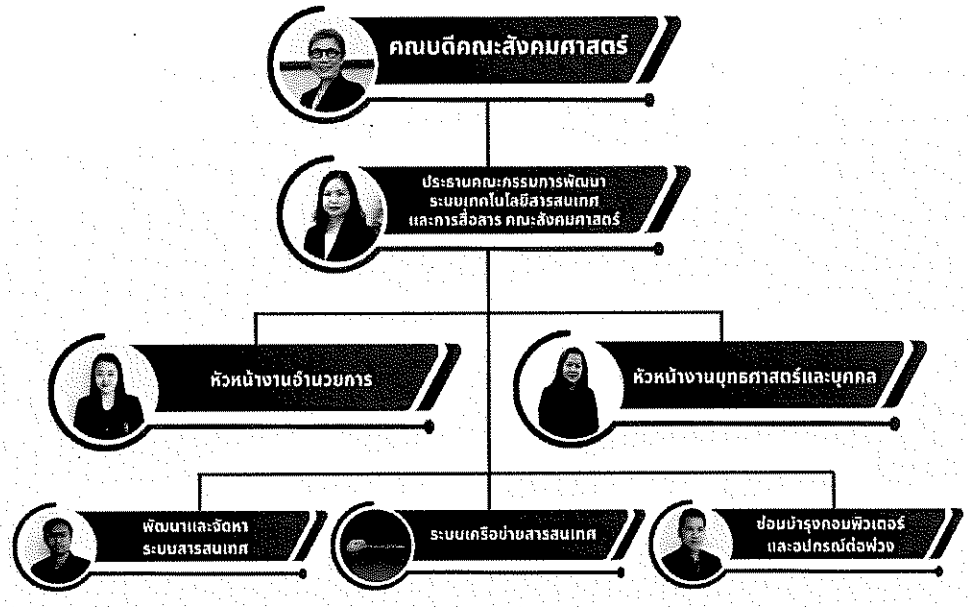
ระบบ/ภารกิจ	ผลกระทบหากหยุดชะงัก	MTPD	RTO	RPO	วิธีทำงานทดแทน
ระบบเครือข่าย Internet/Wi-Fi	การเรียน การประชุม และงานธุรการสะดุด	8 ชม.	4 ชม.	0 ชม.	ใช้ 4G/5G หรือพื้นที่สำรอง
ระบบอีเมล	การสื่อสารราชการล่าช้า	24 ชม.	8 ชม.	4 ชม.	ใช้ Line/โทรศัพท์
เว็บไซต์คณะ	ประชาสัมพันธ์หยุดชะงัก	48 ชม.	24 ชม.	24 ชม.	ใช้เพจของคณะ/ เว็บไซต์ของมหาวิทยาลัย
ระบบจัดเก็บไฟล์	งานเอกสารและรายงาน หยุดชะงัก	24 ชม.	8 ชม.	24 ชม.	ใช้ไฟล์สำรอง/ เอกสาร กระดาษ

สรุปเหตุการณ์สภาวะวิกฤตและผลกระทบจากเหตุการณ์

เหตุการณ์ ภาวะวิกฤต	ผลกระทบ				
	ด้านอาคาร/ สถานที่ ปฏิบัติงานหลัก	ด้านวัสดุอุปกรณ์ ที่ สำคัญ/การ จัดหา จัดส่งวัสดุ อุปกรณ์ ที่สำคัญ	ด้านเทคโนโลยี สารสนเทศและ ข้อมูลที่สำคัญ	ด้านบุคลากร หลัก	ด้านผู้ที่หน่วย เทคโนโลยี สารสนเทศให้และ รับบริการ/ผู้มีส่วน ได้ส่วนเสีย
1) ความขัดข้องด้านเทคนิค อาคารถล่ม หรือไฟฟ้าดับเป็น เวลานาน หรือระบบ คอมพิวเตอร์ ระบบสื่อสาร หลักเกิดความเสียหาย ระบบ ข้อมูลเสียหายรุนแรง เป็นต้น	✓	✓	✓	✓	✓
2) ภัยพิบัติ เช่น อุทกภัย อัคคีภัย วาตภัย	✓	✓	✓	✓	✓
3) โรคระบาด	✓	✗	✗	✓	✓
4) การก่อการร้ายและความ ไม่สงบเรียบร้อยในบ้านเมือง	✓	✓	✓	✓	✓
5) ภัยคุกคามทางไซเบอร์	✗	✓	✓	✓	✓

การบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนรศวร

เพื่อให้แผนบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร สามารถนำไปปฏิบัติได้อย่างมีประสิทธิภาพ หน่วยเทคโนโลยีสารสนเทศจึงได้จัดตั้งโครงสร้างการบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พร้อมกำหนดบทบาทและหน้าที่สอดคล้องกับแผนผังโครงสร้างของหน่วย ดังนี้



รูปภาพแผนผังโครงสร้างการบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(ตามคำสั่งคณะสังคมศาสตร์ ที่ 26/2568

เรื่อง แต่งตั้งคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์)

ทีมงานแผนบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ	
บทบาท	**ผู้รับผิดชอบ**
คณบดีคณะสังคมศาสตร์	ผู้ช่วยศาสตราจารย์ ดร.นภิสา ไวฑูรเกียรติ
ประธานคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศฯ	ดร.พุธิธาดา เดชพิทักษ์
หัวหน้างานอำนวยการ	นางนพมาศ อ่ำอำไพ
หัวหน้างานยุทธศาสตร์และบุคคล	นางพชรวรรธน์ นลินรัตนกุล
พัฒนาและจัดหาระบบสารสนเทศ	นายพิทักษ์พงษ์ เมฆาวรนันท์
ทีมระบบเครือข่ายสารสนเทศ	กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
ซ่อมบำรุงคอมพิวเตอร์และอุปกรณ์ต่อพ่วง	นายสุทธิศักดิ์ กิติคุณภิวัฒน์

รายชื่อหน่วยงานที่เกี่ยวข้องและผู้เกี่ยวข้อง/ผู้มีส่วนได้ส่วนเสีย

ชื่อหน่วยงาน	รายชื่อผู้ติดต่อ	โทรศัพท์ที่ทำงาน	E-Mail
กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร (ผู้อำนวยการฯ)	รศ.ดร.พงศ์พันธ์ กิจสนาโยธิน	055 96 1502	kphongph@nu.ac.th
กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร (งานบริการเทคโนโลยี)	นายสรพงศ์ สุขเกษม	055 96 1556	sarapongs@nu.ac.th
กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร (งานระบบเครือข่าย)	นายภูดิท วงค์อนุ	055 96 1527	phudit@nu.ac.th
กองอาคารสถานที่ (ผู้อำนวยการฯ)	นายรุ่งรัตน์ พระนาค	055 96 8000	roongratp@nu.ac.th
ศูนย์สาธารณภัยและหน่วยบริการประชาชนตำบลท่าโพธิ์	นายธวัชชัย โตสุข	055 22 6396	thapho2558@hotmail.com

ตารางบทบาท หน้าที่ และความรับผิดชอบ (RACI Matrix)

ภารกิจ	คณบดี	ประธาน IT	หน่วย IT	CITCOMS	เจ้าของข้อมูล	งานอาคาร
ประกาศใช้แผน	A	R	C	C	I	I
ประเมินผลกระทบ	I	A	R	C	C	C
กู้คืนระบบ	I	A	R	R/C	C	C
สื่อสารผู้ใช้งาน	A	C	R	C	I	I
รายงานหลังเหตุการณ์	A	R	R	C	C	C

* R = ผู้ดำเนินการ, A = ผู้รับผิดชอบสูงสุด/ผู้อนุมัติ, C = ผู้ให้คำปรึกษา, I = ผู้ต้อง รับทราบ

กระบวนการแจ้งเหตุฉุกเฉิน (Call Tree)

กระบวนการ Call Tree ใช้สำหรับการแจ้งเหตุฉุกเฉินแก่บุคลากรที่เกี่ยวข้อง โดยเริ่มจากคณบดีคณะสังคมศาสตร์ แจ้งประธานคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศ จากนั้นประธานแจ้งต่อหัวหน้างานอำนวยการ และหัวหน้างานยุทธศาสตร์และบุคคล เพื่อติดต่อสื่อสารไปยังบุคลากรในสายงานตามลำดับ

หลักการปฏิบัติ:

- **ในเวลาทำการ** ติดต่อผ่านหมายเลขโทรศัพท์หน่วยงานเป็นอันดับแรก
- **นอกเวลาทำการหรือกรณีสถานที่เสียหาย** ติดต่อผ่านโทรศัพท์มือถือเป็นอันดับแรก

หากติดต่อได้ ให้แจ้งข้อมูลสำคัญ ได้แก่

1. สถานการณ์ฉุกเฉินและการประกาศใช้แผนบริหารความต่อเนื่อง
2. เวลาและสถานที่ประชุมเร่งด่วน
3. ขั้นตอนปฏิบัติงานตามแผน เช่น การอพยพและจุดรวมพล (เช่น ลานจอดรถจักรยานยนต์หรือสนามกีฬาอเนกประสงค์หน้าอาคารคณะสังคมศาสตร์)

แผนการสื่อสารในภาวะวิกฤต

กลุ่มเป้าหมาย	ช่องทางหลัก	ช่องทางสำรอง	ผู้อนุมัติข้อความ
ผู้บริหารคณะ	โทรศัพท์/Line	Email	คณบดีหรือผู้ได้รับมอบหมาย
บุคลากร	Line Group/Email	เว็บไซต์คณะ	คณบดีหรือผู้ได้รับมอบหมาย
นิสิต	เว็บไซต์/เพจคณะ	Email/ประกาศกลาง	คณบดีหรือผู้ได้รับมอบหมาย
หน่วยงานกลางมหาวิทยาลัย	โทรศัพท์/Email	หนังสือราชการ	คณบดีหรือผู้ได้รับมอบหมาย
บุคคลภายนอก	เว็บไซต์/เพจ	ประกาศมหาวิทยาลัย	คณบดีหรือผู้ได้รับมอบหมาย

Checklist ขั้นตอนการบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

เพื่อเป็นแนวทางปฏิบัติอย่างเป็นขั้นตอน เมื่อเกิดเหตุการณ์ฉุกเฉินหรือวิกฤตที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการดำเนินงานของคณะสังคมศาสตร์

1) การแจ้งเหตุฉุกเฉิน (Emergency Notification)

วิธีการดำเนินงาน: เมื่อหัวหน้าทีมความมั่นคงปลอดภัยได้รับแจ้งเหตุ ให้ดำเนินการตามกระบวนการ Call Tree ทันที โดยใช้หมายเลขโทรศัพท์ที่กำหนดไว้ในรายชื่อ (Staff Recall List)

ผลลัพธ์ที่คาดหวัง: บุคลากรที่เกี่ยวข้องรับทราบเหตุการณ์และเตรียมพร้อมเข้าร่วมประชุมหรือปฏิบัติการตามแผน

2) การประชุมทีมงาน (Emergency Meeting)

วิธีการดำเนินงาน: ทีมความมั่นคงปลอดภัยจัดประชุมเร่งด่วน (On-site หรือ Online) เพื่อประเมินสถานการณ์เบื้องต้น ระบุขอบเขตผลกระทบต่อการดำเนินงานและการให้บริการ กำหนดลำดับความสำคัญของระบบหรือบริการที่จะต้องดำเนินการก่อน

ผลลัพธ์ที่คาดหวัง: มีแผนการดำเนินงานเร่งด่วนที่ชัดเจนและได้รับการเห็นชอบจากทีม

3) การประเมินการดำเนินงานระบบสำคัญ (Critical IT System Continuity)

วิธีการดำเนินงาน: ตรวจสอบระบบคอมพิวเตอร์และเครือข่ายที่จำเป็นต่อการดำเนินงานหลัก เช่น Internet, ระบบสารสนเทศนิสิต, ระบบอีเมล ดำเนินการตามแผนกู้คืนระบบ IT (IT Recovery Plan) หากระบบสำคัญไม่สามารถใช้งานได้

ผลลัพธ์ที่คาดหวัง: ระบบสารสนเทศหลักของคณะกลับมาใช้งานได้ต่อเนื่องในระดับที่ยอมรับได้

4) การสื่อสารและรายงานสถานการณ์ (Communication & Reporting)

วิธีการดำเนินงาน: จัดทำข้อความแจ้งสถานการณ์ (Approved Message) ที่ผ่านการพิจารณาจากหัวหน้าทีม สื่อสารแก่บุคลากรในคณะสังคมศาสตร์ ผ่านช่องทาง เช่น โทรศัพท์, Line Group, Email หรือประกาศบนเว็บไซต์คณะฯ รายงานสถานการณ์ต่อผู้บริหารมหาวิทยาลัยตามลำดับขั้น

ผลลัพธ์ที่คาดหวัง: บุคลากรทุกระดับรับทราบข้อมูลที่ถูกต้อง ตรงกัน และทันเวลา

5) การบันทึกเหตุการณ์ (Event Logging)

วิธีการดำเนินงาน: จัดทำบันทึกเหตุการณ์ (Log Book) ระบุวัน เวลา เหตุการณ์ การตัดสินใจ ผู้รับผิดชอบ และการดำเนินการทุกขั้นตอน ใช้แบบฟอร์มมาตรฐานของคณะเพื่อให้การบันทึกเป็นระบบ

ผลลัพธ์ที่คาดหวัง: มีหลักฐานเชิงประจักษ์สำหรับการทบทวน ปรับปรุงแผน และใช้ประกอบการตรวจสอบ

6) การติดตามการกู้คืนทรัพยากร (Resource Recovery Tracking)

วิธีการดำเนินงาน: ติดตามสถานะการซ่อมแซมหรือกู้คืนระบบที่เสียหาย เช่น ไฟฟ้า ระบบเครือข่าย เซิร์ฟเวอร์ หรือฐานข้อมูล บันทึกระยะเวลาที่ใช้ในการกู้คืน และประเมินผลกระทบต่อการดำเนินงาน

ผลลัพธ์ที่คาดหวัง: ทรัพยากรถูกกู้คืนอย่างมีลำดับขั้นตอน พร้อมข้อมูลสำหรับวิเคราะห์ปรับปรุง

7) การประเมินศักยภาพและทรัพยากร (Capability & Resource Assessment)

วิธีการดำเนินงาน: ประเมินความพร้อมของบุคลากร ทีมงาน และอุปกรณ์สำรอง ตรวจสอบความเพียงพอของทรัพยากร เช่น เครื่องสำรองไฟ (UPS), เซิร์ฟเวอร์สำรอง, อุปกรณ์สื่อสาร, สถานที่ทำงานชั่วคราว และระบุข้อจำกัดที่อาจกระทบต่อการดำเนินงาน

ผลลัพธ์ที่คาดหวัง: ทราบศักยภาพจริงและทรัพยากรที่ต้องจัดหาเพิ่มเติมเพื่อให้บริการดำเนินต่อได้

8) การรายงานต่อคณะกรรมการ (Final Reporting)

วิธีการดำเนินงาน:สรุปสถานการณ์ การดำเนินงาน และสถานะการกู้คืนทั้งหมด รายงานต่อประธานคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศ และผู้บริหารที่เกี่ยวข้อง

ผลลัพธ์ที่คาดหวัง: ผู้บริหารรับทราบข้อมูลครบถ้วนเพื่อใช้ประกอบการตัดสินใจและกำหนดแนวทางป้องกันในอนาคต

ตาราง Checklist ขั้นตอนการบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

ลำดับ	รายการตรวจสอบ	วิธีการดำเนินงาน	ผลลัพธ์ที่คาดหวัง	✓/X	วัน-เวลา	ผู้รับผิดชอบ
1	การแจ้งเหตุฉุกเฉิน	แจ้งตาม Call Tree และ Staff Recall List	บุคลากรรับทราบและเตรียมพร้อม	☐		
2	การประชุมทีมงาน	จัดประชุมเร่งด่วน ประเมินสถานการณ์/กำหนดลำดับงาน	มีแผนดำเนินงานเร่งด่วนที่ชัดเจน	☐		
3	การประเมินการดำเนินงานระบบสำคัญ	ตรวจสอบระบบคอมพิวเตอร์ เครือข่าย และดำเนินตาม IT Recovery Plan	ระบบสารสนเทศหลักกลับมาใช้งานได้ต่อเนื่อง	☐		
4	การสื่อสารและรายงานสถานการณ์	จัดทำข้อความแจ้งสถานการณ์ที่อนุมัติแล้ว และสื่อสารผ่านช่องทางที่กำหนด	ข้อมูลถูกต้อง ทันเวลา บุคลากรทุกระดับรับทราบตรงกัน	☐		
5	การบันทึกเหตุการณ์	จัดทำ Log Book หรือบันทึกตามแบบฟอร์ม	มีหลักฐานสำหรับทบทวนและตรวจสอบ	☐		
6	การติดตามการกู้คืนทรัพยากร	ติดตามการซ่อมแซมหรือกู้คืนระบบที่เสียหาย พร้อมบันทึกเวลา	ทรัพยากรถูกกู้คืนตามลำดับ พร้อมข้อมูลวิเคราะห์	☐		
7	การประเมินศักยภาพและทรัพยากร	ตรวจสอบบุคลากร อุปกรณ์ และข้อจำกัด	ทราบศักยภาพและสิ่งที่ต้องจัดหาเพิ่มเติม	☐		
8	การรายงานต่อคณะกรรมการ	สรุปสถานการณ์และรายงานผลต่อผู้บริหาร	ผู้บริหารรับทราบครบถ้วนและกำหนดแนวทางป้องกันได้	☐		

ขอบเขตของแผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ

แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศฉบับนี้ จัดทำขึ้นเพื่อเป็นกรอบการดำเนินงานในการบริหารจัดการและกำกับดูแลด้านความมั่นคงปลอดภัยสารสนเทศของคณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร โดยครอบคลุมการบริหารจัดการในมิติหลักที่สำคัญ ดังนี้

1. การบริหารจัดการเครือข่ายคอมพิวเตอร์ (Network Infrastructure Management)

การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ถือเป็นรากฐานสำคัญในการขับเคลื่อนภารกิจของคณะสังคมศาสตร์ ทั้งด้านการเรียนการสอน การวิจัย และการบริหารจัดการ เนื่องจากระบบเครือข่ายเป็นโครงสร้างพื้นฐานที่เชื่อมโยงบุคลากร นิสิต และระบบสารสนเทศเข้าด้วยกันอย่างเป็นเอกภาพ ดังนั้น การออกแบบ การใช้งาน การควบคุม การตรวจสอบ และการบำรุงรักษาระบบเครือข่ายอย่างมีประสิทธิภาพจึงมีความจำเป็นเพื่อให้มั่นใจได้ว่า ระบบมีความปลอดภัย เสถียรภาพ และความต่อเนื่อง ของการให้บริการสารสนเทศ เพื่อป้องกันความเสียหายที่อาจเกิดจากการใช้งานที่ไม่ถูกต้อง

คณะสังคมศาสตร์จึงได้กำหนด แนวทางการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ ครอบคลุมทั้ง ฮาร์ดแวร์ ซอฟต์แวร์ การกำหนดสิทธิ์การใช้งาน การเข้าถึงจากระยะไกล การตรวจสอบระบบ การซ่อมบำรุง และการดำเนินการเมื่อเกิดเหตุขัดข้อง โดยมีการแบ่งหน้าที่และแนวปฏิบัติที่ชัดเจนสำหรับ ผู้ดูแลระบบ และ ผู้ใช้งาน เพื่อให้การดำเนินงานสอดคล้องกับมาตรฐานความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัยและเป็นไปตามกฎหมายที่เกี่ยวข้อง ดังนี้

แนวปฏิบัติของผู้ดูแลระบบ

1) การจัดการสิทธิ์การใช้งาน

1. จัดทำระเบียบการลงทะเบียนผู้ใช้ใหม่ และการยกเลิกสิทธิ์ในกรณีที่สิ้นสุดการใช้งาน เช่น การจบการศึกษา การลาออก หรือการโยกย้ายตำแหน่ง

2. กำหนดสิทธิ์การเข้าถึงระบบและข้อมูลตามหน้าที่ความรับผิดชอบของผู้ใช้งาน โดยต้องได้รับอนุมัติจากผู้บริหารคณะฯ

3. จัดทำมาตรการอนุญาตให้เข้าถึงระบบจากระยะไกล (Remote Access) โดยใช้การพิสูจน์ตัวตนที่รัดกุม

2) การตรวจสอบและบำรุงรักษาระบบเครือข่าย

1. ตรวจสอบการเชื่อมต่อระหว่างเซิร์ฟเวอร์และโครงข่ายสื่อสารให้พร้อมใช้งานอยู่เสมอ

2. ตรวจสอบการทำงานของอุปกรณ์เครือข่ายหลักและอุปกรณ์สนับสนุน **อย่างน้อยเดือนละ 1 ครั้ง**

3. ตรวจสอบการให้บริการของเครือข่ายไร้สาย (NU Wi-Fi และ EduRoam) ให้ใช้งานได้ตามปกติเป็นประจำ

4. จัดทำแผนการซ่อมบำรุงและเสนอขออนุมัติจากผู้บริหารคณะฯ ไม่น้อยกว่า 5 วันทำการล่วงหน้า หากต้องหยุดระบบเพื่อซ่อมบำรุง

3) การรักษาความมั่นคงปลอดภัย

1. ตรวจสอบความผิดปกติ เช่น การบุกรุก การโจมตีระบบ หรือการเปลี่ยนแปลงโดยไม่ได้รับอนุญาต เป็นประจำทุกเดือน

2. กำหนดมาตรการควบคุมการเข้าถึงเครือข่ายไร้สาย โดยใช้ MAC Address, Username และ Password ที่ได้รับอนุญาตเท่านั้น

3. ติดตั้ง Firewall, โปรแกรมป้องกันไวรัส และจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (เซิร์ฟเวอร์: ใช้บริการ CITCOMS)

4) การจัดการสิ่งแวดล้อมและความปลอดภัยของระบบ

4.1 ควบคุมอุณหภูมิและความชื้นของห้องเซิร์ฟเวอร์ให้อยู่ในเกณฑ์มาตรฐาน (10–26.7 °C, ความชื้น 20–80%)

4.2 ติดตั้งระบบรักษาความปลอดภัย เช่น กล้องวงจรปิด (CCTV) ระบบควบคุมการเข้า–ออก (RFID, สแกนใบหน้า หรือลายนิ้วมือ)

4.3 ติดตั้งระบบไฟฟ้าสำรองและเครื่องกำเนิดไฟฟ้าอัตโนมัติ (เซิร์ฟเวอร์: ใช้บริการ CITCOMS)

4.4 จัดให้มีระบบป้องกันไฟฟ้าจากฟ้าผ่า และอุปกรณ์ป้องกันอัคคีภัยที่ได้มาตรฐาน ติดตั้งฉนวนกันไฟไหม้ในห้องเซิร์ฟเวอร์และห้องควบคุมระบบ

แนวปฏิบัติของผู้ใช้งาน

ผู้บังคับบัญชาหรือเจ้าหน้าที่ที่เกี่ยวข้อง ต้องแจ้งให้หน่วยเทคโนโลยีสารสนเทศคณะฯ ทราบเป็นลายลักษณ์อักษร เมื่อมีการเปลี่ยนแปลง เช่น

- การบรรจุหรือลงทะเบียนผู้ใช้งานใหม่
- การลาออก การโยกย้าย หรือสิ้นสุดการจ้างงาน
- การสิ้นสุดการดำรงตำแหน่งของผู้บริหารหรือบุคลากร
- การถึงแก่กรรมของบุคลากรหรือลูกจ้าง

เพื่อให้ผู้ดูแลระบบดำเนินการกำหนดสิทธิ์หรือยกเลิกสิทธิ์การเข้าถึงระบบเครือข่ายได้อย่างถูกต้องและทันท่วงที

2. การบริหารจัดการครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง (IT Assets and Peripheral Devices Management)

กำหนดให้มีมาตรการและแนวทางในการติดตั้งครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง การติดตั้งซอฟต์แวร์ ระบบปฏิบัติการ การติดตั้งโปรแกรมประยุกต์สำหรับใช้งานกับอุปกรณ์ เพื่อสนับสนุนการปฏิบัติงานเพื่อให้มีแนวปฏิบัติเป็นมาตรฐานเดียวกันอย่างมีประสิทธิภาพ เป็นไปตามข้อกำหนด มาตรการและแนวทางในการใช้งานครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เพื่อความมั่นคงปลอดภัยของคอมพิวเตอร์เพื่อใช้ในการปฏิบัติงาน ซึ่งทั้งที่เป็นทรัพย์สินของมหาวิทยาลัย หรือเป็นทรัพย์สินส่วนตัวของผู้ใช้ที่นำมาใช้งานกับระบบสารสนเทศของมหาวิทยาลัย เพื่อให้การจัดการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์เป็นไปอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้น ได้อย่างรวดเร็ว เนื่องจากการใช้งานเครื่องคอมพิวเตอร์ภายในมหาวิทยาลัยมีการเชื่อมต่อเครือข่ายภายในและภายนอก (ระบบเครือข่ายอินทราเน็ตและเครือข่ายอินเตอร์เน็ต) ซึ่งอาจมีการติดไวรัส คอมพิวเตอร์ หรือ malware ต่างๆ และเครื่องคอมพิวเตอร์เหล่านี้อาจถูกโจมตีและเข้าถึงข้อมูล โดยไม่ได้รับอนุญาต

แนวปฏิบัติของผู้ดูแลระบบ

1. กำหนดคุณลักษณะของอุปกรณ์ฮาร์ดแวร์ให้มีคุณสมบัติที่มีประสิทธิภาพใช้งานได้อย่างเหมาะสมตามลักษณะงาน โดนให้เป็นไปตามประกาศมหาวิทยาลัยนเรศวร เรื่อง รายละเอียดและคุณลักษณะของอุปกรณ์และครุภัณฑ์คอมพิวเตอร์มหาวิทยาลัยนเรศวร

2. ในกรณีที่เป็นการติดตั้งอุปกรณ์ใหม่ เจ้าหน้าที่ต้องทำการติดตั้งระบบปฏิบัติการ ลงโปรแกรม Antivirus, Antispyware และ Firewall เป็นไปตามข้อกำหนด พร้อมทั้งโปรแกรมประยุกต์ที่จะใช้งานให้เสร็จสิ้น พร้อมทั้งทดสอบการทำงานให้สมบูรณ์ก่อนนำเข้าติดตั้งให้แก่ผู้ใช้งาน

3. ดำเนินการลงทะเบียนอุปกรณ์ทุกชิ้นกับผู้รับผิดชอบอุปกรณ์ พร้อมระบุรุ่น เลขที่สัญญา หมายเลขอุปกรณ์ หมายเลขครุภัณฑ์ ระบุตำแหน่งของอุปกรณ์ที่จะทำการติดตั้งให้แก่ผู้ใช้งาน

4. เครื่องคอมพิวเตอร์สำหรับสนับสนุนการปฏิบัติงานภายในองค์กรทุกเครื่องต้องมีการใช้งานรหัสผ่านประจำเครื่องสำหรับเจ้าหน้าที่ผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

5. กำหนดคุณลักษณะเฉพาะและติดตั้งซอฟต์แวร์ต่างๆ โดยให้มีคุณสมบัติครบถ้วนตรงตามความต้องการใช้งาน และง่ายต่อการใช้งานของผู้ใช้งานทุกระดับ

6. ทำการ update โปรแกรมต่างๆ เช่น Windows, Antivirus และ Antispyware เพื่อให้โปรแกรมที่ใช้งานมีความทันสมัยอยู่เสมอ โดยการบำรุงรักษาตามรอบระยะเวลาเป็นประจำเดือนละ 1 ครั้ง

7. เจ้าหน้าที่ต้องเตรียมป้ายชื่ออุปกรณ์ที่ใช้วัสดุและมีรูปแบบการจัดพิมพ์ ติดตั้งให้เห็นชัดเจนบนตัวอุปกรณ์

8. เมื่อมีรายการจำเป็นต้องซ่อมบำรุงให้จัดเตรียมรายงานการติดตั้ง รวมถึงค่าใช้จ่าย ในการดูแลรักษา เพื่อส่งให้กับหัวหน้าและผู้บริหารรับทราบ

9. เมื่อมีการตรวจพบผู้ใช้ที่ฝ่าฝืนข้อปฏิบัติด้านความมั่นคงคอมพิวเตอร์ส่วนบุคคลให้ผู้ดูแลระบบคอมพิวเตอร์เสนอต่อผู้บริหาร

10. การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์เป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

แนวปฏิบัติของผู้ใช้งาน

1. ครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงของคณะฯ เป็นสมบัติของทางราชการ ผู้ใช้งานต้องใช้เพื่อปฏิบัติงานเพื่อประโยชน์ของทางราชการ ภายในองค์กรเท่านั้น

2. หากมีความประสงค์ในการนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงของคณะฯ เพื่อไปใช้งานภายนอกองค์กร ให้ผู้ใช้งานทำหลักฐานการยืมเป็นลายลักษณ์อักษร แสดงเหตุผล และกำหนดวันส่งคืน ซึ่งการนำครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วงของคณะฯ ไปใช้ในกิจการโดยมิใช่เพื่อประโยชน์ของทางราชการจะกระทำมิได้

3. เมื่อเกิดปัญหาการใช้งานครุภัณฑ์คอมพิวเตอร์ให้แจ้งผู้ดูแลระบบ โดยการเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการ โดยแจ้งให้ผู้ดูแลระบบของหน่วยเทคโนโลยีสารสนเทศเข้าไปร่วมประสานงาน โดยต้องได้รับการอนุญาตจากผู้บริหารด้วยทุกครั้ง

4. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

5. ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

6. การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์เพื่อใช้ในการปฏิบัติงาน ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ เช่น ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง และให้ทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่หน้าจอเป็นเวลานาน และต้องเข้ารหัสข้อมูลที่สำคัญไว้ เป็นต้น

7. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

8. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต ด้วยการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทาให้ผู้อื่นเสียหาย ถือเป็น

การละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าตนไม่ได้เป็นผู้กระทำความผิด

9. ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

3. การบริหารจัดการระบบสารสนเทศและข้อมูล (Data and Information Systems Management)

ปัจจุบันสถาบันการศึกษามีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหาร การจัดการเรียนการสอน และการให้บริการเพิ่มมากขึ้น ระบบสารสนเทศจึงมีบทบาทสำคัญต่อการวางแผน วิเคราะห์ ตัดสินใจ และพัฒนาคุณภาพการศึกษาให้มีประสิทธิภาพ โดยการพัฒนาระบบสารสนเทศครอบคลุมการวิเคราะห์ ออกแบบ ติดตั้ง ประเมินผล และพัฒนาระบบให้สามารถรองรับการดำเนินงานได้อย่างต่อเนื่อง

คณะสังคมศาสตร์จึงให้ความสำคัญกับการบริหารจัดการระบบสารสนเทศและข้อมูล (Data and Information Systems Management) ครอบคลุมการจัดเก็บ การเข้าถึง การประมวลผล การควบคุมสิทธิ์ การสำรองข้อมูล การเก็บรักษา และการกู้คืนข้อมูล รวมถึงการรักษาความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลและระบบสารสนเทศ (Confidentiality, Integrity, Availability: CIA) เพื่อให้ข้อมูลมีความถูกต้อง ปลอดภัย และสามารถใช้งานได้อย่างต่อเนื่อง โดยได้กำหนดแนวทางและขั้นตอนด้านการสำรองข้อมูล การเก็บรักษา และการทดสอบการกู้คืนข้อมูล เพื่อรองรับสถานการณ์ฉุกเฉิน และลดความเสี่ยงจากการสูญหายของข้อมูล ดังตารางต่อไปนี้

ข้อมูล/ระบบ	วิธีสำรอง	ความถี่	สถานที่เก็บ	ผู้รับผิดชอบ	ทดสอบกู้ คืน
ข้อมูลเอกสารงาน บริหาร	Incremental + Full	รายวัน/ราย สัปดาห์	Server + Off-site	IT + เจ้าของ ข้อมูล	ทุก 3 เดือน
เว็บไซต์คณะ	Full Backup	รายสัปดาห์	Server + Cloud/Offsite	Web Admin	ทุก 6 เดือน
Log ระบบ	Archive	รายเดือน	Secure Storage	System Admin	ทุก 6 เดือน
เครื่องผู้บริหาร/งานสำคัญ	Manual/Cloud Sync	รายสัปดาห์	External/Cloud	ผู้ใช้งาน + IT	ทุก 3 เดือน

แนวปฏิบัติของผู้ดูแลระบบ

1. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ใช้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้งาน และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

1.1 เปลี่ยนแปลงและการยกเลิกรหัสผ่านเมื่อผู้ใช้งานระบบสารสนเทศลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

1.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ใช้งานได้รับรหัสผ่าน ต้องตอบยืนยันการได้รับรหัสผ่าน

1.3 กำหนดชื่อผู้ใช้งานและรหัสผ่าน ในการเข้าใช้งานระบบสารสนเทศและข้อมูลที่ไม่ซ้ำกัน

1.4 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวเมื่อพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานนั้นต่างจากรหัสผู้ใช้งานตามปกติ

2. แจ้งให้ผู้ใช้งานทราบถึงวันเวลาที่ต้องปิดระบบสารสนเทศเพื่อบำรุงรักษา ปรับปรุง หรือเปลี่ยนแปลงระบบซึ่งส่งผลให้ต้องหยุดบริการในช่วงระยะเวลาหนึ่ง โดยให้แจ้งล่วงหน้าก่อนกำหนดการ 3 วันทำการ แต่ในกรณีฉุกเฉินผู้ดูแลระบบอาจมีความจำเป็นต้องปิดระบบอย่างเร่งด่วนได้

3. กำหนดให้มีกระบวนการสร้างความต่อเนื่องให้กับการดำเนินงานการบริหาร จัดการและการปรับปรุงกระบวนการที่ต้องใช้ในการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ โดยการทำสำรองข้อมูลภายในมหาวิทยาลัยหมายถึงการทำสำรองข้อมูลทั้งหมด ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำหรับไว้เป็นประจำสัปดาห์ละ 1 ครั้ง (ข้อมูลที่ถูกจัดเก็บบนเว็บไซต์คณะสังคมศาสตร์)

4. ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์ไม่สามารถปฏิบัติงานได้ ต้องมีการ มอบหมายหน้าที่ไว้ล่วงหน้าให้กับเจ้าหน้าที่คนอื่น เพื่อให้เจ้าหน้าที่ผู้นั้นสามารถปฏิบัติหน้าที่ หรือประสานงานแทนได้ในกรณีที่จำเป็น

5. ควบคุมการเข้าถึงข้อมูลโดยตั้งรหัสผู้ใช้งานและรหัสผ่าน โดยมีการกำหนดสิทธิ์ของผู้ใช้ตามความรับผิดชอบที่ได้รับมอบหมาย และไม่ให้สำเนาอิเล็กทรอนิกส์ เช่น external drive หรือ thumb drive ยกเว้นได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูล และผู้บริหาร

6. วิธีการลบและทำลายข้อมูลสื่อบันทึกข้อมูลแบบแถบแม่เหล็กให้มีการใช้ ซอฟต์แวร์ประเภทยูทิลิตี้เพื่อป้องกันการกู้ข้อมูลคืนได้

7. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายมีหน้าที่กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้ในการเก็บข้อมูล โดยตัวอย่างรูปแบบการสำรองข้อมูล อาทิ การสำรองข้อมูลทั้งหมด (Full backup) การสำรองข้อมูลแบบสะสม (Incremental backup) หรืออาจเลือกใช้การสำรองข้อมูลรูปแบบอื่นๆ ตามความเหมาะสม แต่ต้องให้มั่นใจว่ามีการสำรองข้อมูลได้ครบถ้วนตามเป้าหมายที่กำหนดไว้ รวมทั้งสามารถกู้กลับคืนได้ด้วย

8. การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน ทั้งนี้เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็วและเพื่อป้องกันระบบจากการถูกโจมตีหรือจากหายนะที่อาจเกิดขึ้น

9. กำหนดให้มีกระบวนการตรวจสอบความถูกต้องและเป็นปัจจุบันของระบบสารสนเทศและข้อมูล โดยการตรวจสอบข้อมูลกับผู้ใช้งานผู้รับผิดชอบระบบสารสนเทศเป็นประจำไตรมาศละ 1 ครั้ง

10. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศ หรือข้อมูลจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้บริหารหรือผู้ที่ได้รับมอบหมาย

11. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานระบบสารสนเทศต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามอย่างเคร่งครัด

2. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลสำคัญตามประเภทชั้นความลับเพื่อควบคุมป้องกันข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล โดยการกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

3. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ได้แก่ CD, DVD และ External Hard Disk

4. ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

5. หลีกเลี่ยง ไม่จัดเก็บข้อมูลในพื้นที่เก็บข้อมูลส่วนกลาง เช่น Network Shared Drive หรือคอมพิวเตอร์ในห้องประชุม

6. หากมีความจำเป็นต้องส่งผ่านข้อมูลไปยังบุคคลหรือหน่วยงานภายนอกมหาวิทยาลัย เจ้าหน้าที่ที่รับผิดชอบในการส่งผ่านข้อมูลจะต้องแจ้งให้กับผู้รับข้อมูลทราบถึงระดับชั้นความลับของข้อมูล และวิธีการในการจัดการกับข้อมูลก่อนนำส่งข้อมูล

7. เจ้าของระบบสารสนเทศและข้อมูล หรือเจ้าหน้าที่ ต้องแจ้งให้หน่วยเทคโนโลยีสารสนเทศทราบเป็นลายลักษณ์อักษร เมื่อบุคลากรมีการว่าจ้างงาน เปลี่ยนแปลงสภาพการจ้างงาน ลาออกหรือมีคาสั่งสิ้นสุดการเป็นผู้บริหารบุคลากรและลูกจ้าง มีการถึงแก่กรรม มีการโอนย้ายข้ามหน่วยงานราช การ เพื่อให้ผู้ดูแลระบบกำหนดสิทธิ์ หรือยกเลิกสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศและข้อมูล

4. การบริหารจัดการสถานการณ์ฉุกเฉินและสภาวะวิกฤต (Emergency and Crisis Management)

เนื่องจากเทคโนโลยีสารสนเทศมีบทบาทสำคัญต่อการดำเนินงานของคณะสังคมศาสตร์ จึงจำเป็นต้องมีการบริหารจัดการสถานการณ์ฉุกเฉินและสภาวะวิกฤต เพื่อเตรียมความพร้อม ป้องกัน ลดผลกระทบ ตอบสนอง และฟื้นฟูการดำเนินงาน (Disaster Recovery and Business Continuity) กรณีเกิดเหตุการณ์ที่ส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ ข้อมูล ทรัพยากร หรือบุคลากร เพื่อให้คณะฯ สามารถดำเนินภารกิจได้อย่างต่อเนื่อง มีประสิทธิภาพ และมีความมั่นคงปลอดภัย

ทั้งนี้ คณะฯ ได้จัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษา แก้ไข และฟื้นฟูระบบเทคโนโลยีสารสนเทศ รวมถึงลดความเสี่ยงและความเสียหายที่อาจเกิดขึ้นต่อฐานข้อมูลและระบบสารสนเทศของคณะ ดังนี้

1) สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค ภัยคุกคามทางไซเบอร์ การเชื่อมโยงเครือข่ายล้มเหลว อุปกรณ์จัดเก็บข้อมูลเสียหาย ไฟฟ้าขัดข้อง

2) สถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติและโรคระบาด ไฟไหม้ น้ำท่วม แผ่นดินไหว สถานการณ์โรคระบาด

3) สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง การก่อการร้าย การชุมนุมประท้วง

4) สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล โจรกรรม ผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

คู่มือกู้คืนระบบสำคัญรายบริการ (Recovery Runbook)

ระบบ	ขั้นตอนกู้คืนหลัก	ผู้รับผิดชอบ	เกณฑ์ว่าสำเร็จ
Network/Wi-Fi	ตรวจอุปกรณ์ ⟶ ตรวจ Link ⟶ ประสาน CITCOMS ⟶ ทดสอบใช้งาน	IT/CITCOMS	ใช้งานได้ ไม่น้อยกว่า 80%
Website	Restore Backup ⟶ ตรวจฐานข้อมูล ⟶ ทดสอบหน้าเว็บ ⟶ แจ้งผู้ใช้	Web Admin	เว็บไซต์เปิดได้ และข้อมูลถูกต้อง
File Storage	ตรวจ Disk/NAS ⟶ Restore ⟶ ตรวจสิทธิ์ ⟶ ให้เจ้าของข้อมูลทดสอบ	IT/เจ้าของ ข้อมูล	เปิดไฟล์สำคัญ ได้ครบ
เครื่องคอมพิวเตอร์ สำคัญ	ตรวจ Hardware ⟶ ลง Image/Software ⟶ Restore Data ⟶ ส่งคืนผู้ใช้	IT	ผู้ใช้ยืนยัน ใช้งานได้

การบริหารจัดการกรณีมีสถานการณ์ฉุกเฉิน

โครงสร้างผู้รับผิดชอบหลัก

หน่วยงาน/ตำแหน่ง	หน้าที่
คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร	กำกับ ติดตาม และอนุมัติแนวทางดำเนินการ
หน่วยเทคโนโลยีสารสนเทศ	ตรวจสอบ วิเคราะห์ แก้ไข และฟื้นฟูระบบ
CITCOMS มหาวิทยาลัยนเรศวร	สนับสนุนด้านเครือข่าย ความมั่นคงปลอดภัย และ Digital Forensics
เจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล (DPO)	ประเมินผลกระทบและดำเนินการตาม PDPA
กองกฎหมาย	ให้คำปรึกษาด้านกฎหมายและดำเนินคดี
ผู้บริหารคณะ	ตัดสินใจเชิงนโยบายและอนุมัติการแจ้งเหตุ
ผู้ดูแลระบบ (System Administrator)	ควบคุมและกู้คืนระบบ
ผู้ใช้งานระบบ	แจ้งเหตุผิดปกติและปฏิบัติตามมาตรการ

ขั้นตอนมาตรฐานการตอบสนองเหตุการณ์ (Incident Response Lifecycle)

ขั้นตอน	รายละเอียด	มาตรฐานอ้างอิง
1. Preparation	เตรียมความพร้อม นโยบาย สำรองข้อมูล และอบรม	ISO/IEC 27001, ISO 22301, NIST CSF
2. Detection & Analysis	ตรวจจับ วิเคราะห์ และประเมินเหตุการณ์	ISO/IEC 27035, NIST SP 800-61
3. Containment	จำกัดผลกระทบและแยกระบบ	ISO/IEC 27035
4. Eradication	กำจัดสาเหตุหรือมัลแวร์	ISO/IEC 27035, CIS Controls
5. Recovery	กู้คืนระบบ และตรวจสอบความปลอดภัย	ISO 22301
6. Lessons Learned	สรุปบทเรียน และปรับปรุงมาตรการ	ISO/IEC 27001 Clause 10

4.1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

4.1.1 กรณีภัยคุกคามทางไซเบอร์ร้ายแรง แยกเป็น 4 กรณี:

1) Ransomware มัลแวร์หรือโปรแกรมประสงค์ร้ายที่โจมตีระบบคอมพิวเตอร์ โดยการเข้ารหัสข้อมูลหรือปิดกั้นการเข้าถึงระบบ และเรียกร้องค่าไถ่เพื่อแลกกับการคืนสิทธิ์ในการใช้งานข้อมูลหรือระบบดังกล่าว โดยมักแพร่กระจายผ่านอีเมลปลอม ไฟล์แนบที่เป็นอันตราย หรือช่องโหว่ของระบบสารสนเทศผลกระทบที่อาจเกิดขึ้น ได้แก่ การสูญเสียข้อมูลสำคัญ การหยุดชะงักของการให้บริการระบบสารสนเทศ ความเสียหายทางการเงิน และความเสี่ยงต่อการรั่วไหลของข้อมูลส่วนบุคคลหรือข้อมูลสำคัญขององค์กร

2) Phishing Phishing คือ การโจมตีทางไซเบอร์ในลักษณะหลอกลวงผู้ใช้งานให้เปิดเผยข้อมูลสำคัญ เช่น ชื่อผู้ใช้ รหัสผ่าน ข้อมูลบัญชี หรือข้อมูลส่วนบุคคล ผ่านอีเมล เว็บไซต์ ข้อความหรือช่องทางสื่อสารปลอมที่เลียนแบบหน่วยงานหรือบุคคลที่น่าเชื่อถือผลกระทบที่อาจเกิดขึ้น ได้แก่ การถูกขโมยบัญชีผู้ใช้งาน การเข้าถึงระบบโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูลสำคัญ และอาจนำไปสู่การโจมตีรูปแบบอื่น เช่น การแพร่กระจายมัลแวร์หรือการโจมตีแบบ Ransomware

3) Data Breach คือ เหตุการณ์ที่ข้อมูลสำคัญหรือข้อมูลส่วนบุคคลถูกเข้าถึง เปิดเผย รั่วไหล สูญหาย หรือถูกใช้งานโดยไม่ได้รับอนุญาต อันอาจเกิดจากการโจมตีทางไซเบอร์ ความผิดพลาดของระบบหรือการปฏิบัติงานที่ไม่เหมาะสมของผู้ใช้งานผลกระทบที่อาจเกิดขึ้น ได้แก่ การละเมิดสิทธิส่วนบุคคล ความเสียหายต่อชื่อเสียงขององค์กร ความเสี่ยงทางกฎหมายตามพระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล (PDPA) และผลกระทบต่อความเชื่อมั่นของผู้รับบริการหรือผู้มีส่วนได้ส่วนเสีย

4) DDoS (Distributed Denial of Service) คือ การโจมตีที่ผู้ไม่หวังดีใช้เครื่องคอมพิวเตอร์จำนวนมากส่งข้อมูลหรือคำร้องขอเข้าไปยังระบบหรือเว็บไซต์เป้าหมายพร้อมกันในปริมาณสูง จนทำให้ระบบไม่สามารถให้บริการแก่ผู้ใช้งานปกติได้ผลกระทบที่อาจเกิดขึ้น ได้แก่ ระบบเครือข่ายหรือเว็บไซต์ไม่สามารถใช้งานได้ การหยุดชะงักของบริการออนไลน์ ประสิทธิภาพของระบบลดลง และอาจส่งผลกระทบต่อการดำเนินงาน การเรียนการสอน หรือบริการสำคัญขององค์กรในวงกว้าง

1) แนวปฏิบัติกรณี Ransomware Attack

วัตถุประสงค์: เพื่อป้องกันและตอบสนองต่อการโจมตีประเภทเรียกค่าไถ่ที่เข้ารหัสข้อมูลหรือทำให้ระบบไม่สามารถใช้งานได้

ขั้นตอน	การดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา	มาตรฐานอ้างอิง
ตรวจพบเหตุ	แจ้งเหตุและแยกเครื่องออกจากเครือข่ายทันที	ผู้ใช้งาน / IT Support	ภายใน 15 นาที	ISO/IEC 27035
ประเมินสถานการณ์	ตรวจสอบขอบเขตผลกระทบและระบบที่ติดเชื้อ	หน่วย IT / CITCOMS	ภายใน 1 ชั่วโมง	NIST SP 800-61
Containment	ปิดระบบที่เกี่ยวข้อง Block IP และบัญชีผู้ใช้	System Admin	ภายใน 2 ชั่วโมง	CIS Controls v8
Forensics	เก็บ Log และหลักฐานดิจิทัล	CITCOMS / กองกฎหมาย	ภายใน 24 ชั่วโมง	ISO/IEC 27037
Recovery	กู้คืนข้อมูลจาก Backup ที่ปลอดภัย	System Admin	ภายใน 1–7 วัน	ISO 22301
Notification	แจ้ง DPO และหน่วยงานกำกับภายใน 72 ชั่วโมง	DPO / กองกฎหมาย	ภายใน 72 ชั่วโมง	PDPA, ISO/IEC 27701
Post Incident Review	วิเคราะห์ Root Cause และปรับปรุงมาตรการ	คกก.IT	ภายใน 14 วัน	ISO/IEC 27001 Clause 10

มาตรการป้องกันกรณี Ransomware

- สำรองข้อมูลแบบ Offline/Immutable Backup : สำรองข้อมูลแยกจากระบบหลักและไม่สามารถแก้ไขหรือลบได้
- Endpoint Detection and Response (EDR) : ระบบตรวจจับและตอบสนองภัยคุกคามบนอุปกรณ์ผู้ใช้งาน
- Patch Management : การอัปเดตช่องโหว่และความปลอดภัยของระบบอย่างสม่ำเสมอ
- Multi-Factor Authentication (MFA) : การยืนยันตัวตนมากกว่าหนึ่งขั้นตอนก่อนเข้าใช้งานระบบ
- Network Segmentation : การแบ่งเครือข่ายเพื่อลดการกระจายของการโจมตี

2) แนวปฏิบัติกรณี Phishing Attack

วัตถุประสงค์: เพื่อป้องกันการหลอกลวงผ่านอีเมล เว็บไซต์ หรือข้อความปลอมที่มุ่งขโมยข้อมูลบัญชีผู้ใช้

ขั้นตอน	การดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา	มาตรฐานอ้างอิง
แจ้งเหตุ	ผู้ใช้แจ้งอีเมล/ลิงก์ต้องสงสัย	ผู้ใช้งาน	ทันที	ISO/IEC 27035
วิเคราะห์	ตรวจสอบ Header, URL และ Malware	IT Security	ภายใน 1 ชั่วโมง	NIST SP 800-61
Containment	Block Domain/IP และ Reset Password	System Admin	ภายใน 2 ชั่วโมง	CIS Controls
แจ้งเตือน	แจ้งเตือนบุคลากรทั้งองค์กร	หน่วย IT	ภายใน 4 ชั่วโมง	ISO/IEC 27001 A.6
ตรวจสอบความเสียหาย	ตรวจสอบบัญชีที่ถูกเข้าถึง	DPO / IT Security	ภายใน 24 ชั่วโมง	ISO/IEC 27701
ฟื้นฟู	บังคับเปลี่ยนรหัสผ่านและเปิด MFA	IT Support	ภายใน 24 ชั่วโมง	CIS Controls
สรุปบทเรียน	จัดอบรม Awareness เพิ่มเติม	HR / หน่วย IT	ภายใน 30 วัน	ISO/IEC 27001

มาตรการป้องกันกรณี Phishing

- Email Security Gateway : ระบบกรองและป้องกันอีเมลอันตรายก่อนถึงผู้ใช้งาน
- Anti-Spam / Anti-Phishing : ระบบป้องกันอีเมลขยะและอีเมลหลอกลวง
- MFA ทุกบัญชีสำคัญ : เพิ่มความปลอดภัยให้บัญชีสำคัญด้วยการยืนยันหลายขั้นตอน
- Security Awareness Training : การอบรมให้ผู้ใช้งานตระหนักรู้ด้านภัยไซเบอร์
- DMARC, SPF, DKIM : มาตรฐานยืนยันตัวตนอีเมลเพื่อป้องกันการปลอมแปลง

3) แนวปฏิบัติกรณี Data Breach

วัตถุประสงค์: เพื่อบริหารจัดการเหตุการณ์ข้อมูลส่วนบุคคลรั่วไหลหรือถูกเข้าถึงโดยไม่ได้รับอนุญาต

ขั้นตอน	การดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา	มาตรฐานอ้างอิง
ตรวจพบเหตุ	แจ้ง DPO และผู้บริหาร	ผู้พบเหตุ / IT	ทันที	PDPA
ประเมินผลกระทบ	ประเมินประเภทและจำนวนข้อมูลที่รั่วไหล	DPO / กองกฎหมาย	ภายใน 24 ชั่วโมง	ISO/IEC 27701
จำกัดผลกระทบ	ปิดช่องโหว่และจำกัดการเข้าถึง	System Admin	ภายใน 4 ชั่วโมง	ISO/IEC 27035
เก็บหลักฐาน	เก็บ Log และ Digital Evidence	CITCOMS	ภายใน 24 ชั่วโมง	ISO/IEC 27037
แจ้งหน่วยงานกำกับ	แจ้ง สคส. ภายใน 72 ชั่วโมง	DPO	ภายใน 72 ชั่วโมง	PDPA
แจ้งเจ้าของข้อมูล	แจ้งนิสิต/ผู้ปกครองที่ได้รับผลกระทบ	DPO / คณะ	โดยเร็ว	ISO/IEC 27701
ฟื้นฟูระบบ	ปรับปรุง Security Control	IT Security	ภายใน 7 วัน	ISO/IEC 27001
ทบทวนเหตุการณ์	จัดทำ Incident Report	คกก.IT	ภายใน 14 วัน	ISO/IEC 27035

มาตรการป้องกันกรณี Data Breach

- Data Classification : การจัดระดับความสำคัญของข้อมูลเพื่อกำหนดมาตรการคุ้มครอง
- Encryption at Rest / In Transit : การเข้ารหัสข้อมูลทั้งขณะจัดเก็บและส่งผ่านเครือข่าย
- Access Control ตามหลัก Least Privilege : กำหนดสิทธิ์เข้าถึงเฉพาะที่จำเป็นต่อการปฏิบัติงาน
- DLP (Data Loss Prevention) : ระบบป้องกันการรั่วไหลหรือส่งออกข้อมูลโดยไม่ได้รับอนุญาต
- Log Monitoring และ SIEM : ระบบติดตาม วิเคราะห์ และแจ้งเตือนเหตุผิดปกติจาก Log

4) แนวปฏิบัติกรณี DDoS Attack

วัตถุประสงค์: เพื่อรับมือการโจมตีที่ทำให้ระบบหรือเว็บไซต์ไม่สามารถให้บริการได้

ขั้นตอน	การดำเนินการ	ผู้รับผิดชอบ	ระยะเวลา	มาตรฐานอ้างอิง
ตรวจจับ	ตรวจสอบ Traffic ผิดปกติ	Network Admin	Real-time	NIST CSF Detect
วิเคราะห์	วิเคราะห์ Source และ Pattern	CITCOMS	ภายใน 1 ชั่วโมง	ISO/IEC 27035
Containment	Block IP / Geo-blocking / Rate Limit	Network Admin	ภายใน 2 ชั่วโมง	CIS Controls
ประสาน ISP	ขอความร่วมมือ ISP และ CDN	CITCOMS	ภายใน 4 ชั่วโมง	ISO 22301
เปิดใช้ระบบสำรอง	Activate Failover / Backup Site	System Admin	ภายใน 4 ชั่วโมง	ISO 22301
Monitoring	เฝ้าระวังต่อเนื่อง	NOC / IT Security	ตลอดเหตุการณ์	NIST CSF
Recovery	คืนค่าระบบและตรวจสอบเสถียรภาพ	IT Operations	ภายใน 24 ชั่วโมง	ISO 22301
Post Review	วิเคราะห์แนวโน้มและปรับปรุงระบบ	คกก.IT	ภายใน 7 วัน	ISO/IEC 27001

มาตรการป้องกันกรณี DDoS

- Web Application Firewall (WAF) : ระบบป้องกันการโจมตีเว็บไซต์และเว็บแอปพลิเคชัน
- CDN และ Anti-DDoS Protection : ระบบกระจายโหลดและป้องกันการโจมตี DDoS
- Load Balancer : ระบบกระจายปริมาณการใช้งานไปยังหลายเซิร์ฟเวอร์
- Redundant Network : เครือข่ายสำรองเพื่อรองรับกรณีระบบหลักขัดข้อง
- Traffic Monitoring : ระบบเฝ้าระวังและตรวจสอบปริมาณการใช้งานเครือข่าย

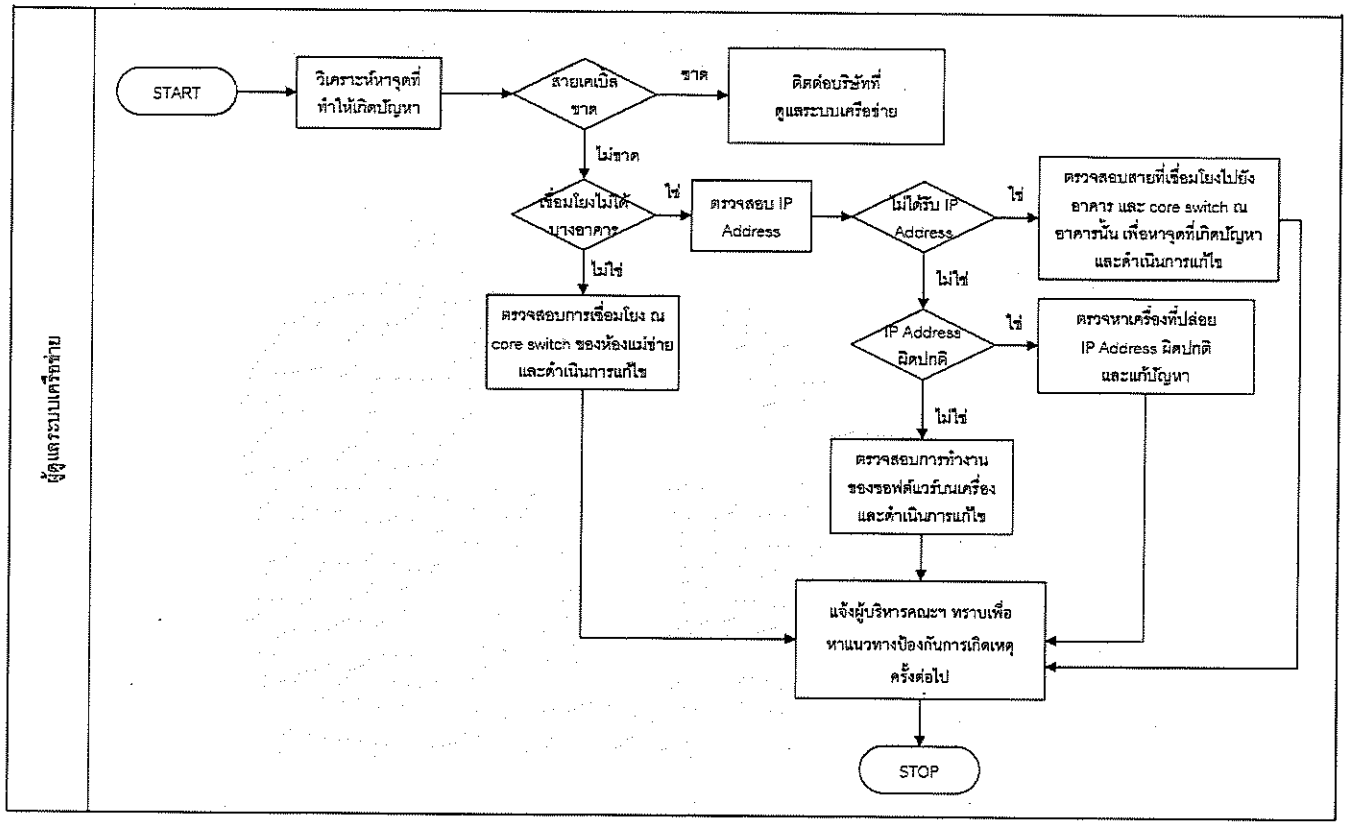
4.1.2 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

1) รีบดำเนินการวิเคราะห์หาจุดที่ทำให้เกิดปัญหา

2) หากสายเคเบิ้ลขาด ให้รีบติดต่อเจ้าหน้าที่บริษัทที่ดูแลบำรุงรักษาระบบเครือข่าย เพื่อดำเนินการซ่อมแซมสายเคเบิ้ลให้เสร็จเรียบร้อยโดยเร็ว

3) หากเชื่อมโยงเครือข่ายไม่ได้เฉพาะบางอาคาร ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว



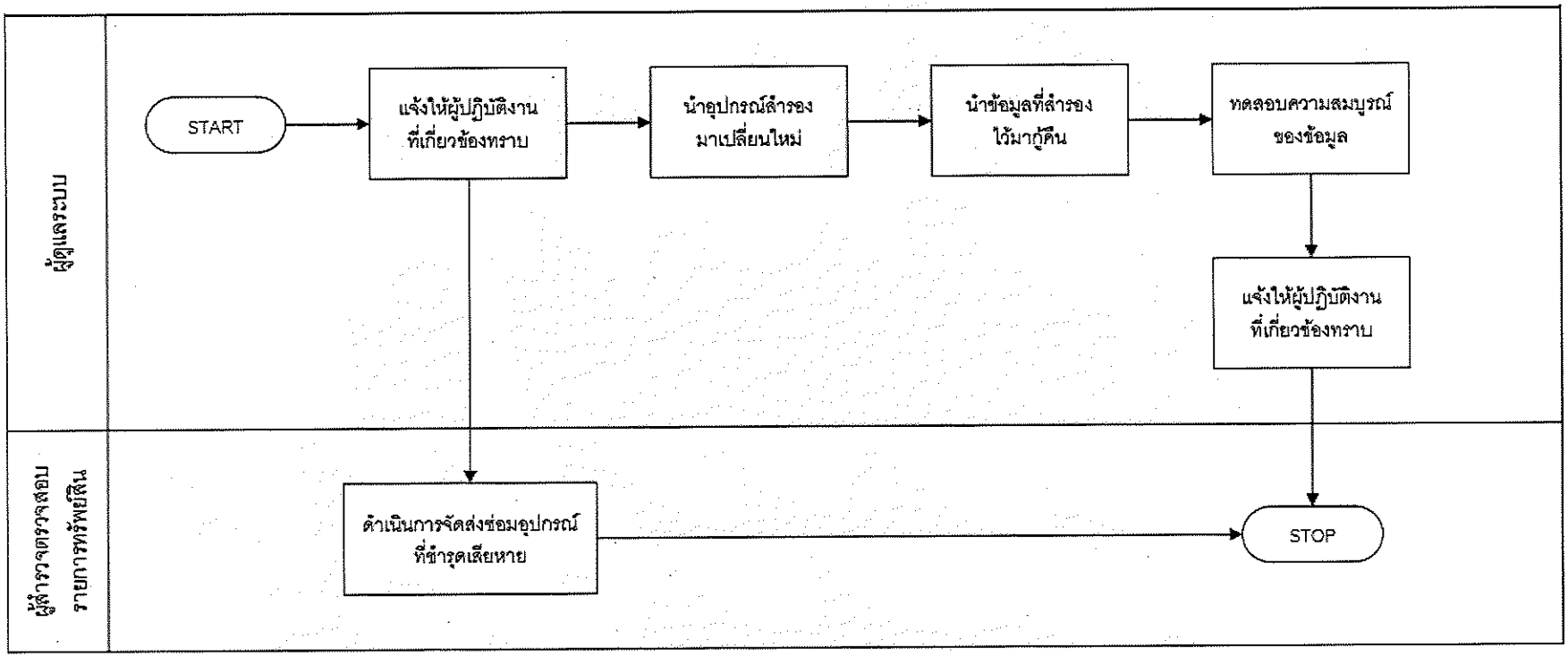
4.1.3 กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย

1) แจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

2) รีบดำเนินการจัดหาอุปกรณ์จัดเก็บข้อมูลมาเปลี่ยนใหม่ และนำข้อมูลที่ได้สำรองไว้มากู้คืนข้อมูลโดยเร็ว

3) ทดสอบความสมบูรณ์ของข้อมูล และแจ้งให้ผู้ปฏิบัติงานที่เกี่ยวข้องทราบ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีอุปกรณ์จัดเก็บข้อมูลเสียหาย



4.1.4 กรณีไฟฟ้าขัดข้อง

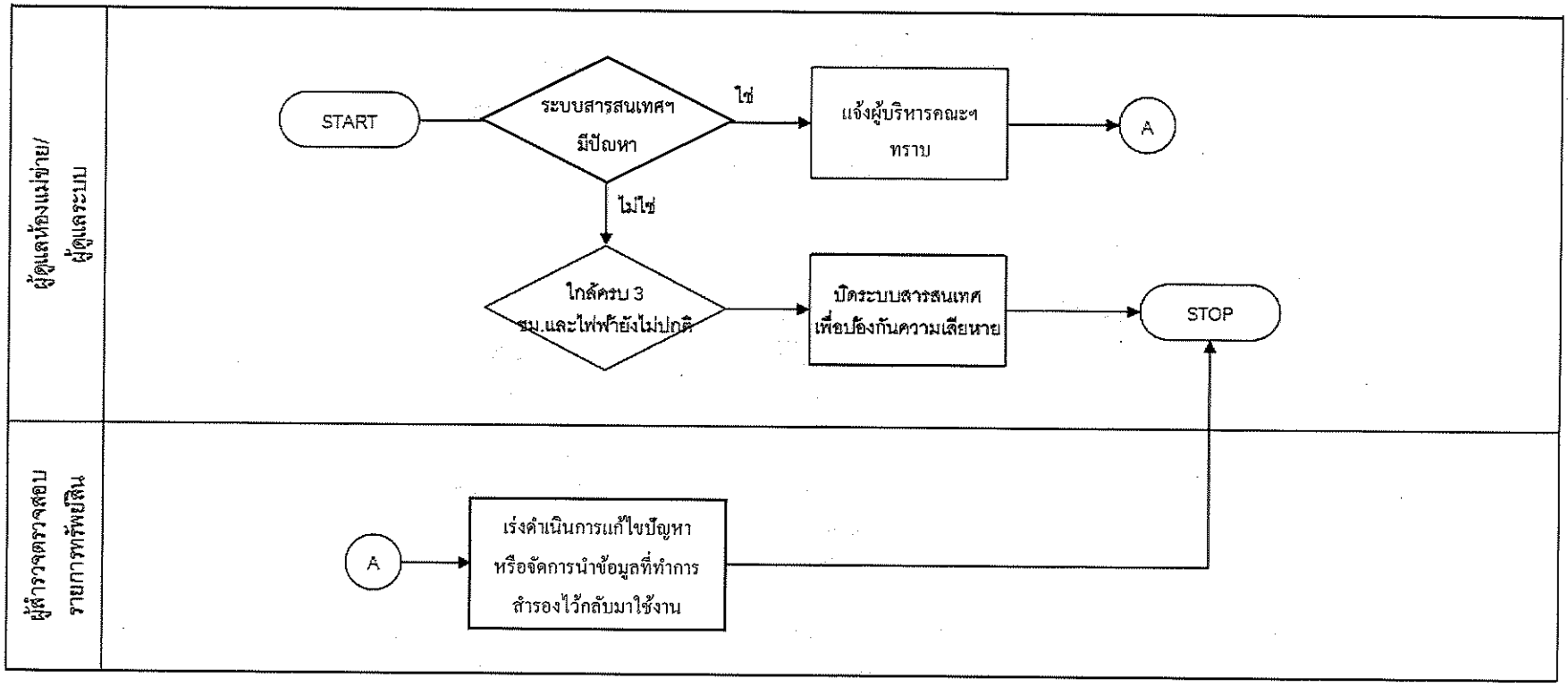
1) ระบบฐานข้อมูลสารสนเทศของคณะฯ ซึ่งติดตั้งไว้ที่กองบริการเทคโนโลยีสารสนเทศและการสื่อสารมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 3 ชั่วโมง

2) หากใกล้ครบ 3 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้มีการประสานงานแจ้งเตือนไปยังผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

3) ผู้ดูแลระบบดำเนินการปิดระบบเพื่อป้องกันความเสียหาย

4) หากระบบฐานข้อมูลสารสนเทศของคณะฯ มีปัญหา ให้แจ้งผู้บังคับบัญชาและเร่งดำเนินการแก้ไขปัญหาที่เกิดขึ้น

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง



4.2 สถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติและโรคระบาด

4.2.1 กรณีไฟไหม้

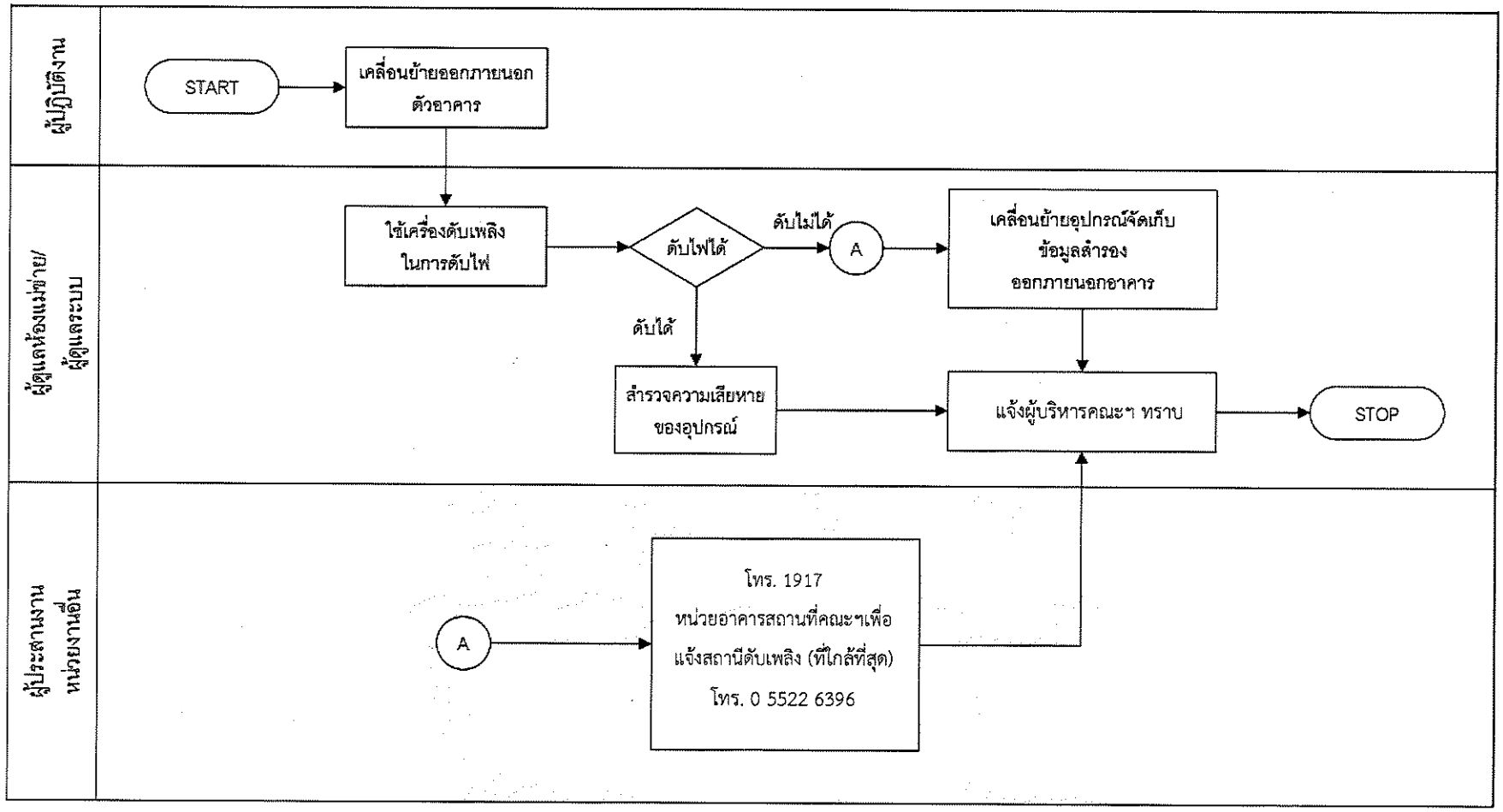
1) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

2) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานอาคารสถานที่และโทรแจ้งสถานีดับเพลิงที่ใกล้ที่สุด คือ องค์การบริหารส่วนตำบลท่าโพธิ์ หมายเลขโทรศัพท์ 0 5522 6396

3) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การ ปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

4) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้



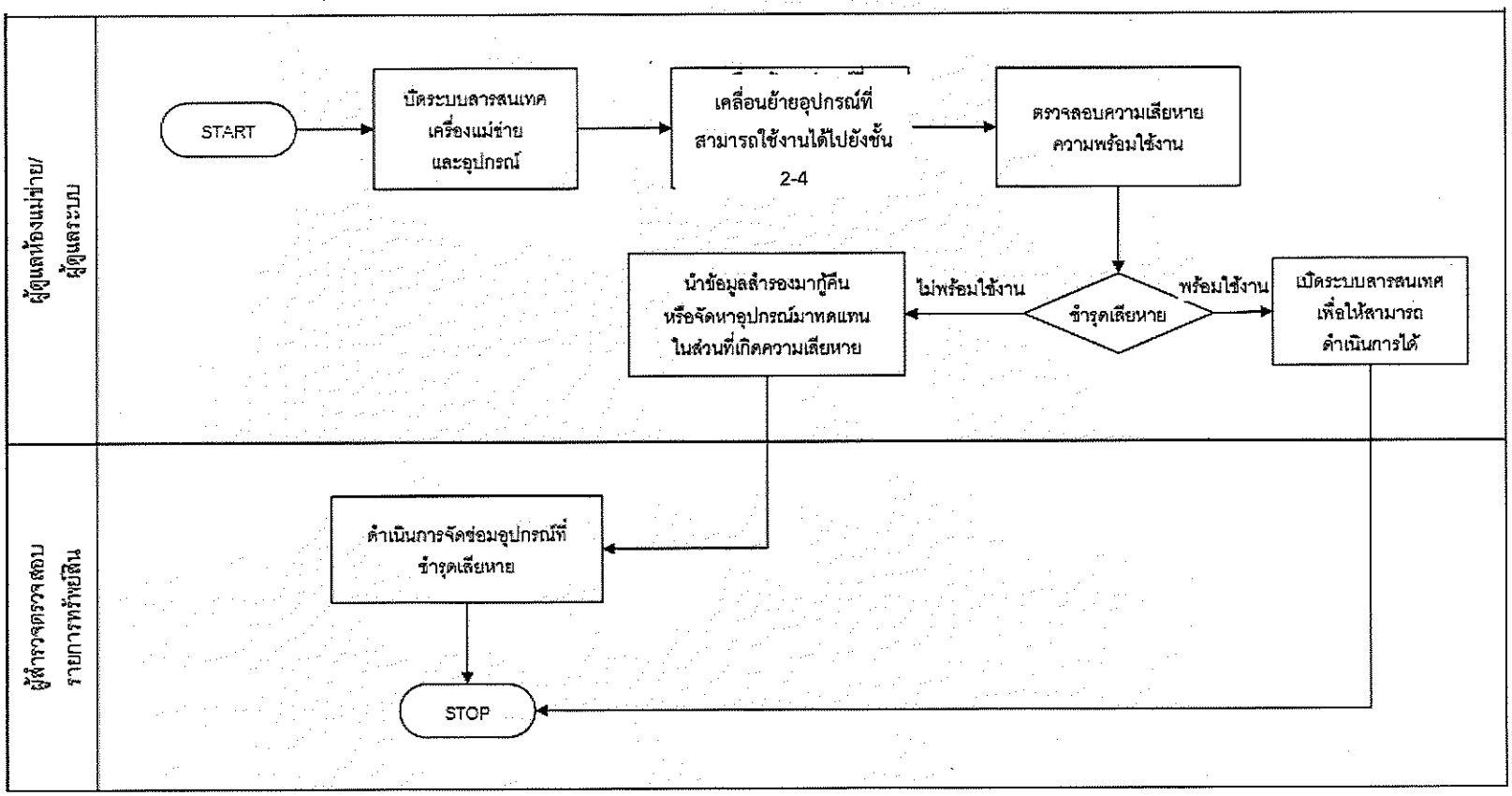
4.2.2 กรณีน้ำท่วม

1) ผู้ดูแลระบบปิดระบบและทำการเคลื่อนย้ายอุปกรณ์ต่าง ๆ บริเวณอาคารคณะฯ ชั้น 1 ที่ยังสามารถใช้งานได้ ไปติดตั้งในบริเวณ ชั้น 2, 3 หรือ ชั้น 4

2) ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

3) ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีน้ำท่วม



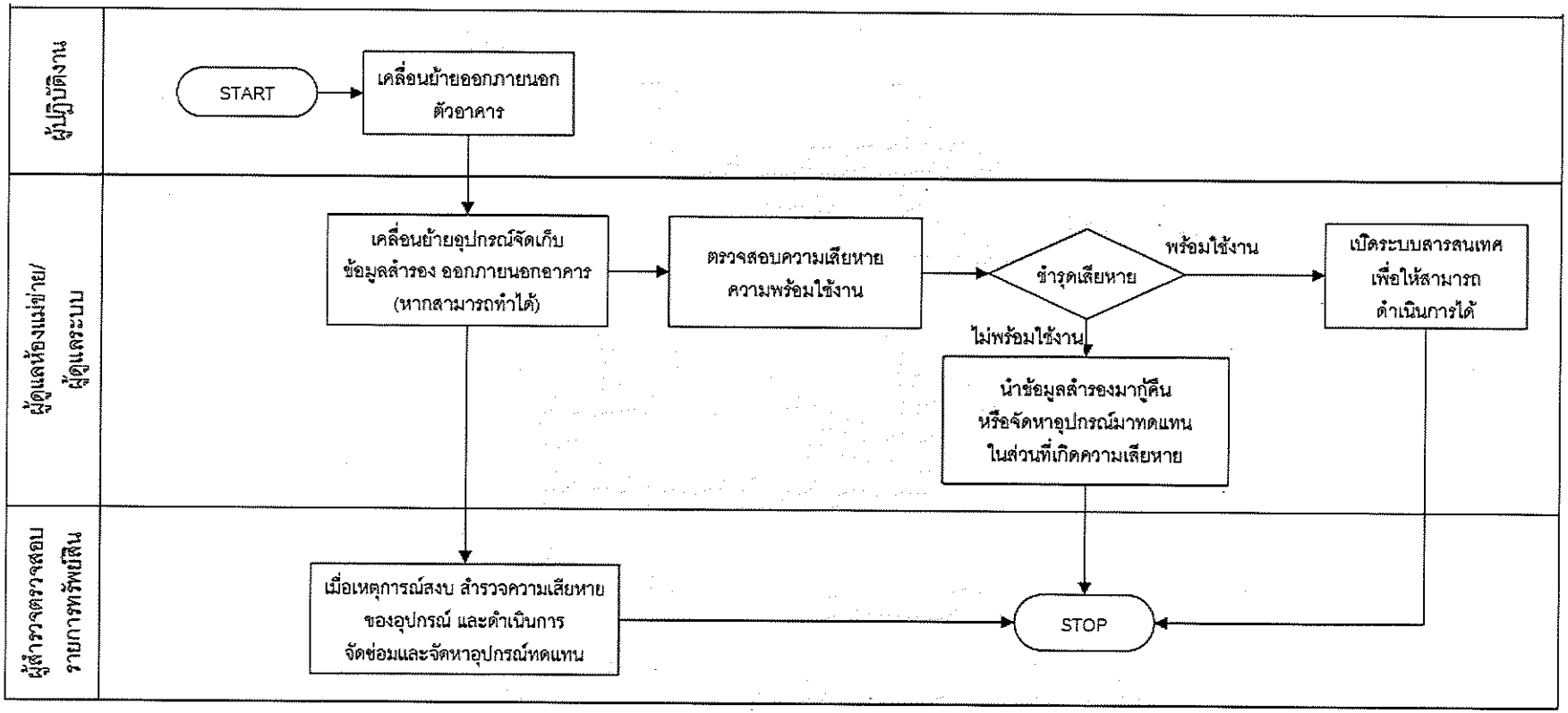
4.2.3 กรณีแผ่นดินไหว

1) ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร

2) ผู้ดูแลระบบนำข้อมูลสำรอง เคลื่อนย้ายไปด้วยหากสามารถทำได้

3) เมื่อเหตุการณ์สงบ ตรวจสอบความชำรุดเสียหาย และดำเนินการแก้ไขเพื่อให้ระบบสามารถดำเนินการต่อไปได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีแผ่นดินไหว



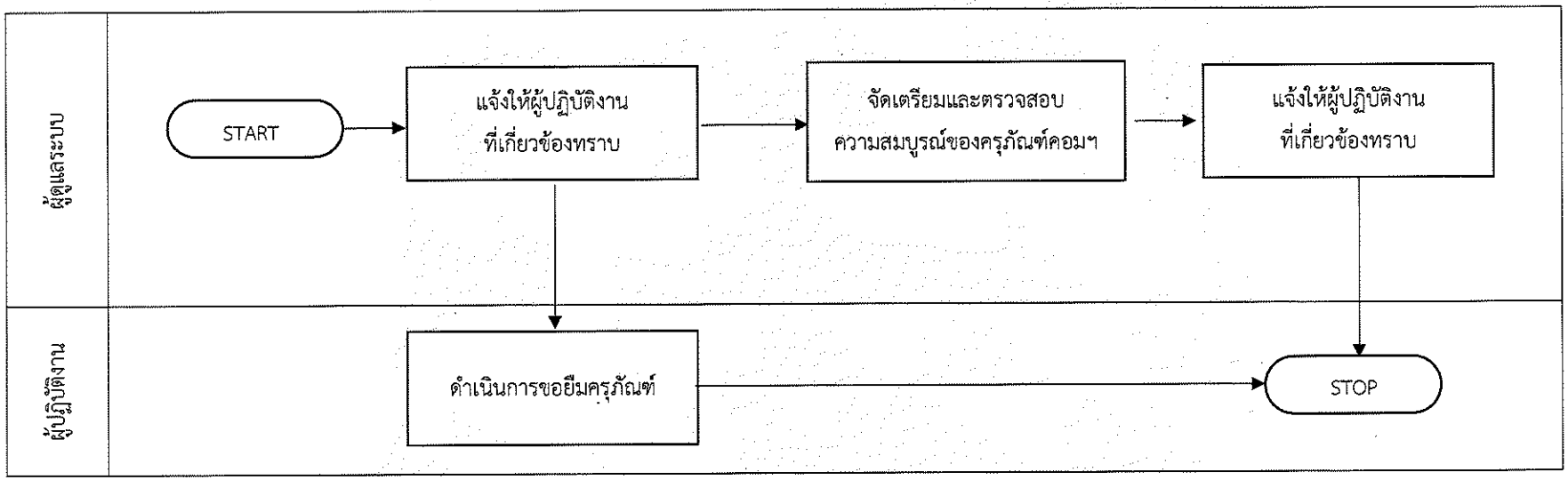
4.2.4 กรณีเกิดสถานการณ์โรคระบาด

1) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้บริหารคณะฯ แจ้งผู้ปฏิบัติงานให้สามารถขอยืมครุภัณฑ์คอมพิวเตอร์เพื่อไปปฏิบัติงาน ณ ที่พักอาศัยได้

2) ผู้ดูแลระบบเร่งดำเนินการประสานงานกับผู้ปฏิบัติงานในการแจ้งความประสงค์ต่อผู้บริหารคณะฯ เพื่อขอยืมครุภัณฑ์คอมพิวเตอร์เพื่อไปปฏิบัติงาน ณ ที่พักอาศัย

3) หลังเหตุการณ์โรคระบาดกลับสู่สภาวะปกติ ให้ผู้ปฏิบัติงาน นำครุภัณฑ์คอมพิวเตอร์ที่ได้ยืมไปมาคืนต่อผู้ดูแลระบบเพื่อตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการในส่วนที่เกี่ยวข้องต่อไป

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีเกิดสถานการณ์โรคระบาด



4.3 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

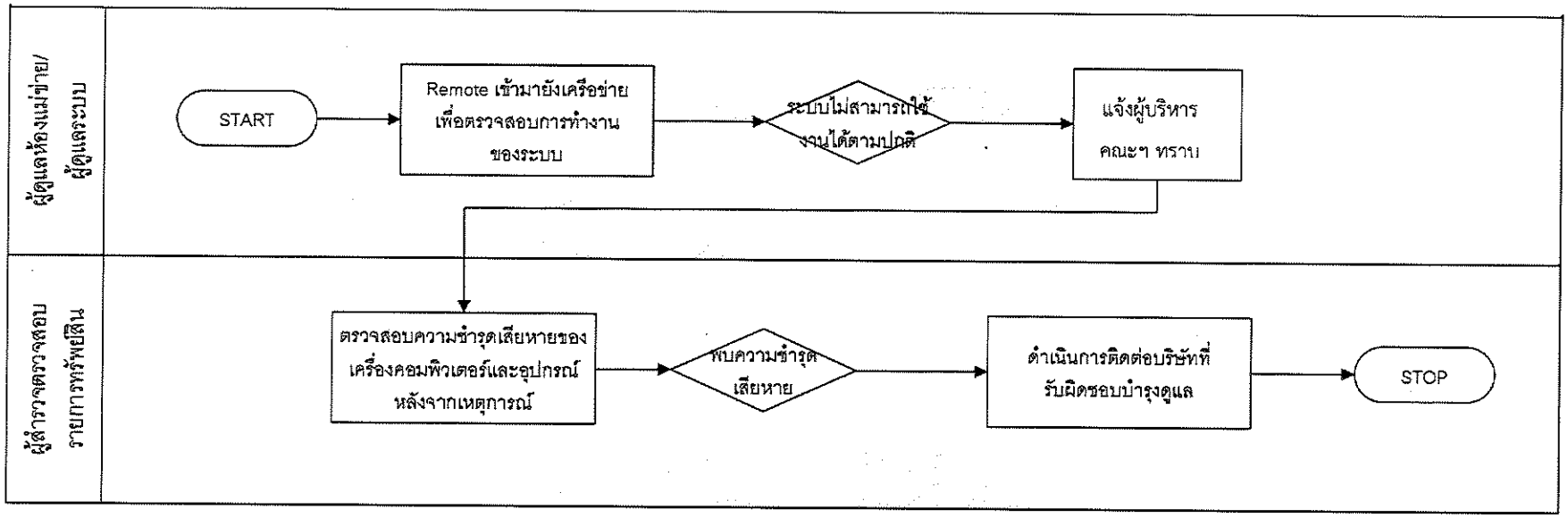
4.3.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

1) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ

2) แจ้งผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสารทราบ

3) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง



4.4 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

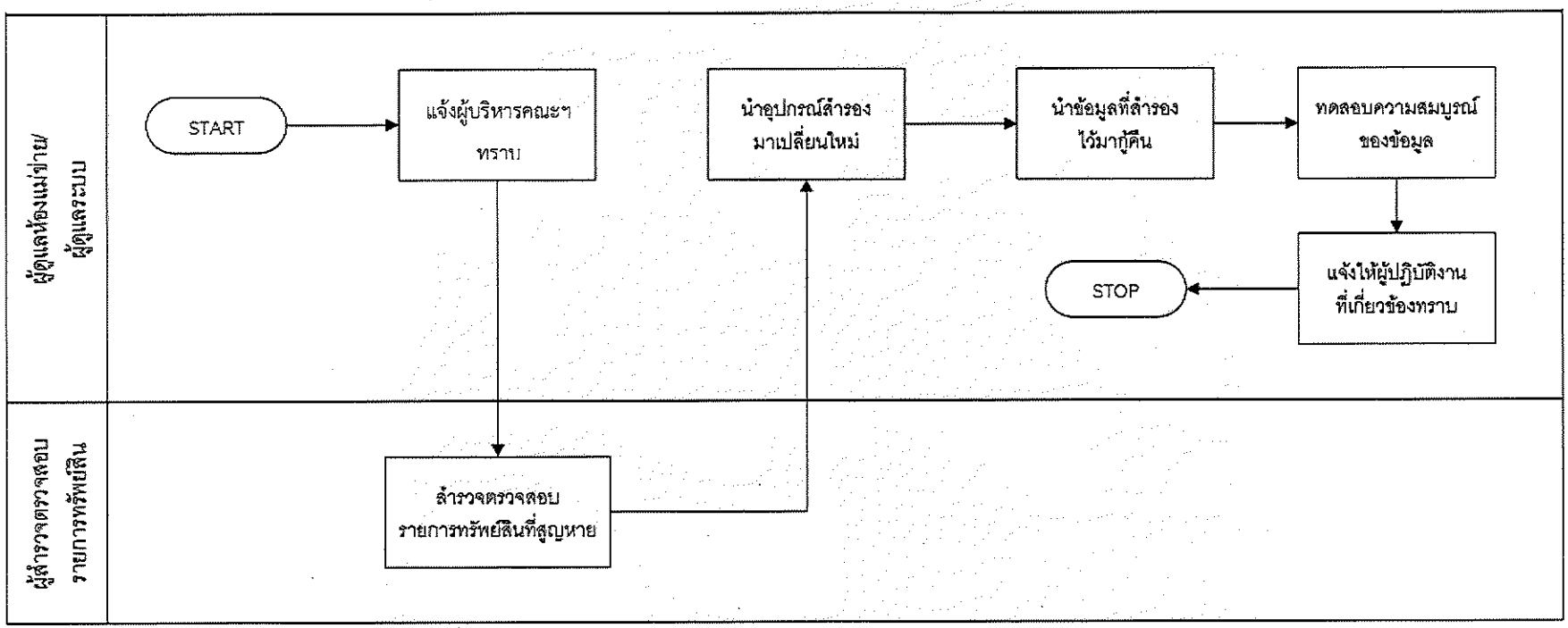
4.4.1 กรณีโจรกรรม

1) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

2) สำรวจตรวจสอบรายการทรัพย์สินที่สูญหาย

3) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้ กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้ตามปกติโดยเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีโจรกรรม

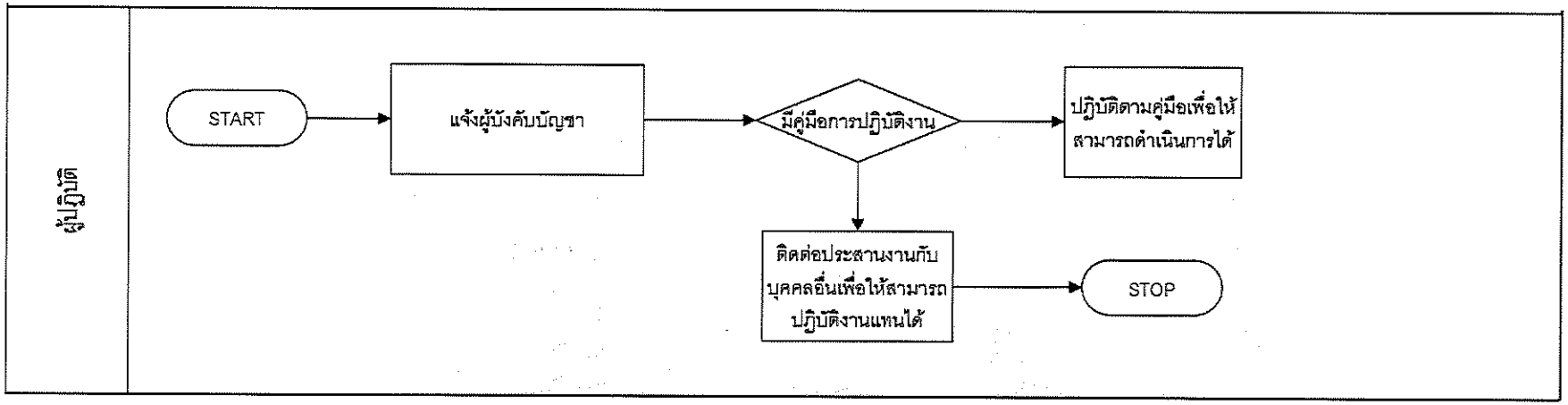


4.4.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

1) แจ้งผู้บังคับบัญชาทราบ

2) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้



การปรับปรุงแผนบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

แผนบริหารความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ คณะสังคมศาสตร์ ต้องได้รับการปรับปรุงอย่างสม่ำเสมอ อย่างน้อยปีละหนึ่งครั้ง หรือภายใน 3 เดือนหลังการทดสอบหรือมีการเปลี่ยนแปลงที่สำคัญ เช่น รายชื่อผู้รับแจ้งเหตุ (Staff Recall List) ซึ่งควรปรับปรุงทุกไตรมาส ทั้งนี้ ต้องจัดทำสำเนาส่งให้เลขานุการคณะกรรมการบริหารความต่อเนื่องด้านเทคโนโลยีสารสนเทศ เพื่อให้ทราบถึงการเปลี่ยนแปลงหน้าที่ ขั้นตอนการปฏิบัติ และฐานข้อมูลที่เกี่ยวข้อง โดยต้องรักษาความเป็นปัจจุบันอยู่เสมอ

แผนการซักซ้อม ทดสอบ และประเมินผลแผน

รอบเวลา	รูปแบบการทดสอบ	หลักฐานที่ต้องเก็บ
ทุก 3 เดือน	ทดสอบ Call Tree	รายงานผลการติดต่อ
ทุก 6 เดือน	Tabletop Exercise	รายงานช่องว่างและข้อเสนอแก้ไข
ปีละ 1 ครั้ง	ทดสอบกู้คืนข้อมูลจริง	รายงาน Restore Test
ปีละ 1 ครั้ง	ซ้อมเหตุการณ์ระบบล่ม/ทำงานสำรอง	รายงานผลการซ้อม

การถอดบทเรียนหลังเหตุการณ์และการปรับปรุงแผน (Log Book)

ประเด็น	รายละเอียด
เหตุการณ์/การซ้อม	.....
วันที่และเวลา	.....
สิ่งที่ทำได้ดี	.....
ปัญหาที่พบ	.....
สิ่งที่ต้องแก้ไข	.....
ผู้รับผิดชอบ	.....
กำหนดแล้วเสร็จ	.....

ภาคผนวก

มาตรฐาน กฎหมาย และแนวปฏิบัติ สำหรับ แผนบริหารความมั่นคงปลอดภัยและความต่อเนื่องของระบบเทคโนโลยีสารสนเทศ ของคณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

มาตรฐานสากล (International Standards)

- AXELOS. (2019). *ITIL 4 Foundation: ITIL 4 Edition*. AXELOS. https://www.axelos.com/certifications/itil-4-foundation
- ISACA. (2019). *COBIT 2019: Governance and Management Objectives*. ISACA. https://www.isaca.org/resources/cobit
- International Organization for Standardization (ISO). (2013). *ISO/IEC 27001:2013 Information security management systems — Requirements*. ISO. https://www.iso.org/isoiec-27001-information-security.html
- International Organization for Standardization (ISO). (2018). *ISO/IEC 27005:2018 Information security risk management*. ISO. https://www.iso.org/standard/75281.html
- International Organization for Standardization (ISO). (2019a). *ISO 22301:2019 Security and resilience — Business continuity management systems — Requirements*. ISO. https://www.iso.org/standard/75106.html
- International Organization for Standardization (ISO). (2019b). *ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. ISO. https://www.iso.org/standard/71670.html
- International Organization for Standardization (ISO). (2022). *ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls*. ISO. https://www.iso.org/standard/75652.html
- National Institute of Standards and Technology (NIST). (2020). *NIST Special Publication 800-53 Revision 5: Security and privacy controls for information systems and organizations*. U.S. Department of Commerce. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

กฎหมายไทย (Thai Laws)

- พระราชบัญญัติคุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562. (2562). ราชกิจจานุเบกษา. https://www.pdpa.or.th
- พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550. (2550). ราชกิจจานุเบกษา. https://ictlawcenter.etda.or.th/th/laws/detail/21
- พระราชบัญญัติว่าด้วยการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562. (2562). ราชกิจจานุเบกษา. https://www.dga.or.th/th/news/news-detail/2533/

ระเบียบและแนวทางภาครัฐ/สถาบัน (Institutional Regulations and Guidelines)

- มหาวิทยาลัยนเรศวร. (ม.ป.ป.). *ระเบียบมหาวิทยาลัยนเรศวรว่าด้วยการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ*. มหาวิทยาลัยนเรศวร.
- สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) [DGA]. (2563). *แนวทางมาตรฐานเทคโนโลยีสารสนเทศสำหรับหน่วยงานภาครัฐ*. https://www.dga.or.th/th/services/standards/

เอกสารและข้อมูลอ้างอิงอื่น (Other References)

- คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร. (2568). *คำสั่งคณะสังคมศาสตร์ ที่ 26/2568 เรื่อง แต่งตั้งคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์.* (https://nu365-my.sharepoint.com/:b:/g/personal/socialsci_nu_ac_th/EUSmQiKK6zpOhfljb7d-EclBtsG-iJxgCZWQBkKShlPJSA?e=KivZOp)
- คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร. (2566). *คำสั่งคณะสังคมศาสตร์ ที่ 53/2566 เรื่อง แต่งตั้งคณะกรรมการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร คณะสังคมศาสตร์.* https://nu365-my.sharepoint.com/:b:/g/personal/sutthisakk_nu_ac_th/EU6sl6tw3PxHsAdAMDwVUOwB5kLOBjyk2Oy2GhpEgKunvg?e=wafopy