แผนรองรับภาวะฉุกเฉินด้านระบบสารสนเทศ
คณะมนุษยศาสตร์และสังคมศาสตร์ มหาวิทยาลัยสงขลานครินทร์

1. วัตถุประสงค์

เพื่อกำหนดแนวทางรองรับเหตุขัดข้องด้านระบบสารสนเทศและโครงสร้างพื้นฐานดิจิทัลให้คณะฯสามารถดำเนินภารกิจสำคัญต่อได้อย่างเหมาะสม ลดผลกระทบต่อผู้ใช้บริการ และสนับสนุนข้อมูลที่มีคุณภาพ พร้อมใช้ และปลอดภัย

2. ขอบเขตระบบและบริการที่เกี่ยวข้อง

แผนฉบับนี้ครอบคลุมระบบและบริการดิจิทัลที่ใช้สนับสนุนภารกิจหลักของคณะฯ เช่น การเรียน การสอน การบริหารจัดการภายใน การเงินและงบประมาณ การบริการนักศึกษา การสื่อสารองค์กร และ การจัดเก็บข้อมูลที่จำเป็นต่อการดำเนินงาน

1) เว็บไซต์คณะฯ และเว็บไซต์หน่วยงานต่าง ๆ

2) ระบบสารสนเทศและระบบบริหารจัดการข้อมูลต่าง ๆ ของคณะฯ ได้แก่ ระบบ Intranet คณะระบบจองห้องประชุมคณะ ระบบจองห้องเรียน ระบบงบประมาณและติดตามงบประมาณ ระบบสนับสนุนงานทะเบียน งานวิชาการ งานทรัพยากรบุคคล งานอาคารสถานที่ งานพัสดุ งานสารบรรณ ระบบ E-meeting งานเทคโนโลยีสารสนเทศ งานวิรัชกิจและสื่อสารองค์กร และระบบฐานข้อมูลอื่น ๆ ที่เกี่ยวข้อง

3) โครงสร้างพื้นฐานด้านเครือข่าย ได้แก่ Internet, LAN, WiFi, Server, ห้องปฏิบัติการคอมพิวเตอร์ และ Smart Classroom

4) ระบบออนไลน์ภายใต้บัญชีผู้ใช้ของมหาวิทยาลัย เช่น Email, Microsoft 365, Google Workspace, Google Drive, Google Form, Google Sheet และ Microsoft Teams

การจำแนกระบบและบริการด้านเทคโนโลยีสารสนเทศในแผนฉบับนี้ เพื่อกำหนดลำดับความสำคัญในการตอบสนองและดำเนินการเมื่อเกิดเหตุขัดข้องหรือเหตุฉุกเฉิน โดยพิจารณาจากจำนวนผู้ได้รับผลกระทบ ความเกี่ยวข้องกับภารกิจหลักของคณะ ความจำเป็นในการให้บริการต่อเนื่อง และระดับความรุนแรงของเหตุการณ์ ทั้งนี้ ระยะเวลาในการแก้ไขหรือกู้คืนระบบให้กลับมาใช้งานได้ปกติอาจแตกต่างกันตามประเภทของเหตุการณ์ ระดับความรุนแรง สาเหตุของปัญหา ขอบเขตผลกระทบ ความเสียหายของระบบหรืออุปกรณ์ และหน่วยงานที่เกี่ยวข้องในการดำเนินการแก้ไข

3. การจำแนกระบบและเป้าหมายการกู้คืน

ระดับความสำคัญ	ตัวอย่างระบบ/บริการ	SLA การตอบสนองเบื้องต้น	แนวทางและ เป้าหมายการดำเนินการ
ระดับวิกฤต (Critical)	ระบบหรือเหตุการณ์ที่กระทบต่อผู้ใช้งานจำนวนมาก หรือเกี่ยวข้องกับภารกิจหลักของคณะ เช่น ระบบยืนยันตัวตนการเข้าใช้งานอินเทอร์เน็ตระบบ MIS/e-Document ระบบ e-Project ระบบ Dashboard/ระบบข้อมูลเพื่อการบริหาร ระบบเครือข่าย เครื่องแม่ข่าย/Server ที่เกี่ยวข้อง รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น ตรวจพบไวรัสหรือ Malware	ภายใน 15 นาที - 1 ชั่วโมง ตามประเภทเหตุการณ์	ตอบสนองเร่งด่วน โดยแจ้งผู้เกี่ยวข้อง ตรวจสอบสถานะระบบ แยกอุปกรณ์ที่มีความเสี่ยง ประสานผู้ดูแลระบบ ผู้พัฒนา หรือศูนย์ IT มหาวิทยาลัย และจัดช่องทางสำรองระหว่างดำเนินการแก้ไข โดยมีเป้าหมายให้ระบบหรือบริการสำคัญกลับมาใช้งานได้เร็วที่สุดตามระดับความรุนแรงของเหตุการณ์

ระดับสำคัญ (Important)	ระบบหรือบริการที่สนับสนุนการทำงานประจำของคณะ เช่น เว็บไซต์คณะ ระบบติดตามงบประมาณ ระบบ TA ระบบฐานข้อมูลและระบบสารสนเทศระดับคณะภายใน และบริการสื่อสารดิจิทัลต่างๆ	ภายในระยะเวลาที่เหมาะสมตามความสำคัญและผลกระทบของงาน	แก้ไขตามลำดับความสำคัญและผลกระทบต่อการปฏิบัติงานและกำหนดวิธีทำงานทดแทนชั่วคราวหากยังไม่สามารถกู้คืนระบบได้ทันที เช่น ใช้ Email, Google Sheet, Excel หรือ Microsoft Teams เพื่อให้การดำเนินงานสามารถต่อเนื่องได้
ระดับสนับสนุน (Support)	เครื่องคอมพิวเตอร์สำนักงานของผู้ใช้ ห้องปฏิบัติการคอมพิวเตอร์ และอุปกรณ์ปลายทาง	ภายใน 30 นาที หรือตามช่องทางรับแจ้งเหตุที่กำหนด	รับคำร้อง ตรวจสอบปัญหาเบื้องต้น และดำเนินการแก้ไขตามลำดับคิวงานและระดับผลกระทบ จัดหาอุปกรณ์สำรองหรือวิธีปฏิบัติทดแทนเฉพาะหน้า เพื่อให้ผู้ใช้งานสามารถปฏิบัติงานหรือจัดการเรียนการสอนได้ต่อเนื่องเท่าที่จำเป็น ทั้งนี้ หากเหตุขัดข้องกระทบต่อภารกิจสำคัญหรือผู้ใช้งานจำนวนมากให้พิจารณายกระดับการดำเนินการตามความเหมาะสม

หมายเหตุ: SLA (Service Level Agreement) หมายถึง กรอบเวลาในการรับทราบเหตุและตอบสนองเบื้องต้น ไม่ใช่ระยะเวลาที่รับประกันว่าจะแก้ไขหรือกู้คืนระบบได้แล้วเสร็จสมบูรณ์ โดยระยะเวลาการแก้ไขและกู้คืนขึ้นอยู่กับระดับความรุนแรงของเหตุการณ์ ขอบเขตผลกระทบ สาเหตุของปัญหา และหน่วยงานที่เกี่ยวข้องในแต่ละกรณี

4. มาตรฐานการตอบสนองเมื่อพบปัญหาฉุกเฉิน (SLA)

เมื่อเกิดเหตุขัดข้องด้านระบบสารสนเทศหรือโครงสร้างพื้นฐานดิจิทัล งานเทคโนโลยีดิจิทัลดำเนินการตอบสนองตามระดับความรุนแรงของเหตุการณ์ระดับวิกฤต (Critical) โดยให้ความสำคัญกับเหตุที่กระทบต่อผู้ใช้จำนวนมาก ระบบสำคัญของคณะ หรือความมั่นคงปลอดภัยของข้อมูลเป็นลำดับต้น

ประเภทเหตุการณ์ฉุกเฉิน	ระดับ	SLA เป้าหมาย	การดำเนินการหลัก	ผู้รับผิดชอบ
คอมพิวเตอร์สำนักงานขัดข้อง	สูง	ภายใน 30 นาที	รับคำร้องผ่านระบบ/ช่องทางที่กำหนด ตรวจสอบปัญหาเบื้องต้น จัดหาอุปกรณ์สำรอง หรือประสานการซ่อมแซมตามความเหมาะสม	ทีม IT

ระบบสารสนเทศหยุดทำงาน เช่น MIS / e-Document / ระบบงานภายใน	สูงมาก	ภายใน 15 นาที	แจ้งผู้ใช้งานผ่านช่องทางที่เหมาะสม ตรวจสอบระบบ และประสานผู้ดูแลระบบหรือผู้พัฒนา	ทีม IT + ผู้ดูแลระบบ
ตรวจพบไวรัสหรือ Malware	สูงมาก	ภายใน 1 ชั่วโมง	แยกอุปกรณ์ออกจากเครือข่าย ตรวจสอบความปลอดภัยของอุปกรณ์ และจัดการปัญหาตามขั้นตอน Incident Response	ทีม IT
ระบบเครือข่ายหรือเครื่องแม่ข่ายหยุดทำงาน	สูงมาก	ภายใน 30 นาที	ตรวจสอบอุปกรณ์เครือข่าย เครื่องแม่ข่าย และระบบที่เกี่ยวข้อง พร้อมประสานศูนย์ IT มหาวิทยาลัย	ทีม IT

5. แผนเตรียมการในภาวะฉุกเฉิน

งานเทคโนโลยีดิจิทัลดำเนินการเตรียมความพร้อมด้านระบบสารสนเทศ โดยมีแผนเตรียมการในภาวะฉุกเฉิน ครอบคลุมการสำรองข้อมูล การกู้คืนข้อมูล การป้องกันภัยไซเบอร์ และระบบไฟฟ้า/ความต่อเนื่องของระบบ ดังนี้

รายการ	การดำเนินการ	รอบ/ระยะเวลา	ผู้รับผิดชอบ
การสำรองข้อมูล (Backup)	สำรองชุดคำสั่งโปรแกรมและฐานข้อมูลของระบบสำคัญ พร้อมตรวจสอบความสมบูรณ์ของข้อมูลสำรอง จัดเก็บเป็นไฟล์ ZIP บนเครื่องแม่ข่าย และมีสำเนาเพิ่มเติมที่เครื่องผู้ดูแล/ผู้พัฒนาระบบ จำนวน 2 เครื่อง	ทุกเดือนพร้อมตรวจสอบความสมบูรณ์	เจ้าหน้าที่ IT
การกู้คืนข้อมูล (Recovery)	ดำเนินการตามแผนกู้คืนข้อมูล ทดสอบความถูกต้องของข้อมูลและระบบก่อนเปิดใช้งาน และรายงานผลเพื่อปรับปรุงแนวทางป้องกัน	ทดสอบทุก 6 เดือน และดำเนินการทันทีเมื่อเกิดเหตุ	เจ้าหน้าที่ IT
การป้องกันไวรัสและความพร้อมของระบบ	ใช้ PSU Passport หรือบัญชีผู้ใช้มหาวิทยาลัยเป็นกลไกหลักในการยืนยันตัวตน กำหนดสิทธิ์ตามบทบาทผู้ใช้ ดูแลและปรับปรุงระบบป้องกันไวรัส ตรวจสอบความพร้อมของอุปกรณ์และระบบสารสนเทศอย่างต่อเนื่อง	อัปเดตทุกไตรมาส ตรวจสอบทุกวัน	เจ้าหน้าที่ IT
ระบบไฟฟ้าและความต่อเนื่องของระบบ	ดูแลระบบสำรองไฟและอุปกรณ์สำคัญ เช่น Server อุปกรณ์เครือข่าย และระบบที่เกี่ยวข้อง พร้อมติดตามความเสี่ยงด้านโครงสร้างพื้นฐาน	ตรวจสอบทุก 6 เดือน ตามแผน BCP	เจ้าหน้าที่ IT

6. แนวทางปฏิบัติในภาวะฉุกเฉิน

6.1 กรณีเกิดภัยคุกคามต่อระบบเทคโนโลยีสารสนเทศ (Cyber Attack)

กรณีตรวจพบหรือสงสัยว่ามีภัยคุกคามทางไซเบอร์ เช่น บัญชีผู้ใช้ถูกเข้าถึงโดยไม่ได้รับอนุญาต มัลแวร์/ไวรัส ข้อมูลผิดปกติ ระบบทำงานผิดปกติ หรือมีความเสี่ยงต่อการรั่วไหลของข้อมูล ให้ดำเนินการตามช่วงเวลาดังนี้

ช่วงเวลา/มาตรการ	แนวทางปฏิบัติ
ก่อนเกิดเหตุ	สำรองข้อมูลตามรอบที่กำหนด กำหนดสิทธิ์ผู้ใช้ตามบทบาท ใช้ PSU Passport/บัญชีมหาวิทยาลัย ให้คำแนะนำการใช้งานรหัสผ่าน /MFA ตรวจสอบและปรับปรุงระบบเมื่อมีความจำเป็น
ขณะเกิดเหตุ	รับแจ้งและบันทึกรายละเอียด แยกเครื่องหรือบัญชีที่สงสัยออกจากการใช้งานเมื่อจำเป็น ปิดระบบชั่วคราว/เปิด Maintenance Mode หากกระทบวงกว้าง ประสานผู้ดูแลระบบและหน่วยงานกลางที่เกี่ยวข้อง แจ้งผู้ใช้ผ่านช่องทางที่เหมาะสม
หลังเกิดเหตุ	ตรวจสอบสาเหตุและขอบเขตผลกระทบ กู้คืนข้อมูลจากไฟล์สำรองเมื่อจำเป็น ทดสอบความถูกต้องของระบบก่อนเปิดใช้งาน เปลี่ยนรหัสผ่าน/ปรับสิทธิ์ผู้ใช้ที่เกี่ยวข้อง สรุปเหตุการณ์และแนวทางป้องกันซ้ำ
การป้องกันเพิ่มเติม	จำกัดสิทธิ์เท่าที่จำเป็น ใช้บัญชีมหาวิทยาลัยในการยืนยันตัวตน สำรองข้อมูลหลายจุด แจ้งเตือนผู้ใช้เรื่องลิงก์/ไฟล์แนบเสี่ยง ทบทวนขั้นตอนการรับมือและช่องทางติดต่อ

ขั้นตอนการตอบสนอง กรณี Cyber Attack

พบเหตุ/ รับแจ้ง	→	ตรวจสอบ เบื้องต้น	→	แยกความเสี่ยง/ จำกัดสิทธิ์	→	ประเมิน ผลกระทบ	→	กู้คืนและทดสอบ	→	แจ้งผู้ใช้/ สรุปรายงาน

6.2 กรณีเกิดไฟฟ้าดับหรือไฟฟ้าขัดข้อง

กรณีไฟฟ้าดับหรือไฟฟ้าขัดข้องอาจส่งผลต่อ Server อุปกรณ์เครือข่าย ห้องปฏิบัติการคอมพิวเตอร์ และ Smart Classroom จึงกำหนดแนวทางแยกเป็น 2 กรณี ได้แก่ กรณีทราบล่วงหน้า และกรณีไม่ทราบล่วงหน้า

สถานการณ์	แนวปฏิบัติ
กรณีทราบล่วงหน้า	รับทราบกำหนดการจากหน่วยงานที่เกี่ยวข้อง แจ้งผู้ใช้ล่วงหน้าตามช่องทางที่เหมาะสม สำรองข้อมูลก่อนช่วงเวลาดับไฟ ปิดระบบหรืออุปกรณ์ที่จำเป็นอย่างปลอดภัย เตรียมช่องทางทำงานสำรอง เช่น Email, Google Drive, Google Sheet, Teams
กรณีไม่ทราบล่วงหน้า	ตรวจสอบผลกระทบต่อ Server/เครือข่าย/อุปกรณ์สำคัญ ใช้ UPS เพื่อพยุงระบบเท่าที่ทำได้ หากคาดว่าจะดับนานให้ปิดระบบอย่างปลอดภัยและแจ้งผู้ใช้ถึงสถานะและช่องทางสำรอง ตรวจสอบระบบหลังไฟกลับก่อนเปิดใช้งานเต็มรูปแบบ

หลังไฟฟ้ากลับสู่ปกติ	เปิดระบบตามลำดับความสำคัญ ตรวจสอบ Server ฐานข้อมูล และบริการเครือข่าย ทดสอบการเข้าใช้งานระบบสำคัญ แจ้งผู้ใช้เมื่อระบบกลับมาใช้งานได้ บันทึกปัญหาเพื่อปรับปรุงแผน

ขั้นตอนการตอบสนอง กรณีไฟฟ้าดับหรือไฟฟ้าขัดข้อง

ทราบเหตุหรือรับแจ้ง	→	ประเมินผลกระทบ	→	สำรอง/ปิดระบบปลอดภัย	→	ใช้ช่องทางสำรอง	→	เปิดระบบหลังไฟกลับ	→	ทดสอบและแจ้งผู้ใช้

6.3 กรณีระบบ IT ล้มเหลว/Server หรือฐานข้อมูลขัดข้อง

ขั้นตอน	แนวทางปฏิบัติ
รับแจ้งและตรวจสอบ	รับแจ้งจากผู้ใช้หรือพบความผิดปกติจากการตรวจสอบระบบ ระบุระบบที่ได้รับผลกระทบ เวลาเกิดเหตุ และกลุ่มผู้ใช้ที่ได้รับผลกระทบ
ควบคุมสถานการณ์	ประเมินว่าควรปิดระบบชั่วคราว เปิด Maintenance Mode หรือจำกัดการเข้าใช้งานบางส่วน เพื่อป้องกันข้อมูลผิดพลาดเพิ่มเติม
กู้คืนระบบ	ตรวจสอบไฟล์ระบบ ฐานข้อมูล และเครื่องแม่ข่าย กู้คืนจากไฟล์สำรองเมื่อจำเป็น และทดสอบความถูกต้องก่อนเปิดให้ผู้ใช้ใช้งาน
ช่องทางสำรอง	ระหว่างระบบหลักขัดข้อง ให้หน่วยงานใช้ Email, Google Form, Google Sheet, Excel, Google Drive และ Microsoft Teams เพื่อให้การดำเนินงานสำคัญยังดำเนินต่อได้
สรุปและป้องกันซ้ำ	สรุปสาเหตุ ผลกระทบ ระยะเวลาหยุดชะงัก และข้อเสนอแนะเพื่อปรับปรุงรอบการสำรอง การแจ้งเตือน หรือขั้นตอนการดูแลระบบ

ขั้นตอนการตอบสนอง กรณีระบบ IT ล้มเหลว/Server หรือฐานข้อมูลขัดข้อง

รับแจ้ง/พบปัญหา	→	ตรวจสอบระบบ	→	ควบคุม/ปิดชั่วคราว	→	กู้คืนจาก Backup	→	ทดสอบระบบ	→	เปิดใช้งานและสรุปเหตุ

7. ช่องทางสื่อสารและการประสานงาน

1) ช่องทางแจ้งผู้ใช้ ได้แก่ เว็บไซต์คณะ อีเมล เพจ HUSO ICT และช่องทางประสานงานภายใน

2) ช่องทางทำงานสำรอง ได้แก่ Email, Google Drive, Google Form, Google Sheet, Excel และ Microsoft Teams

3) การประสานงาน ได้แก่ งานเทคโนโลยีดิจิทัล หน่วยงานเจ้าของข้อมูล ผู้ดูแลระบบ ผู้บริหารที่เกี่ยวข้อง และหน่วยงานกลางของมหาวิทยาลัยเมื่อเป็นระบบ/บริการกลาง

8. ผลลัพธ์ที่คาดหวัง

1) ระบบสารสนเทศสำคัญยังสามารถสนับสนุนการดำเนินงานของคณะได้อย่างต่อเนื่อง หรือมีช่องทางสำรองรองรับ

2) ลดความเสี่ยงจากการสูญหายของข้อมูลสำคัญ และสามารถตรวจสอบหรือนำข้อมูลกลับมาใช้ได้เมื่อเกิดเหตุจำเป็น

3) ผู้ใช้บริการรับทราบสถานะของระบบ แนวทางปฏิบัติ และช่องทางขอความช่วยเหลืออย่างชัดเจน