แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
และ
แผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ

(ฉบับปรับปรุง พ.ศ.2567)

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร
Faculty of Social Sciences, Naresuan University

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ และแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

(ฉบับปรับปรุง พ.ศ.2567)

สารบัญ

หน้า

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

หลักการ

คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร มีการนำเทคโนโลยีสารสนเทศมาใช้ในการบริหารจัดการภายในองค์กรและสนับสนุนการปฏิบัติงานเพื่อความสะดวกในการใช้งานและความสะดวกในการสร้างข้อมูลสารสนเทศอันมีประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานตามภาระหน้าที่ความรับผิดชอบของบุคลากร ซึ่งข้อมูลสารสนเทศต่าง ๆ จะมีจำนวนเพิ่มมากขึ้น ดังนั้น องค์กรจำเป็นจะต้องมีการจัดทำแผนรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ อาศัยอำนาจตามความในมาตรา 20 มาตรา 21 และมาตรา 37 แห่งพระราชบัญญัติมหาวิทยาลัยนเรศวร พ.ศ. 2533 ประกอบกับมติคณะกรรมการบริหารมหาวิทยาลัยนเรศวร ในการประชุมครั้งที่ 19/2566 เมื่อวันที่ 17 ตุลาคม 2566 ให้กำหนดแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ มหาวิทยาลัยนเรศวร จึงจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวรขึ้นเพื่อให้เป็นไปตามพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

โดยวิธีปฏิบัติดังกล่าวต้องได้รับความร่วมมือจากผู้ดูแลระบบ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง ในการถือปฏิบัติตามอย่างเคร่งครัด จึงหวังเป็นอย่างยิ่งว่าแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ฉบับนี้ จะเป็นคู่มือให้กับผู้ดูแลระบบ และผู้ใช้บริการ ในการถือปฏิบัติ เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร ต่อไป

วัตถุประสงค์

1. เพื่อให้มีแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ คณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร โดยสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง สำหรับผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง ใช้เป็นคู่มือและถือปฏิบัติอย่างเคร่งครัด ตามหลักจริยธรรม
2. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที
3. เพื่อสร้างความตระหนักและความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่ผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง
4. ช่วยลดความสูญเสียหรือความเสียหายจากภัยคุกคามด้านความมั่นคงปลอดภัย ที่อาจเกิดขึ้นกับข้อมูลสารสนเทศขององค์กร
5. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของหน่วยงาน

นิยามศัพท์

“มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยนเรศวร

"ส่วนงาน" หมายความว่า สำนักงานอธิกรบดี บัณฑิตวิทยาลัย คณะ วิทยาลัย สถาบัน สำนัก ศูนย์ และหน่วยงานที่เรียกชื่ออย่างอื่นมีฐานะเทียบเท่าคณะที่เป็นส่วนราชการและที่สภามหาวิทยาลัยประกาศจัดตั้ง

“ผู้ดูแลระบบส่วนกลาง” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีภาระหน้าที่รับผิดชอบในการดูแล รักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายในระดับมหาวิทยาลัย

“ผู้ดูแลระบบ” หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีภาระหน้าที่รับผิดชอบในการดูแล รักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายของคณะสังคมศาสตร์ มหาวิทยาลัยนเรศวร

“ผู้พัฒนาระบบ” หมายความว่า ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศของคณะสังคมศาสตร์

“เจ้าของข้อมูล” หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย ซึ่งหมายถึงข้อมูลส่วนบุคคล และข้อมูลของหน่วยงาน ภายในคณะสังคมศาสตร์

“ผู้ใช้งาน” หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของคณะสังคมศาสตร์ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของคณะสังคมศาสตร์

“ผู้บริหาร” หมายความว่า คณบดี รองคณบดี ผู้ช่วยคณบดี หัวหน้าสำนักฯ หัวหน้างาน ของคณะสังคมศาสตร์

“เจ้าหน้าที่” หมายความว่า ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ของคณะสังคมศาสตร์

“นิสิต” หมายความว่า นิสิตระดับปริญญาตรีปริญญาโท ปริญญาเอก ของคณะสังคมศาสตร์

“บุคลากรผู้ประสานงานภายนอก” หมายความว่า เจ้าหน้าที่ หรือบุคลากรภายนอกคณะสังคมศาสตร์ที่คอยติดต่อประสานงานเมื่อเกิดปัญหาการใช้งานที่มีความเกี่ยวข้อง เช่น เจ้าหน้าที่กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยนเรศวร

“NU Account” หมายความว่า บัญชีเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัยนเรศวร ซึ่งประกอบด้วย Username และ Password ซึ่งถูกสร้างขึ้นเพื่อเป็นการกำหนดสิทธิการเข้าถึงข้อมูลสารสนเทศส่วนบุคคลของตนเองและสารสนเทศส่วนกลางของมหาวิทยาลัย ผู้ใช้งานจำเป็นต้องรักษา NU Account ของตนเองโดยไม่เผยแพร่แก่ผู้อื่น หรือใช้งานร่วมกับผู้อื่น เพื่อป้องกันข้อมูลส่วนบุคคลถูกนำไปใช้งานโดยไม่ได้รับอนุญาต

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Cyber Security Plan)

อ้างอิงมาตรฐาน:

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/CyberSecurityAct-2019.pdf

2. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วย งานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/CyberSecuritySTDFramework-2021.pdf

3. กรอบมาตรฐานการรักษาความปลอดภัยไซเบอร์ ISO 27001 (ISO/IEC 27001)

   แหล่งอ้างอิง: https://www.omnex.com/aerospace/consulting-implementation-coaching-aerospace-iso-27001-cybersecurity

4. กรอบมาตรฐานการรักษาความปลอดภัยไซเบอร์ NIST Cybersecurity Framework (CSF)

   แหล่งอ้างอิง: https://verveindustrial.com/resources/whitepaper/5-steps-to-greater-security-maturity-with-nist-csf/

5. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/EcommSecuritySTD.pdf

1. การบริหารจัดการระบบเครือข่ายคอมพิวเตอร์

คณะสังคมศาสตร์มีการให้บริการระบบเครือข่ายคอมพิวเตอร์ภายในคณะฯ ภายใต้การควบคุมกำกับดูแลการบริหารจัดการของกองบริการเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยนเรศวร โดยมีแนวทางในการบริหารระบบเครือข่าย เพื่อป้องกันความเสียหายอันเกิดจากการกระทำที่ไม่ถูกต้อง และให้เป็นแนวปฏิบัติงานอย่างมีประสิทธิภาพแก่บุคลากร และนิสิตของมหาวิทยาลัย ทั้งในด้านฮาร์ดแวร์และซอฟต์แวร์ ข้อกำหนด เกี่ยวกับการจัดการไอพีแอดเดรส (IP address) การตรวจสอบระบบเครือข่าย การเข้าถึงระบบจากระยะไกล การซ่อมบำรุง และการดำเนินการเมื่อระบบขัดข้อง โดยมีการบริหารจัดการ ดังนี้

แนวปฏิบัติของผู้ดูแลระบบ

1. การลงทะเบียนผู้ใช้ใหม่ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องจัดทำระเบียบปฏิบัติในการลงทะเบียนผู้ใช้ใหม่เพื่อให้สามารถใช้งานระบบสารสนเทศและต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งาน ในกรณีที่มีการยกเลิกการใช้งาน เช่น การจบการศึกษาของนิสิตหรือการลาออกของ บุคลากร

2. การบริหารสิทธิ์การเข้าถึงระบบคอมพิวเตอร์และเครือข่ายของผู้ใช้ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายจะกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบรวมทั้งกำหนดสิทธิ์แยกตาม หน้าที่ที่รับผิดชอบ ตามที่ผู้บริหารมหาวิทยาลัยหรือคณะหรือสำนักงานต่างๆ เป็นผู้กำหนด

3. กำหนดสิทธิ์ในการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนตามประเภทของงานที่ได้รับ อนุมัติให้ใช้ระบบจากระยะไกล

4. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัย ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัยสามารถเข้าใช้งาน เครือข่ายและระบบสารสนเทศได้

5. ตรวจสอบการเชื่อมโยงเซิร์ฟเวอร์กับเส้นทางเชื่อมโยงการสื่อสารของเครือข่ายเพื่อให้ระบบสามารถให้บริการได้ตามปกติ

6. ตรวจสอบการทำงานของอุปกรณ์เครือข่ายหลักและระบบสนับสนุนการให้บริการเป็นประจำทุกเดือน

7. ตรวจสอบการให้บริการของอุปกรณ์ที่มีหน้าที่ในการกระจายสัญญาณอินเทอร์เน็ตในเครือข่ายไร้สาย NU Wi-Fi และ Edu roam ให้สามารถพร้อมใช้งานได้เป็นปกติเป็นประจำทุกเดือน

8. ในกรณีที่ต้องหยุดระบบเครือข่ายเพื่อซ่อมบำรุง ผู้ดูแลระบบต้องจัดทำแผนและขั้นตอนการซ่อมบำรุงรักษา ระบบ เสนอขออนุมัติจากผู้บริหารคณะฯ ก่อนดำเนินการล่วงหน้าไม่ น้อยกว่า 3 วันทำการ

9. ตรวจสอบการโจมตี บุกรุก การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีหน้าที่รับผิดชอบ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายเป็นประจำทุกสัปดาห์

10. เลือกใช้วิธีการควบคุม MAC Address ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งานรหัสผ่านที่กำหนดไว้เท่านั้น เข้าใช้งานระบบเครือข่ายไร้สายได้อย่างถูกต้อง

11. มีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) และติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และเก็บข้อมูลจราจรผ่านระบบครือข่ายตาม พรบ. ว่าด้วยการกระทำผิดทางคอมพิวเตอร์ 2550 (เครื่องเซิฟเวอร์: ใช้บริการ CITCOMS)

12. มีระบบปรับอากาศแบบควบคุมอุณหภูมิ (10 - 26.7°C) และความชื้นสัมพัทธ์ (20 - 80%) (เครื่องเซิฟเวอร์: ใช้บริการ CITCOMS)

13. ติดตั้งระบบรักษาความปลอดภัยในห้อง เช่น กล้อง CCTV ระบบการเข้า-ออกอาคาร/ห้องทำงานโดยระบบ RFID แสกนใบหน้า หรือ แสกนลายนิ้วมือ

14. มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้า (เครื่องเซิฟเวอร์: ใช้บริการ CITCOMS)

15. มีระบบป้องกันไฟฟ้าจากฟ้าผ่า และระบบและอุปกรณ์ป้องกันอัคคีภัย

16. ติดตั้งฉนวนกันไฟไหม้ที่ฝ้าเพดานและผนังกำแพงห้อง

ผลลัพธ์: 1) สามารถระบุและแก้ไขปัญหาเชิงระบบเมื่อพบปัญหา ทำให้การทำงานของคณะฯ ได้ตามปรกติได้

2) สามารถให้คำแนะนำการป้องกันแก่ผู้ใช้งานได้

แนวปฏิบัติของผู้ใช้งาน

เจ้าหน้าที่งานบุคคลผู้รับผิดชอบ ต้องแจ้งให้หน่วยเทคโนโลยีสารสนเทศทราบเป็นลายลักษณ์อักษร เมื่อบุคลากรมีการว่าจ้างงาน เปลี่ยนแปลงสภาพการจ้างงาน ลาออกหรือมีคำสั่งสิ้นสุดการเป็นผู้บริหาร บุคลากรและลูกจ้าง มีการถึงแก่กรรม มีการโอนย้ายข้ามหน่วยงานราชการ เพื่อให้ผู้ดูแลระบบกำหนดสิทธิ์ หรือยกเลิกสิทธิ์การเข้าถึงระบบเครือข่าย

ผลลัพธ์: 1) สามารถเข้าใช้งานระบบสารสนเทศที่ตนเองมีสิทธิเข้าใช้งานได้

2) ข้อมูลส่วนบุคคลไม่ถูกนำไปใช้โดยมิได้ยินยอม

2. การบริหารจัดการครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง

กำหนดให้มีมาตรการและแนวทางในการติดตั้งครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง การติดตั้งซอฟต์แวร์ ระบบปฏิบัติการ การติดตั้งโปรแกรมประยุกต์สำหรับใช้งานกับอุปกรณ์ เพื่อสนับสนุนการปฏิบัติงานเพื่อให้มีแนวปฏิบัติเป็นมาตรฐานเดียวกันอย่างมีประสิทธิภาพ เป็นไปตามข้อกำหนด มาตรการและแนวทางในการใช้งานครุภัณฑ์คอมพิวเตอร์และอุปกรณ์ต่อพ่วง เพื่อความมั่นคงปลอดภัยของคอมพิวเตอร์เพื่อใช้ในการปฏิบัติงาน ซึ่งทั้งที่เป็นทรัพย์สินของมหาวิทยาลัย หรือเป็นทรัพย์สินส่วนตัวของผู้ใช้ที่นำมาใช้งานกับระบบสารสนเทศของมหาวิทยาลัย เพื่อให้การจัดการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์เป็นไปอย่างเป็นระบบ มีแบบแผนและสามารถจัดการปัญหาความปลอดภัยที่อาจจะเกิดขึ้น ได้อย่างรวดเร็ว เนื่องจากการใช้งานเครื่องคอมพิวเตอร์ภายในมหาวิทยาลัยมีการเชื่อมต่อเครือข่ายภายในและภายนอก (ระบบเครือข่ายอินทราเน็ตและเครือข่ายอินเตอร์เน็ต) ซึ่งอาจมีการติดไวรัสคอมพิวเตอร์ 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 ในการดูแล รักษา เพื่อส่งให้กับหัวหน้าและผู้บริหารรับทราบ

9. เมื่อมีการตรวจพบผู้ใช้ที่ฝ่าฝืนข้อปฏิบัติด้านความมั่นคงคอมพิวเตอร์ส่วนบุคคลให้ผู้ดูแลระบบคอมพิวเตอร์เสนอต่อผู้บริหาร

10. การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์เป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

ผลลัพธ์: 1) มีครุภัณฑ์คอมพิวเตอร์ที่สามารถสนับสนุนการปฏิบัติงานได้อย่างมีประสิทธิภาพ

2) เมื่อพบปัญหาการใช้งานครุภัณฑ์คอมพิวเตอร์ซึ่งไม่สามารถใช้ในการปฏิบัติงานได้ตามปรกติ สามารถซ่อม แก้ไข หรือหาทดแทนได้ภายใน 1 วันทำการ

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 หากตรวจพบว่ามีการติดตั้งชุดโปรแกรมเปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

5. ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

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

7. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์

8. ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต ด้วยการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่นหรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทาให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าตนไม่ได้เป็นผู้กระทำความผิด

9. ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

ผลลัพธ์: 1) สามารถระบุและแก้ไขปัญหาเชิงระบบเมื่อพบปัญหา ทำให้การทำงานของคณะฯ ได้ตามปรกติได้

2) สามารถให้คำแนะนำการป้องกันแก่ผู้ใช้งานได้

3. การบริหารจัดการระบบสารสนเทศและข้อมูล

ปัจจุบันการนำเทคโนโลยีสารสนเทศมาใช้กันมากขึ้นในระดับสถาบันการศึกษามีการพัฒนาระบบสารสนทศเพื่อใช้ในการบริหารมากขึ้น โดยเฉพาะในยุคของการปฏิรูปการศึกษา โดยมุ่งหวังในการปฏิรูปการศึกษาประสบความสำเร็จในพัฒนาคุณภาพของผู้เรียนตามเป้าหมายของการปฏิรูปการศึกษาอย่างมีประสิทธิภาพสูงสุด การเตรียมการพัฒนาระบบสารสนเทศ การพัฒนาระบบสารสนเทศเป็นกระบวนการวิเคราะห์และออกแบบระบบการจัดหา การติดตั้งการประเมินระบบ ตลอดจนกำหนดแนวทางในการพัฒนาระบบสารสนเทศในอนาคต เพื่อให้สามารถดำเนินงานอย่างมีประสิทธิภาพ การพัฒนาระบบสารสนเทศเพื่อใช้ในสถานศึกษาทั้งการบริหาร การเรียนการสอนและการบริการจะขึ้นอยู่กับผู้บริหารเป็นสำคัญเพื่อให้การดำเนินงานเตรียมความพร้อมในการพัฒนาระบบสารสนเทศในสถานศึกษาประสบความสำเร็จ

สถานศึกษาที่มีระบบสารสนเทศที่สมบูรณ์ ครบถ้วน เป็นปัจจุบันเรียกใช้ได้สะดวกและตรงตามความต้องการ จะทำให้สถานศึกษานั้นสามารถดำเนินการพัฒนาคุณภาพของการจัดสถานศึกษาได้อย่างมีประสิทธิภาพ มีกระบวนการวิเคราะห์ มีความเป็นเหตุเป็นผล ซึ่งระบบสารสนเทศสามารถนำไปประกอบการตัดสินใจในการวางแผนดำเนินการพัฒนาแนวความคิดและสร้างทางเลือกใหม่ ๆ ได้

แนวปฏิบัติของผู้ดูแลระบบ

1. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ใช้บริการ รหัสผ่าน สิทธิที่ได้รับเพื่อให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้งาน และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน โดยผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

1.1 เปลี่ยนแปลงและการยกเลิกรหัสผ่านเมื่อผู้ใช้งานระบบสารสนเทศลาออก หรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

1.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ใช้งานได้รับรหัสผ่านต้องตอบยืนยันการได้รับรหัสผ่าน

1.3 กำหนดชื่อผู้ใช้งานและรหัสผ่าน ในการเข้าใช้งานระบบสารสนเทศและข้อมูลที่ไม่ซ้ำกัน

1.4 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวเมื่อพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานนั้นต่างจากรหัสผู้ใช้งานตามปกติ

2. แจ้งให้ผู้ใช้งานทราบถึงวันเวลาที่ต้องปิดระบบสารสนเทศเพื่อบำรุงรักษา ปรับปรุง หรือ เปลี่ยนแปลงระบบซึ่งส่งผลให้ต้องหยุดบริการในช่วงระยะเวลาหนึ่ง โดยให้แจ้งล่วงหน้าก่อนกำหนดการ 3 วันทำการ แต่ในกรณีฉุกเฉินผู้ดูแลระบบอาจมีความจำเป็นต้องปิดระบบอย่างเร่งด่วนได้

3. กำหนดให้มีกระบวนการสร้างความต่อเนื่องให้กับการดำเนินงานการบริหาร จัดการและการปรับปรุงกระบวนการที่ต้องใช้ในการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ โดยการทำการสำรองข้อมูลภายในมหาวิทยาลัย หมายถึง การสำรองข้อมูลทั้งหมด โดยผู้ดูแลระบบคอมพิวเตอร์ต้องทำการสำรองข้อมูลที่จัดเก็บไว้เป็นประจำ อย่างน้อยวันละ 1 ครั้ง

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. กำหนดให้มีกระบวนการตรวจสอบความถูกต้องและเป็นปัจจุบันของระบบสารสนเทศและข้อมูลโดยการตรวจสอบข้อมูลกับผู้ใช้งานผู้รับผิดชอบระบบสารสนเทศเป็นประจำไตรมาสละ 1 ครั้ง

10. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบสารสนเทศ หรือข้อมูลจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบให้ผู้ดูแลระบบมีหน้าที่ดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้บริหารหรือผู้ที่ได้รับมอบหมาย

11. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

ผลลัพธ์: 1) มีการให้บริการสำรองข้อมูลแก่ผู้ใช้งาน

2) เมื่อเกิดการโจมตีระบบสารสนเทศ สามารถกู้ข้อมูลที่สำรองไว้กลับคืนได้

แนวปฏิบัติของผู้ใช้งาน

1. ผู้ใช้งานระบบสารสนเทศต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามอย่างเคร่งครัด

2. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลสำคัญตามประเภทชั้นความลับ เพื่อควบคุมป้องกันข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล โดยการกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูล แต่ละประเภทชั้นความลับ

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 ลาออกหรือมีคำสั่งสิ้นสุดการเป็นผู้บริหารบุคลากรและลูกจ้าง มีการถึงแก่กรรม มีการโอนย้ายข้ามหน่วยงานราชการ เพื่อให้ผู้ดูแลระบบกำหนดสิทธิ์ หรือยกเลิกสิทธิ์การเข้าถึงข้อมูลและระบบสารสนเทศและข้อมูล

ผลลัพธ์: 1) สามารถระบุที่มาของปัญหาและสามารถแก้ไขปัญหาได้

2) หาแนวทางในการป้องกันและแก้ไขปัญหาในอนาคตได้

แผนรองรับสถานการณ์ฉุกเฉินและภัยพิบัติ (Contingency Plan)

อ้างอิงมาตรฐาน: พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. 2562

เนื่องจากภารกิจของคณะฯ มีความหลากหลาย เทคโนโลยีสารสนเทศจึงเข้ามามีบทบาทสำคัญต่อการปฏิบัติงาน ซึ่งจำเป็นต้องมีการบริหารจัดการกรณีมีสถานการณ์ฉุกเฉินด้านสารสนเทศ เพื่อหาวิธีการป้องกันปัญหา และลดโอกาสความเสียหายที่อาจเกิดขึ้น อันจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศ เพื่อให้ระบบเทคโนโลยีสารสนเทศของคณะฯ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และเพื่อให้การนำเทคโนโลยีสารสนเทศมาสนับสนุนการปฏิบัติงานให้เกิดประโยชน์สูงสุด จึงจำเป็นจะต้องจัดทำแผนรองรับสถานการณ์ฉุกเฉิน เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบเทคโนโลยีสารสนเทศ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อฐานข้อมูลและระบบเทคโนโลยีสารสนเทศของคณะฯ ดังนี้

1) สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค: เป็นความเสี่ยงที่อาจเกิดขึ้นจากการทำงานผิดพลาดของอุปกรณ์ในระบบ การทำงานผิดพลาดของระบบ Software กรหยุดชะงักการให้บริการของระบบเครือข่ายโทรคมนาคม และระบบไฟฟ้า

2) สถานการณ์ฉุกเฉินที่เกิดจากบุคคล: เป็นความเสี่ยงที่อาจเกิดขึ้นการทำงานผิดพลาดหรือการใช้งานผิดวิธี การจารกรรมหรือวินาศกรรม ปัญหาการติดไวรัสของระบบและข้อมูลข่าวสาร ปัญหาการก่อการร้ายเป็นต้น

3) สถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติและโรคระบาด: เป็นความเสี่ยงที่อาจเกิดจากภัยพิบัติตามธรรมชาติหรือสถานการณ์ร้ายแรงที่ก่อให้เกิดความเสียหายร้ายแรงกับข้อมูลสารสนเทศ เช่น อุทกภัย อัคคีภัย แผ่นดินไหว เป็นต้น

4) สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง: สถานการณ์ที่อาจเป็นภัยต่อความมั่นคงหรือความปลอดภัยแห่งรัฐ หรืออาจทำให้รัฐตกอยู่ในภาวะคับขัน การก่อความไม่สงบ การประกาศสงครามหรือการประกาศสถานการณ์ฉุกเฉิน ซึ่งอาจมีผลให้เจ้าหน้าที่บางฝ่ายต้องหยุดการปฏิบัติการตามอำนาจหน้าที่ลงชั่วคราว และอาจนำไปสู่การห้ามออกจากเคหสถาน หรือการห้ามมั่วสุมชุมนุมกันเพื่อการใด ๆ

1 สถานการณ์ฉุกเฉินที่เกิดจากความขัดข้องด้านเทคนิค

1.1 กรณีการป้องกันไวรัสคอมพิวเตอร์เกิดความล้มเหลว

คณะสังคมศาสตร์ ได้ดำเนินการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ตามแนวปฏิบัติการให้บริการของมหาวิทยาลัยที่กำหนด

1) กรณีถูกไวรัสคอมพิวเตอร์หรือผู้บุกรุกในเครื่องคอมพิวเตอร์ของผู้ใช้งานของคณะสังคมศาสตร์ เพื่อจำกัดความเสียหายที่อาจแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการจำกัดการเชื่อมต่อเข้าระบบเครือข่าย

2) วิเคราะห์หาสาเหตุและผลกระทบที่เกิดจากไวรัสคอมพิวเตอร์ที่ระบาดดำเนินการป้องกันระบบเครือข่ายเพื่อหยุดยั้งการระบาดของไวรัสคอมพิวเตอร์

3) ตรวจสอบและติดตามเครื่องที่ติดไวรัสคอมพิวเตอร์และดำเนินการแก้ไข

4) กรณีที่ทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ได้ตามปกติ ให้แจ้งเหตุต่อเจ้าหน้าที่กองบริการเทคโนโลยีสารสนเทศและการสื่อสารทราบ ทั้งนี้กรณีมีเหตุอันทำให้กองบริการเทคโนโลยีสารสนเทศและการสื่อสารไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ ให้ประสานงานกับผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสารเพื่อป้องกันระบบเครือข่ายและหยุดยั้งการระบาดของไวรัสคอมพิวเตอร์

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

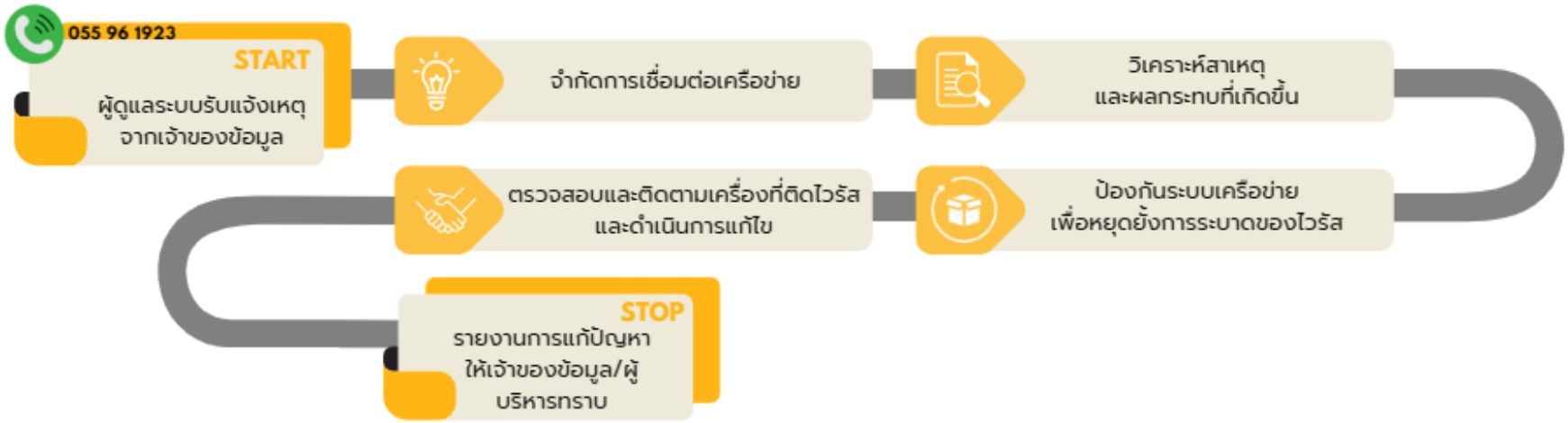
2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถจำกัดความเสียหายและหยุดยั้งการระบาดของไวรัสคอมพิวเตอร์ได้

2) สามารถระบุที่มาของปัญหาและความเสียหายของข้อมูล รวมถึงสามารถแก้ไขปัญหา รวมถึงหาแนวทางในการป้องกันและแก้ไขปัญหาในอนาคตได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสคอมพิวเตอร์ล้มเหลว



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันไวรัสคอมพิวเตอร์ล้มเหลว

1.2 กรณีการป้องกันผู้บุกรุกล้มเหลว

1) กรณีที่มีผู้บุกรุก ผู้ดูแลระบบต้องวิเคราะห์หาสาเหตุของการเข้ามาในระบบและผลของความเสียหายที่เกิดขึ้น โดยตรวจสอบจาก log และตรวจสอบการตั้งค่าของ Firewall

2) เมื่อตรวจสอบพบปัญหาให้ผู้ดูแลระบบแจ้งผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสารให้ทราบโดยด่วน

3) ผู้ดูแลระบบส่วนกลางตรวจสอบปัญหา และดำเนินการหยุดยั้งการบุกรุก ปิดช่องโหว่ต่างๆที่ทำให้ผู้บุกรุกเข้ามาได้

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถหาสาเหตุของการถูกจู่โจมและควบคุมความเสียหายที่เกิดขึ้นได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการป้องกันผู้บุกรุกล้มเหลว

1.3 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

1) กรณีเครือข่ายล้มเหลวให้ผู้ดูแลระบบตรวจสอบสาเหตุเพื่อระบุปัญหาและขอบเขตของผลกระทบที่เกิดขึ้น

2) กรณีเครือข่ายล้มเหลวจากระบบเครือข่ายในระดับคณะฯ ให้ดำเนินการตรวจสอบสายที่เชื่อมต่อไปยังอาคาร และ core switch ที่ติดตั้งอยู่ ณ อาคารนั้น ๆ

3) กรณีเครือข่ายล้มเหลวจากระบบเครือข่ายในระดับของมหาวิทยาลัย ให้แจ้งผู้ดูแลระบบส่วนกลางของกองบริการเทคโนโลยีสารสนเทศฯ เพื่อแก้ไขปัญหา หรือเปลี่ยนอุปกรณ์ให้บริการ โดยสามารถแก้ไขให้สามารถกลับมาใช้งานได้ภายใน 1 ชั่วโมง และรายงานผลการดำเนินการให้ผู้บริหารทราบ

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถตรวจสอบปัญหาที่เกิดขึ้นและแจ้งปัญหาให้กับเจ้าหน้าที่ของกองบริการเทคโนโลยีสารสนเทศฯ ให้ตรวจสอบและแก้ไขได้อย่างรวดเร็ว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการเชื่อมโยงเครือข่ายล้มเหลว

1.4 กรณีไฟฟ้าขัดข้อง

1) เมื่อพบปัญหาให้ผู้ดูแลระบบติดต่อเจ้าหน้าที่หน่วยอาคารสถานที่ของคณะสังคมศาสตร์เพื่อแก้ปัญหาการใช้งานอุปกรณ์คอมพิวเตอร์ภายในคณะสังคมศาสตร์

2) ผู้ดูแลระบบติดต่อผู้ดูแลระบบส่วนกลางเพื่อหาแนวทางแก้ปัญหาการใช้ระบบฐานข้อมูลและระบบสารสนเทศ ของคณะสังคมศาสตร์ซึ่งติดตั้งไว้ที่กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร ซึ่งมี UPS ซึ่งสามารถสำรองกระแสไฟฟ้าได้ 3 ชั่วโมง

2) หากใกล้ครบ 3 ชั่วโมงแล้ว ระบบไฟฟ้ายังไม่ปกติ ให้ผู้ดูแลระบบทำการประสานงานแจ้งเตือนไปยังผู้ดูแลระบบส่วนกลางของมหาวิทยาลัย

3) ผู้ดูแลระบบดำเนินการแจ้งข้อมูลการปิดระบบเพื่อป้องกันความเสียหายให้กับเจ้าหน้าที่ภายในคณะสังคมศาสตร์ทราบ

4) หากระบบฐานข้อมูลสารสนเทศของคณะฯ มีปัญหา ให้รายงานผู้บริหารและเร่งดำเนินการแก้ไขปัญหาที่เกิดขึ้น

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์	เมฆาวรนันท์	โทร. 055 961 923
2) นายสุทธิศักดิ์	กิติคุณภิวัฒน์	โทร. 055 961 923
3) นายสมนึก	แสงอบ	โทร. 055 961 917

ผลลัพธ์:

1) สามารถแก้ไขให้ระบบสารสนเทศกลับมาใช้งานได้ภายในระยะเวลา 3 ชั่วโมง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีการไฟฟ้าขัดข้อง

2 สถานการณ์ฉุกเฉินที่เกิดจากการบุคคล

2.1 กรณีโจรกรรม

1) ผู้ปฏิบัติงานแจ้งผู้บังคับบัญชาให้ทราบโดยด่วน

2) ตรวจสอบรายการทรัพย์สินที่สูญหาย

3) ผู้ดูแลระบบรีบดำเนินการจัดหาอุปกรณ์เพื่อติดตั้งทดแทนอุปกรณ์เดิม และนำข้อมูลที่ได้สำรองไว้ กู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานต่าง ๆ ได้ตามปกติโดยเร็ว

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืนให้ผู้ปฏิบัติงานสามารถใช้ระบบงานได้ตามปกติ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีโจรกรรม

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีโจรกรรม

2.2 กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

1) แจ้งผู้บังคับบัญชาทราบ

2) ปฏิบัติตามคู่มือการดำเนินการหากมีการจัดทำไว้ หรือติดต่อประสานงานกับบุคคลอื่นเพื่อให้สามารถปฏิบัติงานแทนได้

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถบริหารจัดการให้มีผู้ปฏิบัติงานแทนได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีผู้ปฏิบัติงานไม่สามารถมาปฏิบัติงานได้

3 สถานการณ์ฉุกเฉินที่เกิดจากภัยพิบัติและโรคระบาด

3.1 กรณีไฟไหม้

1) หากเกิดไฟไหม้ขณะปฏิบัติงานอยู่ ให้ผู้ปฏิบัติงานรีบเคลื่อนย้ายออกภายนอกตัวอาคาร ให้ผู้ที่สามารถการใช้เครื่องดับเพลิงได้ ใช้เครื่องดับเพลิงที่ติดตั้งอยู่ทำการดับไฟ

2) หากไม่สามารถควบคุมไฟได้ ผู้ดูแลระบบต้องรีบเคลื่อนย้ายอุปกรณ์จัดเก็บข้อมูลสำรองออกภายนอกตัวอาคาร ผู้ติดต่อประสานงานโทรแจ้งงานอาคารสถานที่และโทรแจ้งสถานีดับเพลิงที่ใกล้ที่สุด คือ องค์การบริหารส่วนตำบลท่าโพธิ์ หมายเลขโทรศัพท์ 0 5522 6396

3) หากเกิดไฟไหม้ขณะที่ไม่มีผู้ปฏิบัติงาน แล้วปรากฏว่าอุปกรณ์ต่างๆ ชำรุดเสียหาย ให้รีบดำเนินการจัดซ่อมหรือจัดหาอุปกรณ์ต่างๆ มาเพื่อให้การปฏิบัติงานดำเนินต่อไปได้ และออกแบบติดตั้งระบบตรวจจับไฟ และดับไฟอัตโนมัติ

4) อบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงานอย่างสม่ำเสมอ อย่างน้อยปีละ 1 ครั้ง

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

3) นายสมนึก แสงอบ โทร. 055 961 917

ผลลัพธ์:

1) มีการอบรมวิธีการใช้งานเครื่องดับเพลิงและการหนีไฟให้กับผู้ปฏิบัติงาน

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีไฟไหม้

3.2 กรณีน้ำท่วม

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

2) ผู้ดูแลระบบนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

3) ผู้ตรวจสอบรายการทรัพย์สิน สำรวจความชำรุด เสียหาย จัดส่งซ่อมหรือจัดหาเพื่อให้สามารถดำเนินการได้

เจ้าหน้าที่ผู้รับผิดชอบ

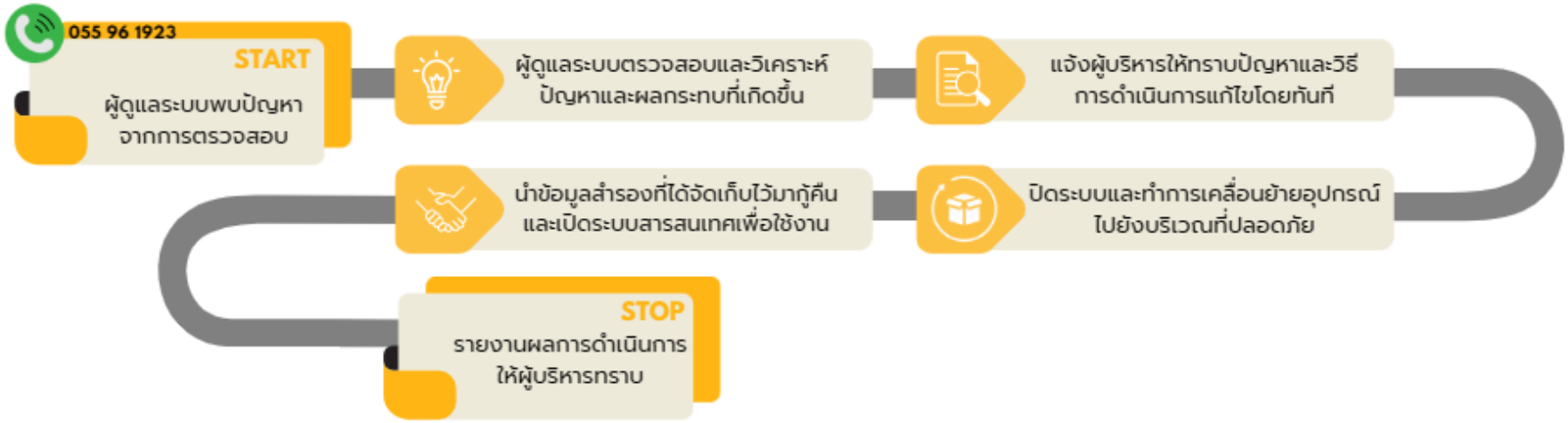
1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) สามารถนำข้อมูลสำรองที่ได้จัดเก็บไว้มากู้คืน ในส่วนที่เกิดความเสียหาย

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีน้ำท่วม



แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีน้ำท่วม

3.3 กรณีเกิดสถานการณ์โรคระบาด

1) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้บริหารคณะฯ แจ้งผู้ปฏิบัติงานให้สามารถขอยืมครุภัณฑ์คอมพิวเตอร์เพื่อไปปฏิบัติงาน ณ ที่พักอาศัยได้

2) ผู้ดูแลระบบเร่งดำเนินการประสานงานกับผู้ปฏิบัติงานในการแจ้งความประสงค์ต่อผู้บริหารคณะฯ เพื่อขอยืมครุภัณฑ์คอมพิวเตอร์เพื่อไปปฏิบัติงาน ณ ที่พักอาศัย

3) หลังเหตุการณ์โรคระบาดกลับสู่สภาวะปกติ ให้ผู้ปฏิบัติงาน นำครุภัณฑ์คอมพิวเตอร์ที่ได้ยืมไปมาคืนต่อผู้ดูแลระบบเพื่อตรวจสอบความชำรุดเสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการในส่วนที่เกี่ยวข้องต่อไป

เจ้าหน้าที่ผู้รับผิดชอบ

1) นายพิทักษ์พงษ์ เมฆาวรนันท์ โทร. 055 961 923

2) นายสุทธิศักดิ์ กิติคุณภิวัฒน์ โทร. 055 961 923

ผลลัพธ์:

1) มีการบริหารจัดการให้ผู้ปฏิบัติงานสามารถยืมครุภัณฑ์คอมพิวเตอร์เพื่อไปปฏิบัติงานเมื่อเกิดโรคระบาดได้

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีเกิดสถานการณ์โรคระบาด

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉินกรณีเกิดสถานการณ์โรคระบาด

4 สถานการณ์ฉุกเฉินที่เกิดจากความไม่สงบเรียบร้อยในบ้านเมือง

4.1 กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง เช่น การก่อการร้าย การชุมนุมประท้วง

1) กรณีที่ไม่สามารถเข้ามาปฏิบัติงานได้ ผู้ดูแลระบบ Remote เข้ามาเพื่อตรวจสอบการทำงานของระบบ หากพบว่าระบบไม่สามารถดำเนินการได้ตามปกติ

2) แจ้งผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสารทราบ

3) หลังเหตุการณ์ความไม่สงบ ให้ผู้ดูแลระบบและผู้ตรวจสอบรายการทรัพย์สินตรวจสอบความชำรุด เสียหายซึ่งอาจได้รับจากเหตุการณ์ดังกล่าว หากพบความชำรุดเสียหาย ให้ดำเนินการติดต่อบริษัทที่รับผิดชอบดูแลบำรุงรักษา

ผลลัพธ์:

1) สามารถดำเนินการจัดหาหรือซ่อมแซมอุปกรณ์ที่เกิดความเสียหายได้ ภายในระยะเวลา 1 วันทำการ

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

แผนผังแสดงขั้นตอนการรับมือสถานการณ์ฉุกเฉิน กรณีเกิดสถานการณ์ความไม่สงบเรียบร้อยในบ้านเมือง

ภาคผนวก

1. พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/CyberSecurityAct-2019.pdf

2. ประกาศคณะกรรมการกำกับดูแลด้านความมั่นคงปลอดภัยไซเบอร์ เรื่อง ประมวลแนวทางปฏิบัติและกรอบมาตรฐานด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ สำหรับหน่วย งานของรัฐและหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศ พ.ศ.2564

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/CyberSecuritySTDFramework-2021.pdf

3. กรอบมาตรฐานการรักษาความปลอดภัยไซเบอร์ ISO 27001 (ISO/IEC 27001)

   แหล่งอ้างอิง: https://www.omnex.com/aerospace/consulting-implementation-coaching-aerospace-iso-27001-cybersecurity

4. กรอบมาตรฐานการรักษาความปลอดภัยไซเบอร์ NIST Cybersecurity Framework (CSF)

   แหล่งอ้างอิง: https://verveindustrial.com/resources/whitepaper/5-steps-to-greater-security-maturity-with-nist-csf/

5. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

   แหล่งอ้างอิง: https://www.socsci.nu.ac.th/th/wp-content/uploads/2024/05/EcommSecuritySTD.pdf