แนวนโยบายและแนวปฏิบัติ

ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

คำนำ

ตามที่ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ มาตรา ๖ มาตรา ๗ กำหนดให้หน่วยงานของภาครัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานหรือการให้บริการต่างๆ ของหน่วยงานรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้

ดังนั้น มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ จึงได้จัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบสารสนเทศ เป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและแนวปฏิบัติจากทุกหน่วยงาน รวมทั้งต้องทำอย่างต่อเนื่อง มีการตรวจสอบและปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ จึงหวังเป็นอย่างยิ่งว่า นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแล ระบบสารสนเทศ และผู้ที่เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ถือปฏิบัติโดยเคร่งครัดต่อไป

สารบัญ

คำนิยาม

๑. มหาวิทยาลัย หมายความว่า มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

๒. สำนัก หมายความว่า สำนักวิทยบริการและเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

๓. ผู้บริหารระดับสูงสุด หมายความว่า อธิการบดี หรือ รองอธิการบดีที่อธิการบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศ

๔. ผู้ใช้งาน หมายความว่า บุคลากร นักศึกษา ในสังกัดมหาวิทยาลัย และบุคคลภายนอกผู้ได้รับอนุญาตให้ใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

๕. สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นๆที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๖. สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับมหาวิทยาลัย

๗. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนข้อปฏิบัติเกี่ยวกับการเข้าถึงระบบสารสนเทศโดยมิชอบ

๘. ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของระบบสารสนเทศ

๙. เหตุการณ์ด้านความมั่นคงปลอดภัย หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๐. สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑๑. ระบบอินเทอร์เน็ต (Internet) หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของมหาวิทยาลัยเข้ากับเครือข่ายอินเทอร์เน็ตระบบสากล

๑๒. ระบบสารสนเทศ หมายความว่า ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริการ การสนับสนุนให้การบริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น คอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

๑๓. ผู้ดูแลระบบ (System Administrator) หมายความว่า ผู้ที่ได้รับมอบหมายจากมหาวิทยาลัยให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๔. บุคคลภายนอก หมายความว่า บุคคลธรรมดาหรือนิติบุคคลที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานระบบสารสนเทศของมหาวิทยาลัย โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๑๕. จดหมายอิเล็กทรอนิกส์ (E-mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโปรโตคอล ต่าง ๆ เช่น SMTP, POP3, IMAP ฯลฯ

๑๖. สื่อบันทึกพกพา (Portable Media) หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, flash drive, external hard disk ฯลฯ

๑๗. ชื่อผู้ใช้ (Username) หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งาน

๑๘. รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

๑๙. การเข้ารหัสลับ (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. การพิสูจน์ยืนยันตัวตน (Authentication) หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบทั่วไปและจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ และรหัสยืนยัน

๒๑. SSID (Service set identifier) หมายความว่า ชื่อระบุเครือข่ายไร้สาย

๒๒. MAC Address (Media access control address) หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับเน็ตเวิร์กการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกันตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๒๓. VPN (Virtual Private Network) หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๔. แผนผังระบบเครือข่าย (Network diagram) หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

ส่วนที่ ๑

การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหารระดับสูงสุด ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้และเข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. หน่วยงานภายในมหาวิทยาลัย ที่รับผิดชอบดูแลระบบ

อ้างอิงมาตรฐาน

-

แนวทางปฏิบัติ

๑. การเข้าถึงและควบคุมการใช้งานสารสนเทศ

๑.๑ เกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิหรือการมอบอำนาจ

(๑) สิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง

- อ่านอย่างเดียว กลุ่มผู้ใช้งาน
- สร้างข้อมูล กลุ่มผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
- ป้อนข้อมูล กลุ่มผู้ใช้งาน,กลุ่มผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
- แก้ไข กลุ่มผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
- อนุมัติ กลุ่มผู้บริหารระดับสูงสุด
- ไม่มีสิทธิ

(๒) เกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักหรือผู้ที่ได้รับมอบหมาย

๑.๒ ขั้นตอนปฏิบัติเพื่อจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี

- ข้อมูลสารสนเทศตามพันธกิจ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลทีมีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๕) เวลาที่ได้เข้าถึงของผู้ใช้งานระบบ

(๖) จำนวนช่องทางที่สามารถเข้าถึง

๒. ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน

(๑) ควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) ปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

ควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๓.๑ หลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

๓.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓.๓ ขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) ระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) ชื่อผู้ใช้งานจะกำหนดอย่างเป็นรูปแบบเดียวกันจำแนกตามประเภทของผู้ใช้งาน

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๗) ทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) เกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักหรือผู้ที่ได้รับมอบหมาย

(๙) ยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออกจากงาน เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง

๓.๔ การบริหารจัดการสิทธิของผู้ใช้งาน (User management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) กำหนดระดับสิทธิในการเข้าถึงสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมาย สิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) บันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓.๕ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๑) มีขั้นตอนปฏิบัติที่ดีสำหรับการตั้ง เปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๔) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๕) การเปลี่ยนแปลงรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๖) ในกรณีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบโดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาพิเศษที่ได้รับ และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๖ ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน เมื่อมีการเปลี่ยนแปลง เช่น มีการออกจากงาน เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ ดังนี้

๔.๑ การใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๑) ตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๒) รหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๔) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๕) ไม่ใช่รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) ไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล

(๙) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๐) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๑) เปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๒) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๓) ผู้ดูแลระบบต้องเปลี่ยนรหัส บ่อยครั้งกว่าผู้ใช้งานทั่วไป

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัยในขณะที่ไม่มีผู้ดูแล

(๑) กำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๖) ล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) โดยต้องควบคุมทรัพย์สินสารสนเทศ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศที่อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๑) มาตรการป้องกันทรัพย์สินของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ไม่ปลอดภัย

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ ประกาศหรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) ป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๔) กำหนดขอบเขตของการป้องกัน

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์โดยไม่ได้รับอนุญาต เช่น กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร

๔.๔ การเข้ารหัสข้อมูล กรณีข้อมูลเป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

๕. การควบคุมการเข้าถึงเครือข่าย (Network access control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๕.๑ การใช้บริการเครือข่าย กำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) ระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบบเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) ข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) การใช้งานระบบสารสนเทศที่สำคัญ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (internet) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ ๑ ครั้ง

๕.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User authentication for external connection) มีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัยสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

(๒) มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยทำการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

(๓) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยจากอินเตอร์เน็ต ให้มีการตรวจสอบผู้ใช้งาน

๕.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in network) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

๕.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๑) ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๕.๕ การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๕.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๕.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP address plan)

(๒) กำหนดให้มีการเปลี่ยนแปลงหมายเลขเครือข่าย สำหรับเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิ์ในการใช้บริการเครือข่าย

๕.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบจากระยะไกล (Remote access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน วิธีการเข้ารหัส

(๓) ควบคุมพอร์ต(Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๖.๑ ขั้นตอนปฏิบัติการเข้าใช้งาน การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ

(๑) ไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสารมารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command line เนื่องจาก อาจสร้างความเสียหายได้กับระบบได้

๖.๒ ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ให้มีผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม รองรับการกล่าวอ้างว่าเป็นผู้ใช้งานระบบโดยมีแนวทางปฏิบัติ

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

(๒) การอนุญาตให้ใช้ชื่อผู้ใช้งานและรหัสผ่าน ร่วมกัน ต้องได้รับอนุญาตโดยขึ้นอยู่กับความจำเป็นทางด้านเทคนิค

๖.๓ การบริหารจัดการรหัสผ่าน (Password management system) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๖.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ ให้ดำเนินการ

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(๑) ยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) กรณีไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ ระบบงานที่มีความสำคัญสูง และระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and information access control) โดยต้องมีการควบคุม

๗.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและผู้ดูแลระบบการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๗.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย

(๑) แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

(๒) ควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๓) ควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติการงานจากภายนอกมหาวิทยาลัย (Mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๗.๓ อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ปฏิบัติตามมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๔ การปฏิบัติงานภายนอกมหาวิทยาลัย (teleworking) กำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกมหาวิทยาลัย

ส่วนที่ ๒

การสำรองข้อมูลระบบสารสนเทศ

วัตถุประสงค์

๑. ระบบสารสนเทศของมหาวิทยาลัย ให้บริการได้อย่างต่อเนื่อง

๒. เป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัยเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. หน่วยงานภายในมหาลัย ที่รับผิดชอบดูแลระบบ

อ้างอิงมาตรฐาน

-

แนวปฏิบัติ

๑. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินปีละ ๑ ครั้ง

๑.๒. มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

(๑) แบ่งประเภทของข้อมูลที่ต้องทำการสำรองข้อมูล และความถี่ในการสำรอง

(๒) รูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองข้อมูลทั้งการสำรองข้อมูลแบบเต็ม (Full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)

(๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ

(๔) ตรวจสอบข้อมูลของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกูเรชั่น (Configuration) ข้อมูลในฐานข้อมูล

(๕) จัดเก็บข้อมูลที่สำรองนั้นใส่ในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อ และนำไปเก็บในสถาที่ซึ่งห่างจากมหาวิทยาลัยเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับมหาวิทยาลัย เช่น ไฟไหม้ น้ำท่วม

(๖) ป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่ใช้จัดเก็บข้อมูลนอกสถานที่

(๗) ทดสอบการอ่านข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(๘) ทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(๙) ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

(๑๐)กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

๒.๑. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียด

(๑) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น

(๓) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

(๕) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟแวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) สร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

๒.๒. ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ ๑ ครั้ง

๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

๕. ทบทวนระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่อยงานในมหาวิทยาลัย ปีละ ๑ ครั้ง

ส่วนที่ ๓

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑. มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. หน่วยงานภายในมหาลัย ที่รับผิดชอบดูแลระบบ

อ้างอิงมาตรฐาน

-

แนวปฏิบัติ

๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา

๑.๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit and assessment) ปีละ ๑ ครั้ง

๑.๒. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง

๒.๑. ทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ ๑ ครั้ง

๒.๒. ตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๓. ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีละ ๑ ครั้ง

๒.๔. มีมาตรการในการตรวจประเมินระบบสารสนเทศ

(๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทำลายหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(๕) เครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. รายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง ต่อคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

๔. แสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ภาคผนวก

แผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

1. หลักการและเหตุผล

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

สำนักวิทยบริการและเทคโนโลยีสารสนเทศตระหนักถึงความสำคัญของระบบฐานข้อมูลสารสนเทศ ซึ่งอาจมีทั้งปัจจัยภายนอกและปัจจัยภายในมากระทบทำให้ระบบฐานข้อมูลสารสนเทศรวมทั้งอุปกรณ์เสียหายได้ โดยเฉพาะอย่างยิ่งฐานข้อมูลสารสนเทศที่ใช้ในการบริหารจัดการ ดังนั้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศ จึงจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ ขึ้นเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

2. วัตถุประสงค์

2.1 เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความปลอดภัยของฐานข้อมูลสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

2.2 เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของฐานข้อมูลสารสนเทศให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

2.3 เพื่อให้การปฏิบัติงานเป็นไปอย่างมีระบบและต่อเนื่อง และสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที กรณีเกิดสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.4 เพื่อเป็นการลดความเสียหายและเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจเกิดขึ้นกับระบบข้อมูลสารสนเทศ

3. คำนิยาม

“ระบบสารสนเทศ” หมายความว่า ระบบข้อมูลข่าวสารของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ที่นำเอาเทคโนโลยีของระบบคอมพิวเตอร์และเทคโนโลยีของระบบสื่อสารมาช่วยในการสร้างระบบสารสนเทศที่มหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิสามารถนำมาใช้ในการบริหาร การพัฒนาและการควบคุม มีองค์ประกอบดังนี้

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

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

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

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

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

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

“เครือข่ายระบบสารสนเทศ” หมายความว่า การติดต่อสื่อสารหรือการส่งข้อมูลกันระหว่างระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ

4. วิเคราะห์ปัจจัยความเสี่ยง

ปัจจัยที่อาจเกิดและทำให้เสียหายกับระบบฐานข้อมูลสารสนเทศ ของมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิ ได้แก่

4.1 ปัจจัยภายนอก

4.1.1 ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลักหรือเครื่องแม่ข่ายหลัก (Server) ของระบบฐานข้อมูล เช่น อุทกภัย อัคคีภัย

4.1.2 การถูกเจาะหรือลักลอบ (Hack) เข้าสู่ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

4.1.3 ระบบการสื่อสารของเครือข่ายคอมพิวเตอร์หลักเสียหาย/ขัดข้อง

4.1.4 ระบบกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ

4.1.5 การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

4.2 ปัจจัยภายใน

4.2.1 ระบบฐานข้อมูลหลักเสียหายหรือข้อมูลถูกทำลายจากไวรัสคอมพิวเตอร์และผู้ใช้งานภายในหน่วยงาน

4.2.2 ระบบเครือข่ายภายในขัดข้อง ไม่สามารถใช้งานได้

4.2.3 การชำรุดเสียหายของตัวเครื่องประมวลผลหลักหรือแม่ข่ายหลัก (Server) จากการเคลื่อนย้ายหรืออื่น ๆ

4.2.4 บุคลากรขาดความรู้ ความเข้าใจในการใช้เครื่องมือทั้งด้านฮาร์ดแวร์และซอฟท์แวร์ อันอาจทำให้ระบบสารสนเทศเสียหาย

5. แนวทางการป้องกันและการเตรียมการเบื้องต้น

5.1 การประกาศแผน (Activation)

มีการประกาศใช้แผนเตรียมความพร้อมกรณีฉุกเฉินด้านเทคโนโลยีสารสนเทศ ขึ้นเพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจส่งผลกระทบต่อฐานข้อมูลสารสนเทศอย่างเป็นทางการ เพื่อให้เจ้าหน้าที่ทุกคนทราบและปฏิบัติตามอย่างเคร่งครัด โดยมีเอกสารยืนยันแสดงให้เห็นว่าเจ้าหน้าที่ทุกคนรับทราบ รวมทั้งมีการจัดอบรมเพื่อเป็นแนวทางในการปฏิบัติตามแผนด้วย

5.2 กระบวนการดำเนินงาน (Procedure)

มีการเตรียมขั้นตอนการปฏิบัติกับเหตุการณ์ที่ผิดปกติ โดยเมื่อเกิดเหตุการณ์ฉุกเฉินจะต้องมีการเลือกขั้นตอนปฏิบัติที่เหมาะสมกับสถานการณ์ต่าง ๆ ที่เกิดขึ้น ทั้งการรวบรวมเหตุการณ์ การระบุที่มาของปัญหา ระบบงานต่าง ๆ ที่มีความสำคัญต้องมีการเตรียมอุปกรณ์สำรอง เพื่อใช้ในการกู้คืนเมื่อเกิดปัญหา

5.3 การติดต่อสื่อสาร (Communication)

มีการจัดทำบัญชีรายชื่อและข้อมูลสำหรับติดต่อกรณีที่มีความจำเป็นฉุกเฉิน

5.4 การจัดเตรียมอุปกรณ์ที่จำเป็น (Preparation)

มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์ขัดข้องไม่สามารถใช้งานได้โดยมีการติดตั้งอุปกรณ์ที่ปลายทางเพื่อรองรับและทดแทนอุปกรณ์หลักได้

5.5 การสำรองข้อมูล (Backup)

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

5.6 การเสริมสร้างความปลอดภัย (Enhancing)

5.6.1 มีมาตรการควบคุมการเข้าออกห้องเครื่องคอมพิวเตอร์และการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากมีความจำเป็นให้มีเจ้าหน้าที่ที่รับผิดชอบนำเข้าไป

5.6.2 มีการติดตั้ง Firewall เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ โดยจะเปิดใช้งาน Firewall ตลอดเวลา

5.6.3 มีการติดตั้งอุปกรณ์เพื่อใช้ในการตรวจจับการบุกรุกของผู้ที่ไม่ประสงค์ดี ซึ่งจะทำการวิเคราะห์ข้อมูลทั้งหมดที่ผ่านเข้า-ออกภายในเครือข่ายที่มีลักษณะการทำงานเป็นความเสี่ยงเพื่อป้องกันการบุกรุกผ่านเครือข่าย

5.6.4 มีเจ้าหน้าที่ดูแลระบบเครือข่าย ทำการตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ระบบสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

5.6.5 การเรียกใช้ระบบสารสนเทศผู้ใช้ระบบจะต้องมีการป้อนชื่อผู้ใช้ (Username) และรหัสผ่าน (password) เพื่อตรวจสอบก่อนระบบอนุญาตให้ใช้งานได้ ตามอำนาจหน้าที่และความรับผิดชอบ

5.6.6 มีการปฏิบัติตาม พ.ร.บ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 เพื่อเสริมสร้างมาตรการป้องกันการบุกรุกและภัยคุกคามคอมพิวเตอร์

6. มาตรการในการป้องกันและแก้ไขปัญหา

6.1 กรณีเครื่องลูกข่าย

6.1.1 ในกรณีที่เครื่องคอมพิวเตอร์ไม่สามารถใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่แจ้งเหตุแก่ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลฐานข้อมูลสารสนเทศ หรือในกรณีเกิดจากไม่สามารถให้บริการด้านเครือข่ายหรือระบบสารนเทศได้ ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศประกาศให้ทุกหน่วยงานในมหาวิทยาลัยเทคโนโลยีราชมงคลสุวรรณภูมิทราบ

6.1.2 กรณีเกิดการขัดข้องเนื่องจากไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ตัดการเชื่อมต่อระบบเครือข่าย

6.2 กรณีเครื่องแม่ข่ายบริการ (Server)

6.2.1 ตัดการเชื่อมต่อระบบเครือข่าย จากนั้นทำการปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

6.2.2 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายโดยพิจารณาตามลำดับความสำคัญของการให้บริการ ทั้งนี้การปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ให้พิจารณาจากระยะเวลาที่ไฟฟ้าดับและประสิทธิภาพของเครื่องสำรองกระแสไฟฟ้า

6.2.3 กรณีไฟไหม้ ให้ตัดระบบจ่ายไฟและใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

6.2.4 ตรวจสอบปัญหาที่เกิดขึ้น ในกรณีสถานการณ์ยังไม่ปลอดภัยให้ขนย้ายเครื่องและอุปกรณ์ไปไว้ในที่ปลอดภัย

7. ขั้นตอนการปฏิบัติ

7.1 กรณีกระแสไฟฟ้าขัดข้อง/ไฟฟ้าดับ/ไฟฟ้ากระชาก

1. หากคาดการณ์ว่ากระแสไฟฟ้าดับเป็นเวลานานเกินกว่าที่เครื่องสำรองกระแสไฟฟ้าจะทำงานได้ ให้ปิดอุปกรณ์เครือข่ายและ Shutdown เครื่องคอมพิวเตอร์แม่ข่าย

2. เมื่อระบบไฟฟ้าใช้การได้แล้ว ให้เปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย พร้อมกับตรวจสอบการทำงานของระบบและอุปกรณ์ต่างๆ

ผู้รับผิดชอบ

1.	นายจตุพร	ระเวงจิตร์	ดูแลภาพรวมสี่ศูนย์พื้นที่	0815868614
2.	นายณัฐพล	พรหมมี	ดูแลศูนย์พื้นที่หันตรา	0826897776
3.	นายจิรวัฒน์	พงษ์วิเชียร	ดูแลศูนย์พื้นที่วาสุกรี	0938987579
4.	นายสิริพงษ์	เกียรติพิทักษ์สุข	ดูแลศูนย์พื้นที่นนทบุรี	0879016915
5.	นายณัฐวัฒน์	เขาแก้ว	ดูแลศูนย์พื้นที่สุพรรณบุรี	0841218985

หน่วยงานที่เกี่ยวข้อง

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

7.2 กรณีเกิดอัคคีภัย

1. หากพบเห็นเพลิงไหม้ให้หาตำแหน่งสัญญาณเตือนเพลิงไหม้และนำอุปกรณ์ดับเพลิงฉีดพ่นระงับไม่ให้ไฟไหม้ลุกลาม

2. ประเมินสถานการณ์หากสามารถ Shutdown เครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายได้ทัน ให้ดำเนินการ

3. ขนย้ายอุปกรณ์แม่ข่าย และนำข้อมูลที่ได้สำรองไว้ไปยังสถานที่ที่ปลอดภัย ศูนย์พระนครศรีอยุธยา หันตรา ย้ายไปไว้ที่ อาคาร 24 ชั้น 8 ,ศูนย์พระนครศรีอยุธยา วาสุกรี ย้ายไปไว้ที่ อาคาร 7 ชั้น 2,ศูนย์นนทบุรีย้ายไปไว้ที่ อาคาร 5 ชั้น 3,ศูนย์สุพรรณบุรีย้ายไปไว้ที่ อาคาร 2 ชั้น 2

4. ให้เจ้าหน้าที่ทุกคนอพยพออกจากอาคารไปตามทางบันไดหนีไฟ ห้ามใช้ลิฟท์

5. เมื่อเพลิงสงบแล้วให้สำรวจ ประเมินความเสียหายที่เกิดขึ้นกับห้องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบงานต่างๆ รายงานให้ผู้บริหารรับทราบ

6. จัดหาสถานที่ดำเนินการติดตั้ง กู้คืนระบบให้สามารถใช้งานได้ จากข้อมูลที่ได้สำรองไว้

7. ตรวจสอบการทำงานของระบบและอุปกรณ์ต่างๆ ให้ทำงานได้ตามปกติ

ผู้รับผิดชอบ

1.	นายจตุพร	ระเวงจิตร์	ดูแลภาพรวมสี่ศูนย์พื้นที่	0815868614
2.	นายณัฐพล	พรหมมี	ดูแลศูนย์พื้นที่หันตรา	0826897776
3.	นายจิรวัฒน์	พงษ์วิเชียร	ดูแลศูนย์พื้นที่วาสุกรี	0938987579
4.	นายสิริพงษ์	เกียรติพิทักษ์สุข	ดูแลศูนย์พื้นที่นนทบุรี	0879016915
5.	นายณัฐวัฒน์	เขาแก้ว	ดูแลศูนย์พื้นที่สุพรรณบุรี	0841218985

หน่วยงานที่เกี่ยวข้อง

กองกลาง (หันตรา)	035-709101
กองบริหารทรัพยากร วาสุกรี	035-324180
กองบริหารทรัพยากร นนทบุรี	0-2969-1369
กองบริหารทรัพยากร สุพรรณบุรี	035-5544301
แจ้งเหตุเพลิงไหม้ 24 ชั่วโมง	199

7.3 กรณีเกิดอุทกภัย

1. ประเมินสถานการณ์ และความรุนแรงของเหตุการณ์

2. ในกรณีที่มีโอกาสน้ำท่วมถึงและมีความจำเป็นต้องตัดกระแสไฟฟ้า ให้แจ้งผู้ใช้งานก่อนปิดระบบเครือข่าย และคอมพิวเตอร์แม่ข่าย

3. ขนย้ายคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และนำข้อมูลที่ได้สำรองไว้ไปยังสถานที่ที่ปลอดภัย ศูนย์พระนครศรีอยุธยา หันตรา ย้ายไปไว้ที่ อาคาร 24 ชั้น 8 ,ศูนย์พระนครศรีอยุธยา วาสุกรี ย้ายไปไว้ที่ อาคาร 7 ชั้น 2,ศูนย์นนทบุรีย้ายไปไว้ที่ อาคาร 5 ชั้น 3,ศูนย์สุพรรณบุรีย้ายไปไว้ที่ อาคาร 2 ชั้น 2

4. จัดหาสถานที่ดำเนินการติดตั้ง กู้คืนระบบให้สามารถใช้งานได้ จากข้อมูลที่ได้สำรองไว้ โดยตรวจสอบการทำงานของระบบและอุปกรณ์ต่างๆ ให้ทำงานได้ตามปกติ

5. เมื่อเหตุการณ์ปกติ ให้ประเมินความเสียหายและหาแนวทางป้องกันต่อไป

ผู้รับผิดชอบ

1.	นายจตุพร	ระเวงจิตร์	ดูแลภาพรวมสี่ศูนย์พื้นที่	0815868614
2.	นายณัฐพล	พรหมมี	ดูแลศูนย์พื้นที่หันตรา	0826897776
3.	นายจิรวัฒน์	พงษ์วิเชียร	ดูแลศูนย์พื้นที่วาสุกรี	0938987579
4.	นายสิริพงษ์	เกียรติพิทักษ์สุข	ดูแลศูนย์พื้นที่นนทบุรี	0879016915
5.	นายณัฐวัฒน์	เขาแก้ว	ดูแลศูนย์พื้นที่สุพรรณบุรี	0841218985

หน่วยงานที่เกี่ยวข้อง

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

7.4 กรณีโดนเจาะระบบ

1. ตัด Internet Connection เครื่องแม่ข่ายของระบบนั้น เพื่อหยุดการทำงานของระบบที่ Firewall (หรือดึงสาย Lan ออก) แล้วรายงานผู้บังคับบัญชา

2. ตรวจสอบ log ที่เครื่องแม่ข่าย และที่อุปกรณ์จัดเก็บ log

3. ตรวจสอบความเสียหายของระบบและเครื่องแม่ข่าย

- หากระบบข้อมูลเสียหายเป็นบางส่วน ให้กู้คืนจากข้อมูลที่สำรองไว้
- หากระบบไม่สามารถใช้งานได้ ให้ติดตั้งระบบใหม่ทั้งหมดจากข้อมูลที่สำรองไว้

4. ทดสอบการทำงานของระบบและอุปกรณ์ต่างๆที่กู้คืน

ผู้รับผิดชอบ

1.	นายจตุพร	ระเวงจิตร์	ดูแลภาพรวมสี่ศูนย์พื้นที่	0815868614
2.	นายณัฐพล	พรหมมี	ดูแลศูนย์พื้นที่หันตรา	0826897776
3.	นายจิรวัฒน์	พงษ์วิเชียร	ดูแลศูนย์พื้นที่วาสุกรี	0938987579
4.	นายสิริพงษ์	เกียรติพิทักษ์สุข	ดูแลศูนย์พื้นที่นนทบุรี	0879016915
5.	นายณัฐวัฒน์	เขาแก้ว	ดูแลศูนย์พื้นที่สุพรรณบุรี	0841218985

7.5 กรณีการเชื่อมโยงเครือข่ายล้มเหลว

1. ตรวจสอบหาจุดและสาเหตุที่ทำให้เกิดปัญหา

2. หากสายไฟเบอร์ออฟติกขาด ให้ติดต่อเจ้าหน้าที่บริษัทที่ดูแลรับผิดชอบ เพื่อดำเนินการแก้ไขให้แล้วเสร็จโดยเร็ว

3. กรณีที่บริษัทที่ดูแลรับผิดชอบไม่สามารถดำเนินการแก้ไขได้โดยเร็ว ให้ใช้ระบบเครือข่ายสำรอง

4. ทดสอบการทำงานของระบบเครือข่ายสำรอง

ผู้รับผิดชอบ

1.	นายจตุพร	ระเวงจิตร์	ดูแลภาพรวมสี่ศูนย์พื้นที่	0815868614
2.	นายณัฐพล	พรหมมี	ดูแลศูนย์พื้นที่หันตรา	0826897776
3.	นายจิรวัฒน์	พงษ์วิเชียร	ดูแลศูนย์พื้นที่วาสุกรี	0938987579
4.	นายสิริพงษ์	เกียรติพิทักษ์สุข	ดูแลศูนย์พื้นที่นนทบุรี	0879016915
5.	นายณัฐวัฒน์	เขาแก้ว	ดูแลศูนย์พื้นที่สุพรรณบุรี	0841218985

หน่วยงานที่เกี่ยวข้อง

ฝ่ายบริหารเครือข่าย สำนักงานบริหารเทคโนโลยีสารสนเทศเพื่อพัฒนาการศึกษา (UniNet) 02-232-4000,02-354-5678 #4001-4005, noc@uni.net.th

บริษัท กสท โทรคมนาคม จำกัด (มหาชน) เบอร์โทรศัพท์ 1332,02-104-1100 ,cat1322@cattelecom.com,นนทบุรีGDW50603,หันตราGDW050783,วาสุกรีGDW050782, สุพรรณบุรีGDW050781

8. การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery)

ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ โดยปกติจะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ ตลอดเวลา 24 ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ ดังนี้

1. จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน
2. เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย
3. ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน 48 ชั่วโมง
4. นำ Backup Tape/CD-ROM/Hard disk ที่ได้สำรองข้อมูลไว้นำกลับมา restore
5. ทำการตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

9. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินงานหรือผลการตรวจสอบให้ผู้บังคับบัญชาทราบ และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ในทุกกรณีตามที่ระบุไว้

10. ผู้รับผิดชอบ

1. รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษาตลอดจน ติดตาม กำกับดูแล ควบคุมตรวจสอบ ได้แก่

1.1	นายอาคม	สงเคราะห์	ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
1.2	นายสุทิน	เกษตรรัตนชัย	รองผู้อำนวยการด้านเทคโนโลยีสารสนเทศ
1.3	นายอภิชาติ	โชคเหรียญสุขชัย	หัวหน้างานวิศวกรรม
1.4	นายแสงทอง	บุญยิ่ง	หัวหน้างานบริการสารสนเทศ
1.5	นายจตุพร	ระเวงจิตร์	หัวหน้างานซ่อมบำรุงคอมพิวเตอร์และระบบเครือข่าย

2. ผู้รับผิดชอบตามแผนป้องกันจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดกับระบบสารสนเทศ

2.1	นายจตุพร	ระเวงจิตร์	นักวิชาการคอมพิวเตอร์
2.2	นายนัฐพล	พรหมมี	นักวิชาการคอมพิวเตอร์
2.3	นายณัฐวัฒน์	เขาแก้ว	นักวิชาการคอมพิวเตอร์
2.4	นายจิรวัฒน์	พงษ์วิเชียร	นักวิชาการคอมพิวเตอร์
2.5	นายฐิตินันท์	ภู่พันธ์	นักวิชาการคอมพิวเตอร์
2.6	นายสิริพงษ์	เกียรติพิทักษ์สุข	นักวิชาการคอมพิวเตอร์
2.7	นายศรัณย์พงษ์	ศรีพูน	นักวิชาการคอมพิวเตอร์
2.8	นายธนากร	แสงเปี่ยม	นักวิชาการคอมพิวเตอร์
2.9	นายบุรินท์	สุภีวี	นักวิชาการคอมพิวเตอร์
2.10	นายสุวิชัย	แช่มชื่น	นักวิชาการคอมพิวเตอร์
2.11	นายชรัช	แสวงเจริญ	นักวิชาการคอมพิวเตอร์
2.12	น.ส.มุทิตา	มาทมูล	นักวิชาการคอมพิวเตอร์
2.13	นายดำรงศักดิ์	พุ่มจำปา	นักวิชาการคอมพิวเตอร์