เอกสารแนบท้ายประกาศ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของมหาวิทยาลัยแม่ฟ้าหลวง พ.ศ. ๒๕๖๓

เอกสารแนบท้ายประกาศ

เรื่อง แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยแม่ฟ้าหลวง

ว่าด้วยนิยาม

๑. **มหาวิทยาลัย** หมายความว่า มหาวิทยาลัยแม่ฟ้าหลวง

๒. **ศูนย์** หมายความว่า ศูนย์เทคโนโลยีสารสนเทศมหาวิทยาลัยแม่ฟ้าหลวง

๓. **ผู้บริหาร** หมายความว่า อธิการบดี หรือผู้ที่อธิการบดีมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศด้านต่างๆ ของมหาวิทยาลัย

๔. **ผู้ใช้งาน** หมายความว่า บุคลากร พนักงาน ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้างในมหาวิทยาลัย หรือผู้ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของมหาวิทยาลัย

๕. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๖. **สินทรัพย์** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตน อันมีมูลค่าหรือคุณค่าสำหรับมหาวิทยาลัย

๗. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๘. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งาน ของระบบเทคโนโลยีสารสนเทศ

๙. **เหตุการณ์ด้านความปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๐. **สถานการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๑๑. **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายต่างๆ ของมหาวิทยาลัยเข้ากับเครือข่ายอินเทอร์เน็ตสากล

๑๒. ระบบสารสนเทศ หมายความว่า ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยมรการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผนการบริหาร การสนับสนุนให้การบริการ การพัฒนาและควบคุม การ

ติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น คอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

๑๓. **ผู้ดูแลระบบ (System administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษา หรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๔. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิใรการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล

๑๕. **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับผ่านโพรโทคอลต่างๆ เช่น SMTP, POP3, IMAP ฯลฯ

๑๖. **สื่อบันทึกพกพา (Portable media)** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึก หรือจัดเก็บข้อมูล เช่น CD, DVD, flash drive, external harddisk ฯลฯ

๑๗. **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๑๘. **รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อการควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๙. **การเข้ารหัสลับ (Encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับ เพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. **อุปกรณ์จัดเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทาง และค้นหาเส้นทาวเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๒๑. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ และรหัสผ่าน

๒๒. **SSID (Service set identifier)** หมายความว่า ชื่อระบุเครือข่ายไร้สาย

๒๓. **WPA (Wi-Fi protected access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย พัฒนาขึ้นมาใหม่มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๒๔. **MAC address (Media access control address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทาง และปลายทางได้อย่างถูกต้อง

๒๕. **VPN (Virtual private network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเตอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นจนไปถึงปลายทาง

๒๖. **แผนผังระบบเครือข่าย (Network diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

สารบัญ

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๒. เพื่อให้ผู้รับผิดชอบและผู้ที่มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูและระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์บริการเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (รุ่น ๒.๕)

แนวทางปฏิบัติ

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข

- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมาย

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบายข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลงบประมาณการเงินและบัญชี ฯลฯ
- ข้อมูลสารสนเทศตามพันธกิจ เช่น ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับการเข้าถึง

- ระดับชั้นสำหรับผู้บริการ
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึง

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Mission Requirement For Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ

(๒) มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้ (User Access Management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๒.๑ มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๓ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User Registration) ครอบคลุมในเรื่องต่อไปนี้

(๑) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งานจะกำหนดจากรหัสประจำตัวของผู้ใช้งาน

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์ หรือผู้ที่ได้รับมอบหมาย

(๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เช่น ลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง ฯลฯ

๒.๔ มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียด ที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) มีการกำหนดระดับสิทธิในการเข้าถึงสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้ง เปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๖) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งาน และรหัสผ่านปัจจุบัน ให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๗) ในกรณีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่สิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่อยงานเจ้าของระบบ โดยมีการกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันที เมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนด ให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๘) การจัดเก็บรหัสผ่านต้องไม่ใช้วิธีการจัดเก็บโดยตรง ควรใช้วิธีการจัดเก็บแบบเข้ารหัส เช่น MD5 หรือ SHA-256 หรือวิธีการที่ดีกว่า และมีวิธีการกู้รหัสผ่านที่ปลอดภัย

๒.๖ ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ และปรับปรุงบัญชีผู้ใช้งาน ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการว่าจ้าง ฯลฯ

๓. กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติ ดังนี้

๓.๑ มีการกำหนดวิธีการปฏิบัติการใช้งานรหัสผ่าน (Password Use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ควรกำหนดรหัสผ่านให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อ หรือนามสกุลของตนเอง หรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน

(๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านข่ายคอมพิวเตอร์

(๗) เก็บรักษารหัสผ่านทั้งของตนเอง และของกลุ่มไว้เป็นความลับ

(๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล

(๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น

(๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

(๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดิม

(๑๔) ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน ถี่กว่าผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัยในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหาย หรือเข้าถึงโดยไม่ได้รับอนุญาต

(๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

(๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอได้

(๖) ต้องล็อคอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้ง โดยไม่ได้ดูแลชั่วคราว

๓.๓ การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น

เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่ง ไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) มีการกำหนดมาตรการป้องกันทรัพย์สินของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานการณ์ที่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ เช่น

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

(๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ
- วัฒนธรรมองค์กร

(๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

(๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้ โดยไม่ได้รับอนุญาต เช่น กล้องดิจิตอล เครื่องสำเนาเอกสาร ฯลฯ
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) ต้องแสดงหลักฐานเกณฑ์ในการกำหนดเครื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

(๒) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

๔ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตดังนี้

๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศ ได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบุเครือข่ายหรือบริการที่อนุญาตให้มีการใช้งานได้

(๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศสำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (Wireless Lan) ระบบอินเตอร์เน็ท (Internet) ฯลฯ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ เป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ ๑ ครั้ง

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connection) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานภายนอกมหาวิทยาลัยสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

(๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน การใช้สมาร์ทการ์ด หรือการใช้ User Token ที่ใช้เทคโนโลยี PKI ฯลฯ

(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานในมหาวิทยาลัย ๑ วิธี

(๔) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยจากอินเตอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพ และทางเครือข่าย

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ทที่ใช้สำหรับตรวจสอบ

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ทที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับอนุญาตจากผู้ที่รับผิดชอบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Network) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกัน หรือเชื่อมต่อระหว่างกัน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวทางปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address Plan)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๒) การเข้าสู่ระบบระยะไกล (Remote Access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน วิธีการเข้ารหัส ฯลฯ

(๓) วิธีการใดๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศ และเครือข่ายได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

(๔) ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผล หรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้อำนวยการศูนย์อย่างเป็นทางการ

(๕) มีการควบคุมพอร์ท (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามานั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบ และวิธีการหมุนเข้าต้องได้รับอนุญาตอย่างถูกต้อง และเหมาะสมแล้วเท่านั้น

(๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๕.๑ ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของมหาวิทยาลัย และกำหนดชื่อผู้ใช้งาน และรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๕.๒ กำหนดขั้นตอนปฏิบัติการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญ หรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

(๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

(๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์ทการ์ด RFID หรือเครื่องอ่านลายพิมพ์นิ้วมือ ฯลฯ

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งาน หรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัด และควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้ปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยง หรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลง หรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

(๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศ หรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง ฯลฯ กำหนดให้ใช้งานได้เฉพาะช่วงเวลาการทำงานของมหาวิทยาลัยตามปกติเท่านั้น

(๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือ ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน ฯลฯ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access Control)

โดยต้องมีการควบคุมดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลระทบและมีความสำคัญต่อมหาวิทยาลัย จะต้องดำเนินการดังนี้

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ และแสดงให้เห็นถึงผลกระทบ และระดับความสำคัญต่อมหาวิทยาลัย

(๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

(๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๖.๔ การปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของทางมหาวิทยาลัยจากภายนอกมหาวิทยาลัย

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการศูนย์

๗.๒ ผู้ดูแลระบบ (System Administrator) ต้องดำเนินการดังต่อไปนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระข่ายสัญญาณ (Access Point) เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ควรทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าโดยปริยายมาจากผู้ผลิตทันทีที่นำอุปกรณ์สัญญาณ (Access Point) มาใช้งาน

(๕) ควรเปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๖) ต้องมีการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

(๗) ควรหลีกเลี่ยงการติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

(๘) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์ทราบโดยทันที

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๘.๑ ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๑) ให้ศูนย์เป็นผู้กำหนดพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย และพื้นที่ใช้งานระบบเครือข่ายไร้สาย

(๒) ให้ศูนย์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

(๓) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในมหาวิทยาลัยจะต้องได้รับการอนุญาต จากผู้อำนวยการศูนย์

(๔) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดับเพลิงระบบปรับอากาศและควบคุมความชื้นและให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอให้มั่นใจได้ว่า ระบบทำงานตามปกติและลดความเสี่ยงต่อการล้มเหลวในการทำงานของระบบ

(๕) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของมหาวิทยาลัยในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการป้องกันสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและอุปกรณ์เพื่อป้องกันการตัดต่อสายสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจสอบหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๘.๓ การบำรุงรักษาอุปกรณ์

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๘.๔ การนำทรัพย์สินของมหาวิทยาลัยออกนอกมหาวิทยาลัย

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกมหาวิทยาลัย

(๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกมหาวิทยาลัย

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกมหาวิทยาลัย

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกไปใช้งานนอกมหาวิทยาลัย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๘.๕ การจัดการอุปกรณ์ที่ใช้งานอยู่นอกมหาวิทยาลัย

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยออกไปใช้งาน เช่น การขนส่ง และการเกิดอุบัติเหตุกับอุปกรณ์ ฯลฯ

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเหมือนเป็นทรัพย์สินของตนเอง

๘.๖ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์ไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลที่สำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

(๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

(๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น

(๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น ฯลฯ

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น

(๒) ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย

(๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนดำเนินการ

(๔) ไม่ควรติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) กำหนดให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ ฯลฯ

(๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๘) ให้มีการจัดเก็บซอฟต์แวร์รุ่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมและขั้นตอนการปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้รุ่นเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในกำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่มหาวิทยาลัยต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ควรจัดให้มีการควบคุมพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคลหรือหน่วยงานภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่าง ๆ ที่ทำการติดตั้งก่อนดำเนินการติดตั้ง

๘.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และรุ่นที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

(๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบการดำเนินการ ดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของมหาวิทยาลัย
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเพื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
(๓) ข้อมูลวันเวลาที่ออกจากระบบ
(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
(๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
(๗) ข้อมูลความพยายามคอนฟิกกูเรชัน (Configuration) ของระบบ
(๘) ข้อมูลแสดงการใช้งานแอพพลิเคชัน
(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน หรืออ่านไฟล์ ฯลฯ
(๑๐) ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง
(๑๑) ข้อมูลโพรโทคอลเครือข่ายที่ใช้
(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ การใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

(๒) โปรแกรมที่ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกภาพต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ไม่วางสื่อแม่เหล็กไว้ใกล้กับจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

(๗) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ ฯลฯ

(๘) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๙) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๑๐) การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

(๑๑) ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ และเครื่องดื่มต่าง ฯลฯ

(๑๒) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

(๑๓) ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอร์รี่

๑๐.๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD และ External Hard Disk ฯลฯ

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน

๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๑.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีการปฏิบัติในการจัดเก็บข้อมูลและวิธีการปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑๑.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ ปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

๑๑.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption ฯลฯ

๑๒. การเข้าใช้งานระบบอินเทอร์เน็ต (Internet Access)

๑๒.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นที่ไม่ได้รับการอนุมัติจากผู้อำนวยการศูนย์

๑๒.๒ การใช้งานคอมพิวเตอร์จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการ อุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

๑๒.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์เชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อ ความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย ฯลฯ

๑๒.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๒.๕ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๒.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย การทำลายความสัมพันธ์กับบุคคลากรของหน่วยงานอื่นๆ

๑๓. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๓.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น

๑๓.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งศูนย์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๔. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

เพื่อให้ข้อมูลจราจรคอมพิวเตอร์ (Log) มีความถูกต้องและสามารถระบุถึงตัวตนบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

๑๔.๑ จัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๔.๒ ห้ามผู้ดูและระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

๑๔.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Log) และบันทึกรายละเอียดของการป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึก

การพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๔.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัย ให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัยเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ศูนย์บริการเทคโนโลยีสารสนเทศ

๒. ผู้ดูและระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (รุ่น ๒.๕)

แนวปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่การเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้นโดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องการทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) ฯลฯ
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (Configuration) ข้อมูลในฐานข้อมูล ฯลฯ

- จัดเก็บข้อมูลสำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บสำรองกับมหาวิทยาลัยควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับมหาวิทยาลัย เช่น ไฟไหม้ น้ำท่วม ฯลฯ
- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. ต้องจัดทำแผนตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดดังนี้

(๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ ฯลฯ

(๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้

(๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ ฯลฯ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่เมื่อเกิดเหตุเร่งด่วน

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ ๑ ครั้ง

๓. ต้องการการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานในมหาวิทยาลัย ปีละ ๑ ครั้ง

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑.เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑.ศูนย์บริการเทคโนโลยีสารสนเทศ

๒.หน่วยตรวจสอบภายใน(Internal Auditing Unit)

๓.ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (รุ่น ๒.๕)

แนวปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ปีละ ๑ ครั้ง

๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ ๑ ครั้ง

๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ปีละ ๑ ครั้ง

๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้

(๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

(๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันอย่างดี

(๓) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(๔) ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง ต่อคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

๔. มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔ นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งาน
๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน
๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑.ศูนย์บริการเทคโนโลยีสารสนเทศ
๒.ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (รุ่น ๒.๕)

แนวปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย ปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ
๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย
๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการจัดฝึกอบรมของมหาวิทยาลัย
๔. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า ๑ ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้
๕. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่ายโดยมีการปรับปรุงความรู้อยู่เสมอ
๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตามประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ส่วนที่ ๕ ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) มหาวิทยาลัยแม่ฟ้าหลวง

วัตถุประสงค์

๑. เพื่อเป็นมาตรฐาน แนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. หน่วยจัดการสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับหมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (รุ่น ๒.๕)

แนวปฏิบัติ

จดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นบริการที่ทางมหาวิทยาลัย ได้จัดทำขึ้นเพื่อสนับสนุนการศึกษา การวิจัย การบริการ วิชาการ ตลอดจน การบริหารจัดการตามภารกิจของหน่วยงาน ผู้ใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย ภายใต้ชื่อโดเมน (Domain) ที่จดทะเบียนโดยมหาวิทยาลัย มีหน้าที่พึงปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ โดยไม่ขัดกับนโยบายการใช้คอมพิวเตอร์ของมหาวิทยาลัย ข้อปฏิบัติฉบับนี้ใช้กับผู้ใช้ซึ่งอยู่ในสังกัดของมหาวิทยาลัย ได้แก่ นักศึกษา อาจารย์ เจ้าหน้าที่ บุคคลที่ปฏิบัติงานภายใต้การมอบอำนาจของหน่วยงานในสังกัดของมหาวิทยาลัย ซึ่งเรียกโดยย่อว่า “ผู้ใช้”

บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้สามารถเข้าถึงโดยการระบุด้วยชื่อบัญชีจดหมายอิเล็กทรอนิกส์และรหัสผ่าน โดยมีหน่วยจัดการสารสนเทศ เป็นหน่วยงานกำกับ ดูแล เพื่อให้การใช้งานจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เป็นไปตามมาตรการเพื่อป้องกัน และปราบปรามการกระทำความผิดเกี่ยวกับ พรบ.คอมพิวเตอร์ รวมทั้งทำหน้าที่ปรับปรุงรายละเอียดข้อปฏิบัติให้ทันสมัยสอดคล้องกับภารกิจของมหาวิทยาลัย ตลอดจนให้ข้อมูล และตอบข้อสงสัยที่เกี่ยวข้องกับข้อปฏิบัติฉบับนี้

๑. ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

๑.๑ ผู้ใช้ มีหน้าที่รับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่าน เพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะบุคคล และไม่อนุญาตให้ผู้อื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้เป็นผู้รับผิดชอบต่อ

ผลกระทบ และผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ ในนามของตนเอง

๑.๒ ผู้ใช้พึ่งทราบว่าผู้ดูแลระบบไม่มีสิทธิ์ที่จะถาม หรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัว เพื่อเข้าใช้งานบัญชีจดหมายอิเล็กทรอนิกส์

๑.๓ ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้อื่นไม่ว่าจะได้รับอนุญาต หรือไม่ก็ตาม

๑.๔ การใช้งานจดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

(๑) การใช้จดหมายอิเล็กทรอนิกส์ เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

(๒) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่จดหมายลูกโซ่

(๓) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลชั้นความลับของมหาวิทยาลัย

(๔) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อมูลการประชุมของที่ประชุมผู้บริหารมหาวิทยาลัย หรือในการประชุมอื่นๆ โดยที่มิได้มีหน้าที่ หรือมิได้รับมอบหมายจากประธานในที่ประชุม

(๕) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดิโอ เสียง ที่กล่าวร้ายต่อบุคคล หรือกลุ่มบุคคล

(๖) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดิโอ เสียง ที่ดูหมิ่นเหยียดหยาม หรือแบ่งแยกทาง เพศ เชื้อชาติ ศาสนา หรือพระมหากษัตริย์

(๗) การส่งจดหมายอิเล็กทรอนิกส์ เผยแพร่ข้อความ ภาพ วีดิโอ เสียง ที่มีลักษณะหยาบคาย หรือลามก อนาจาร

(๘) การส่งจดหมายอิเล็กทรอนิกส์ เพื่อเผยแพร่โปรแกรม งาน หรือเผยแพร่รหัสสำหรับใช้เข้าถึงโปรแกรม หรืองานในลักษณะที่ละเมิดลิขสิทธิ์

(๙) การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา หรือพระมหากษัตริย์ ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

(๑๐) การส่งจดหมายอิเล็กทรอนิกส์ โฆษณาสินค้า ผลิตภัณฑ์ หรือส่งข้อความลักษณะของ สแปมเมล์ (Spam Mail) ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

(๑๑) การส่งจดหมายอิเล็กทรอนิกส์ ซึ่งส่งผลกระทบทำให้ระบบจดหมายอิเล็กทรอนิกส์ หรือเครือข่ายลดทอนประสิทธิภาพลง

(๑๒) การส่งจดหมายอิเล็กทรอนิกส์ กระจายไวรัส หรือรหัสโปรแกรมที่เป็นอันตรายต่อระบบความมั่นคงปลอดภัย

๒. การขอจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์

หน่วยจัดการสารสนเทศ จัดให้มีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อสนับสนุนการศึกษา การวิจัย การบริการ วิชาการ ตลอดจน การบริหารจัดการตามภารกิจของหน่วยงาน โดยมีข้อกำหนดดังนี้

๒.๑ หน่วยจัดการสารสนเทศ จัดให้ผู้ใช้มีบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์โดยไม่ต้องทำการขอจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ โดยจัดให้มีตั้งแต่วันที่เริ่มทำงาน

๒.๒ บุคคลที่ไม่อยู่ในสักกัดของมหาวิทยาลัย สามารถยื่นขอจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ โดยยื่นคำร้องผ่านหัวหน้าหน่วยงานต้นสังกัด พร้อมแนบเหตุผลความจำเป็นในการใช้งาน ระยะเวลาในการใช้งาน และชื่อผู้ใช้ ส่งถึง หน่วยจัดการสารสนเทศ ทั้งนี้หน่วยจัดการสารสนเทศสงวนสิทธิ์ในการตั้งชื่อผู้ใช้จดหมายอิเล็กทรอนิกส์ตามความเหมาะสม

๒.๓ หน่วยงานภายใต้สังกัดของมหาวิทยาลัย สามารถยื่นขอจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์สำหรับการใช้งานเฉพาะของหน่วยงาน โดยยื่นคำร้องผ่านหัวหน้าหน่วยงาน พร้อมแนบเหตุผลความจำเป็นในการใช้งาน และชื่อผู้ใช้ ส่งถึง หน่วยจัดการสารสนเทศ ทั้งนี้ หน่วยจัดการสารสนเทศ สงวนสิทธิ์ในการตั้งชื่อบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ตามความเหมาะสม

๒.๔ หน่วยงานภายใต้สังกัดของมหาวิทยาลัย สามารถยื่นขอจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์สำหรับการใช้งานเฉพาะกิจ เช่น การประชุมวิชาการ เป็นต้น โดยหน่วยงานผู้รับผิดชอบยื่นคำร้องผ่านหัวหน้าหน่วยงาน พร้อมแนบเหตุผลความจำเป็นในการใช้งาน ระยะเวลาในการใช้งาน และชื่อผู้ใช้ ส่งถึงหน่วยจัดการสารสนเทศ ทั้งนี้ หน่วยจัดการสารสนเทศสงวนสิทธิ์ในการตั้งชื่อบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ตามความเหมาะสม

๓. การจัดการรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์

หน่วยจัดการสารสนเทศ จัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ เพื่อสร้างการส่งจดหมายอิเล็กทรอนิกส์แบบกลุ่ม รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์แบบกลุ่มของมหาวิทยาลัยเป็นข้อมูลที่ไม่เผยแพร่ให้ผู้ใช้หรือหน่วยงานใดๆ การใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ดังกล่าวมีข้อกำหนดเฉพาะดังนี้

๓.๑ หน่วยงานที่ได้รับมอบหมาย สามารถใช้รายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่ข่าวสาร และประชาสัมพันธ์ภารกิจของมหาวิทยาลัย

๓.๒ หน่วยจัดการสารสนเทศ จัดให้มีระบบรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ กลุ่มย่อยตามแต่ละหน่วยงาน ทั้งนี้หน่วยจัดสารสนเทศ สงวนสิทธิ์ในการอนุมัติการขอจดทะเบียนชื่อกลุ่ม ตลอดจนการตั้งชื่อกลุ่ม ตามความเหมาะสม

๓.๓ หน่วยงานภายใต้สังกัดขอมหาวิทยาลัย สามารถยื่นจดทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์แบบกลุ่มสำหรับการใช้งานเฉพาะกิจ โดยหน่วยงานผู้รับผิดชอบยื่นคำร้องผ่านหัวหน้าหน่วยงาน พร้อมแนบเหตุผลความจำเป็นในการใช้งาน และรายชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์พร้อมชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของหน่วยงานเพื่อสิทธิในการดูแลรายชื่อบัญชีจดหมาย

อิเล็กทรอนิกส์ ทั้งนี้ หน่วยจัดการสารสนเทศสงวนสิทธิ์ในการตั้งชื่อบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์แบบกลุ่มตามความเหมาะสม

๔. การขอเปลี่ยนแปลงข้อมูลบัญชีจดหมายอิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์จำกัดสิทธิ เพื่อไม่ให้ผู้ใช้งานสามารถเปลี่ยนแปลงข้อมูลใดๆ ระหว่างการใช้งาน ในกรณีที่ผู้ใช้มีความจำเป็นในการเปลี่ยนแปลงข้อมูล ผู้ใช้ ในกรณีที่เป็นอาจารย์ เจ้าหน้าที่ จะต้องดำเนินการผ่านส่วนกลางเจ้าหน้าที่ หรือในกรณีที่เป็น นักศึกษา จะต้องดำเนินการผ่านส่วนทะเบียนและประมวลผล โดยมีข้อปฏิบัติดังนี้

๔.๑ ผู้ใช้ กรณีที่เป็นอาจารย์ เจ้าหน้าที่ สามารถเปลี่ยนแปลงชื่อ นามสกุล ข้อมูลส่วนบุคคล หรือชื่อบัญชีจดหมายอิเล็กทรอนิกส์ โดยผู้ใช้ต้องดำเนินการเปลี่ยนแปลงข้อมูลผ่านส่วนการเจ้าหน้าที่ และมีการแจ้งการปรับปรุงข้อมูลจากส่วนการเจ้าหน้าที่ ส่งถึงหน่วยจัดการสารสนเทศให้เป็นผู้ดำเนินการปรับปรุงข้อมูลบัญชีผู้ใช้โดยอ้างอิงจากฐานข้อมูลหลักของมหาวิทยาลัย

๔.๒ ผู้ใช้ กรณีที่เป็นนักศึกษา สามารถเปลี่ยนแปลงชื่อ นามสกุล หรือข้อมูลส่วนบุคคลในบัญชีจดหมายอิเล็กทรอนิกส์ โดยผู้ใช้ต้องดำเนินการเปลี่ยนแปลงข้อมูลผ่านส่วนทะเบียนและประเมินผล และมีการแจ้งการปรับปรุงข้อมูลโดยส่วนทะเบียนและประเมินผล ส่งถึงหน่วยจัดการสารสนเทศให้เป็นผู้ดำเนินการปรับปรุงข้อมูลบัญชีผู้ใช้โดยอ้างอิงจากฐานข้อมูลหลักของมหาวิทยาลัย

๔.๓ ผู้ใช้สามารถขอเปลี่ยนแปลงรหัสผ่านบัญชีจดหมายอิเล็กทรอนิกส์ โดยแจ้งความประสงค์ผ่านทางระบบขอเปลี่ยนแปลงรหัสผ่านอัตโนมัติ

๔.๓.๑ สำหรับเจ้าหน้าที่ระบบจะดำเนินการส่งข้อมูลวิธีการเปลี่ยนแปลงรหัสผ่านผ่านทางอีเมล์ส่วนตัวที่ให้ไว้กับส่วนการเจ้าหน้าที่

๔.๓.๒ สำหรับนักศึกษาระบบจะดำเนินการส่งข้อมูลวิธีการเปลี่ยนแปลงรหัสผ่านผ่านทางอีเมล์ส่วนตัวที่ให้ไว้กับส่วนทะเบียนและประมวลผล

หากข้อมูลอีเมล์ส่วนตัวผู้ใช้ไม่ถูกต้องให้ผู้ใช้ดำเนินการปรับปรุงข้อมูลให้ถูกต้องก่อนดำเนินการแจ้งความประสงค์เปลี่ยนแปลงรหัสผ่าน

๕. การระงับชื่อบัญชีจดหมายอิเล็กทรอนิกส์

บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่มหาวิทยาลัยเอื้ออำนวยให้ผู้ใช้ ซึ่งผู้ใช้ไม่สามารถโอนสิทธิ์ให้แก่ผู้ใช้อื่นได้ มหาวิทยาลัยคงไว้ซึ่งอำนาจในการ จำกัด ระงับ หรือเพิกถอนสิทธ์ การใช้งานโดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบาย หรืออาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย เสถียรภาพของระบบ การกระทำที่ขัดต่อนโยบาย หรือกฎหมาย การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์มีแนวปฏิบัติ ดังนี้

๕.๑ เมื่อผู้ใช้ กรณีที่เป็นอาจารย์ เจ้าหน้าที่ บุคคล พ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัย หน่วยจัดการสารสนเทศ สามารถระงับบัญชีผู้ใช้ซึ่งส่งผลให้การเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ถูกระงับ

๕.๒ ผู้ใช้สามารถร้องขอการขยายสิทธิ์การใช้บัญชีผู้ใช้เพื่อคงสิทธิ์การใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ก่อนเมื่อต้องพ้นสภาพการอยู่ในสังกัดของมหาวิทยาลัย โดยยื่นคำร้องผ่านหน่วยงานพร้อมแนบเหตุผลความจำเป็น และระยะเวลาในการใช้งาน ส่งถึงหน่วยจัดการสารสนเทศ

๕.๓ บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบ หากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบกับให้ประสิทธิภาพระบบเครือข่ายด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้หน่วยจัดการสารสนเทศมีสิทธิ์ระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า