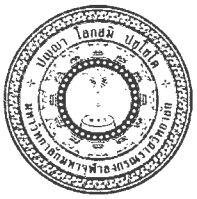

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย พ.ศ. ๒๕๖๘

สารบัญ

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัย เชื่อถือได้ และเพื่ออนุวัติให้เป็นไปตามพระราชบัญญัติการปฏิบัติราชการทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๖๕ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย ได้กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัยเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้ สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่าง ๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ ด้วย

๒. วัตถุประสงค์

มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย ได้กำหนดแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ ดังต่อไปนี้

๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัยเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย และทำให้ดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓. เพื่อเผยแพร่แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ นิสิต และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ ความเข้าใจและ ตระหนักถึงความสำคัญและถือปฏิบัติตามแนวปฏิบัตินี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยมีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัย

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับ ทั้งของมหาวิทยาลัยเองและส่วนงานที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของแนวปฏิบัติ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามแนวปฏิบัติที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย (Information Access Control)
๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)
๕. การใช้งานอินเทอร์เน็ต (Use of the Internet)
๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย
๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๑๐. การเข้าถึงเครื่องคอมพิวเตอร์ที่ส่วนงานจัดไว้ให้งานร่วมกัน
๑๑. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)
๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)
๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator)
๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ส่วนที่ ๒ แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๓ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๔ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Guidelines)

ส่วนที่ ๑ แนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย
๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชีผู้ใช้สารสนเทศของมหาวิทยาลัยโดยเคร่งครัด

ผู้รับผิดชอบ

๑. ส่วนเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย (Information Access Control)

๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

๑.๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๒. กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย ดังนี้

๑.๒.๑. ไม่มีสิทธิ์
๑.๒.๒. อ่านได้อย่างเดียว
๑.๒.๓. สร้างข้อมูล
๑.๒.๔. ป้อนข้อมูล
๑.๒.๕. แก้ไขข้อมูล
๑.๒.๖. ลบข้อมูล
๑.๒.๗. อนุมัติการใช้ข้อมูล

๑.๓. กำหนดประเภทข้อมูลของมหาวิทยาลัยเป็น ๖ ประเภทหลัก ๆ ดังนี้

๑.๓.๑. ข้อมูลนิสิต
๑.๓.๒. ข้อมูลบุคลากร
๑.๓.๓. ข้อมูลการเงินและบัญชี
๑.๓.๔. ข้อมูลทางการศึกษา
๑.๓.๕. ข้อมูลทางการบริหาร

๑.๓.๖. ข้อมูลการจราจรทางคอมพิวเตอร์

๑.๔. กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของมหาวิทยาลัยเป็น ๔ ระดับดังนี้

๑.๔.๑. *ลับ* รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๔.๒. *ใช้ภายในเท่านั้น* เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/ส่วนงาน หรือข้อมูล ที่เผยแพร่เฉพาะภายในมหาวิทยาลัย

๑.๔.๓. *ส่วนบุคคล* ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือส่วนงานที่ดูแลข้อมูลนั้น

๑.๔.๔. *เปิดเผยได้* เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๕. เกณฑ์ในการกำหนดชั้นความลับของข้อมูล

๑.๕.๑. *ประเภทลับ* หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๕.๒. *ประเภทใช้ภายในเท่านั้น* หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/ส่วนงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในมหาวิทยาลัย

๑.๕.๓. *ประเภทส่วนบุคคล* หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือส่วนงานที่ดูแลข้อมูลนั้น

๑.๕.๔. *ประเภทเปิดเผยได้* หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๖. กำหนดระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัยดังนี้

๑.๖.๑. การเข้าถึงสำหรับผู้บริหาร

๑.๖.๒. การเข้าถึงสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

๑.๖.๓. การเข้าถึงสำหรับผู้ดูแลระบบ

๑.๖.๔. การเข้าถึงระดับบุคคล

๑.๖.๕. การเข้าถึงระดับผู้ใช้งานทั่วไป

๑.๗. เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

๑.๗.๑. ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในส่วนงานนั้น

๑.๗.๒. ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

๑.๗.๓. ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๑.๗.๔. บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

๑.๗.๕. ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

๑.๗.๖. การกำหนดสิทธิ์พิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

๑.๗.๗. การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์หรือส่วนงานหลักเท่านั้น

๑.๘. กำหนดให้มีส่วนงานหลักหรือส่วนงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัยในแต่ละประเภทดังนี้

๑.๘.๑. *ข้อมูลนิสิต* ส่วนงานหลักคือ สำนักทะเบียนและวัดผล

๑.๘.๒. *ข้อมูลบุคลากร* ส่วนงานหลักคือ กองกลาง

๑.๘.๓. *ข้อมูลการเงินและบัญชี* ส่วนงานหลักคือ กองคลังและทรัพย์สิน

๑.๘.๔. *ข้อมูลทางการศึกษา* ขึ้นอยู่กับส่วนงานที่มหาวิทยาลัยมอบหมายเป็นส่วนงานหลัก

๑.๘.๕. *ข้อมูลทางการบริหาร* ขึ้นอยู่กับส่วนงานที่มหาวิทยาลัยมอบหมายเป็นส่วนงานหลัก

๑.๘.๖. *ข้อมูลการจราจรทางคอมพิวเตอร์* ส่วนเทคโนโลยีสารสนเทศและส่วนงานที่ให้บริการระบบสารสนเทศ

๑.๘.๗. *การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง* ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของมหาวิทยาลัยมหาจุฬาลงกรณราชวิทยาลัย

๑.๙. การควบคุมการเปลี่ยนแปลง

๑.๙.๑. การเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการดังนี้

(๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง

(๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้น ๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

(๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

๑.๙.๒. ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๑๐. การกำหนดการใช้งานตามภารกิจ

๑.๑๐.๑. การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) *นิสิต* จะให้สิทธิ์ทันทีที่มีสภาพเป็นนิสิตและหมดสิทธิ์เมื่อพ้นสภาพนิสิตไปแล้ว ๙๐ วัน

(๒) *บุคลากร* จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

(๓) *ผู้บริหาร* จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นผู้บริหาร

(๔) *บุคคลภายนอก* ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

๑.๑๐.๒. ข้อจำกัดในการเข้าถึง

(๑) *นิสิต* เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

(๒) *บุคลากร* เข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย

(๓) *ผู้บริหาร* เข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

(๔) *บุคคลภายนอก* เข้าถึงได้ตามที่ได้รับอนุญาต

๑.๑๑. ระยะเวลาการใช้งาน

๑.๑๑.๑. ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานจะเข้าถึงและใช้งานได้ ดังนี้

(๑) การเข้าถึงในเวลาทำการ ๐๙.๐๐-๑๗.๐๐ น.

(๒) การเข้าถึงนอกเวลาทำการ หลัง ๑๗.๐๐ น. เป็นต้นไป

(๓) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนักขัตฤกษ์

๑.๑๑.๒. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(๑) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ ต้องตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ

๑.๑๒. การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๒.๑. บัญชีผู้ใช้หมดอายุ

๑.๑๒.๒. เมื่อมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง

๑.๑๒.๓. ถูกระงับสิทธิ์

๑.๑๓. การทบทวนและตรวจสอบสิทธิ์การเข้าถึงและการใช้งานข้อมูลสารสนเทศ และระบบสารสนเทศ

๑.๑๓.๑. ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศ ปีละ 1 ครั้ง โดย ผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามคณะ/ส่วนงานที่ขอสิทธิ์ จัดส่ง รายชื่อนั้นให้กับส่วนงานที่ขอสิทธิ์เพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือไม่ หรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิ์การเข้าถึงให้ถูกต้องหรือไม่

๑.๑๓.๒. ส่วนงานผู้ขอสิทธิ์แจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

๑.๑๓.๓. ส่วนงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบทันที

๑.๑๔. ช่องทางการเข้าถึง

๑.๑๔.๑. เครือข่ายภายในมหาวิทยาลัย

๑.๑๔.๒. เครือข่ายภายนอกมหาวิทยาลัย

๑.๑๔.๓. เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

๒.๑.๑. ต้องจัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒. อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง

๒.๑.๓. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๒. การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบสารสนเทศของมหาวิทยาลัยจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศของมหาวิทยาลัย ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น ๔ กลุ่ม คือ

๒.๒.๑. นิสิตของมหาวิทยาลัย

๒.๒.๒. บุคลากรของมหาวิทยาลัย อาจารย์พิเศษ นักวิจัย และแขกของส่วนงาน

๒.๒.๓. ลูกค้า

๒.๒.๔. บุคคลอื่น ๆ ที่ มหาวิทยาลัยมอบสิทธิ์ให้

๒.๓. การลงทะเบียนผู้ใช้งาน

๒.๓.๑. นิสิต นิสิตใหม่ทุกคน ได้รับบัญชีผู้ใช้โดยอัตโนมัติ ทันทีที่สำนักทะเบียนและวัดผลป้อนข้อมูลนิสิตเข้าสู่ระบบทะเบียนนิสิต

๒.๓.๒. บุคลากรของมหาวิทยาลัย อาจารย์พิเศษ นักวิจัย และแขกของส่วนงาน ส่วนเทคโนโลยีสารสนเทศ จะสร้างบัญชีบุคลากรใหม่โดยอัตโนมัติทันทีที่กองกลาง ป้อนข้อมูลบุคลากรเข้าระบบสารสนเทศบุคลากร

๒.๓.๓. ลูกค้าของส่วนงาน กรณีส่วนงานต้องการบัญชีผู้ใช้เพื่อบริหารจัดการในการให้บริการลูกค้าเป็นกลุ่มบุคคล ดำเนินการดังนี้

(๑) ดาวน์โหลดแบบฟอร์มได้จาก www.it.mcu.ac.th หัวข้อแบบฟอร์มขอใช้บริการ กรอกข้อมูลให้ครบถ้วนส่งส่วนเทคโนโลยีสารสนเทศ

(๒) ส่วนเทคโนโลยีสารสนเทศจะออกบัญชีผู้ใช้ให้ ตามข้อมูลที่ส่วนงานระบุ และแจ้งผู้รับผิดชอบตามอีเมลที่ระบุไว้ในแบบฟอร์ม

(๓) ผู้รับผิดชอบของส่วนงาน จะต้องรับผิดชอบความเสียหายใด ๆ ที่จะเกิดจากการใช้งานบัญชีผู้ใช้ที่ส่วนเทคโนโลยีสารสนเทศออกให้

(๔) หากต้องการเปลี่ยนแปลงผู้รับผิดชอบบัญชีผู้ใช้ ให้แจ้งส่วนเทคโนโลยีสารสนเทศ เป็นลายลักษณ์อักษรลงนามโดยผู้บริหารของส่วนงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมบัญชีผู้ใช้และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

(๕) หากต้องการยกเลิกบัญชีผู้ใช้ ให้แจ้งส่วนเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรลงนามโดย ผู้บริหารของส่วนงาน ระบุ ชื่อผู้รับผิดชอบ และจ านวนบัญชีผู้ใช้ที่ต้องการยกเลิก

๒.๓.๔. บุคคลอื่น ๆที่ มหาวิทยาลัยมอบสิทธิ์ให้ เช่น บุคคลที่ทำงานในส่วนงานอิสระ บุคคลที่มหาวิทยาลัยมอบสิทธิ์ให้ สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อที่สำนักงานเลขานุการส่วนเทคโนโลยีสารสนเทศ โดยมีหนังสือรับรองจากผู้บริหารระดับคณะ/ส่วนงานขึ้นไป และแสดงบัตรประจำตัวประชาชน หรือหนังสือเดินทาง พร้อมสำเนาที่รับรองสำเนาถูกต้อง 1 ฉบับ

๒.๔. การจัดการบัญชีผู้ใช้ของมหาวิทยาลัย

๒.๔.๑. การบริหารจัดการบัญชีผู้ใช้สำหรับบุคลากรของมหาวิทยาลัย ดำเนินการโดยผ่านผู้แทนของส่วนงาน โดยผู้บริหารของส่วนงานแจ้งชื่อผู้แทนที่จะรับผิดชอบในการดูแลบัญชีผู้ใช้ของบุคลากรในสังกัด เป็นลายลักษณ์อักษรถึงผู้อ านวยการส่วนเทคโนโลยีสารสนเทศ โดยมีรายละเอียด ดังนี้

(๑) ชื่อส่วนงาน

(๒) ชื่อ-สกุลของผู้แทน

(๓) ชื่อบัญชีผู้ใช้ของผู้แทน

(๔) อีเมลของผู้แทน

(๕) หมายเลขโทรศัพท์ของผู้แทน

๒.๔.๒. การเปลี่ยนแปลงผู้แทนของส่วนงาน ให้แจ้งส่วนเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร ลงนามโดยผู้บริหารของส่วนงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมอีเมล และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

๒.๕. การจัดการสิทธิ์ของผู้ใช้งาน

๒.๕.๑. เมื่อเจ้าหน้าที่ของส่วนงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

๒.๕.๒. การแจ้งขอใช้สิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(๑) ลงชื่อโดยผู้บริหารของส่วนงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของส่วนงานหลัก

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) ส่วนงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๒.๕.๓. ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามแนวปฏิบัติการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒.๕.๔. กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา โดยต้องได้รับความเห็นชอบและอนุมัติจากอธิการบดีหรือผู้ที่ได้รับมอบอำนาจจากอธิการบดี

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๒.๖. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๖.๑. ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๒.๖.๒. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๒.๖.๓. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมลเป็นช่องทางในการส่ง

๒.๖.๔. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๒.๖.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

๒.๖.๖. ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็นเวลานาน

๒.๖.๗. กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิ์การใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยน รหัสผ่านเป็นที่เรียบร้อย

๒.๗. การทบทวนสิทธิ์การเข้าถึง

๒.๗.๑. ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๒.๗.๒. บัญชีผู้ใช้จะหมดอายุ ดังนี้

(๑) กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของมหาวิทยาลัย ยกเว้นผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตเท่านั้น

(๒) กรณีนิสิต หมดอายุหลังพ้นสภาพการเป็นนิสิต ๙๐ วัน แต่จะเปลี่ยนสภาพเป็นศิษย์เก่าโดยอัตโนมัติ ซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ต และระบบฐานข้อมูลศิษย์เก่าเท่านั้น

(๓) กรณีที่ไม่ใช่บุคลากรของมหาวิทยาลัย หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี หรือ เมื่อไม่มีการเข้าใช้งานติดต่อกันเกิน ๓ เดือน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑. การใช้งานบัญชีผู้ใช้และรหัสผ่าน

๓.๑.๑. ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๓.๑.๒. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๓.๒. การใช้งานรหัสผ่าน

๓.๒.๑. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่มหาวิทยาลัยกำหนด

๓.๒.๒. ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น ชื่อ นามสกุล ชื่อเล่น ชื่อบิดา ชื่อมารดา ชื่อส่วนงาน หรือคำศัพท์ที่มีใช้ในพจนานุกรม เป็นต้น ต้องประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน

๓.๒.๓. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๓.๒.๔. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๓.๒.๕. หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิ์ใช้งาน

๓.๒.๖. เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๓.๓. การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

๓.๓.๑. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๓.๓.๒. ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแล

๓.๓.๓. ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๓.๔. การจัดวางและการป้องกันอุปกรณ์

๓.๔.๑. จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับอนุญาต

๓.๔.๒. อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๓.๔.๓. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๕. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๕.๑. จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๓.๕.๒. ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

๓.๕.๓. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๓.๕.๔. สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๕.๕. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๓.๕.๖. จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนด อื่น ๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

๓.๕.๗. โปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย เป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

๓.๕.๘. ไม่เก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๓.๕.๙. ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

๓.๕.๑๐. ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๓.๕.๑๑. ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บ ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าว ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๓.๖. การป้องกันโปรแกรมไม่ประสงค์ดี

๓.๖.๑. ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๓.๖.๒. ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๓.๖.๓. ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดีก่อนการรับส่งทุกครั้ง

๓.๖.๔. ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดี ก่อนการเปิดใช้ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่นไฟล์ที่มีนามสกุล .exe .com .bat .vbs .scr .pif .hta เป็นต้น

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑. การเข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย

๔.๑.๑. การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่มหาวิทยาลัยออกให้

๔.๑.๒. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือขายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๔.๑.๓. การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจากภายนอกต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรฐานการเข้าถึงระบบเครือข่ายมหาวิทยาลัยจากภายใน

๔.๑.๔. เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับส่วนเทคโนโลยีสารสนเทศ

๔.๑.๕. จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ตอุปกรณ์เครือข่ายตามความจำเป็น

๔.๑.๖. การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๔.๑.๗. การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของมหาวิทยาลัย ต้องขออนุญาตใช้บัญชีชั่วคราวจากมหาวิทยาลัย ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

๔.๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๔.๒.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในมหาวิทยาลัยจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการส่วนเทคโนโลยีสารสนเทศ หรือผู้บริหารส่วนงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

๔.๒.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจาก ภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖) ต้องเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ ด้วยวิธีที่มีประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น

(๗) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

(๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการส่วนเทคโนโลยีสารสนเทศทราบโดยทันที

๔.๓. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๔.๓.๑. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๔.๓.๒. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิตช์

๔.๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๔.๔.๑. ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๔.๔.๒. ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๔.๔.๓. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกมหาวิทยาลัย แต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่มหาวิทยาลัยกำหนด เช่น VPN เป็นต้น

๔.๔.๔. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๔.๔.๕. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔.๔.๖. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔.๕. การแบ่งแยกเครือข่าย (segregation in networks)

๔.๕.๑. ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔.๕.๒. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่าง ๆ ของมหาวิทยาลัย

๔.๕.๓. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๔.๕.๔. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกส่วนงาน ซึ่งสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานบริการเครือข่ายของส่วนงาน

๔.๖. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

๔.๖.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๔.๖.๒. ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัย ต้องติดตั้งระบบตรวจจับการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี

๔.๗. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

๔.๗.๑. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๔.๗.๒. มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๔.๗.๓. ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๔.๗.๔. ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๔.๗.๕. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๔.๗.๖. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

๔.๘. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connections)

๔.๘.๑. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๔.๘.๒. ผู้ใช้งานที่อยู่ภายนอกส่วนงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

๔.๘.๓. ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๕. การใช้งานอินเทอร์เน็ต (use of the Internet)

๕.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ตามสิทธิ์ที่ได้รับ

๕.๒. ห้ามใช้อินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๕.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น

๕.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๕.๕. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย

๖.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๖.๒. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๖.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (time.mcu.ac.th) ที่มหาวิทยาลัยใช้อ้างอิง

๖.๔. เปิดใช้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัยด้วย

๖.๕. ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่าง ๆ

๖.๖. ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๗. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของส่วนงาน

๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

๗.๑. นิสิต ใช้บัญชีผู้ใช้ที่เป็นตัวเลขรหัสนิสิต ตามด้วย @mcu.ac.th โดยเข้าใช้งานที่ mail.mcu.ac.th และใช้งานทุกระบบของ G Suite ของมหาวิทยาลัย ด้วยบัญชีผู้ใช้เดียว

๗.๒. บุคลากร ลงทะเบียนเพื่อใช้บริการระบบจดหมายอิเล็กทรอนิกส์ (MCU-Mail) ที่ www.it.mcu.ac.th และใช้งานทุกระบบของ G Suite ของมหาวิทยาลัย ด้วยบัญชีผู้ใช้เดียว

๗.๓. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ

๗.๔. กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงบนหัวข้อจดหมาย อิเล็กทรอนิกส์

๗.๕. ผู้ใช้งานมีหน้าที่จะต้องรักษาบัญชีผู้ใช้ และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง เพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี

๗.๖. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

๗.๗. ในการตรวจสอบความผิดปกติของการใช้งานจดหมายอิเล็กทรอนิกส์ หากพบว่าผู้ใช้งานรายใดส่งจดหมายอิเล็กทรอนิกส์มากกว่าจำนวนที่ควรจะเป็น ระบบจะทำการระงับบัญชีผู้ใช้ชั่วคราว เพื่อป้องกันความเสียหายที่จะเกิดกับระบบของมหาวิทยาลัย

๗.๘. ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิงก์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

๗.๙. ต้องไม่ส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน บัญชีผู้ใช้ หมายเลขบัตรประชาชน หมายเลขบัตรเครดิต ฯลฯ ผ่านจดหมายอิเล็กทรอนิกส์

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System access control)

๘.๑. ผู้ดูแลระบบ (System Administrator)

๘.๑.๑. ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๘.๒. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๘.๒.๑. ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๘.๒.๒. ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๘.๒.๓. จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๘.๒.๔. จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจาก อาจสร้างความเสียหายให้กับระบบได้

๘.๓. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๘.๓.๑. ผู้ใช้งานต้องมีบัญชีผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

๘.๓.๒. สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม โดยใช้สมาร์ทการ์ด RFID หรือ เครื่องอ่านลายพิมพ์นิ้วมือ หรือวิธีการอื่นที่มีความปลอดภัย

๘.๔. การบริหารจัดการรหัสผ่าน (Password Management System)

๘.๔.๑. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่า ผู้ดูแลระบบจะปลดล็อกให้

๘.๔.๒. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๘.๔.๓. มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๘.๔.๔. ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๘.๔.๕. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๘.๔.๖. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๘.๕. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๘.๕.๑. จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๘.๕.๒. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๘.๕.๓. ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๘.๕.๔. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๘.๕.๕. โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

๘.๕.๖. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๘.๖. การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

๘.๖.๑. ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๘.๖.๒. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๘.๖.๓. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๘.๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๘.๗.๑. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถ

ใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง เป็นต้น และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของมหาวิทยาลัยเท่านั้น

๘.๗.๒. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๘.๗.๓. กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑. หัวหน้าส่วนงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องแต่งตั้งผู้มีสิทธิ์ และกำหนดจำนวนผู้มีสิทธิ์ในการเข้าถึงระบบปฏิบัติการ

๙.๒. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๙.๓. ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๙.๔. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๙.๕. ผู้ดูแลระบบต้องยุติการให้บริการทันทีในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

๙.๖. ห้ามการติดตั้งซอฟต์แวร์อื่น ๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่มหาวิทยาลัยไม่อนุญาต

๙.๗. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญ อย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๙.๘. ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

๙.๙. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ เป็นต้น

๙.๑๐. ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๙.๑๑. ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๑๐. การเข้าถึงเครื่องคอมพิวเตอร์ที่ส่วนงานจัดไว้ใช้งานร่วมกัน

๑๐.๑. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๑๐.๒. ระบบต้องไม่แสดงรายละเอียดสำคัญก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๑๐.๓. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อเมื่อพบว่ามีความพยายามคาดเดารหัสผ่าน

๑๐.๔. ระบบจะต้องจำกัดสิทธิ์ผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

๑๑.การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (application and information access control)

๑๑.๑. การจำกัดการเข้าถึงสารสนเทศ

๑๑.๑.๑. การจำกัดการเข้าถึงของผู้ใช้งาน

(๑) เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

(๓) ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๑๑.๑.๒. แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของมหาวิทยาลัย ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

๑๑.๑.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูล พฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

(๑) ชื่อบัญชีผู้ใช้

(๒) วันเวลาที่เข้าถึงระบบ

(๓) วันเวลาที่ออกจากระบบ

(๔) เหตุการณ์สำคัญที่เกิดขึ้น

(๕) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ

(๘) แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์เป็นต้น

(๙) หมายเลขไอพีแอดเดรสที่เข้าถึง

(๑๐) แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(๑๑) แสดงการหยุดการทำงานของระบบงานที่สำคัญ ๆ

๑๑.๑.๔. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๑๑.๑.๕. การควบคุมผู้รับเหมาช่วง (outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

(๑) มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟท์แวร์ รวมถึงระบบสนับสนุนอื่น ๆ เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่ส่วนงานต้องการ

(๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

(๓) ส่วนงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของส่วนงาน

(๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

(๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๑๑.๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อส่วนงาน จะต้องดำเนินการดังนี้

๑๑.๒.๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ได้แก่ ระบบสารสนเทศบุคลากร ระบบสารสนเทศนิสิต และระบบสารสนเทศทางการเงิน ต้องแยกออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

๑๑.๒.๒. ต้องควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวนโดยเฉพาะ

(๑) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

(๒) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น

(๓) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

(๔) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๑๑.๒.๓. ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

๑๑.๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๑.๓.๑. แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสือสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ

(๑) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่ กรณีที่นำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(๔) ไม่ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

(๕) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ

(๖) ไม่เก็บข้อมูลสำคัญของส่วนงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูลทุกครั้ง

(๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในมหาวิทยาลัย

(๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(๙) มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

๑๑.๓.๒. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึก ข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๑.๔.๑. ผู้ใช้งานงานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๑๑.๔.๒. ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในมหาวิทยาลัย

๑๑.๔.๓. มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๑๑.๔.๔. ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศ ของมหาวิทยาลัยในสถานที่ดังกล่าว

๑๑.๔.๕. ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศของมหาวิทยาลัย จากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม

๑๑.๔.๖. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ของมหาวิทยาลัยที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๒.การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (traffic log management)

๑๒.๑. ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำส่วนงาน และมี Log server ของส่วนงานสำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของมหาวิทยาลัยเมื่อมีการร้องขอ

๑๒.๒. กำหนดวิธีการในการน าส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของส่วนงาน

๑๒.๓. บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้าออกระบบ ซึ่งประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โปรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๒.๔. ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๒.๕. กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่าง ๆ และจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๓.หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (system administrator responsibilities)

๑๓.๑. **ผู้ดูแลระบบ** แบ่งออกเป็น ๓ กลุ่ม

๑๓.๑.๑. ผู้ดูแลระบบเครือข่าย (system administrator)

๑๓.๑.๒. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (network administrator)

๑๓.๑.๓. ผู้ดูแลระบบสารสนเทศ (application administrator)

๑๓.๒. ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๒.๑. ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑๓.๒.๒. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนถูกต้องและความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ได้มีการกำหนดผู้ที่ สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของส่วนงาน หรือบุคคลที่ส่วนงานมอบหมาย

(๒) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๓) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ time.mcu.ac.th

๑๓.๓. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๓.๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของส่วนงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามแนวปฏิบัตินี้ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่ส่วนงานให้ผู้ดูแลระบบพิจารณา ระงับการใช้งานของผู้ใช้งานทันที

๑๓.๓.๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๑๓.๓.๓. ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

๑๓.๓.๔. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๑๓.๓.๕. ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๓.๔. ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๔.๑. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๓.๔.๒. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้น ให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑๓.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

๑๓.๕.๑. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

๑๓.๕.๒. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑๓.๕.๓. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

๑๔.การใช้งานเครือข่ายสังคมออนไลน์ (social network)

๑๔.๑. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๑๔.๒. ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๑๔.๓. ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย

๑๔.๔. หากผู้ใช้งานทราบหรือรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งส่วนเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๕.การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

๑๕.๑. การจัดการบริเวณแวดล้อมทางกายภาพ

๑๕.๑.๑. กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๑๕.๑.๒. กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๑.๓. ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่า ยังใช้งานได้ตามปกติ

๑๕.๒. การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

๑๕.๒.๑. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๒. ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๕.๒.๓. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว

๑๕.๒.๔. ต้องพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องศูนย์กลางข้อมูล (data center)

๑๕.๒.๕. ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการ ตรวจสอบในภายหลังเมื่อมีความจำเป็น

๑๕.๒.๖. มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก

๑๕.๒.๗. ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน และป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

๑๕.๒.๘. ต้องควบคุมส่วนงานภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๙. สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๑๐. เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง/ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอดระยะเวลาการปฏิบัติงาน

๑๕.๒.๑๑. ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๑๒. ต้องทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๕.๓. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๑๕.๓.๑. จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๕.๓.๒. จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๑๕.๓.๓. จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในมหาวิทยาลัย

๑๕.๓.๔. ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน

๑๕.๓.๕. ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

๑๕.๔. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

๑๕.๔.๑. จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๑๕.๔.๒. ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น

๑๕.๔.๓. ควบคุมการเข้าถึงเอกสารที่เกียวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไข เอกสารนั้น

๑๕.๕. การนำทรัพย์สินของมหาวิทยาลัยออกนอกสำนักงาน

๑๕.๕.๑. ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกมหาวิทยาลัย

๑๕.๕.๒. บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกนอกสำนักงาน เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๕.๕.๓. ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยเสมือนเป็นทรัพย์สินของตนเอง

๑๕.๖. ระบบและอุปกรณ์สนับสนุนการทำงาน

๑๕.๖.๑. ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งาน โดยให้มี

(๑) ระบบสำรองกระแสไฟฟ้า

(๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง

(๓) ระบบระบายอากาศ

(๔) ระบบปรับอากาศและควบคุมความชื้น

(๕) ระบบป้องกันอัคคีภัย

๑๕.๖.๒. ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑๕.๖.๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติหรือหยุดทำงาน

๑๕.๖.๔. จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

ส่วนที่ ๒ แนวปฏิบัติการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศส่วนงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. ส่วนเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ของคณะ/ส่วนงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ระบบสำรอง (disaster recovery site: DR site)

๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๑.๒. ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

๑.๒.๑. มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๑.๒.๒. มีระบบไฟฟ้าสำรอง

๑.๒.๓. มีระบบปรับอากาศและความชื้นที่เหมาะสม

๑.๒.๔. มีระบบป้องกันอัคคีภัย

๑.๒.๕. มีระบบส่องสว่างที่เหมาะสม

๑.๒.๖. มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

๑.๒.๗. มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล (Data Backup)

๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของส่วนงานที่จะทาการสำรองข้อมูล และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๒.๓. กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๒.๔. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๒.๕. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

๒.๖. จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

๒.๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๒.๘. มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๘.๑. ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๘.๒. ต้องประเมินความเสี่ยงสำหรบระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

๒.๘.๓. ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๘.๔. ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๘.๕. ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล (Data Recovery)

๓.๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลปฏิบัติอย่างสม่ำเสมอผลของขั้นตอน

๓.๒. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๓.๓. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๓.๔. ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑. ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่าง ๆ ซึ่งทำให้ระบบสารสนเทศของมหาวิทยาลัยหรือของส่วนงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

๑. ส่วนเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. สำนักงานตรวจสอบภายใน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ส่วนงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ

๑.๑. ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของส่วนงานเพื่อการประเมินความเสี่ยงนั้น ดังต่อไปนี้

๒.๑. ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่าน ระบบอินเทอร์เน็ต

๒.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๓. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการ

๒.๔. ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๒.๕. ความเสี่ยงที่เกิดจากการลักลอบใช้บัญชีผู้ใช้และรหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๖. ความเสี่ยงที่เกิดจากความเสียหายทางกายภาพ เช่น ไฟไหม้ น้ำท่วม อุปกรณ์สูญหาย เป็นต้น

๓. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔.๑. ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ

๔.๒. ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๔.๓. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๔.๔. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๕. ต้องแสดงผลการตรวจสอบตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔ แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Guidelines)

วัตถุประสงค์

เพื่อเผยแพร่แนวปฏิบัติให้กับบุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. ส่วนเทคโนโลยีสารสนเทศ
๒. ส่วนงานที่ได้รับมอบหมายในการจัดฝึกอบรม
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย
๔. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวปฏิบัติเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของส่วนงาน
๒. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
๓. จัดฝึกอบรมการใช้งานสารสนเทศของมหาวิทยาลัยอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
๔. จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และเผยแพร่ทางเว็บไซต์ของส่วนงาน
๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์ ฯลฯ
๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้