เอกสารแนบท้ายประกาศมหาวิทยาลัยอุบลราชธานี

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๕

ประกาศ ณ วันที่ ๒๖ ธันวาคม พ.ศ. ๒๕๖๕

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยอุบลราชธานี เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ มหาวิทยาลัยอุบลราชธานีจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

สารบัญ

	หน้า
คำนิยาม	5
ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย	6
ส่วนที่ ๒ การกำหนดหน้าที่ความรับผิดชอบ	7
ส่วนที่ ๓ การควบคุมการเข้าถึง	9
ส่วนที่ ๔ การควบคุมการเข้าถึงระบบเครือข่าย	22
ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ	27
ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ	29
ส่วนที่ ๗ การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์	35
ส่วนที่ ๘ แนวปฏิบัติการใช้งานอินเตอร์เน็ต	36
ส่วนที่ ๙ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์	37
ส่วนที่ ๑๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์	39
ส่วนที่ ๑๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	40
ส่วนที่ ๑๒ ระบบสำรองของสารสนเทศ	42
ภาคผนวก ก แผนเตรียมความพร้อมกรณีฉุกเฉิน	46

๑. วัตถุประสงค์ของการกำหนดนโยบาย

1. เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย
2. เพื่อเป็นกรอบและแนวปฏิบัติในการกำหนดมาตรฐาน ขั้นตอนการปฏิบัติงาน รวมถึงสิ่งอำนวยความสะดวกด้านคอมพิวเตอร์สำหรับการติดตั้งและใช้งานระบบเพื่อการรักษาความมั่นคงปลอดภัยของสารสนเทศ
3. เพื่อให้มหาวิทยาลัยสามารถกำหนดบทบาทความรับผิดชอบของผู้เกี่ยวข้องได้อย่างชัดเจน
4. เพื่อให้มั่นใจว่านักศึกษาและบุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศ โดยทุกคนต้องมีส่วนร่วมรับผิดชอบในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย
5. เพื่อให้มั่นใจว่านักศึกษาและบุคลากรทุกคนได้ตระหนักถึงความสำคัญของการปฏิบัติตามกฎหมายที่เกี่ยวข้องกับคอมพิวเตอร์
6. นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

๒. องค์ประกอบของนโยบาย

คำนิยาม
ส่วนที่ ๑ การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
ส่วนที่ ๒ การกำหนดหน้าที่ความรับผิดชอบ
ส่วนที่ ๓ การควบคุมการเข้าถึง
ส่วนที่ ๔ การควบคุมการเข้าถึงระบบเครือข่าย
ส่วนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ
ส่วนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
ส่วนที่ ๗ การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์
ส่วนที่ ๘ แนวปฏิบัติการใช้งานอินเตอร์เน็ต
ส่วนที่ ๙ แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
ส่วนที่ ๑๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์
ส่วนที่ ๑๑ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
ส่วนที่ ๑๒ ระบบสำรองของสารสนเทศ

คำนิยาม

มหาวิทยาลัย หมายถึง มหาวิทยาลัยอุบลราชธานี

สำนักคอมพิวเตอร์ หมายถึง สำนักคอมพิวเตอร์และเครือข่าย มหาวิทยาลัยอุบลราชธานี

ผู้อำนวยการ หมายถึง ผู้อำนวยการ สำนักคอมพิวเตอร์และเครือข่าย มหาวิทยาลัยอุบลราชธานี

หน่วยงาน หมายถึง คณะ สถาบัน สำนัก ศูนย์ ซึ่งเป็นส่วนงานตามโครงสร้างของมหาวิทยาลัยอุบลราชธานี

ผู้ใช้งาน หมายถึง นักศึกษาหรือบุคลากรของมหาวิทยาลัยอุบลราชธานีที่ได้รับสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย รวมถึงบุคคลจากหน่วยงานภายนอกซึ่งได้รับอนุญาตให้เข้าใช้งานสารสนเทศของมหาวิทยาลัย

สิทธิของผู้ใช้งาน หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

ระบบเครือข่าย หมายถึง ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยอุบลราชธานี ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์และเครือข่าย

สินทรัพย์ หมายถึง เครื่องคอมพิวเตอร์ ระบบเครือข่าย ข้อมูลและระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิด และความน่าเชื่อถือ

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุก หรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัยและ/หรือหน่วยงาน

ผู้ดูแลระบบ หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์หรือระบบเครือข่ายหรือระบบสารสนเทศ

Firewall หมายถึง ระบบรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ ไม่ให้ถูกโจมตีจากผู้ไม่หวังดีหรือการสื่อสารที่ไม่ได้รับอนุญาต ซึ่งส่วนใหญ่จะมาจากระบบเครือข่ายอินเตอร์เน็ต รวมถึงเครือข่าย LAN ด้วย ซึ่งในปัจจุบัน Firewall มีทั้งอุปกรณ์ที่เป็น Hardware และ Software

ส่วนที่ ๑
นโยบายและแนวปฏิบัติการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
(Network System Control Room)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของมหาวิทยาลัย

2. แนวปฏิบัติการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

1. ภายในสำนักคอมพิวเตอร์และเครือข่าย มีการติดตั้งกล้องวงจรปิด เพื่อจุดประสงค์ในการเฝ้าระวังและการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้
2. ผู้ที่เกี่ยวข้อง บทบาทและหน้าที่รับผิดชอบ
   - 2.1. ผู้อำนวยการ
     - 2.1.1.อนุมัติสิทธิเข้าออกพื้นที่ห้องควบคุมระบบเครือข่าย
     - 2.1.2.อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
   - 2.2. ผู้ดูแลห้องควบคุมระบบเครือข่าย
     - 2.2.1.ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด
3. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
   - 3.1. ผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ของมหาวิทยาลัยมีแนวทางปฏิบัติดังนี้
     - 3.1.1.ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะเจ้าหน้าที่ภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้อง และมีการบันทึกทะเบียนผู้มีสิทธิเข้าออกพื้นที่
     - 3.1.2.ต้องจัดทำระบบเก็บบันทึกการเข้าออกห้องควบคุมระบบเครือข่าย
     - 3.1.3.กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องมีเจ้าหน้าที่ผู้ดูแลห้องระบบเครือข่ายควบคุมดูแล

3.2. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ห้องควบคุมระบบเครือข่ายเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ห้องควบคุมระบบ เครือข่าย ปีละ ๒ ครั้ง เป็นอย่างน้อย พร้อมทำรายงานเสนอผู้อำนวยการ

ส่วนที่ ๒
การกำหนดหน้าที่ความรับผิดชอบ

1. วัตถุประสงค์

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2. การกำหนดหน้าที่ความรับผิดชอบ

ระดับนโยบาย

อธิการบดีและผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย ติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ทั้งนี้ให้ผู้บริหารสูงสุดของหน่วยงาน เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ระดับปฏิบัติ

1. รองผู้อำนวยการฝ่ายพัฒนา สำนักคอมพิวเตอร์และเครือข่าย รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบเครือข่าย วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงปลอดภัยของระบบเครือข่าย พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้
   1.1. ควบคุมการเข้า-ออกห้องเซิร์ฟเวอร์ ตามการกำหนดสิทธิการเข้าถึง
   1.2. กำกับดูแล ตรวจสอบและบำรุงรักษาระบบเครือข่ายที่ให้บริการภายในมหาวิทยาลัย
   1.3. กำกับดูแล การติดตั้ง รื้อถอนระบบเครือข่าย ที่ให้บริการภายในมหาวิทยาลัย
   1.4. รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่าย ให้แก่ผู้บังคับบัญชาทราบทุกเดือน
   1.5. กำกับดูแล ติดตามและตรวจสอบการเข้าใช้งานและการเข้าถึงระบบ ตามสิทธิการเข้าถึง
   1.6. กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

1.7. กำกับดูแล ตรวจสอบและบำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และระบบปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเซิร์ฟเวอร์ ของระบบสารสนเทศที่ให้บริการภายในมหาวิทยาลัย

1.8. กำกับดูแล ตรวจสอบการกำหนดแก้ไขหรือเปลี่ยนแปลงเงื่อนไขต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย

1.9. อื่น ๆ ตามที่ได้รับมอบหมาย

2. ผู้ดูแลระบบ มีหน้าที่ความรับผิดชอบดังนี้

2.1. ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

2.2. บริหารจัดการสิทธิการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ไม่ได้รับอนุญาต

2.3. ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

2.4. รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

2.5. แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

2.6. กำหนด แก้ไข หรือเปลี่ยนแปลงเงื่อนไขต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

2.7. รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

2.8. บำรุงรักษาอุปกรณ์เซิร์ฟเวอร์ และอุปกรณ์เครือข่าย (Network) ของระบบสารสนเทศทั้งหมดที่ให้บริการภายในมหาวิทยาลัย ให้สามารถใช้งานได้เป็นปกติ รวมทั้งแก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายภายในมหาวิทยาลัย

ส่วนที่ ๓
นโยบายและแนวปฏิบัติการควบคุมการเข้าถึง
(Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของมหาวิทยาลัย โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ

2. แนวปฏิบัติในการควบคุมการเข้าถึง

2.1. การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

2.1.1. ผู้ดูแลระบบ ต้องจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน ได้แก่ ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น

2.1.2. ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิบุคคลในการเข้า-ออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องเท่านั้น

2.1.3. กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้า-ออกห้องควบคุมระบบเครือข่าย ต้องมีมาตรการการควบคุมอย่างรัดกุม

2.1.4. สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นเข้าใช้งานได้เท่านั้น

2.1.5. ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทุก ๖ เดือนเป็นอย่างน้อย ทั้งนี้ ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.1.6. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบข้อมูลได้

2.1.7. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

2.1.8. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

2.2. แนวปฏิบัติการเข้าถึงระบบเครือข่าย (Network access control)

2.2.1. ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งาน กลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ ได้แก่ โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2.2. การเข้าสู่ระบบเครือข่ายภายในของมหาวิทยาลัยโดยผ่านทางอินเตอร์เน็ต หรืออินทราเน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย ก่อนที่จะสามารถใช้งานได้ ในทุกกรณี

2.2.3. ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

2.2.4. ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

2.2.5. ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่ายเพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่นๆ ได้

2.2.6. ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมี การทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

2.2.7. ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัยควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ Firewall หรือ Hardware อื่นๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

2.2.8. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

2.2.9. การเข้าสู่ระบบงานเครือข่ายภายในมหาวิทยาลัยโดยผ่านทางอินเตอร์เน็ตจำเป็นต้องมีการ Login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

2.2.10. หมายเลขไอพีแอดเดรสภายในของระบบเครือข่ายภายในของมหาวิทยาลัยจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

2.2.11. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบัน อยู่เสมอ

2.2.12. การใช้เครื่องมือต่างๆ (Tools) เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.2.13. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักคอมพิวเตอร์และเครือข่ายเท่านั้น

2.3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

2.3.1. ผู้ดูแลระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นตามหน้าที่งาน หรือตามความจำเป็นขั้นต่ำเท่านั้น

2.3.2. ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

2.3.3. เจ้าของข้อมูล และ เจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยง ในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

2.3.4. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

2.4. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

2.4.1. ผู้ดูแลระบบต้องกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

2.4.2. ผู้ดูแลระบบต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

2.4.3. ผู้ดูแลระบบต้องเปิดให้บริการ (Service) เท่าที่จำเป็นเท่านั้น ได้แก่ บริการ ftp, ssh, ping เป็นต้น

2.4.4. ผู้ดูแลระบบต้องดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ ได้แก่ web server เป็นต้น

2.4.5. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ที่ได้รับมอบหมายเท่านั้น

2.5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

2.5.1. ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

2.5.2. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม

2.5.3. การใช้งานโปรแกรมอรรถประโยชน์ ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

2.5.4. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบปฏิบัติการนั้น (Session time-out)

2.6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

2.6.1. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ของมหาวิทยาลัย ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน ได้แก่ เมื่อเปลี่ยนตำแหน่งงานภายในมหาวิทยาลัย ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน หมดวาระ เกษียณอายุราชการ เป็นต้น

2.6.2. ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.6.3. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน

2.6.3.1. กำหนดเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

2.6.3.2. กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.6.4. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.6.5. การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงของผู้ใช้งานสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น

2.6.6. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ

2.6.7. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสาร

2.6.8. การควบคุมการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking) ต้องกำหนดข้อปฏิบัติและมาตรการ เพื่อปรับใช้สำหรับการปฏิบัติงานของมหาวิทยาลัยจากภายนอก

2.6.9. การจำกัดระยะเวลาการเชื่อมต่อระบบ(limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

3. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

3.1. การลงทะเบียนเจ้าหน้าที่ใหม่ของมหาวิทยาลัย

3.1.1. จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

3.1.2. ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิจากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศ และบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิจากผู้บริหารอย่างชัดเจน

3.1.3. ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

3.1.4. ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัย

3.1.5. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

3.1.6. การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

3.1.7. การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

3.1.8. เจ้าหน้าที่ใหม่ของมหาวิทยาลัยกรอกข้อมูลคำขอใช้บริการลงแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

3.1.9. ยื่นคำขอกับเจ้าหน้าที่ของสำนักคอมพิวเตอร์และเครือข่ายที่ได้รับมอบหมาย เพื่อขออนุมัติจากผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย

3.1.10. ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

3.2. การบริหารจัดการสิทธิผู้ใช้งาน (User Management)

3.2.1. ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิอนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

3.2.2. ผู้ดูแลระบบต้องตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

3.2.3. ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้ โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.2.4. ผู้ดูแลระบบต้องกำหนดระดับสิทธิในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

3.2.5. ผู้ดูแลระบบต้องมอบหมายสิทธิ ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

3.2.6. ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิให้แก่ผู้ใช้งาน

3.2.7. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิพิเศษที่ได้รับด้วยว่าการเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.2.8. ผู้ใช้บริการต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

3.2.9. การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ

3.2.9.1. หัวหน้างานหรือผู้บังคับบัญชา กรอกข้อมูลลงในแบบฟอร์ม และ ยื่นคำขอกับผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย

3.2.9.2. ผู้ดูแลระบบยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์มและลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

3.2.9.3. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะที่เกี่ยวกับการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.3. การบริหารจัดการรหัสผ่าน (Password Management)

3.3.1. ระบบบริหารจัดการรหัสผ่าน ต้องให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและเป็นความรับผิดชอบของแต่ละคนได้

3.3.2. ระบบบริหารจัดการรหัสผ่าน ต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง และมีขั้นตอนปฏิบัติเพื่อยืนยันรหัสผ่านใหม่ที่ตั้ง

3.3.3. ระบบบริหารจัดการรหัสผ่าน ต้องให้ผู้ใช้งานตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น โดยกำหนดให้รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัว ประกอบด้วย ตัวเลข ตัวอักษรตัวพิมพ์เล็กและตัวพิมพ์ใหญ่อย่างน้อย ๑ ตัว

3.3.4. ระบบบริหารจัดการรหัสผ่าน ต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ ทุกๆ ๖ เดือน

3.3.5. ระบบบริหารจัดการรหัสผ่าน ต้องให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งาน และทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

3.3.6. ระบบบริหารจัดการรหัสผ่าน ต้องสามารถระบุข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งานได้

3.3.7. ระบบบริหารจัดการรหัสผ่าน ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน โดยต้องให้แสดงเป็นเครื่องหมายจุด หรือดอกจัน หรือสัญลักษณ์อื่นๆ บนหน้าจอ

3.3.8. ระบบบริหารจัดการรหัสผ่าน ต้องมีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้วเพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ภายในระยะเวลา 6 เดือน

3.3.9. การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

3.3.10. ระบบบริหารจัดการรหัสผ่าน ต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้และ/หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต จากการเข้ารหัสลับข้อมูลการคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

3.4. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

3.4.1. ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

3.4.2. ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ต้องเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

3.4.3. ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

3.4.4. ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับและไม่มอบให้ผู้อื่นนำไปใช้งาน

3.4.5. กำหนดให้รหัสผ่านต้องมีไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็กและตัวเลขเข้าด้วยกัน)

3.4.6. ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน ได้แก่ “abcdef” “aaaaaa” “๑๒๓๔๕”

3.4.7. ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน ได้แก่ ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

3.4.8. ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

3.4.9. กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน ๔ ครั้ง

3.4.10. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ

3.4.11. ไม่จดหรือบันทึกรหัสผ่านไว้ในที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

3.4.12. ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log out) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศที่ตนเองลงชื่อเข้าใช้ไว้ และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

3.4.13. เมื่อผู้ใช้งานมีปัญหาในการลืมชื่อผู้ใช้งานและรหัสผ่าน ให้ติดต่อผู้ดูแลระบบเพื่อดำเนินการรีเซ็ตชื่อผู้ใช้งานหรือรหัสผ่าน

3.4.14. การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยใส่ซองปิดผนึกและประทับตรา “ลับ”

3.5. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of user access right)

3.5.1. สิทธิการเข้าถึงข้อมูลของผู้ใช้ต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอ ตามช่วงระยะเวลาที่กำหนด ทุกๆ ๖ เดือน และทุกครั้งที่มีการปรับเปลี่ยน การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง

3.5.2. สิทธิการเข้าถึงข้อมูลต้องได้รับการทบทวนและจัดสรรใหม่ เมื่อมีการโยกย้ายเจ้าหน้าภายในคณะ/สำนัก/หน่วยงาน/มหาวิทยาลัย

3.5.3. การให้สิทธิการเข้าถึงพิเศษ ต้องมีการทบทวนอย่างน้อย ทุก ๓ เดือน

3.5.4. การจัดสรรสิทธิพิเศษต้องได้รับการตรวจสอบอย่างสม่ำเสมอ ตามช่วงระยะเวลาที่กำหนดเพื่อให้มั่นใจได้ว่า ไม่มีการให้สิทธิพิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

3.5.5. การเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิพิเศษต้องถูกบันทึกเพื่อการทบทวน

3.6. การใช้งานรหัสผ่าน (Password Use)

3.6.1. ผู้ใช้งานต้องเก็บรหัสผ่านไว้เป็นความลับ

3.6.2. ผู้ใช้งานต้องเปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

3.6.3. ผู้ใช้งานต้องจัดเก็บรหัสผ่านไว้ในสถานที่ที่ปลอดภัย โดยหลีกเลี่ยงการบันทึกรหัสผ่านลงในกระดาษ ในแฟ้มข้อมูลหรือในอุปกรณ์พกพาต่างๆ

3.6.4. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมอ อย่างน้อยทุกๆ ๖ เดือน

3.6.5. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

3.6.6. ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวอย่างน้อย ๘ ตัวอักษร

3.6.7. ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

3.6.8. ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว เกินกว่า 2 ครั้งติดต่อกัน

3.6.9. ผู้ใช้งานไม่ควรกำหนดให้มีการบันทึกรหัสผ่านอัตโนมัติ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง

3.6.10. ผู้ใช้งานต้องไม่ใช้รหัสผ่านร่วมกับผู้อื่น

3.6.11. ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบต่างๆ ที่ใช้งาน

3.7. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

3.7.1. ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศ ระบบงานเครื่องคอมพิวเตอร์แม่ข่าย หรือเครื่องคอมพิวเตอร์ส่วนบุคคลโดยทันทีเมื่อเสร็จสิ้นการใช้งาน

3.7.2. ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานระบบหรือเครื่องคอมพิวเตอร์ที่รับผิดชอบ

3.7.3. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง

3.7.4. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอเมื่อไม่มีการใช้งานเกินกว่า ๑๕ นาที และกำหนดให้ผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

3.7.5. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

3.7.6. ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.7.7. ผู้ใช้งานต้องจัดเก็บอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่มีผู้ดูแล

3.8. มาตรการการทำลายข้อมูลและสื่อบันทึกข้อมูลอิเล็กทรอนิกส์

3.8.1. ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

3.8.2. ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการทำลายหรือจำหน่าย

3.8.3. ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจานวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่มีความลับระดับต่ำ หรือแบบเขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน DoD ๕๒๒๐.๒๒- M สำหรับข้อมูลที่มีความลับระดับปานกลาง หรือแบบเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

3.8.4. ต้องลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ ๕ ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

3.8.5. ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

3.8.6. มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ มีวิธีการดังนี้

3.8.6.1. ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการเปลี่ยน หรือ ทดแทนอุปกรณ์

3.8.6.2. ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลายหรือจำหน่าย

3.8.6.3. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลายแผ่น CD/DVD

3.8.6.4. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DDS, DAT, LTO ต้องทำการลบ ข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป

3.8.6.5. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices แบบ USB, Flash drive, SD cards ให้ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหมสหรัฐอเมริกา ว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้

3.8.6.6. ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php

3.8.6.7. ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php

3.9. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

3.9.1. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานระยะเวลาในการเข้าถึง ช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

3.9.1.1. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน

3.9.1.2. ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

3.9.1.3. ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

3.9.2. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล ได้แก่ TLS VPN หรือ XML Encryption เป็นต้น

3.9.3. ต้องกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

3.9.4. ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน ได้แก่ การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

3.9.5. ผู้ใช้สามารถนำการเข้ารหัสลับมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ มีแนวปฏิบัติ ดังนี้

3.9.5.1. การประเมินความเสี่ยงเพื่อระบุระดับความสำคัญ และระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน

3.9.5.2. กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูลโดยใช้การเข้ารหัสลับข้อมูล

3.9.5.3. การจัดการ username และ password จะต้องทำการเข้ารหัสลับของข้อมูลเมื่อมีการรับหรือส่งข้อมูลระหว่างเครือข่าย (data-in-transit encryption) ได้แก่ โพรโทคอล TLS และมีการเข้ารหัสลับของข้อมูลที่จัดเก็บ (data-at rest encryption) ได้แก่ AES ใน field ของ password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

3.9.5.4. ต้องมีการเชื่อมต่อโดยการเข้ารหัสลับ TLS ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application เพื่อเป็นการเข้ารหัสลับข้อมูลที่ส่งระหว่างบราว์เซอร์และเว็บเซิร์ฟเวอร์

3.9.5.5. กำหนดช่องทางการรับ–ส่งข้อมูลสำคัญ หรือข้อมูลลับที่เหมาะสมกับมหาวิทยาลัย สำหรับช่องทาง ดังต่อไปนี้

-ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต

-เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย

-สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

3.9.5.6. ห้ามแชร์ไฟล์ข้อมูลลับบนเครือข่ายของมหาวิทยาลัยเพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

3.9.5.7. ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูล ว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

3.9.5.8. ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน ว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

3.9.5.9. ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

3.10. การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล แฟ้มข้อมูล เครื่องคอมพิวเตอร์ อุปกรณ์ต่อพ่วง ระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อกาเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน มีแนวทางปฏิบัติดังนี้

3.10.1. ผู้ใช้งานต้องป้องกันทรัพย์สินของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่างๆ ประกอบด้วย

3.10.1.1. การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)

3.10.1.2. การควบคุมการเข้า – ออกพื้นที่ (Physical Entry control)

3.10.1.3. การจัดบริเวณสำหรับการเข้าถึง และส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and loading area)

3.10.1.4. การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)

3.10.1.5. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

3.10.2. การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

3.10.2.1. แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

3.10.2.2. กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ

3.10.2.3. วัฒนธรรมองค์กร

3.10.3. ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของมหาวิทยาลัย ก่อนเข้าใช้งานโดยใช้วิธีการพิสูจน์ตัวตนที่เหมาะสม

3.10.4. ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

3.10.4.1. ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย

3.10.4.2. จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับ หรือสื่อบันทึกข้อมูลไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ

3.10.4.3. ลงชื่อออกจากเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

3.10.4.4. ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือส่งข้อมูลสำคัญ เมื่อไม่มีผู้ใช้งาน

3.10.4.5. ป้องกันตู้ หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

3.10.4.6. ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

3.10.4.7. นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

3.10.5. ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่างๆ ได้แก่ เอกสาร สื่อบันทึกคอมพิวเตอร์ หรือสารสนเทศออกจากคณะ/หน่วยงาน/มหาวิทยาลัย ต้องขออนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

3.10.6. ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

3.10.7. ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของมหาวิทยาลัย เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย

3.10.8. ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่าย ในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

3.10.9. มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ มีวิธีการดังนี้

3.10.9.1. ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการเปลี่ยน หรือ ทดแทนอุปกรณ์

3.10.9.2. ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูล ก่อนทำการทำลาย หรือจำหน่าย

3.10.9.3. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลายแผ่น CD/DVD

3.10.9.4. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DDS, DAT, LTO ต้องทำการลบ ข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป

3.10.9.5. ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices แบบ USB, Flash drive, SD cards ให้ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหมสหรัฐอเมริกา ว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้

3.10.9.6. ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php

3.10.9.7. ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php

3.11. แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

3.11.1. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ทุกครั้ง

3.11.2. ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน (password)

3.11.3. ผู้ใช้งานที่ทำการเชื่อมต่อจากภายนอกมหาวิทยาลัยต้องทำการเข้ารหัสลับข้อมูลในการเข้าถึงระบบพิสูจน์ตัวตนจากระยะไกลผ่านระบบ VPN (Virtual Private Network) ของมหาวิทยาลัย

3.11.4. การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

3.12. การควบคุมการเข้าใช้งานระบบเครือข่ายจากภายนอก

3.12.1. การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ผู้ดูแลระบบต้องกำหนดมาตรการการรักษาความปลอดภัยที่สูงขึ้นกว่ามาตรฐานการเข้าสู่ระบบจากภายใน

3.12.2. ก่อนทำการให้สิทธิในการเข้าสู่ระบบเครือข่ายจากระยะไกลของบุคคลภายนอก ต้องให้หน่วยงานที่เกี่ยวข้องแสดงหลักฐานระบุเหตุผลและความจำเป็นในการดำเนินงานกับมหาวิทยาลัย และต้องได้รับอนุมัติจากผู้บังคับบัญชา

3.12.3. ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

3.12.4. การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และตัดการเชื่อมต่อเมื่อไม่ได้มีการใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

3.12.5. การพิสูจน์ตัวตนสำหรับผู้ใช้งานจากภายนอก ต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน ได้แก่ รหัสผ่าน เป็นต้น

4. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลแต่ละประเภท ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบเครือข่าย ตามประเภทของข้อมูล ความสำคัญของข้อมูล ความลับของข้อมูลและลำดับชั้นการเข้าถึงของข้อมูล โดยการเข้าถึงนั้นจะต้องเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น

การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ซึ่งระเบียบดังกล่าว เป็นมาตรการที่ละเอียดรอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม

4.1. ต้องมีการกำหนดประเภทของข้อมูล ซึ่งมีการจัดแบ่งไว้เป็น ๒ ประเภท คือ

4.1.1. ข้อมูลที่เปิดเผยได้ทั่วไป

4.1.2. ข้อมูลที่เปิดเผยเฉพาะ ที่มีการจำกัดการเข้าถึง ประกอบด้วย

4.1.2.1. ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลการเงินงบประมาณและบัญชี เป็นต้น

4.1.2.2. ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

4.2. ต้องมีการจัดลำดับความสำคัญของข้อมูล โดยแบ่งออกเป็น ๓ ลำดับ คือ

4.2.1. ข้อมูลที่มีระดับความสำคัญมาก ตามพันธกิจหลักของมหาวิทยาลัย ได้แก่ ข้อมูลนักศึกษาข้อมูลบุคลากร ข้อมูลการเงิน ข้อมูลวิจัย

4.2.2. ข้อมูลที่มีระดับความสำคัญปานกลาง ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ โครงการ/กิจกรรม อาคารสถานที่ หนังสือราชการ

4.2.3. ข้อมูลที่มีระดับความสำคัญน้อย ได้แก่ ข้อมูลทั่วไป ข่าวสาร ประกาศข้อบังคับ

4.3. **ต้องมีการจัดลำดับชั้นความลับ โดยแบ่งออกเป็น ๔ ลำดับ คือ**

4.3.1. ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด กระทบต่อชื่อเสียง ภาพลักษณ์และความน่าเชื่อถือของมหาวิทยาลัย

4.3.2. ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

4.3.3. ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

4.3.4. ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

4.4. ต้องมีการกำหนดระดับชั้นการเข้าถึง โดยมีการกำหนดชื่อผู้ใช้งานและรหัสผ่านเพื่อใช้ในการยืนยันตัวตนของผู้ใช้ข้อมูลในแต่ละชั้นการเข้าถึง โดยแบ่งระดับชั้นออกเป็น ๒ ระดับ คือ

4.4.1. ประเภทของข้อมูลทั่วไป กำหนดสิทธิให้ทุกคนสามารถเข้าถึงข้อมูลได้

4.4.2. ประเภทของข้อมูลที่ต้องกำหนดสิทธิการเข้าถึง มีระดับการเข้าถึง ดังนี้

4.4.2.1. ระดับผู้ปฏิบัติงาน คือ ผู้ที่สามารถเข้าถึงข้อมูลตามหน้าที่ที่ได้รับมอบหมาย

4.4.2.2. ระดับผู้บริหาร คือ ผู้ที่สามารถเข้าถึงข้อมูลตามพันธกิจของมหาวิทยาลัยตามที่ได้รับมอบหมาย

4.4.2.3. ระดับผู้ดูแลระบบ คือ ผู้ที่สามารถเข้าถึงและดูแลระบบตามหน้าที่ที่ได้รับมอบหมาย

4.5. ต้องกำหนดระยะเวลาในการเข้าถึง และวิธีการในการระงับการใช้งานเมื่อพ้นระยะเวลาดังกล่าว ดังนี้

4.5.1. ระบบงานบริการ (Front Office) สำหรับผู้ใช้งานทั่วไป สามารถเข้าถึงระบบได้ตามช่วงเวลา ดังต่อไปนี้

4.5.1.1. ในเวลาราชการ (๐๘.๓๐ น. – ๑๖.๓๐ น.)

4.5.1.2. นอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.)

4.5.1.3. ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

4.5.2. ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในมหาวิทยาลัย สามารถเข้าถึงระบบได้ตามช่วงเวลา ดังต่อไปนี้

4.5.2.1. ในเวลาราชการ (๐๘.๓๐ น. – ๑๖.๓๐ น.)

4.5.2.2. นอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.)

4.5.2.3. ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

4.6. ต้องกำหนดช่องทางในการเข้าถึงข้อมูลในแต่ละประเภท ว่ามีการเข้าถึงได้โดยตรงหรือการเข้าถึงผ่านระบบงาน ดังนี้

4.6.1. ผู้ใช้งานเข้าใช้บริการผ่านระบบเครือข่ายภายในมหาวิทยาลัย ได้ตลอด ๒๔ ชั่วโมง

4.6.2. ผู้ใช้งานเข้าใช้ผ่านระบบเครือข่ายจากภายนอกมหาวิทยาลัย สามารถเข้าใช้บริการ ผ่านระบบ VPN ได้ตลอด ๒๔ ชั่วโมง

4.7. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

4.7.1. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

4.7.2. จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย/คณะ/หน่วยงาน หรือในระบบ DMS ของมหาวิทยาลัย

4.7.3. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

4.7.4. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้

เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

4.7.5. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนาไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

4.7.6. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

4.8. ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) ดังนี้

4.8.1. การควบคุมการเข้าถึงสารสนเทศตามภารกิจ มหาวิทยาลัยอุบลราชธานี จัดให้มีการบริการสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใช้ประโยชน์ตามภารกิจของมหาวิทยาลัย ได้แก่ การเรียนการสอน การวิจัย การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม และการบริหารจัดการ ทั้งนี้การใช้งานตามภารกิจ ต้องอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่น เคารพและปฏิบัติให้ถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใดๆ โดยกำหนดสิทธิการเข้าถึง จะแบ่งตามลำดับชั้นการบริหารจัดการ ดังนี้

4.8.1.1. ผู้บริหารระดับสูง ได้แก่ อธิการบดี รองอธิการบดี สามารถเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายให้กำกับดูแล

4.8.1.2. ผู้บริหารระดับหน่วยงาน/หลักสูตร ได้แก่ ผู้อำนวยการ คณบดี ประธานหลักสูตร สามารถเข้าถึงข้อมูลภายใต้ความรับผิดชอบดูแล

4.8.1.3. ผู้ปฏิบัติงาน สามารถเข้าถึงได้เฉพาะส่วนงานที่ตนเองได้รับมอบหมาย

4.8.2. การอนุญาตและการทบทวนสิทธิการเข้าถึงตามภารกิจ

4.8.2.1. ผู้ใช้งานจะต้องได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลและผู้ดูแลระบบตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

4.8.2.2. เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะส่วนที่จำเป็นตามหน้าที่งานที่ได้รับมอบหมายเท่านั้น

4.8.2.3. ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ ผู้ใช้งาน ซึ่งต้องมีการจัดทำเอกสารขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนาม อนุมัติ

4.8.2.4. กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจให้เป็นไปตามแนวปฏิบัติการบริหารจัดการการ เข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

4.8.3. ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิสำหรับผู้ใช้งาน

4.8.3.1. ตำแหน่ง / ตำแหน่งทางการบริหาร

4.8.3.2. หน่วยงานต้นสังกัด

4.8.3.3. คำสั่งมอบหมายงานและหน้าที่รับผิดชอบ

4.8.3.4. สำเนาสัญญาจ้าง (สำหรับบุคลากรจ้างเหมา)

4.8.3.5. วันที่เริ่มต้น-สิ้นสุดสัญญา

4.8.3.6. ลายเซ็นอนุมัติจากหัวหน้างาน

ส่วนที่ ๔
การควบคุมการเข้าถึงระบบเครือข่าย
(Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย โดยการกำหนดสิทธิของผู้ใช้งานในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่าย

2. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

1. ผู้ดูแลระบบ ต้องมีการออกแบบการเข้าถึงระบบเครือข่ายตามกลุ่มผู้ใช้งาน เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ
2. การเข้าสู่ระบบเครือข่ายภายในของมหาวิทยาลัย จะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการก่อน จึงจะสามารถใช้งานได้
3. ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น
4. ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงเงื่อนไขการกำหนดค่าต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องมีการทบทวนการกำหนดเงื่อนไขต่าง ๆ อย่างน้อยปีละครั้ง และต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง
5. ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัยต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering ได้แก่ การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ
6. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย
7. ต้องมีระบบที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันตัวตน
8. การเข้าสู่ระบบเครือข่ายภายในมหาวิทยาลัย โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องทุกครั้ง

9. IP address ของระบบเครือข่ายภายในของมหาวิทยาลัย จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้
10. ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
11. การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักคอมพิวเตอร์และเครือข่าย หรือผู้ที่ได้รับมอบหมายเท่านั้น
12. ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือกระทำการใด ๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความความเสียหายแก่ระบบเครือข่ายหลักของมหาวิทยาลัย
13. ในกรณีที่ ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของมหาวิทยาลัย อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน
14. ห้ามทำการวางสายเครือข่ายที่เชื่อมต่อกับเครือข่ายหลักของมหาวิทยาลัยโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สาย (Wireless Network) ด้วย
15. ต้องมีการควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

3. การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

3.1. ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการรายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

3.2. กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

3.3. อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.4. ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

4. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

4.1. บุคคลภายนอกที่เข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออก” ให้ถูกต้องและต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

4.2. บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับชั้น

4.3. ผู้ดูแลระบบต้องกำหนดการเปิด–ปิด พอร์ตของอุปกรณ์เครือข่ายเพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์

4.4. ต้องยกเลิกหรือปิดพอร์ต และบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

4.5. ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งทางกายภาพ และทางระบบเครือข่าย

4.6. ทำการล็อคอุปกรณ์เครือข่ายที่ใช้สำหรับการปรับแต่งค่าคอนฟิกกูเรชันด้วยกุญแจเพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

4.7. ตรวจสอบพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยทุกๆ ๓ เดือน

5. การแบ่งแยกเครือข่าย (segregation in networks)

5.1. มหาวิทยาลัยแบ่งแยกเครือข่ายเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ เพื่อควบคุมการเข้าถึงเครือข่ายโดยไม่ได้รับอนุญาต

5.2. มหาวิทยาลัยจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ โดยคณะ/หน่วยงานของมหาวิทยาลัยสามารถใช้งานระบบผ่านระบบเครือข่ายภายในได้ แต่ไม่สามารถใช้งานระบบผ่านเครือข่ายภายนอกได้เพื่อความปลอดภัยของฐานข้อมูล

5.3. มหาวิทยาลัยทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการ ผู้ใช้งาน และระบบงานต่างๆ ของมหาวิทยาลัย

5.4. ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวงเครือข่ายหนึ่งได้โดยตรง

5.5. ต้องควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบนเครือข่าย หรืออื่นๆ โดยไม่ได้รับอนุญาต

5.6. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

5.7. ต้องกรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

5.8. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอกมหาวิทยาลัย

5.9. ต้องแยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของมหาวิทยาลัย

5.10. ต้องมีการแยกกลุ่มเครือข่ายเป็น ๔ ประเภทใหญ่ๆ คือ

5.10.1. ระบบเครือข่ายภายใน

5.10.2. ระบบเครือข่ายภายนอก

5.10.3. ส่วนที่มีความสำคัญสูง (DMZ Zone) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

5.10.4. เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่างๆ ของมหาวิทยาลัย

5.11. มีการจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยต้องมีการปรับปรุงให้เป็นปัจจุบันหรืออย่างน้อยปีละครั้ง

6. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

6.1. ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกหน่วยงาน ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering ได้แก่ การใช้ IPS, Firewall, Proxy และ Mail Gateway

6.2. ติดตั้งระบบตรวจจับและป้องกันการบุกรุก (IDS/IPS) สำหรับตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติผ่านเครือข่ายหรือมีการแก้ไข เปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

6.3. การเชื่อมต่อเข้าสู่ระบบเครือข่ายของมหาวิทยาลัย ผู้ใช้งานต้องมีการ Login ด้วย Username และ Password และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

6.4. ในกรณีที่ผู้ดูแลระบบตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติ ต่อระบบเครือข่ายหลักของมหาวิทยาลัย จะทำการหยุดให้บริการโดยการตัดการเชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

6.5. จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับ ขอบเขต (Zone) ของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

6.6. ให้ผู้ดูแลระบบใช้เครื่องมือ (Tool) ได้แก่ Cacti Monitoring หรือ Dashboard IAM เพื่อทำการตรวจสอบการเชื่อมต่อระบบเครือข่าย

6.7. กำหนดให้มีการบันทึกการทำงานของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เพื่อประโยชน์ในการตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน

6.8. มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานและรายงานต่อผู้บังคับบัญชาอย่างสม่ำเสมอ

7. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing control)

ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ ใช้งานตามภารกิจ ดังนี้

7.1. ผู้ดูแลระบบต้องดำเนินการกำหนดตารางการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์ค้นหาเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมการใช้งานเฉพาะเส้นทางที่ ได้รับอนุญาตเท่านั้น

7.2. ผู้ดูแลระบบต้องจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ของผู้ใช้งานไปยังอุปกรณ์เครือข่ายที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ให้กำหนดเฉพาะชุด IP Address ของผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงได้

7.3. ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด ตั้งค่า แก้ไข หรือเปลี่ยนแปลงค่าตัวแปร (Parameter) ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่าตัวแปร (Parameter) ต่างๆ อย่างน้อยปีละ ๑ ครั้ง

7.4. ข้อมูลหมายเลขไอพี (IP Address) ภายใน (Local) ของระบบงานเครือข่ายภายในมหาวิทยาลัย ต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

7.5. ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาติ ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network)

7.6. ต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขไอพี (IP Address)

7.7. ต้องกำหนดให้มีการแยกวงหมายเลขไอพี เพื่อแยกเครือข่ายย่อย

7.8. ต้องกำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมเครือข่ายปลายทางผ่านทางที่กำหนดไว้เท่านั้น หรือจำกัดสิทธิในการใช้บริการเครือข่าย

7.9. ต้องมีการใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบ IP Address ของทั้งต้นทางและปลายทาง และควบคุมการไหลของข้อมูลผ่านเครือข่ายต่างๆ จากเครือข่ายหนึ่งไปยังอีกเครือข่ายหนึ่ง

7.10. ต้องมีการกำหนดให้มีการแปลงหมายเลขไอพี เพื่อแยกเครือข่ายภายในและภายนอกมหาวิทยาลัย

7.11. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

ส่วนที่ ๕
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของมหาวิทยาลัยให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

2.1. ผู้ใช้งานต้องใช้รหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

2.2. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานนานกว่า 15 นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

2.3. ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง

2.4. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

2.5. ผู้ใช้งานต้องทำการลงชื่อออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานเกินกว่า 15 นาที

2.6. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

2.7. ซอฟต์แวร์ลิขสิทธิของมหาวิทยาลัย ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบถือว่าเป็นความผิด ส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

2.8. ซอฟต์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้งถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

2.9. ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัยเพื่อประโยชน์ทางการค้า

2.10. ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม ในการสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

2.11. ห้ามผู้ใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาต

3. แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

3.1. ต้องตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกันระหว่างบัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบ บัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนาระบบบัญชีของเจ้าหน้าที่ทางเทคนิคอื่นๆ

3.2. ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

3.3. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนใช้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

3.4. ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูง ต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูงโดยใช้วิธีการเข้ารหัสลับข้อมูล วิธีการทางชีวภาพโดยใช้การแสกนลายนิ้วมือ เรตินา ฝ่ามือ เสียง

3.5. ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิการเข้าถึงระบบปฏิบัติการจากผู้บังคับบัญชาของหน่วยงานหรือเจ้าของระบบงานเท่านั้น

3.6. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้น เกิดจากการกระทำของผู้อื่น

3.7. ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น

3.8. ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

4. แนวปฏิบัติการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System Utilities)

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว โดยมีแนวทางปฏิบัติ ดังนี้

4.1. ต้องจัดทำบัญชีรายชื่อโปรแกรมลิขสิทธิประเภทยูทิลิตี้ที่อนุญาตให้ใช้งานได้เท่านั้น

4.2. ต้องจำกัดผู้ที่สามารถใช้งานโปรแกรมยูทิลิตี้ และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้

4.3. ผู้ใช้งานต้องใช้งานโปรแกรมยูทิลิตี้ที่เป็นลิขสิทธิของมหาวิทยาลัยเท่านั้น และต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องมีการลงนามเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร หากผู้ใช้งานทำการติดตั้งหรือใช้งานโปรแกรมละเมิดลิขสิทธิ จะถือเป็นความรับผิดชอบของผู้ใช้งานรายนั้นเอง

4.4. การใช้งานโปรแกรมยูทิลิตี้ จะต้องได้รับอนุญาตให้ใช้งานตามระดับสิทธิในการใช้งานที่มหาวิทยาลัยกำหนดไว้แล้วโดยจะได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้เป็นรายครั้งไป

4.5. ต้องทำการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ทุกครั้ง แม้จะเป็นการใช้งานเพียงชั่วคราว

4.6. ต้องแยกจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน โดยแยกไว้ในไดเร็คทอรี่ต่างหากเพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

4.7. ต้องบันทึกข้อมูลล็อกแสดงการใช้งานโปรแกรมยูทิลิตี้

4.8. ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้ที่ไม่มีความจำเป็นในการใช้งานแล้ว

4.9. ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

4.10. ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ ระดับสิทธิของผู้ขออนุมัติ และการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

4.11. ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

4.12. มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

4.13. ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

5. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

5.1. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งาน หลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาเกินกว่า ๑๕ นาที

5.2. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการพักหรือปิดหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลาเกินกว่า ๑๕ นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

5.3. ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้น ๕ นาที สำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ทางด้านระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

5.4. กำหนดให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย สำหรับระบบที่มีความสำคัญสูง จะต้องมีการตัดและหมดเวลาการใช้งาน โดยมีกำหนดให้ไม่เกิน ๑๐ นาทีต่อการพิสูจน์ตัวตนเข้าใช้งาน

5.5. ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้ง หลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

6. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

6.1. ระบบเทคโนโลยีสารสนเทศต้องมีการจำกัดระยะเวลาการเชื่อมต่อ สำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ ๑ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงาน ของสำนักงานตามปกติเท่านั้น

6.2. ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่สาธารณะ หรือพื้นที่ภายนอกมหาวิทยาลัยที่มีความเสี่ยงต้องมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ โดยกำหนดให้ใช้งานได้ ๓๐ นาทีต่อการเชื่อมต่อหนึ่งครั้ง

6.3. ระบบเทคโนโลยีสารสนเทศต้องมีการจำกัดช่วงระยะเวลาการใช้งาน ต้องมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ ทุกๆ ๑ ชั่วโมง

ส่วนที่ ๖
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
(Application and Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ ของมหาวิทยาลัย โดยการกำหนดสิทธิของผู้ใช้งานระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้งานระบบต้องผ่านการอนุญาตและกำหนดสิทธิการเข้าใช้งานจากผู้ดูแลระบบ

2. แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

2.1. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนเจ้าหน้าที่ใหม่ของมหาวิทยาลัย ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน ได้แก่ การลาออกหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน

2.2. ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเตอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.3. ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้

2.3.1. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

2.3.2. ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

2.3.3. กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

2.3.4. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

2.3.5. กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

2.3.6. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.4. เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ มหาวิทยาลัยควรกำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่มหาวิทยาลัยพัฒนาในรูปแบบของ Web Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายในเท่านั้น

2.5. เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงานเพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

2.6. ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติดังนี้

2.6.1. ผู้ดูแลระบบต้องป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วง โดยไม่ได้รับอนุญาต

2.6.2. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ระยะเวลาในการใช้บริการ

2.6.3. ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

2.6.4. เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการประกอบ ด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2.6.5. เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับสำหรับข้อมูลสำคัญ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

2.6.5.1. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2.6.5.2. ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

2.6.5.3. ต้องกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

2.6.5.4. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล

2.6.5.5. ต้องเปลี่ยนรหัสผ่านของระบบที่มีลำดับความสำคัญตามระยะเวลาที่กำหนด

2.7. ต้องมีการใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

2.8. ต้องมีการลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัด หรือให้สิทธิการเข้าถึงข้อมูลและฟังก์ชันต่างๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

2.9. ต้องมีการควบคุมหรือจำกัดสิทธิการเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง โดยควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่างๆ ที่จำเป็นต้องใช้งานเท่านั้น

2.10. ต้องมีการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น

2.11. ต้องมีการแสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

2.12. ต้องมีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อกอินเสร็จแล้ว

2.13. ต้องมีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิเข้าถึงระบบงาน

2.14. ต้องมีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใดๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ

2.15. ต้องมีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งาน ในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน

2.16. ต้องมีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด

2.17. ต้องมีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

2.18. ต้องมีการบันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

3. แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน (Sensitive System isolation)

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ได้แก่ ระบบ MIS ระบบบริการการศึกษา ระบบทะเบียน ระบบ UBU-FMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่ายและการบริหารทรัพยากร ดูแลรับผิดชอบโดยกรมบัญชีกลางจะต้องดำเนินการดังนี้

3.1. ต้องมีการระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อมหาวิทยาลัย

3.2. ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบงานอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย หรือแยกเครือข่ายโดยใช้วิธีการทางเทคนิค VLAN

3.3. ต้องทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์แม่ข่ายเครื่องหนึ่งต่างหาก

3.4. ต้องมีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า

3.5. ต้องมีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

3.6. ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

3.7. ต้องทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ในFirewall

4. แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติดังนี้

4.1. มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ของมหาวิทยาลัยที่จำเป็นต้องปฏิบัติงานของมหาวิทยาลัยจากภายนอก หรือจากระยะไกล

4.2. มีขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกลการกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

4.3. ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการและต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

4.4. ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

4.5. มีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

4.5.1. ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล

4.5.2. ระบบงานหรือบริการต่างๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล

4.5.3. ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน

4.5.4. ชั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

4.6. มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกลเพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

4.7. มีการป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลกับระบบงานต่างๆ ภายในมหาวิทยาลัย

4.8. มีการกำหนดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันระหว่างมหาวิทยาลัยกับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

4.9. มีการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล รวมทั้งมาตรการควบคุมการใช้บริการเครือข่ายไร้สายจากที่บ้าน ทั้งนี้เพื่อป้องกันการเข้าถึงระบบหรือข้อมูลของมหาวิทยาลัยโดยไม่ได้รับอนุญาต

4.10. มีการสงวนสิทธิในการเข้าถึงอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล

4.11. มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

4.12. มีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็นในอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล

4.13. มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล และอุปกรณ์สื่อสาร

4.14. มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกล

4.15. มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

4.16. มีการตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

4.17. ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของ มหาวิทยาลัยจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยมหาวิทยาลัย

4.18. มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล เพื่อป้องกันการโต้แย้งกันว่าใครเป็นเจ้าของทรัพย์สินทางปัญญานั้น

4.19. ไม่อนุญาตให้ครอบครัว หรือเพื่อนของผู้ปฏิบัติงานจากระยะไกลเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของมหาวิทยาลัย

5. แนวปฏิบัติการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ (Mobile computing and communication)

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา ได้แก่ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน แท็ปเล็ต รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

5.1. มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

5.2. สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกมหาวิทยาลัย

5.3. ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสลับข้อมูล

5.4. ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์ฯ

5.5. สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

5.6. มีการควบคุมการเข้าถึงระบบงานของมหาวิทยาลัยจากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ

5.7. มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของมหาวิทยาลัยจากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา สมาร์ทโฟน แท็ปเล็ต

5.8. มีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของมหาวิทยาลัย

5.9. ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน เข้ามาปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้า - ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

5.10. กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกันว่าเป็นพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area)

6. แนวปฏิบัติการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)

6.1. ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่ายต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหลัก หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

6.2. คณบดี /ผู้อานวยการ / หัวหน้าหน่วยงานต้องมีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหลัก หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของคณะ/หน่วยงานได้

6.3. หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากมหาวิทยาลัย/คณะ/หน่วยงานของมหาวิทยาลัย โดยจะต้องแจ้งรายชื่อผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศล่วงหน้า มายังมหาวิทยาลัย/คณะ/หน่วยงานดังกล่าว ก่อนการดำเนินงาน ในกรณีที่มีการเปลี่ยนแปลงรายชื่อ หน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

6.4. ในการเข้าปฏิบัติงานภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หน่วยงานภายนอกจะต้องบันทึกรายละเอียดตามเอกสารแบบฟอร์มที่มหาวิทยาลัยจัดไว้ให้โดยต้องระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

6.4.1. เหตุผลในการขอใช้

6.4.2. ระยะเวลาในการใช้

6.4.3. การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

6.4.4. การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

6.4.5. การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

6.5. หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัย/คณะ/หน่วยงานของมหาวิทยาลัย ไม่ว่าจะทำงานอยู่ภายในหรือนอกสถานที่ จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัย โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

6.6. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้นและให้หน่วยงานภายนอกลงนาม ในสัญญาไม่เปิดเผยข้อมูล

6.7. สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญ ของมหาวิทยาลัย ผู้บริหาร/ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

6.8. มหาวิทยาลัยมีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

6.9. หน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

6.10. ทุกครั้งที่จะทำการแก้ไขค่า Config ของอุปกรณ์ทุกชนิดภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หน่วยงานภายนอกจะต้องทำการสารองค่า Config เดิมไว้ก่อน รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมาให้สามารถใช้งานได้ตามสภาพเดิม

6.11. ทุกครั้งที่มีการแก้ไขหรือเปลี่ยนแปลงค่า Config ระบบงานสารสนเทศหรือเปลี่ยนแปลงโครงสร้างฐานข้อมูล หน่วยงานภายนอกจะต้องทำการสำรองโปรแกรม/โมดูล หรือฐานข้อมูลเดิมที่มีการแก้ไข รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการ จะต้องทำการเรียกข้อมูลที่ได้ทาการสำรองไว้กลับมา ให้สามารถใช้งานได้ตามสภาพเดิม

6.12. ในกรณีที่หน่วยงานภายนอกจะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยในวันหยุดหรือนอกเวลาราชการ จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือผู้ดูแลระบบของ มหาวิทยาลัยล่วงหน้าก่อนทุกครั้ง และการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบของมหาวิทยาลัย

6.13. หากหน่วยงานภายนอกจะทำการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยจะต้องแจ้งให้ผู้รับผิดชอบหรือผู้ดูแลระบบของมหาวิทยาลัยทราบล่วงหน้าก่อนทุกครั้ง ซึ่งจะต้องระบุวัน เวลา ระยะเวลาในการทำงานให้ชัดเจน

6.14. ในกรณีที่เจ้าหน้าที่ของหน่วยงานภายนอกประมาท ทำให้อุปกรณ์และระบบสารสนเทศของมหาวิทยาลัยได้รับความเสียหายหรือสูญหาย หน่วยงานภายนอกนั้น จะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

7. แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา

7.1. เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

7.2. โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิมาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

7.3. ไม่อนุญาตให้ผู้ใช้ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคล ของมหาวิทยาลัย

7.4. การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคล จะต้องกำหนดโดยเจ้าหน้าที่ ของมหาวิทยาลัยเท่านั้น

7.5. การเคลื่อนย้าย หรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ ของคณะ /หน่วยงาน/มหาวิทยาลัยเท่านั้น

7.6. ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ควรมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

7.7. ไม่ควรเก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

7.8. ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของมหาวิทยาลัย

7.9. ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติ ดังนี้

7.9.1. ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

7.9.2. ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

7.10. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

7.11. ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username)และรหัสผ่าน(Password)ของตน ในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

7.12. ในระหว่างเวลาพักกลางวันและหลังเลิกงาน ผู้ใช้งานควร Logout ออกจากเครื่องคอมพิวเตอร์ หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ ๑๐ นาที

7.13. มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

7.14. ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

7.15. ผู้ใช้งานมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

7.16. ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ ได้แก่ Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

7.17. ผู้ใช้งานควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเตอร์เน็ตด้วยโปรแกรมป้องกันไวรัส ก่อนใช้งาน

7.18. ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

7.19. ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD DVD External Hard Disk เป็นต้น

7.20. ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.21. ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไป ก็ไม่กระทบต่อการดำเนินการของมหาวิทยาลัย

ส่วนที่ ๗

การใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

(Firewall Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานที่อยู่ภายในมหาวิทยาลัย สามารถใช้บริการเครือข่ายภายในได้เต็มประสิทธิภาพและใช้บริการเครือข่ายภายนอกได้อย่างปลอดภัย

2. แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

1. ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์
2. ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบตัวตนจริง และสิทธิการเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ที่รัดกุมเพียงพอ
3. ผู้ดูแลระบบต้องกำหนดค่า (Configuration) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ป้องกันผู้บุกรุก ไวรัส รวมทั้ง malicious code ต่าง ๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์
4. ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติ ในการตรวจสอบการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าเงื่อนไขในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้บังคับบัญชาโดยทันที
5. การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากผู้อำนวยการ ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม
6. ผู้ดูแลระบบต้องเปิดใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ตลอดเวลา
7. ผู้ดูแลระบบต้องออกจากระบบงาน (Log Out) ของระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์
8. ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งานของระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ โดยการจัดให้มีบัญชีผู้ใช้งาน
9. ผู้ดูแลระบบการใช้งานต้องบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการตรวจสอบผู้ใช้งานก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไข เปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง
10. ผู้บังคับบัญชาต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่าเงื่อนไข ต่าง ๆ อย่างชัดเจน
11. ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด
12. วัตถุประสงค์ในการขอใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่าง ๆ ของมหาวิทยาลัยและต่อกฎหมายที่เกี่ยวข้อง
13. ผู้ขอใช้งานพอร์ตพิเศษ ต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้อำนวยการ โดยระบุข้อมูลดังนี้

13.1. หมายเลข Port ที่ต้องการขอให้เปิด

13.2. หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร

13.3. วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

13.4. วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

14. ในการขอใช้งานหากพบว่าการขัดต่อนโยบาย ประกาศ ระเบียบของมหาวิทยาลัยหรือกฎหมาย หรืออาจทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ จะไม่อนุญาตให้ใช้งาน

15. ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบายประกาศระเบียบ ของมหาวิทยาลัย หรือกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของมหาวิทยาลัย จะยกเลิกการให้บริการทันที

ส่วนที่ ๘
แนวปฏิบัติการใช้งานอินเตอร์เน็ต
(Internet Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ได้แก่ การส่งข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัย ถูกระงับ ชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

๒. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

1. ผู้ใช้งานต้องใช้ทรัพยากรเครือข่ายเพื่อการศึกษาและการปฏิบัติงาน เท่านั้น
2. ผู้ใช้งานต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์
3. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านรหัสผู้ใช้งาน (User Account) ของตนโดยเด็ดขาด
4. ผู้ใช้งานต้องไม่ใช้งาน เพื่อการกระทำการดังต่อไปนี้
   4.1. เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่สถาบันชาติ ศาสนา พระมหากษัตริย์ มหาวิทยาลัย หน่วยงานอื่น และบุคคลอื่น
   4.2. เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน
   4.3. เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน
   4.4. เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา
   4.5. เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

4.6. เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่มหาวิทยาลัย

4.7. เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หรือของผู้ใช้งานอื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ไม่สามารถใช้งานได้ตามปกติ

4.8. เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัยไปยังที่อยู่ของเว็บ (website) ใด ๆ ในลักษณะที่ก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

4.9. เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายของมหาวิทยาลัย

5. ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวทางการใช้ระบบเครือข่ายที่มหาวิทยาลัยกำหนด

ส่วนที่ ๙
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย

2. แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

ผู้ดูแลระบบ

1. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ ได้แก่ การลาออก เป็นต้น
2. ผู้ดูแลระบบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

ผู้ใช้งาน

1. ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์
2. ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัย หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย
3. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

4. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
5. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file ได้แก่ .exe .com เป็นต้น
6. ผู้ใช้งานไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
7. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัย ทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์
8. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
9. ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองอย่างสม่ำเสมอ
10. ผู้ใช้งานต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัวต้องขออนุญาต ผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไป จดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลต้องได้รับการเข้ารหัสลับอย่างปลอดภัย (Encryption)
11. ผู้ใช้งานต้องใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ
12. ผู้ใช้งานต้องไม่ส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที
13. ผู้ใช้งานต้องไม่ส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม
14. ผู้ใช้งานต้องทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง
15. ผู้ใช้งานจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริง ตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น
16. ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง
17. จดหมายของผู้ใช้งาน ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือ ดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้นผู้ใช้งานจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

18. ผู้ใช้งานต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในมหาวิทยาลัยและสังคม

ส่วนที่ ๑๐
การจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (log)

1. วัตถุประสงค์

เพื่อเป็นการเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (log) ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

2. แนวปฏิบัติในการจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์

2.1. ผู้ดูแลระบบ ต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดขั้นตอนความลับในการเข้าถึง

2.2. ห้ามมิให้มีการแก้ไข ดัดแปลงข้อมูลการจราจรทางคอมพิวเตอร์ (log) ที่เก็บรักษาไว้

2.3. กำหนดให้มีการบันทึกการทำงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ใช้ในการตรวจสอบและเก็บบันทึกไว้อย่างน้อย ๙๐ วัน ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

2.4. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงข้อมูลต่าง ๆ และกำหนดสิทธิการเข้าถึงข้อมูลตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ส่วนที่ ๑๑
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Information Security Audit and Assessment Policy)

1. วัตถุประสงค์

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศนั้นมีวัตถุประสงค์ เพื่อให้มั่นใจว่ามาตรฐานต่างๆ ด้านความปลอดภัยสารสนเทศมีการปฏิบัติตามอย่างมีประสิทธิภาพ ในทางปฏิบัติมหาวิทยาลัยจำเป็นต้องมีการตรวจสอบอย่างสม่ำเสมอ ทั้งทางด้านกระบวนการทำงานรวมถึงด้านเทคนิค

2. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจเกิดขึ้นกับระบบสารสนเทศ(Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง โดยมีวิธีการปฏิบัติ ดังนี้

2.1.1. มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

2.1.2. มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.1.3. มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

2.1.4. มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

2.2. การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย โดยมีวิธีการปฏิบัติ ดังนี้

2.2.1. กำหนดให้หน่วยตรวจสอบภายในของมหาวิทยาลัย เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศ และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

2.2.2. มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

2.2.3. มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ ในลักษณะที่อ่านได้เพียงอย่างเดียว

2.2.4. มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

2.2.5. มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

2.2.6. มีการทำลาย หรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

2.2.7. มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

2.2.8. มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

2.2.9. มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแล หรือรับผิดชอบ)

2.3. มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

2.3.1. มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

2.3.2. มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

2.3.3. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ ให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบ เพื่อนำไปปฏิบัติ

2.4. มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อยดังนี้

2.4.1. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

2.4.2. ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

2.4.3. ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.4.4. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

2.4.5. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

2.5. รายการที่สอบทาน

2.5.1. การป้องกันการบุกรุกระบบ

2.5.2. การสำรองข้อมูล

2.5.3. การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

2.5.4. การควบคุมผู้เข้า-ออกอาคาร

2.5.5. การซ้อมรับสถานการณ์ฉุกเฉิน

2.5.6. สอบทานการเข้าถึงระบบสารสนเทศ

2.5.7. สอบทานการกำหนดการใช้งานตามภารกิจ

2.6. การกำกับดูแลการปฏิบัติตามด้านเทคนิค

2.6.1. ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่า เจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่ จากการปฏิบัติตามมาตรฐานความปลอดภัยของสารสนเทศ

2.6.2. มหาวิทยาลัยต้องสอบทานและตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น

2.6.3. ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ ได้แก่ การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัย

2.6.4. เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมดรวมถึงซอฟต์แวร์ ระบบงานและเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้อง จากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะหน่วยงานที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

ส่วนที่ ๑๒
นโยบายการสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

1. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยสามารถให้บริการได้อย่างต่อเนื่อง และเพื่อมาตรฐานในการปฏิบัติและความรับผิดชอบของผู้ดูแลระบบ โดยตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยเป็นสำคัญ

2. การสำรองข้อมูลและระบบคอมพิวเตอร์

ผู้ดูแลระบบหรือคณะทำงานที่เกี่ยวข้อง จะต้องระบุแนวปฏิบัติสำหรับการจัดทำระบบสำรองข้อมูลที่ชัดเจนเพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติดังนี้

2.1. กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองข้อมูลของมหาวิทยาลัย

2.2. ผู้ดูแลระบบ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศของมหาวิทยาลัย

2.3. ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

2.4. ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของมหาวิทยาลัย

2.5. มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

2.6. จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

2.7. ดำเนินการตามกระบวนการสำรองข้อมูล สำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

2.8. มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูล

2.9. การจัดทำบันทึกการสำรองข้อมูล (Operation logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก

2.10. มีขั้นตอนปฏิบัติในการสำรองข้อมูลและกู้คืนข้อมูล แยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

2.11. การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

2.12. ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

2.13. ในกรณีที่พบปัญหาในการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหา และรายงานต่อผู้บังคับบัญชาทราบ

2.14. ให้ผู้ดูแลระบบ กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

2.15. ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสลับข้อมูล (Encrypted backup) ในการสำรองข้อมูลที่สำคัญโดยการใช้เทคโนโลยีการเข้ารหัสลับที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

2.16. ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

3. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

3.1. ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติ หรือทำการสำรองข้อมูลของระบบซึ่งอยู่ในความรับผิดชอบของตนเอง โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ดังนี้

3.1.1. Web servers: สำรองข้อมูลเผยแพร่บนเว็บไซต์ ๑ ครั้งต่อเดือน

3.1.2. Database servers: สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ ๑ ครั้งต่อสัปดาห์

3.1.3. Firewall server: สำรองข้อมูล Rule ของ Firewall ๑ ครั้งต่อเดือน

3.1.4. Server อื่นๆ: สำรองข้อมูลบน Server อื่นๆ ๑ ครั้งต่อเดือน

3.2. ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่า การสำรองข้อมูลตามรายละเอียดข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

3.3. หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

3.4. ผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละ ๑ ครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ

3.5. ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ของมหาวิทยาลัย และเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลของมหาวิทยาลัย โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

4. การทดสอบและการกู้คืนระบบ

มหาวิทยาลัยต้องกำหนดแผนการทดสอบกู้คืนข้อมูล ตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้วเพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติดังนี้

4.1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย จนเป็นเหตุทำให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึก และสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชา หรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาทราบ

4.2. การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

4.3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่าย กระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

4.4. กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ ๑ ครั้ง

5. การกู้คืนข้อมูล

เพื่อให้การฟื้นฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์ หรือการประมวลผลของ

คอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิม ทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลา หรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติ มีมาตรการในการกู้คืนข้อมูลดังนี้

5.1. ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

5.2. ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์ และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

5.3. ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

6. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยมีรายละเอียดอย่างน้อย ดังนี้

6.1. มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

6.2. มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น ได้แก่ ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

6.3. มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

6.4. มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

6.5. มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

6.6. การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

6.7. มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

ภาคผนวก ก
แผนเตรียมความพร้อมกรณีฉุกเฉิน
ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
มหาวิทยาลัยอุบลราชธานี (IT Contingency Plan)

1. หลักการและเหตุผล

มหาวิทยาลัยอุบลราชธานีเป็นสถาบันการศึกษา ที่มีพันธกิจสำคัญ ๔ ประการ ได้แก่ ๑) สร้างบัณฑิตที่มีคุณภาพ มาตรฐาน มุ่งสู่ความเป็นเลิศทางวิชาการและวิชาชีพ ๒) สร้างองค์ความรู้และนวัตกรรมที่นำไปประยุกต์ใช้ประโยชน์เพื่อพัฒนาคุณภาพชีวิตของประชาชนในภาคตะวันออกเฉียงเหนือและภูมิภาคลุ่มน้ำโขง ๓) บริการวิชาการอย่างมีส่วนร่วมเพื่อพัฒนาคุณภาพชีวิตของประชาชนในภาคตะวันออกเฉียงเหนือและภูมิภาคลุ่มน้ำโขง ๔) ทำนุบำรุงศิลปวัฒนธรรม ภูมิปัญญาท้องถิ่นและสร้างความเข้าใจในวัฒนธรรมที่หลากหลายของภูมิภาคลุ่มน้ำโขง เพื่อให้การขับเคลื่อนพันธกิจต่างๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล มหาวิทยาลัยอุบลราชธานี จึงได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการงานและการให้บริการด้านต่างๆ เพื่อให้นักศึกษาได้รับความสะดวกมากขึ้น ขณะเดียวกันระบบสารสนเทศของมหาวิทยาลัยอาจได้รับความเสียหายจากภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศ อาทิ ไฟฟ้าดับ ไวรัสคอมพิวเตอร์ การบุกรุก (Hacker) หรือความเสียหายจากการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ สถานการณ์ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผย หรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่นๆ และ/หรือปัจจัยอื่นๆ ที่เกี่ยวข้อง เพื่อเป็นการป้องกัน แก้ไขปัญหา และรองรับสถานการณ์ที่อาจเกิดขึ้น แผนนี้จึงจัดแบ่งออกเป็น ๓ ด้าน ได้แก่ ๑) แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ (Contingency Plan) ๒) แผนดำเนินการเพื่อให้ระบบเทคโนโลยีสารสนเทศ ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation plan) ๓) แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Plan)

2. วัตถุประสงค์

2.1. เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยอุบลราชธานี สามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2.2. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

2.3. เพื่อลดความเสียหายที่อาจเกิดขึ้นแก่ระบบสารสนเทศของมหาวิทยาลัยอุบลราชธานี

2.4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยอุบลราชธานี

3. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ (Contingency Plan)

กรณีเครื่องลูกข่าย

1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของคณะ/หน่วยงานทราบ หรือกรณีมีเหตุอันทำให้สำนักคอมพิวเตอร์และเครือข่าย ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ สำนักคอมพิวเตอร์และเครือข่ายจะต้องประกาศให้ทุกคณะ/หน่วยงานในมหาวิทยาลัยอุบลราชธานีทราบ
2. กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่าย ให้ทำการดึงสายเชื่อมต่อระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็วและแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการ
3. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่องาน/หน่วยงาน ภายในอาคารที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากคอมพิวเตอร์เครื่องนั้นทันที
4. ปิดระบบไฟฟ้าที่เข้าเครื่องคอมพิวเตอร์ทั้งหมด
5. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย
6. ให้เจ้าหน้าที่สำนักคอมพิวเตอร์และเครือข่าย แจ้งเหตุขัดข้องนั้นให้ผู้อำนวยการทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (Server) และอุปกรณ์เครือข่าย

1. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ
2. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์โดยพิจารณาตามลำดับความสำคัญของการให้บริการ, ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า
3. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว
4. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย
5. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบคอมพิวเตอร์แม่ข่าย และ/หรือผู้เชี่ยวชาญระบบเครือข่ายที่เกี่ยวข้องโดยเร็วที่สุด
6. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบ นำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด
7. ผู้ดูแลระบบ ต้องแจ้งให้ผู้อำนวยการทราบโดยเร็วที่สุด

4. ผู้รับผิดชอบตามแผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยอุบลราชธานีที่เกิดจากภัยพิบัติ ให้ใช้งานได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ มหาวิทยาลัยอุบลราชธานีได้จัดองค์กรปฏิบัติการฉุกเฉิน หรือผู้รับผิดชอบตามสายการบังคับบัญชา (Lines of Authority) ดังนี้

4.1. **ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย**

4.1.1.เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

4.1.2. มีอำนาจสั่งการให้ทุกคณะ/หน่วยงานหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

4.1.3. มีอำนาจสั่งทำลายกุญแจ เพื่อการระงับเหตุฉุกเฉิน

4.1.4. ประชุมหารือกับคณะกรรมการที่เกี่ยวข้อง

4.1.5. ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

4.2. **ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย (รองผู้อำนวยการฝ่ายพัฒนา)**

4.2.1. วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย

4.2.2. มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้น จนกว่าผู้อำนวยการจะมาถึงที่เกิดเหตุ

4.2.3. สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

4.2.4. ทำหน้าที่แทนผู้อำนวยการตามที่ได้รับมอบหมาย หรือขณะที่ผู้อำนวยการไม่อยู่

4.2.5. ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง ได้แก่ งานไฟฟ้า ยานพาหนะ และหน่วยดับเพลิง เป็นต้น

4.2.6. รายงานให้ผู้อำนวยการทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

4.2.7. กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

4.2.8. ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

4.3. **ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ (Network Administer)**

4.3.1. กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

4.3.2. พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ มาช่วย

4.3.3. ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

4.3.4. ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ไม่ให้ได้รับความเสียหาย

4.3.5. หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ ที่ชำรุดเสียหาย แล้วรายงานให้ผู้อำนวยการทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

4.3.5.1. ทำการตรวจสอบระบบ Firewall

4.3.5.2. ทำการตรวจสอบ Virus, Worm, Spyware

4.3.5.3. ทำการตรวจสอบอุปกรณ์ระบบสำรองกระแสไฟฟ้า (UPS)

4.3.5.4. ทำการตรวจสอบ Transaction log files

4.3.5.5. ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

4.3.5.6. ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่างๆ

4.3.5.7. ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

4.3.5.8. ทำการตรวจสอบค่า Configuration ของระบบ

4.3.6. เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ Software ตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

4.3.7. ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ระบบ

4.3.8. ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ

4.3.9. นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

4.4. **ที่ปรึกษาด้านเทคนิค (เจ้าหน้าที่บริษัทที่ปรึกษา)**

4.4.1. ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉิน ที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

4.4.2. ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญ หรือหน่วยราชการที่เกี่ยวข้อง

4.4.3. ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

4.5. **หัวหน้าหน่วยงานที่เกิดเหตุ**

4.5.1. แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

4.5.2. ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ผู้อำนวยการ

4.5.3. นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

5. แผนการสำรองและกู้คืนข้อมูล (Backup and Recovery Plan)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยอุบลราชธานีอยู่ในสภาพพร้อมรองรับการให้บริการได้ตลอด ๒๔ ชั่วโมง ให้ผู้ดูแลระบบปฏิบัติตามแผนการ Backup and Recovery Plan ดังนี้

5.1. **แผนการสำรองข้อมูล (Backup Plan)**

5.1.1.มหาวิทยาลัยมีระบบสารสนเทศหลักที่สำคัญต่อการขับเคลื่อนภารกิจอยู่ 4 ระบบได้แก่ ระบบบุคลากร ระบบบริการการศึกษาและทะเบียน ระบบการเงินและพัสดุ และระบบงานวิจัย ซึ่งหากระบบสารสนเทศดังกล่าวเกิดความเสียหาย และไม่สามารถกู้ระบบคืนระบบกลับมาได้ จะส่งผลกระทบอย่างรุนแรงต่อการขับเคลื่อนภารกิจของมหาวิทยาลัย ดังนั้นการจัดทำแผนการสำรองและกู้คืนข้อมูลจึงคัดเลือกระบบสารสนเทศดังกล่าวข้างต้นบรรจุไว้ในแผนการสำรองและกู้คืนข้อมูล โดยมีรายการ ดังนี้

5.1.1.1. ระบบบุคลากร

5.1.1.2. ระบบบริการการศึกษาและทะเบียน

5.1.1.3. ระบบการเงินและพัสดุ

5.1.1.4. ระบบงานวิจัย

5.1.2. บุคลากรผู้รับผิดชอบ

5.1.2.1. ระบบบุคลากร

	หมายเลขโทรศัพท์
๑. ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย	๐๘๑-๔๔๘-๗๑๘๔
๒. รองผู้อำนวยการฝ่ายพัฒนา	๐๘๔-๗๔๕-๒๓๓๒
๓. หัวหน้าฝ่ายพัฒนาซอฟต์แวร์	๐๘๑-๕๙๓-๒๓๖๘
๔. หัวหน้าฝ่ายพัฒนาเครือข่าย	๐๘๔-๖๐๖-๑๘๙๓
๕. นางสาวกมลวรรณ จันทป	๐๔๕-๓๕๓-๑๑๐
๖. นางสาวทัศนีย์ หนองกก	๐๔๕-๒๘๘-๔๐๐

5.1.2.2. ระบบบริการการศึกษาและระบบทะเบียน

	หมายเลขโทรศัพท์
๑. ผู้อำนวยการกองบริการการศึกษา	๐๔๕-๓๕๓-๑๒๓
๒. หัวหน้างานทะเบียน	๐๔๕-๓๕๓-๑๒๔
๓. นางสาวอุษา ปัตเสน	๐๔๕-๓๒๓-๑๘๑
๔. นายวรวิทย์ ชาลีพรหม	๐๔๕-๓๕๓-๑๑๙

5.1.2.3. ระบบการเงินและพัสดุ

	หมายเลขโทรศัพท์
๑. ผู้อำนวยการกองคลัง	๐๔๕-๓๕๓-๐๒๘
๒. นายบรรชา ไพอุปรี	๐๔๕-๓๕๓-๐๒๑
๓. นายพจนารถ พันธัง	๐๔๕-๓๕๓-๐๒๑

5.1.2.4. ระบบงานวิจัย

	หมายเลขโทรศัพท์
๑. ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย	๐๘๑-๔๔๘-๗๑๘๔
๒. รองผู้อำนวยการฝ่ายพัฒนา	๐๘๔-๗๔๕-๒๓๓๒
๓. หัวหน้าฝ่ายพัฒนาซอฟต์แวร์	๐๘๑-๕๙๓-๒๓๖๘
๔. หัวหน้าฝ่ายพัฒนาเครือข่าย	๐๘๔-๖๐๖-๑๘๙๓
๕. นางสาวกมลวรรณ จันทป	๐๔๕-๓๕๓-๑๑๐
๖. นางสาวทัศนีย์ หนองกก	๐๔๕-๒๘๘-๔๐๐

5.1.3.จัดเตรียม Storage ที่ใช้ในการเก็บข้อมูลที่ต้องการสำรอง รวมถึงระบบ/Software ที่ใช้ในการสำรองและกู้คืน

5.1.4. ทำการทดสอบความพร้อมของระบบ และดำเนินการสำรองระบบงานที่ได้คัดเลือกไว้

5.1.5. ตรวจสอบความถูกต้องของระบบงาน หลังจากที่ทำการสำรอง

5.1.6. บันทึกข้อมูลลงใน แบบฟอร์มบันทึกการสำรองข้อมูล / แบบฟอร์มรายงานข้อผิดพลาดในการสำรองข้อมูล

5.1.7. หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถสำรองข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการสำรองข้อมูลอีกครั้ง

5.2. **แผนการกู้คืนข้อมูล (Recovery Plan)**

5.2.1. รายงานปัญหาหรือสาเหตุ ที่ต้องทำการกู้คืนข้อมูล ต่อผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการทราบ

5.2.2. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที

5.2.3. ใช้ข้อมูล ล่าสุดหรือทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

5.2.3.1. กรณีเกิดความเสียหายขึ้นกับ Source Code จะทำการติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด

5.2.3.2. กรณีเกิดความเสียหายขึ้นกับฐานข้อมูล (Database) จะนำฐานข้อมูลที่เก็บไว้ล่าสุดกู้คืน เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด

5.2.3.3. กรณีเกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ Hardware ยังคงทำงานปกติจะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

5.2.3.4. กรณีเกิดความเสียหายขึ้นกับ Hardware ให้บริษัทผู้ดูแลทำการแก้ไขเบื้องต้นให้ Hardware สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับ OS และระบบงาน จะทำการติดตั้ง OS และระบบงานนั้นใหม่ จาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

5.2.4. ดำเนินการกู้คืนข้อมูลระบบงานที่มีปัญหา

5.2.5. ตรวจสอบความถูกต้องของระบบงาน หลังจากทำการกู้คืนระบบเสร็จเรียบร้อยแล้ว

5.2.6. หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการกู้คืนข้อมูล จนเป็นเหตุให้ไม่สามารถกู้คืนข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการกู้คืนข้อมูลอีกครั้ง

5.2.7. แจ้งผลการกู้คืนข้อมูลให้ผู้อำนวยการและผู้ใช้งานทราบ

6. การเตรียมการป้องกันและการแก้ไข

6.1. การสำรองข้อมูลและระบบงาน (Back up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น เมื่อข้อมูลถูกทำลายหรือถูกบุกรุก หรือไม่สามารถให้บริการได้

6.2. **การป้องกันไวรัสคอมพิวเตอร์**

6.2.1. ติดตั้งโปรแกรมป้องกันและตรวจจับไวรัส (Antivirus) ครอบคลุมทุกเครื่องแม่ข่ายและลูกข่ายเพื่อป้องกันความเสียหายของข้อมูล

6.2.2. Update ข้อมูลไวรัสอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง โดยเจ้าหน้าที่สามารถทำการ Update ไวรัสได้จากเครื่องคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยอุบลราชธานี ซึ่งจะมีการแนะนำถึงขั้นตอนและวิธีการ Update ให้เจ้าหน้าที่สามารถดำเนินการได้ด้วยตนเอง

6.2.3. ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

6.2.4. มีการแนะนำผู้ใช้คอมพิวเตอร์ให้ระวังภัยจากการเปิด File และ E-mail โดย Scan สื่อสำหรับจัดเก็บข้อมูลก่อนการใช้งาน ไม่เปิดอ่าน E-mail โดยไม่รู้ที่มาและให้ลบเมล์นั้นทิ้งทันที

6.3. **การป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ**

6.3.1. ติดตั้งอุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply, UPS) ที่เครื่องของเจ้าหน้าที่ในคณะ/หน่วยงาน ของมหาวิทยาลัยอุบลราชธานี สำหรับในกรณีที่ไฟฟ้าดับ ซึ่งสามารถจะสำรองไฟฟ้าไว้ได้ภายในระยะเวลา ๑๕ นาที ซึ่งเพียงพอที่จะสั่งการให้ระบบทำการ Shutdown โดยที่ไม่เกิดความเสียหายต่ออุปกรณ์หรือข้อมูล

6.3.2. ดำเนินการเชื่อมโยงระบบเครื่องกำเนิดไฟฟ้าของอาคาร

6.4. **การป้องกันความเสี่ยงจากไฟไหม้**

6.4.1. ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลักเพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน(ไฟไหม้) เพื่อการควบคุมเพลิงเบื้องต้นได้

6.4.2. ในกรณีที่เกิดไฟไหม้ภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลัก จะมีการตัดการจ่ายกระแสไฟฟ้าภายในบริเวณใกล้เคียง

6.5. **การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker)** ติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยให้กับระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ ป้องกันการบุกรุกจากภายนอก

6.6. **การป้องกันอุปกรณ์ระบบคอมพิวเตอร์แม่ข่ายชำรุด** มีการใช้ Hard disk แบบ RAID - ๕ เพื่อป้องกันข้อมูลเสียหายให้กับระบบงานต่างๆ

6.7. **การป้องกันความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่** จัดอบรมเสริมสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศเบื้องต้นในด้าน Hardware และ Software เพื่อลดความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ให้น้อยที่สุด

6.8. **การป้องกันความเสี่ยงในกรณีที่ระบบเครือข่ายคอมพิวเตอร์มีปัญหา**

6.8.1. ดำเนินการติดตั้งเส้นทางสำรองสำหรับระบบงานบริการ ให้สามารถบริการได้อย่างต่อเนื่อง

6.8.2. ดำเนินการบำรุงรักษาอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์หลักอย่างสม่ำเสมอ

7. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

7.1. **เจ้าหน้าที่ดูแลระบบงานและฐานข้อมูล** รับผิดชอบดูแล บำรุงรักษาระบบงานและฐานข้อมูล โดยมีหน้าที่ ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบงานคอมพิวเตอร์ และการสำรองระบบงาน/ฐานข้อมูล

7.2. **เจ้าหน้าที่ดูแลระบบเครือข่าย** รับผิดชอบดูแล บำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ และความปลอดภัยของระบบเครือข่ายทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่าย

8. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

8.1. กรณีระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์

8.1.1. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์โดยพิจารณาตามลำดับความสำคัญของการให้บริการ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

8.1.2. ในกรณีไฟไหม้ ให้ตัดระบบจ่ายไฟ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

8.1.3. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายและ/หรือผู้เชี่ยวชาญระบบเครือข่ายคอมพิวเตอร์โดยเร็วที่สุด

8.1.4.ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษานำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

8.2. กรณีเครื่องลูกข่าย

8.2.1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งให้เจ้าหน้าที่ผู้รับผิดชอบ ของคณะ/หน่วยงาน/สำนักคอมพิวเตอร์และเครือข่ายทราบ

8.2.2. กรณีมีเหตุอันทำให้ฝ่ายการให้บริการระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ไม่สามารถให้บริการได้ ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินการแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษารีบดำเนินการให้โดยด่วน

8.2.3. กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการ

9. แผนการนำระบบเทคโนโลยีสารสนเทศกลับสู่สภาพปกติ

การกู้คืนระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ โดยปกติจะต้องอยู่ในสภาพพร้อมให้บริการได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการ จะต้องดำเนินการกู้คืนระบบให้เร็วที่สุดเท่าที่จะทำได้ เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะปกติ เมื่อระบบเสียหายหรือหยุดทำงาน ดังนี้

9.1. ซ่อมอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

9.2. สำรองอุปกรณ์ทดแทนหรือยืมอุปกรณ์จากหน่วยงานอื่นมาใช้ทดแทน

9.3. นำข้อมูลที่ได้ทำการสำรองไว้ (Backup) กลับมาใช้ (Restore) เพื่อกู้ระบบให้กลับมาภายใน ๔๘ ชั่วโมง

9.4. ตรวจสอบระบบปฏิบัติการ ระบบงานและฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลอื่นๆ ที่เกี่ยวข้อง