แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเชียงใหม่

พ.ศ. ๒๕๕๕

รองรับแผนพัฒนาการศึกษา คณะพยาบาลศาสตร์ มช. ระยะที่ 13 (พ.ศ.2566–2570)

วัตถุประสงค์เชิงกลยุทธ์ S05 มุ่งเน้นการพัฒนา

Flagship Program : บูรณาการเทคโนโลยีดิจิทัลในองค์กร

การควบคุมภายใน มช. ด้านงานเทคโนโลยีสารสนเทศ วัตถุประสงค์ : ระบบเครือข่าย คอมพิวเตอร์ ระบบฐานข้อมูลและสารสนเทศของคณะ มีความมั่นคง ปลอดภัย และเป็นไปตาม พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ.2562

การบริหารความเสี่ยง คณะพยาบาลศาสตร์ มช. ประเด็นความเสี่ยงที่ 5 ความไม่พร้อมด้านโครงสร้างพื้นฐานและระบบฐานข้อมูลของระบบเทคโนโลยีสารสนเทศ และประเด็นความเสี่ยงที่ 6 ภัยคุกคามด้านเทคโนโลยีสารสนเทศ (Cyber Attack)

ผู้รับผิดชอบดำเนินการ : หน่วยพัฒนาเทคโนโลยีสารสนเทศ

คำนำ

ปัจจุบันความก้าวหน้าทางด้านเทคโนโลยีสารสนเทศมีพัฒนาการเป็นไปอย่างรวดเร็ว เนื่องจากการใช้งานระบบเทคโนโลยีสารสนเทศในปัจจุบันมีการเชื่อมโยงข้อมูลที่ไร้ขอบเขตจำกัด ในขณะเดียวกันการบุกรุก ทำลายข้อมูลหรือการอาชญากรรมทางคอมพิวเตอร์มีความรุนแรงมากขึ้น ทำให้เกิดปัญหาภัยคุกคามทางอินเทอร์เน็ตสร้างความเสียหายทั้งในระดับบุคคล องค์กรต่าง ๆ อย่างกว้างขวาง

ดังนั้น เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นต่อการใช้งานอินเทอร์เน็ตของมหาวิทยาลัยเชียงใหม่ จึงได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นไปตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ เพื่อใช้เป็นแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำหรับทุกส่วนงานของมหาวิทยาลัยเชียงใหม่ ใช้เป็นแนวปฏิบัติร่วมกัน

คณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร
มหาวิทยาลัยเชียงใหม่

สารบัญ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเชียงใหม่

๑. ที่มา

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

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเชียงใหม่ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยจากภัยคุกคามในด้านต่างๆ และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง มหาวิทยาลัยจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๒. วัตถุประสงค์

๑.๑ จัดทำแนวนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศเพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเชียงใหม่ เพื่อให้การดำเนินงานเป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๑.๒ กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศอ้างอิงตามกรอบแนวคิดมาตรฐานสากลและมีการปรับปรุงอย่างต่อเนื่อง

๑.๓. กำหนดมาตรฐานแนวทางปฏิบัติและวิธีปฏิบัติให้หัวหน้าส่วนงาน เจ้าหน้าที่ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัยตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและปฏิบัติตามอย่างเคร่งครัด

๑.๔ กำหนดให้หัวหน้าส่วนงาน รับผิดชอบกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืน

การปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยหัวหน้าส่วนงานต้องรับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๑.๕ เผยแพร่ให้เจ้าหน้าที่ทุกระดับในมหาวิทยาลัยได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๑.๖ ดำเนินการตรวจสอบและประเมินนโยบายตามระยะเวลา ๑ ครั้งต่อปี

องค์ประกอบของนโยบายการการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแต่ละส่วนที่กล่าวข้างต้นประกอบด้วยวัตถุประสงค์รายละเอียดของมาตรฐาน (Standard) และแนวทางปฏิบัติ (Guideline) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อทำให้มีมาตรการในการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อทรัพย์สินของมหาวิทยาลัย และทำให้สามารถดำเนินงานด้านเทคโนโลยีสารสนเทศได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย ซึ่งเจ้าหน้าที่ของมหาวิทยาลัย และหน่วยงานภายนอกต้องปฏิบัติตามอย่างเคร่งครัด

๓. เนื้อหาของนโยบายและแนวปฏิบัติ

ส่วนที่ ๑ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

ส่วนที่ ๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ (Access Control)

ส่วนที่ ๓ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

ส่วนที่ ๔ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security)

ส่วนที่ ๕ การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

ส่วนที่ ๖ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ส่วนที่ ๗ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access control)

ส่วนที่ ๘ การสำรอ งและการกู้คืนข้อมูล (Data Backup and Recovery)

ส่วนที่ ๙ การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ (Data Center Access Control Room)

ส่วนที่ ๑๐ การประเมินความเสี่ยงและการควบคุม (Risk Assessment and Control)

๔. คำนิยามศัพท์ที่ใช้ในนโยบายและแนวปฏิบัติ นี้

๑. **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยเชียงใหม่

๒. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยเชียงใหม่

๓. **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบเทคโนโลยีสารสนเทศประกอบด้วยเทคโนโลยีฮาร์ดแวร์ ซอฟต์แวร์ และระบบเครือข่าย ที่หน่วยงาน นำมาใช้ประโยชน์ในการดำเนินงาน การวางแผนบริหาร การสนับสนุนการศึกษาและให้บริการการศึกษา และควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่นระบบคอมพิวเตอร์ระบบเครือข่ายโปรแกรมข้อมูลและสารสนเทศ เป็นต้น

๔. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งานหรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเชียงใหม่ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (role) ของผู้ใช้งาน

๕. **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

๖. **ผู้ดูแลระบบเทคโนโลยีสารสนเทศ** หมายถึง ผู้ที่ได้รับมอบหมายให้มีหน้าที่รับผิดชอบในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๗. **ผู้บริหารมหาวิทยาลัย** หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี

๘. **หัวหน้าส่วนงานหรือผู้ที่ได้รับมอบหมาย** หมายถึง คณบดี ผู้อำนวยการ คณะ สำนัก และสถาบัน

๙. **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑๐. **ทรัพย์สิน** หมายถึง ข้อมูลระบบข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศ หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย เครื่องคอมพิวเตอร์ซอฟต์แวร์และข้อมูล เป็นต้น

๑๑. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้น

สำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

๑๒. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๑๓. **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๑๔. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยคุกคาม

๑๕. **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงานโดยจะได้รับสิทธิในการใช้งานตามอำนาจและต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๖. **รหัสผ่าน** (password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๑๗. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูลข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๘. **ข้อมูลอิเล็กทรอนิกส์** หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร ดังนั้น เอกสารอิเล็กทรอนิกส์ จึงถือได้ว่าเป็นข้อมูลอิเล็กทรอนิกส์ และมีผลทำให้ต้องปฏิบัติตามหลักกฎหมาย

๑๙. **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่ใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของมหาวิทยาลัยได้ เช่น ระบบเครือข่ายภายใน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)

- ระบบเครือข่ายภายใน หรือระบบอินทราเน็ต (Intranet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
- ระบบอินเทอร์เน็ต (Internet) หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

๒๐. **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ** (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

- พื้นที่การใช้งานในระดับกายภาพ (Physical) ประกอบด้วย
  - หมายถึง พื้นที่ทำงานทั่วไป (General working area) ได้แก่ พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล
  - หมายถึง พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT equipment or network area)
- พื้นที่การใช้งานแบบลอจิคัล (Logical)
  - หมายถึง พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)

๒๑. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒๒. Login หมายถึง การเริ่มใช้งานระบบโดยมีการยืนยันตัวตน

๒๓. **จดหมายอิเล็กทรอนิกส์** (e-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้ง ตัวอักษรภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

๒๔. <u>ชุดคำสั่งไม่พึงประสงค์</u> หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหายถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติมขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

ส่วนที่ ๑

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน

(User Responsibilities)

๑. วัตถุประสงค์

เพื่อควบคุมและกำหนดมาตรการ การปฏิบัติงานของผู้ใช้งานให้เป็นไปตามหน้าที่ที่ได้รับมอบหมายที่เกี่ยวข้องกับข้อมูลสารสนเทศ และบังคับใช้กับผู้ที่ใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน เพื่อป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๒. แนวทางปฏิบัติในการใช้งานรหัสผ่าน (Password Use)

๒.๑ ผู้ใช้งานควรตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น ดังนี้

๒.๑.๑ ควรตั้งรหัสผ่านที่มีความยาวเกินกว่าขั้นต่ำกำหนดไว้

๒.๑.๒ ควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

๒.๑.๓ ไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

๒.๑.๔ ควรหลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓ , abcd หรือกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑ , aaa เป็นต้น

๒.๑.๕ ควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๒.๑.๖ ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๒.๒ ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเอง

๒.๓ ผู้ใช้งานควรจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๒.๔ ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยทันทีเมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๒.๕ ผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุกๆ ๓ เดือน สำหรับผู้ดูแล และ ๖ เดือน สำหรับผู้ใช้งานระบบ

๒.๖ ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อคอินเข้าสู่ระบบงาน

๒.๗ ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อคอินในภายหลัง

๒.๘ ผู้ใช้งานไม่ควรใช้รหัสผ่านของตนร่วมกับผู้อื่น

๒.๙ ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกัน สำหรับต่างระบบที่ใช้งาน

๒.๑๐ ผู้ใช้งานต้องปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ อย่างเคร่งครัด

๓. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๑ ผู้ใช้งานควรล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๓.๒ ผู้ดูแลระบบควรกำหนดให้พนักงานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตนโดยใส่รหัสผ่านก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

๔. การพัฒนาความรู้

๔.๑ ผู้ใช้งานควรศึกษาหาความรู้เพิ่มเติมในการใช้งานคอมพิวเตอร์ให้มีประสิทธิภาพสูงขึ้นและปลอดภัยมากขึ้น

๔.๒ ผู้ดูแลระบบต้องมีการอบรมให้ความรู้เกี่ยวกับข้อกฎหมาย ระเบียบวิธีการใช้งานคอมพิวเตอร์ที่ถูกต้อง การรักษาความปลอดภัย การตรวจสอบและแก้ไขปัญหาคอมพิวเตอร์เบื้องต้นแก่ผู้ใช้งาน ไม่ต่ำกว่าปีละ ๒ ครั้ง

ส่วนที่ ๒
การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Information Technology Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้อย่างถูกต้อง

๒. แนวทางปฏิบัติเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล

๒.๑ หัวหน้าส่วนงานทำหน้าที่กำหนดผู้รับผิดชอบ ขั้นตอนและสิทธิในการเข้าถึงข้อมูลตามลำดับชั้นความลับของข้อมูล

ประเภทข้อมูลหรือรูปแบบของเอกสารอิเล็กทรอนิกส์ แบ่งได้ดังนี้

๒.๑.๑ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

- การกำหนดชั้นความลับ ตามความสำคัญของข้อมูลเอกสาร ให้กำหนดไว้ ๓ ระดับเป็นอย่างน้อย ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับเป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น
- การควบคุมเอกสาร โดยกำหนดให้มีมาตรการการควบคุมต่างๆ คือ การจัดทำทะเบียน การตรวจสอบ การจัดทำเอกสาร การสำเนาและการแปล การโอน การส่งและการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉินเวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาตเข้าระบบนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐานและมีการจัดทำบัญชีผู้ใช้งานให้สอดคล้องกับหน้าที่ความรับผิดชอบของผู้ใช้งานนั้น

๓.๒ ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

ส่วนที่ ๓
การบริหารจัดการการเข้าถึงของผู้ใช้งาน
(User Access Management)

๑. วัตถุประสงค์

เพื่อกำหนดการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน และไม่อนุญาตให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องสามารถเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายของมหาวิทยาลัยโดยไม่ได้รับอนุญาต รวมถึงการจำกัดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้ตรวจสอบ ติดตาม และสามารถพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒. แนวทางปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration)

๒.๑ หัวหน้าส่วนงานทำหน้าที่กำหนดผู้รับผิดชอบและกำหนดขั้นตอนในการปฏิบัติในการลงทะเบียนผู้ใช้งาน

๒.๒ ทำการออกแบบขั้นตอนการลงทะเบียนผู้ใช้งานโดยมีแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒.๓ ระบบลงทะเบียนผู้ใช้งานต้องสามารถออกเอกสารที่เป็นลายลักษณ์อักษรให้แก่ผู้ใช้งานเพื่อแสดงสิทธิและความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งต้องให้ผู้ใช้งานลงนามในเอกสารดังกล่าวหลังจากทำความเข้าใจแล้ว

๒.๔ ผู้ดูแลระบบต้องให้สิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศที่เหมาะสมต่อหน้าที่และความรับผิดชอบของผู้ใช้งาน

๒.๕ ระบบลงทะเบียนผู้ใช้งานต้องมีระบบในการตรวจสอบการลงทะเบียนผู้ใช้งานทั้งในส่วนการเข้าถึงของผู้ดูแลระบบและรายละเอียดในการออกทะเบียนผู้ใช้งาน

๒.๖ ผู้ดูแลระบบต้องทำการถอดถอนสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศต่างๆ ของมหาวิทยาลัยทันทีเมื่อผู้ใช้งานหมดข้อผูกพันใดๆ ต่อมหาวิทยาลัย

๒.๗ ผู้ดูแลระบบต้องมีการตรวจสอบสิทธิของผู้ใช้งานในการใช้งานบริการต่างๆ ให้เหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งาน

๓. **การบริหารจัดการสิทธิของผู้ใช้งาน** (User Management)

๓.๑ ผู้ดูแลระบบต้องกำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศ โดยให้สิทธิอย่างเหมาะสมกับหน้าที่และความรับผิดชอบของผู้ใช้งานและต้องทบทวนสิทธิที่มอบให้อย่างสม่ำเสมอ

๓.๒ ผู้ดูแลระบบต้องมอบหมายสิทธิให้สอดคล้องกับนโยบายการควบคุมการเข้าถึง

๓.๓ ผู้ดูแลระบบต้องจัดเก็บและมีระบบตรวจสอบการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๓.๔ กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานให้มีสิทธิสูงสุดในระบบ จะต้องมีการกำหนดระยะเวลาการใช้งานและให้ทำการระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว หรือเมื่อพ้นจากความรับผิดชอบ และในการกำหนดสิทธิพิเศษที่ได้รับต้องกำหนดว่าจะสามารถเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๔. **การบริหารจัดการรหัสผ่าน** (Password Management System)

๔.๑ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีภายหลังจากที่ได้รับรหัสผ่านชั่วคราว

๔.๒ บัญชีผู้ใช้งานและรหัสผ่านต้องแยกเป็นรายบุคคลเพื่อให้สามารถติดตามการใช้งานและกำหนดความรับผิดชอบของแต่ละบุคคลได้

๔.๓ ผู้ใช้งานต้องสามารถกำหนดรหัสผ่านของตัวเองได้โดยอิสระผ่านระบบลงทะเบียนผู้ใช้งาน

๔.๔ ผู้ใช้งานต้องสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเองและมีขั้นตอนในการยืนยันรหัสผ่านที่ต้องการเปลี่ยนทุกครั้ง

๔.๕ รหัสผ่านที่ผู้ใช้งานป้อนต้องได้รับการป้องกันการเดาหรือลืมได้โดยการใช้อักษรอื่นแทนข้อความจริงที่แสดง

๔.๖ รหัสผ่านที่ทำการจัดเก็บไว้ในระบบต้องได้รับการป้องกันโดยการเข้ารหัสข้อมูล

๔.๗ มีระบบที่ใช้ในการกู้คืนรหัสผ่านสำหรับผู้ใช้งานกรณีที่ไม่สามารถจดจำรหัสผ่านของตัวเองได้

๔.๘ ระบบที่ใช้ในการเปลี่ยนรหัสผ่านต้องสามารถให้คำแนะนำและมีบริการตรวจสอบรหัสผ่านเพื่อแจ้งเตือนผู้ใช้งานได้ในกรณีที่รหัสผ่านของผู้ใช้งานมีความง่ายต่อการคาดเดา

๕. **การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน** (Review Of User Access Rights)

๕.๑ มีการทบทวนสิทธิในการใช้งานของผู้ใช้งานอย่างน้อย ๑ ครั้งต่อปี

๕.๒ มีการทบทวนสิทธิสำหรับผู้มีสิทธิในระดับสูง ได้แก่ สิทธิสำหรับผู้ดูแลระบบ อย่างน้อย ๑ ครั้งต่อเดือน

๕.๓ มีการทบทวนการเปลี่ยนแปลงของสิทธิตามรอบระยะเวลาที่เหมาะสมหรือมีการเปลี่ยนแปลงใดๆ เกิดขึ้น เช่น การเลื่อนตำแหน่ง ลดตำแหน่ง ย้ายหน่วยงานหรือผู้ใช้งานสิ้นสุดข้อผูกมัดใดๆ กับมหาวิทยาลัย

๕.๔ การเปลี่ยนแปลงใดๆ ที่เกี่ยวข้องกับสิทธิของผู้ใช้งานต้องมีการบันทึกการเปลี่ยนแปลงนั้นทุกครั้ง

๖. **การอบรมให้ความรู้แก่ผู้ใช้งาน** (User Awareness)

๖.๑ ในทุกขั้นตอนของการลงทะเบียนใช้งานของผู้ใช้งานต้องมีข้อความประกอบคำอธิบายเพื่อความเข้าใจในแต่ละขั้นตอนอย่างชัดเจน

๖.๒ มีระบบที่ให้ความรู้ในการใช้งานระบบลงทะเบียนผู้ใช้งานเพื่ออธิบายและทำความเข้าใจให้แก่ผู้ใช้งาน

๖.๓ มีระบบที่ให้ความรู้ในการใช้งานระบบเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้องกับผู้ใช้งานโดยตรงให้แก่ผู้ใช้งาน

ส่วนที่ ๔

การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒. แนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๑. หัวหน้าส่วนงานทำหน้าที่กำหนดผู้รับผิดชอบและขั้นตอนในการปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๒ ให้ผู้รับผิดชอบที่ได้รับมอบหมายจากหัวหน้าส่วนงาน เป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๒.๓. ผู้ดูแลระบบเทคโนโลยีสารสนเทศของคณะ สำนัก สถาบัน เป็นผู้กำหนดสิทธิการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๔. ผู้ดูแลระบบเทคโนโลยีสารสนเทศของคณะ สำนัก สถาบัน กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๒.๕. หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายและอุปกรณ์ต่อพ่วงต่าง ๆ จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

๓. การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๓.๑. การจัดทำบริเวณล้อมรอบ (Physical security perimeter)

๓.๑.๑. มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในห้องระบบสารสนเทศ

๓.๑.๒. มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

๓.๑.๓. ผนังล้อมรอบของพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน ควรสร้างเป็นผนังทึบ

๓.๑.๔. ประตูหรือทางเข้าสำนักงานหรืออาคาร ควรออกแบบเพื่อป้องกันการบุกรุกทางกายภาพ

๓.๑.๕. ประตูหรือทางเข้าของห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

๓.๑.๖. บุคลากรที่ปฏิบัติงานภายในกลุ่มเทคโนโลยีสารสนเทศ ต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอ ภายหลังเลิกงาน และนอกเวลาราชการ

๓.๑.๗. มีการจัดระบบการรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัย (รปภ.) และมีการติดตั้งกล้องวงจรปิดภายในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย เพื่อควบคุมการเข้าถึงของบุคคลภายนอก

๓.๑.๘. ประตูหนีไฟและผนังในบริเวณข้างเคียงต้องมีการก่อสร้างให้มีความทนทานต่อความร้อนอย่างเพียงพอ

๓.๑.๙. ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศของหน่วยงานจากพื้นที่ให้บริการแก่ผู้รับบริการภายนอก

๓.๒. การจัดบริเวณสำหรับการเข้าถึง หรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public access, deliver, and loading areas)

๓.๒.๑. จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๒.๒. จำกัดบุคลากรซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๓.๒.๓. จัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของระบบเทคโนโลยีสารสนเทศหรือห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

๓.๒.๔. ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

๓.๒.๕. กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก โดยให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

๓.๓. การจัดวางและการป้องกันอุปกรณ์ (Equipment location and protection)

๓.๓.๑. ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของผู้ปฏิบัติงานในหน่วยงานให้น้อยที่สุด

๓.๓.๒. ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลที่สำคัญในระบบนั้น โดยบุคคลภายนอก เช่น การหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลภายนอกมองเห็นหน้าจอนั้นได้

๓.๓.๓. ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย

๓.๓.๔. ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ห้องควบคุมระบบคอมพิวเตอร์

๓.๓.๕. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบคอมพิวเตอร์เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบว่าระดับอุณหภูมิ อยู่ในระดับปกติหรือไม่ หรือมีน้ำรั่ว

๓.๓.๖. มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายที่เกิดจากกระแสไฟฟ้าไม่แน่นอน หรือความไม่สม่ำเสมอของกระแสไฟฟ้า

๓.๔. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting utilities)

๓.๔.๑. ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อความต้องการใช้งาน เช่น ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้าสำรอง เป็นต้น และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอเพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๓.๔.๒. ต้องมีการใช้ระบบสำรองไฟกับระบบเทคโนโลยีสารสนเทศเพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้าและต้องทดสอบระบบสำรองไฟอย่างสม่ำเสมอโดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

๓.๕. การรักษาความมั่นคงปลอดภัยสำหรับห้องทำงาน และทรัพย์สินอื่นๆของระบบเทคโนโลยีสารสนเทศ

๓.๕.๑. เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สินของหน่วยงาน

๓.๕.๒. เจ้าหน้าที่ต้องออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

๓.๕.๓. ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของราชการ

๓.๕.๔. ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่างๆ โดยไม่ได้รับอนุญาต เช่น เครื่องคอมพิวเตอร์ กล้องดิจิตอล เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

๓.๕.๕. นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

ส่วนที่ ๕
การควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการให้หน่วยงานและผู้ใช้งานจะต้องปฏิบัติตามข้อกำหนดของการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย เพื่อให้การใช้งานระบบเครือข่ายเป็นไปด้วยความเรียบร้อย และป้องกันไม่ให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของมหาวิทยาลัย

๒. แนวทางปฏิบัติในการควบคุมการเข้าถึงและใช้บริการเครือข่าย (Policy on use of network services)

๒.๑ ผู้มีสิทธิใช้ระบบเครือข่ายของมหาวิทยาลัย ได้แก่ บุคลากรและนักศึกษาของมหาวิทยาลัย หรือหน่วยงานที่ได้รับอนุญาต หรือผู้ที่ได้รับอนุญาตจากมหาวิทยาลัยเท่านั้น

๒.๒ การใช้ระบบเครือข่ายของมหาวิทยาลัยจะต้องใช้งาน เพื่อการศึกษา การวิจัย และการให้บริการทางวิชาการตามนโยบายและภารกิจของมหาวิทยาลัย

๒.๓ ห้ามมิให้ใช้ระบบเครือข่ายที่ขัดต่อนโยบายของมหาวิทยาลัย หรือกฎระเบียบของมหาวิทยาลัย หรือกฎหมาย หรือศีลธรรมอันดีแห่งสาธารณชน

๒.๔ ห้ามมิให้ใช้ระบบเครือข่ายในการประกอบธุรกิจ เพื่อประโยชน์อื่นใดในเชิงธุรกิจ หรือการแสวงหาผลกำไร

๒.๕ ผู้ใดหรือหน่วยงานใดที่ทำการเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัย จะต้องดำเนินการและปฏิบัติตามระเบียบและข้อกำหนดการใช้งานที่ประกาศโดยมหาวิทยาลัย หรือหน่วยงานที่ได้รับมอบหมายให้ดูแลระบบเครือข่ายของมหาวิทยาลัยอย่างเคร่งครัด

๒.๖ ผู้ใดที่ใช้งานผิดจากวัตถุประสงค์หรือข้อกำหนดการใช้งานระบบเครือข่ายของมหาวิทยาลัย ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบต่อความเสียหายที่อาจเกิดขึ้นจากการใช้งานนั้น โดยมหาวิทยาลัยไม่มีส่วนร่วมรับผิดชอบต่อความเสียหายดังกล่าว

๒.๗ หน่วยงานหรือผู้ใดที่จะทำการเชื่อมต่อทางเครือข่ายการเข้าถึงหรือใช้งานเครือข่ายของมหาวิทยาลัยจะต้องได้รับอนุญาตจากมหาวิทยาลัยก่อน

๒.๘ หน่วยงานที่ทำการเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยหรือให้บริการระบบเครือข่ายจะต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ และปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ ตลอดจนถึงกฎหมาย หรือประกาศ หรือระเบียบอื่นใดที่เกี่ยวข้องอย่างเคร่งครัด

๓. **การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร** (User authentication for external connections)

๓.๑ ส่วนงานที่ทำการเชื่อมต่อกับระบบเครือข่ายจากภายนอก จะต้องมีระบบป้องกันและระบบรักษาความปลอดภัยด้านระบบเครือข่ายที่ดีพอ โดยจะต้องได้รับการตรวจสอบและได้รับอนุญาตจากมหาวิทยาลัยก่อน

๓.๒ ส่วนงานที่ให้บริการการเชื่อมต่อระบบเครือข่ายจากภายนอก จะต้องมีระบบการยืนยันตัวบุคคลก่อนการเข้าใช้งานเครือข่ายและระบบสารสนเทศขององค์กรได้

๓.๓ การเชื่อมต่อใดๆ จากระบบเครือข่ายภายนอกต้องมีกระบวนการในการเข้ารหัสข้อมูลเสมออย่างน้อยในขั้นตอนการพิสูจน์ตัวตน

๔. **การระบุอุปกรณ์บนเครือข่าย** (Equipment identification in networks)

๔.๑ อุปกรณ์เครือข่ายจะต้องทำการกำหนดชื่อหรือหมายเลข หรือหมายเลขไอพีที่สามารถระบุถึงอุปกรณ์บนเครือข่ายที่ให้บริการได้

๔.๒ มีรายการเพื่อระบุอุปกรณ์และข้อมูลรายละเอียดที่สำคัญของอุปกรณ์ระบบเครือข่ายทั้งหมด

๔.๓ มีระบบตรวจสอบการทำงานของอุปกรณ์ระบบเครือข่ายทั้งหมดเพื่อให้สามารถทราบสถานะการทำงานของอุปกรณ์ทั้งหมดได้

๕. **การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ** (Remote diagnostic and configuration port protection)

๕.๑ อุปกรณ์เครือข่ายจะต้องมีการตรวจสอบบัญชีผู้ใช้และรหัสผ่านก่อนเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ และหน่วยงานที่ดูแลสถานที่ติดตั้งอุปกรณ์เครือข่ายจะต้องดูแลรักษาความเรียบร้อยและตรวจสอบไม่ให้บุคคลที่ไม่มีส่วนเกี่ยวข้องเข้าถึงอุปกรณ์เครือข่ายได้

๕.๒ พอร์ตที่ใช้ในการปรับแต่งระบบแบบต่อตรงกับอุปกรณ์ระบบเครือข่ายต้องมีการป้องกันการเข้าถึงด้วยรหัสผู้ใช้งานและรหัสผ่าน

๕.๓ ส่วนงานที่มหาวิทยาลัยเชียงใหม่ได้มอบหมายให้ดูแลระบบเครือข่ายของมหาวิทยาลัยสามารถเข้าตรวจสอบอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยที่ติดตั้งในหน่วยงานใดๆ ได้ตลอดเวลา โดยแจ้งให้หน่วยงานนั้นๆ ทราบล่วงหน้า ซึ่งหน่วยงานที่ได้รับแจ้งจะต้องจัดให้ผู้มีหน้าที่ดูแลรับผิดชอบ เป็นผู้ประสานงานให้ความช่วยเหลือ และอำนวยความสะดวกตามสมควร

๖. **การแบ่งแยกเครือข่าย** (Segregation in networks)

๖.๑ การออกแบบและใช้งานระบบเครือข่ายจะต้องมีการแบ่งแยกเครือข่ายตามกลุ่มของผู้ใช้บริการ สารสนเทศตามลักษณะการใช้งานหรือระดับชั้นความลับของข้อมูล

๖.๒ มีการแบ่งแยกเครือข่ายย่อยสำหรับระบบที่มีความสำคัญสูง ได้แก่ ระบบเครือข่ายสำหรับระบบเครื่องแม่ข่าย เป็นต้น

๖.๓ กำหนดชุดหมายเลขไอพีให้เหมาะสมกับการใช้งานของระบบเครือข่ายทั่วไปและระบบเครือข่ายสำหรับเครื่องแม่ข่าย

๖.๔ การแบ่งแยกระบบเครือข่ายที่มีความสำคัญสูง ได้แก่ ระบบเครือข่ายสำหรับเครื่องแม่ข่ายต้องถูกแบ่งแยกโดยอุปกรณ์รักษาความปลอดภัยเครือข่าย(Firewall)

๗. **การควบคุมการเชื่อมต่อทางเครือข่าย** (Network connection control)

๗.๑ หน่วยงานที่ให้บริการระบบเครือข่าย จะต้องมีการติดตั้งระบบหรือวิธีการตรวจสอบและอนุญาตให้เฉพาะผู้มีสิทธิใช้งานสามารถเข้าถึงระบบเครือข่ายได้เท่านั้น

๗.๒ หน่วยงานที่มหาวิทยาลัยได้มอบหมายให้ดูแลระบบเครือข่ายของมหาวิทยาลัยมีอำนาจที่จะระงับ หรือยุติการให้บริการอย่างใด ๆ ในการใช้ระบบคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยที่ส่งผลหรืออาจส่งผลกระทบต่อระบบเครือข่ายของมหาวิทยาลัยได้

๘. **การควบคุมการจัดเส้นทางบนเครือข่าย** (Network routing control)

๘.๑ การควบคุมการจัดเส้นทางบนเครือข่าย ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับข้อปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามนโยบายและภารกิจของมหาวิทยาลัย

ส่วนที่ ๖
การควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่ความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจ ตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของส่วนงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

๒. แนวทางปฏิบัติในการกำหนดขั้นตอนการติดตั้งระบบปฏิบัติการ

๒.๑ การติดตั้งระบบปฏิบัติการต้องกระทำโดยเจ้าหน้าที่ที่รับผิดชอบในหน่วยงานนั้นๆ หรือผู้ที่ได้รับอนุญาต

๒.๒ แผ่น CD/DVD หรือสื่อบันทึกอื่นๆ ที่ใช้ในการติดตั้งระบบปฏิบัติการต้องเป็นแผ่นต้นฉบับหรือสำเนาจากผู้ผลิตที่ไม่มีการดัดแปลงหรือเปลี่ยนแปลงข้อมูลใดๆ ที่มีผลให้ละเมิดลิขสิทธิ์ หรือทำให้ระดับความปลอดภัยในการใช้งานลดลง

๒.๓ ควรทำการปรับปรุงระบบปฏิบัติการ ไดรเวอร์ (Driver) และเฟิร์มแวร์ (Firmware) เป็นระยะ ให้เป็นปัจจุบัน

๒.๔ กำหนดผู้ใช้งานและรหัสผ่านผู้ดูแลระบบ (Administrator) ให้มีความซับซ้อนที่ประกอบด้วยอักษรตัวใหญ่ตัวเลขตัวเลขและสัญลักษณ์ รวมไม่ต่ำกว่า ๘ ตัวอักษร และเป็นรหัสผ่านที่คาดเดาได้ยาก

๒.๕ การลงทะเบียนการใช้งานระบบปฏิบัติการและซอฟต์แวร์ (Software Activation) ที่สำคัญต้องกระทำโดยเจ้าหน้าที่ที่รับผิดชอบลิขสิทธิ์ซอฟต์แวร์ของส่วนงานหรือผู้ที่ได้รับมอบหมายหน้าที่โดยเฉพาะเท่านั้น

๒.๖ ควรติดตั้งซอฟต์แวร์โปรแกรมป้องกันการประสงค์ร้าย (Malware) ที่มีประสิทธิภาพสูงและมีปรับปรุงให้เป็นปัจจุบัน (update) อย่างสม่ำเสมอ

๓. การกำหนดขั้นตอนการปฏิบัติเพื่อการใช้งานที่มั่นคงปลอดภัย

๓.๑ ผู้ใช้งานต้องกำหนดรหัสผ่านในการเข้าใช้เครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓.๒ ผู้ติดตั้งระบบปฏิบัติการต้องเปิดระบบตรวจสอบรหัสผ่านอัตโนมัติแบบปลอดภัยขึ้นมาใช้งานเพื่อให้การกำหนดรหัสผ่านเป็นไปอย่างปลอดภัยและมีคุณภาพ

๓.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

๓.๔ ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่รหัสผู้ใช้งานและรหัสผ่าน

๓.๕ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

๓.๖ ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานานและเมื่อไม่มีการใช้เป็นเวลานานจนถึงเวลาที่กำหนดไว้ ให้ระบบปฏิบัติการทำการสิ้นสุดการใช้งานของผู้ใช้งานโดยอัตโนมัติทันที

๓.๗ ห้ามเปิดหรือใช้งานโปรแกรมที่มีความเสี่ยงที่จะก่อให้เกิดความเสียหายแก่ระบบ เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๘ ซอฟต์แวร์ที่หน่วยงานใช้มีลิขสิทธ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล จะถือเป็นความรับผิดชอบของผู้ใช้งานนั้นๆ แต่เพียงผู้เดียว

๓.๙ ซอฟต์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

๓.๑๐ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

๓.๑๑ ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม

๓.๑๒ ห้ามผู้ใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ส่วนที่ ๗
การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ
(Application and Information Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศของหน่วยงาน จากบุคคล หรือโปรแกรมชุดคำสั่ง อันไม่พึงประสงค์ ที่ทำให้เสี่ยงหรือเกิดความเสียหายต่อข้อมูล หรือ ระบบสารสนเทศ ให้สามารถตามสอบที่มาของการเข้าถึงระบบสารสนเทศโดยไม่พึงประสงค์เหล่านั้นได้

๒. แนวทางปฏิบัติในการจำกัดการเข้าถึงสารสนเทศ (Information Access Control)

๒.๑. หัวหน้าส่วนงานทำหน้าที่กำหนดนโยบายการจำกัดการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ

๒.๒. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนในการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัย ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๓. ผู้ดูแลระบบควรกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบสารสนเทศเพื่อการจัดการมหาวิทยาลัย (CMU MIS) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๔. ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ (Limitation Of Connection Time) ที่ใช้ในการปฏิบัติงานและการเข้าถึงระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกินกว่าเวลาที่กำหนด ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการ Log in เข้าระบบสารสนเทศอีกครั้ง

๒.๕. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๒.๕.๑. กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๕.๒. ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-Mail) ตลอดจน IT Account ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๒.๕.๓. ส่วนงานผู้ให้บริการระบบสารสนเทศต้องกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน

๒.๕.๔. กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึงตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย หรือ หน่วยงาน

๒.๕.๕. ผู้ดูแลระบบสารสนเทศ ต้องดำเนินการกำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานที่ไม่ซ้ำกัน

๒.๕.๖. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๖. ผู้ดูแลระบบควรบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานในแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๒.๖.๑. ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๒.๖.๒. ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๖.๓. กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๖.๔. การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL หรือ XML Encryption เป็นต้น

๒.๖.๕. กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๒.๖.๖. กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๓. **การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ** (Limitation of connection time)

๓.๑. ผู้ดูแลระบบต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งานเพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้นในการเชื่อมต่อแต่ละครั้ง

๓.๒. ผู้ดูแลระบบต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งาน มีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้

๔. **การจัดการกับระบบซึ่งไวต่อการรบกวน**

๔.๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ได้แก่ ระบบงบประมาณ พัสดุ การเงิน และบัญชีกองทุน โดยเกณฑ์พึงรับ-พึงจ่าย ลักษณะ ๓ มิติ หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ จะได้รับการแยกออกจากระบบสารสนเทศอื่น ๆ ของมหาวิทยาลัย

๔.๒. ระบบซึ่งไวต่อการรบกวน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๕. **การปฏิบัติงานจากภายนอกสำนักงาน** (Teleworking)

๕.๑. หัวหน้าส่วนงาน ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่างๆ ภายในองค์กร ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๕.๒. หัวหน้าส่วนงาน ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานของมหาวิทยาลัย

๕.๓. หัวหน้าส่วนงาน ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยในสถานที่ดังกล่าว

๕.๔. ผู้ดูแลระบบ (System Administrator) ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่มหาวิทยาลัยต้องการ

๕.๕. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

๕.๖. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำ สำหรับการปฏิบัติงานจากอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ของมหาวิทยาลัยที่อนุญาตให้เข้าถึงได้จากอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

ส่วนที่ ๘
การสำรองและการกู้คืนข้อมูล
(Data Backup and Recovery)

๑. วัตถุประสงค์

เพื่อกำหนดข้อปฏิบัติเกี่ยวกับการสำรองข้อมูลและการกู้คืนระบบ โดยมีวัตถุประสงค์เพื่อให้ผู้ดูแลระบบคอมพิวเตอร์และระบบเครือข่ายสามารถดำเนินการสำรองข้อมูลได้อย่างถูกต้องและสามารถกู้คืนระบบได้ในกรณีที่จำเป็น เมื่อพบว่าระบบไม่สามารถทำงานได้อย่างปกติ

๒. แนวทางการปฏิบัติงานการสำรองข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย

๒.๑. หัวหน้าส่วนงานทำหน้าที่กำหนดนโยบายในการสำรองข้อมูลระบบคอมพิวเตอร์และระบบเครือข่าย

๒.๒ ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่ทำการสำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของมหาวิทยาลัย

๒.๓ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ ต้องทำการบันทึก รายละเอียดเกี่ยวกับการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่ทำการบันทึก

๒.๔ มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติงานจะแยกตามระบบสารสนเทศแต่ละระบบ

๒.๕ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีแก้ไขด้วย

๒.๖ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้ ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

๒.๗ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหาและรายงานต่อหัวหน้างานตามลำดับชั้น

๒.๘ ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลแบ่งเป็นสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๒.๙ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอน Backup Procedure โดยเคร่งครัด

๓. การปฏิบัติเกี่ยวกับการสำรองข้อมูล

๓.๑. ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่ ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
Mail server	ค่า Configuration	ก่อนและหลังเปลี่ยนแปลง
	ข้อมูลในเมล์บ็อกซ์	อย่างน้อย 1 สัปดาห์
Web server	ค่า Configuration	ก่อนและหลังเปลี่ยนแปลง
	ข้อมูลเผยแพร่บนเว็ปไซต์	อย่างน้อย 1 สัปดาห์
Database server	ค่า Configuration	ก่อนและหลังเปลี่ยนแปลง
	ข้อมูลของระบบฐานข้อมูลของระบบที่สำคัญ	อย่างน้อย 1 สัปดาห์
Firewall server	ค่า Configuration	ก่อนและหลังเปลี่ยนแปลง
	ข้อมูลกฎ ของ firewall	อย่างน้อย 1 สัปดาห์
Server อื่น ๆ เช่น ระบบงานต่าง ๆ	ค่า Configuration	ก่อนและหลังเปลี่ยนแปลง
	ข้อมูลบนเครื่องแม่ข่ายอื่น ๆ	อย่างน้อย 1 สัปดาห์
หมายเหตุ ทุกรายการที่ปรากฏในตารางจะใช้วิธีสำรองข้อมูลเต็มรูปแบบ (Full Backup)		

๓.๒. ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองเพื่อเป็นการยืนยันว่า การแบ็คอัพตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

๔. การกู้คืนระบบ

๔.๑. ในกรณีที่พบปัญหาที่ส่งผลให้เกิดความผิดพลาดหรือความเสียหายต่อระบบคอมพิวเตอร์และ/ หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงานต่อหัวหน้ากลุ่มเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากหัวหน้ากลุ่มเทคโนโลยีสารสนเทศทราบ

๔.๒. ให้ทำการกู้คืนข้อมูลที่ได้สำรองไว้ โดยให้ยึดเอาข้อมูลที่ทันสมัยที่สุด (Latest Update) หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๔.๓. หากมีความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายที่กระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานให้ทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการกู้คืนระบบเสร็จสิ้นอย่างสมบูรณ์

๔.๔. ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

๕. การจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan)

นโยบายเกี่ยวกับการจัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศ (IT Contingency Plan) หัวหน้าส่วนงานต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการ ดังต่อไปนี้

๕.๑. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕.๒. กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

๕.๓. ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัดหรือไม่สามารถใช้งานได้อันเป็นผลจากภัยพิบัติที่กำหนดไว้

๕.๔. จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

๕.๕. ให้มีการทดสอบ ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๙
การควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์
(Computing System Control Room)

๑. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับโดยมาตรการนี้ จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๒. แนวทางปฏิบัติในการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ (Computing System Control Room)

๒.๑ หัวหน้าส่วนงานมีหน้าที่กำหนดนโยบายการควบคุมการเข้าออกห้องควบคุมระบบคอมพิวเตอร์ภายในส่วนงาน

๒.๒ หน่วยงานต้องมีการจำแนกและกำหนดพื้นที่ของเครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย ระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสมโดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๒.๓ กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและเครือข่ายให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General working area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data storage area)เป็นต้น

๒.๔ ควรกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถมีมีสิทธิในการเข้าถึงพื้นที่เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย

๒.๔.๑. จัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๒.๔.๒. กำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออก ดังกล่าวโดยจัดทำเป็นเอกสาร“บันทึกการเข้าออกพื้นที่”

๒.๔.๓. จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศ ปีละ ๑ ครั้ง เป็นอย่างน้อย

๒.๕. บุคคลภายนอกเข้ามาติดต่อต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้า-ออกให้ถูกต้องและจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๖. บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

ส่วนที่ ๑๐
การประเมินความเสี่ยงและการควบคุม
(Risk Assessment and Control)

๑. วัตถุประสงค์

ติดตาม ตรวจสอบ และประเมินความเสี่ยงอย่างเป็นระบบโดยคำนึงถึงเป้าหมายขององค์กรโดยความร่วมมือจากทุกส่วนงาน ทุกระดับ เพื่อให้เหตุการณ์และจุดอ่อนที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศของมหาวิทยาลัย ได้รับการดำเนินการที่ถูกต้องในช่วงระยะเวลาที่เหมาะสม

๒. แนวทางการปฏิบัติการบริหารความเสี่ยง

๒.๑ หัวหน้าส่วนงานทำหน้าที่กำหนดนโยบายในการตรวจสอบและประเมินความเสี่ยง

๒.๒ จัดทำกระบวนการบริหารจัดการความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ภายใต้กระบวนการ PDCA ดังนี้

๒.๒.๑ การกำหนดระบบการบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ (Plan)

- กำหนดแนวทางและแผนความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ
- กำหนดโครงสร้างการบริหารความเสี่ยง
- กำหนดขอบเขตและวัตถุประสงค์ของระบบการบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ โดยพิจารณาจากลักษณะสภาพแวดล้อม การดำเนินงาน ทรัพย์สิน และเทคโนโลยีที่มหาวิทยาลัยมีอยู่
- กำหนดนโยบายความมั่นคงปลอดภัยสอดคล้องตามขอบเขตและวัตถุประสงค์ที่กำหนด และควรบันทึกเป็นลายลักษณ์อักษร
- กำหนดแผนและขั้นตอนการปฏิบัติสำหรับการบริหารจัดการความเสี่ยงสำหรับทรัพย์สินสารสนเทศของมหาวิทยาลัยโดยพิจารณาจากวัตถุประสงค์
- จัดทำแผนการบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ
- นำเสนอภาพรวม และขออนุมัติสำหรับความเสี่ยงที่ยังหลงเหลืออยู่

- จัดทำเอกสารรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย (Statement of Applicability)
- กำหนดคำนิยามที่เกี่ยวข้องกับความเสี่ยง และการบริหารความเสี่ยงเป็นแบบเดียวกัน เพื่อให้เกิดประสิทธิภาพในการกำหนดวัตถุประสงค์ นโยบาย กระบวนการ เพื่อใช้ในการบ่งชี้และประเมินความเสี่ยง
- กำหนดมาตรการการจัดการความเสี่ยง การลดความเสี่ยง (สามารถเลือกใช้มาตรฐานใดมาตรฐานหนึ่งมาใช้ในการลดความเสี่ยง)
- กำหนดหน้าที่และความรับผิดชอบตามโครงสร้างการบริหารความเสี่ยง

๒.๒.๒ การดำเนินการจัดทำระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ (Do)

- ปฏิบัติตามแผนที่ได้กำหนดไว้
- สร้างกระบวนการโดยมีขั้นตอนสนับสนุนให้เกิดตัวบ่งชี้ การประเมิน การจัดการ และการรายงานความเสี่ยงอย่างต่อเนื่อง เพื่อลดโอกาสที่จะเกิดความเสี่ยง หรือลดความเสียหายของผลกระทบ
- กำหนดแผนการติดตาม ตรวจสอบและประเมินความเสี่ยง การวัดผลสัมฤทธิ์ของระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศเพื่อใช้ในการติดตามประเมินผลในภาพรวม
- ดำเนินการฝึกอบรมและสร้างความตระหนัก เพื่อให้ความรู้แก่บุคลากรเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างมีประสิทธิภาพ ประสิทธิผล รวมทั้งระบบสารสนเทศมีความปลอดภัยจากความเสี่ยง
- บริหารจัดการทรัพยากรต่าง ๆ เพื่อการดำเนินงานรักษาความปลอดภัยของระบบฐานข้อมูลและสารสนเทศ ภายใต้ขอบเขตเพื่อให้เป็นไปตามนโยบายและแนวปฏิบัติด้านความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศ
- จัดทำคู่มือการปฏิบัติ และ/หรือ มาตรการที่จำเป็นสำหรับติดตามประเมินผล และบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ (Security incident management procedures and controls) ที่อาจเกิดขึ้น รวมทั้งกำหนดผู้รับผิดชอบและผู้เกี่ยวข้องให้ปฏิบัติตามโดยเคร่งครัด

- กำหนดระยะเวลาการรายงานความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ
- ประเมินความเสี่ยง กำหนดทางเลือกในการจัดการกับความเสี่ยง และกำหนดมาตรการลดความเสี่ยง (สามารถนำมาตรการต่าง ๆ ในมาตรฐาน ISO/IEC ๒๗๐๐๑ มาใช้ในการลดความเสี่ยง)

๒.๒.๓ การเฝ้าระวังและทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ (Check)

- ดำเนินการตามขั้นตอนปฏิบัติและมาตรการในการเฝ้าระวังและติดตาม (ที่กำหนดไว้ในนโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ) เช่น ตรวจหาข้อผิดพลาดจากการประมวลผล ตรวจหาการละเมิดหรือความพยายามในการละเมิดความมั่นคงปลอดภัย ตรวจหาเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น ตรวจสอบการดำเนินการจัดการกับเหตุการณ์การละเมิดความมั่นคงปลอดภัยที่ได้ดำเนินการไปแล้วได้ผลหรือไม่ เป็นต้น
- ดำเนินการทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศอย่างสม่ำเสมอ
- ดำเนินการทบทวนความสัมฤทธิ์ผลของระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศอย่างสม่ำเสมอ โดยพิจารณาจากแผนการจัดความสัมฤทธิ์ผลฯ เพื่อให้เป็นไปตามเป้าหมายหรือตัวชี้วัดที่กำหนดไว้ในแผน
- ทบทวนผลการประเมินความเสี่ยงของระบบฐานข้อมูลสารสนเทศเป็นระยะ (เช่น ทุก ๓ เดือน ๖ เดือน) ทบทวนระดับความเสี่ยงที่ยังเหลืออยู่ และระดับความเสี่ยงที่ยอมรับได้ ตามการเปลี่ยนแปลงต่าง ๆ ที่เกิดขึ้นกับมหาวิทยาลัย เทคโนโลยีที่ใช้ วัตถุประสงค์และกระบวนการของมหาวิทยาลัย ภัยคุกคามที่มีการระบุเพิ่มเติมหรือเปลี่ยนแปลง ความสัมฤทธิ์ผลของมาตรการต่าง ๆ ที่ใช้ ตลอดจนการเปลี่ยนแปลงจากเหตุการณ์ภายนอก
- ติดตาม ตรวจสอบ ประเมินระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศตามรอบระยะเวลาที่กำหนดไว้
- บันทึกข้อมูลการดำเนินการและเหตุการณ์ต่าง ๆ ที่อาจมีผลกระทบต่อความสัมฤทธิ์ผลหรือประสิทธิภาพของระบบบริหารจัดการความมั่นคง

ปลอดภัยของระบบฐานข้อมูลและสารสนเทศ เช่น การประชุมทบทวนด้านความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศโดยระดับบริหารของมหาวิทยาลัย จัดทำรายงานการประชุมและแจ้งเวียนมติให้ผู้ที่เกี่ยวข้องได้รับทราบและปฏิบัติตาม การปฏิบัติตามนโยบายและขั้นตอนปฏิบัติต่าง ๆ ในนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัย ให้ผู้รับผิดชอบบันทึกหลักฐานการปฏิบัติตามนโยบายและขั้นตอนการปฏิบัติเหล่านั้นไว้ เพื่อให้สามารถติดตามและตรวจสอบได้ในภายหลัง

๒.๒.๔ การทบทวนและปรับปรุงระบบการบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ (Act)

- ปรับปรุงระบบบริหารจัดการด้านความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศตามผลของการเฝ้าระวัง ติดตามประเมินผล และทบทวนระบบบริหารจัดการความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ เช่น การปฏิบัติตามมติการประชุมทบทวนโดยผู้บริหาร การปรับปรุงนโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ การจัดการหรือแก้ไขความไม่สอดคล้องกับนโยบายความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศ การกำหนดมาตรการเพิ่มเติมเพื่อลดการเกิดขึ้นของเหตุการณ์ด้านความมั่นคงปลอดภัยของระบบฐานข้อมูลและสารสนเทศสารสนเทศที่เคยเกิดขึ้นแล้ว การปฏิบัติตามแผนการลดความเสี่ยง การปฏิบัติตามแผนด้านความมั่นคงปลอดภัย การปฏิบัติตามคำแนะนำและผลตอบกลับจากผู้ที่เกี่ยวข้อง เป็นต้น
- แจ้งการปรับปรุงและดำเนินการให้แก่ทุกหน่วยงานที่เกี่ยวข้องทราบ โดยให้รายละเอียดที่เพียงพอและเหมาะสมตรวจสอบว่าการปรับปรุงที่ได้ดำเนินการไปแล้วนั้น บรรลุผลตามที่ต้องการหรือไม่
- ปรับปรุงแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ

๒.๓ การวางแผนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ ดังนี้

๒.๓.๑ จัดทำแผนการบริหารความเสี่ยง เพื่อกำจัด ป้องกันหรือลดการเลิกความเสียหายในรูปแบบต่าง ๆ โดยสามารถฟื้นฟูระบบสารสนเทศ การสำรอง และกู้คืนข้อมูลจากความเสียหาย (Backup and Recovery)

๒.๓.๒ จัดทำแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดกับระบบสารสนเทศ (IT Contingency Plan)

๒.๓.๓ จัดทำแผนการรักษาความมั่นคงปลอดภัย (Security) ของระบบฐานข้อมูลและสารสนเทศ เช่น ระบบป้องกันไวรัส ระบบไฟฟ้าสำรอง เป็นต้น

๒.๓.๔ กำหนดนโยบายในการให้สิทธิผู้ใช้งานในแต่ละระดับ (Access Rights)

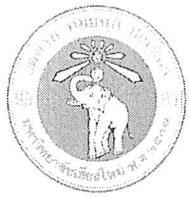
๒.๔ ทบทวนระบบบริหารความเสี่ยงของระบบฐานข้อมูลและสารสนเทศเป็นประจำทุกปี อย่างน้อยปีละ ๑ ครั้ง

๒.๕ จะต้องมีการตรวจสอบและประเมินความเสี่ยงโดยผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง

ภาคผนวก

แบบฟอร์มสำหรับการขอใช้บริการเทคโนโลยีสารสนเทศ

แบบฟอร์ม มช.-๐๐๑



แบบฟอร์ม การขอใช้บริการติดตั้ง ซ่อมบำรุงเครื่องคอมพิวเตอร์และตรวจสอบระบบงาน มหาวิทยาลัยเชียงใหม่

<u>ส่วนที่ ๑</u> สำหรับผู้ขอใช้บริการ

ข้าพเจ้า (นาย/นาง/นางสาว) .....ตำแหน่ง.....

หน่วยงานสังกัด.....

ขอแจ้งใช้บริการ

☐ ซ่อม ☐ ตรวจเช็คระบบ ☐ ย้าย – ติดตั้งเครื่องคอมพิวเตอร์

☐ Hardware ระบุ ..... ☐ Software ระบุ ..... ☐

ระบบงาน อื่นๆ ระบุ .....

อาการของเครื่องคอมพิวเตอร์ / ลักษณะปัญหาการใช้ระบบงาน

.....

.....

.....

ลงชื่อ..... (ผู้ขอใช้บริการ) ลงชื่อ.....(ผู้มีอำนาจลงนาม)

(.....) (.....)

ตำแหน่ง ..... ตำแหน่ง .....

วันที่..... วันที่.....

ส่วนที่ ๒ สำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ วันที่รับเรื่อง...../...../..... เวลา .....

ชื่อผู้ดำเนินการ .....สถานที่ดำเนินงาน .....

วันที่ดำเนินการ ...../...../..... เวลา ..... เสร็จวันที่ ...../...../..... เวลา .....

ผลการปฏิบัติงาน .....

.....

.....

.....

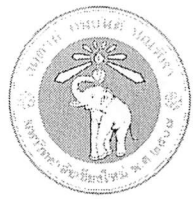
หมายเลขเครื่อง (Serial No.) ..... รหัสครุภัณฑ์ .....หมายเลข IP Address.....

ลงชื่อ.....(ผู้ดำเนินการ) ลงชื่อ.....(ผู้มีอำนาจลงนาม)

(.....) (.....)

วันที่..... วันที่.....

แบบฟอร์ม มช.-๐๐๒



แบบฟอร์ม การขอชื่อผู้ใช้และรหัสผ่านเพื่อใช้งาน
มหาวิทยาลัยเชียงใหม่

<u>ส่วนที่ ๑</u> สำหรับผู้ขอใช้บริการ

คำนำหน้า : ☐ นาย ☐ นาง ☐ นางสาว

ชื่อ (ไทย) .....นามสกุล (ไทย).....

Title : ☐ Mr. ☐ Mrs. ☐ Ms.

First Name (English) : .....Last Name (English) : .....

หมายเลขประจำตัวประชาชน ๑๓ หลัก

☐ ☐☐☐☐-☐☐☐☐☐-☐☐-☐

ตำแหน่ง .....

สังกัด.....

ระบบงานที่ขอใช้ .....

เหตุผลการขอใช้.....

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้นเป็นความจริงทุกประการและจะปฏิบัติตามระเบียบข้อกำหนด และนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยทุกประการ

ลงชื่อ..... (ผู้ขอใช้บริการ)
(.....)
ตำแหน่ง .....
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
ตำแหน่ง .....
วันที่.....

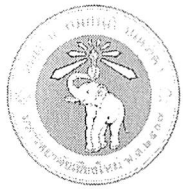
ส่วนที่ ๒ สำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ วันที่รับเรื่อง...../...../..... เวลา .....

ได้ดำเนินการสร้างชื่อผู้ใช้และรหัสผ่านเพื่อใช้งานระบบสารสนเทศของมหาวิทยาลัยเรียบร้อยแล้ว และแจ้งให้ผู้ขอรับบริการทาง .....

ลงชื่อ.....(ผู้ดำเนินการ)
(.....)
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
วันที่.....

แบบฟอร์ม มช.-๐๐๓



แบบฟอร์ม การขอชื่อผู้ใช้และรหัสผ่านเพื่อใช้งานอินเทอร์เน็ต
มหาวิทยาลัยเชียงใหม่

<u>ส่วนที่ ๑</u> สำหรับผู้ขอใช้บริการ

คำนำหน้า : ☐ นาย ☐ นาง ☐ นางสาว

ชื่อ (ไทย) .....นามสกุล (ไทย).....

Title : ☐ Mr. ☐ Mrs. ☐ Ms.

First Name (English) : .....Last Name (English) : .....

หมายเลขประจำตัวประชาชน ๑๓ หลัก

☐ ☐☐☐☐-☐☐☐☐☐-☐☐-☐

ตำแหน่ง .....

สังกัด.....

ระบบงานที่ขอใช้.....

เหตุผลการขอใช้.....

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้นเป็นความจริงทุกประการและจะปฏิบัติตามระเบียบข้อกำหนด ตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ทุกประการ

ลงชื่อ..... (ผู้ขอใช้บริการ)
(.....)
ตำแหน่ง .....
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
ตำแหน่ง .....
วันที่.....

ส่วนที่ ๒ สำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ วันที่รับเรื่อง...../...../..... เวลา .....

ได้ดำเนินการสร้างชื่อผู้ใช้และรหัสผ่านเพื่อใช้งานอินเทอร์เน็ตของมหาวิทยาลัยเรียบร้อยแล้ว และแจ้งให้ผู้ขอรับบริการทาง .....

ลงชื่อ.....(ผู้ดำเนินการ)
(.....)
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
วันที่.....

แบบฟอร์ม มช.-๐๐๔

แบบฟอร์ม การขอใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail address)

มหาวิทยาลัยเชียงใหม่

<u>ส่วนที่ ๑</u> สำหรับผู้ขอใช้บริการ

คำนำหน้า : ☐ นาย ☐ นาง ☐ นางสาว

ชื่อ (ไทย) .....นามสกุล (ไทย).....

Title : ☐ Mr. ☐ Mrs. ☐ Ms.

First Name (English) : .....Last Name (English) : .....

หมายเลขประจำตัวประชาชน ๑๓ หลัก

☐ ☐☐☐☐-☐☐☐☐☐-☐☐-☐

ตำแหน่ง .....

สังกัด.....

ระบบงานที่ขอใช้.....

เหตุผลการขอใช้.....

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้นเป็นความจริงทุกประการและจะปฏิบัติตามระเบียบข้อกำหนด ตาม พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ทุกประการ

ลงชื่อ..... (ผู้ขอใช้บริการ) ลงชื่อ.....(ผู้มีอำนาจลงนาม)

(.....) (.....)

ตำแหน่ง ..... ตำแหน่ง .....

วันที่..... วันที่.....

ส่วนที่ ๒ สำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ วันที่รับเรื่อง...../...../..... เวลา .....

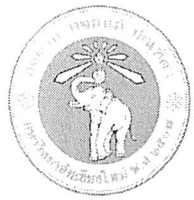
ได้ดำเนินการสร้างชื่อผู้ใช้และรหัสผ่านเพื่อใช้งานอินเทอร์เน็ตของมหาวิทยาลัยเรียบร้อยแล้ว และแจ้งให้ผู้ขอรับบริการทาง .....

ลงชื่อ.....(ผู้ดำเนินการ) ลงชื่อ.....(ผู้มีอำนาจลงนาม)

(.....) (.....)

วันที่..... วันที่.....

แบบฟอร์ม มช.-๐๐๕



แบบฟอร์ม การขอใช้บริการติดตั้ง ซ่อมบำรุงเครื่องคอมพิวเตอร์และตรวจสอบระบบงาน มหาวิทยาลัยเชียงใหม่

<u>ส่วนที่ ๑</u> สำหรับผู้ขอใช้บริการ

ข้าพเจ้า (นาย/นาง/นางสาว) .....ตำแหน่ง.....

สังกัด.....

มีความประสงค์ขอนำเครื่องคอมพิวเตอร์เชื่อมต่อกับเครือข่ายของมหาวิทยาลัยฯ เพื่อใช้ในงาน.....

.....

โดยมีรายละเอียดดังนี้

☐ ติดตั้งสายสัญญาณเครือข่าย (LAN) ระบุจำนวนจุดติดตั้ง.....

☐ เครื่องคอมพิวเตอร์ตั้งโต๊ะ (PC) ระบุคุณสมบัติของเครื่อง .....

MacAddress .....

☐ เครื่องคอมพิวเตอร์พกพา (Notebook) ระบุคุณสมบัติของเครื่อง .....

MacAddress .....

☐ สถานที่ติดตั้ง .....

ข้าพเจ้าขอรับรองว่าข้อมูลข้างต้น เป็นความจริงทุกประการ และจะปฏิบัติตามระเบียบข้อกำหนด และนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยทุกประการ

ลงชื่อ..... (ผู้ขอใช้บริการ)
(.....)
ตำแหน่ง .....
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
ตำแหน่ง .....
วันที่.....

ส่วนที่ ๒ สำหรับผู้ใช้งานเทคโนโลยีสารสนเทศ วันที่รับเรื่อง...../...../..... เวลา .....

ได้ดำเนินการติดตั้งสายสัญญาณเครือข่ายตามร้องขอ จำนวน .....จุด และกำหนดหมายเลข IP Address คือ .....และตรวจสอบด้านความปลอดภัยของเครื่องคอมพิวเตอร์เรียบร้อยแล้ว ผู้ใช้สามารถใช้งานและบริการต่าง ๆ ผ่านระบบเครือข่ายได้

ลงชื่อ.....(ผู้ดำเนินการ)
(.....)
วันที่.....

ลงชื่อ.....(ผู้มีอำนาจลงนาม)
(.....)
วันที่.....