ประกาศสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
เรื่อง นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย จัดทำขึ้นเพื่อกำหนดแนวทางไว้เป็นกรอบและเป็นแผนที่นำทางในระดับกลยุทธ์ เพื่อยกระดับมาตรฐานการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ให้อยู่ระดับมาตรฐานสากลโดยอ้างอิงจากกรอบมาตรฐานสากล ISO/IEC 27001 อีกทั้งต้องการลดผลกระทบจากเหตุ ตลอดจนการกู้คืนระบบอย่างรวดเร็วหลังจากการโจมตีสิ้นสุดลงแล้ว และเป็นแนวทางปฏิบัติของผู้ใช้งานเทคโนโลยีสารสนเทศและเครือข่าย มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร โดยมีรายละเอียดดังต่อไปนี้

1. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและเครือข่าย เพื่อให้ระบบต่าง ๆ ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนครสามารถดำเนินการได้ต่อเนื่องและมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานเทคโนโลยีสารสนเทศและเครือข่ายที่ไม่ถูกต้อง ขาดความตระหนักในปัญหาที่อาจจะเกิดขึ้นของผู้ใช้งานภายในเอง หรือจากการถูกคุกคามจากภายนอก

มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครจึงเห็นสมควรกำหนดนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย โดยกำหนดให้มี มาตรฐาน (Standard) แนวปฏิบัติ (Guideline) และขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านต่าง ๆ

2. วัตถุประสงค์

2.1 เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานเทคโนโลยีสารสนเทศ โดยการคงไว้ด้วยความลับ ความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งาน (Availability) โดยจะต้องสามารถตรวจสอบความถูกต้อง (Authenticity) ความรับผิดชอบ (Accountability) ไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation) และมีความน่าเชื่อถือ (Reliability)

2.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศที่มีมาตรฐานและมีการปรับปรุงอย่างต่อเนื่อง

2.3 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้เทคโนโลยีสารสนเทศและเครือข่ายของมหาวิทยาลัย

3. นโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่าย

3.1 ส่งเสริมความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายของมหาวิทยาลัยให้สามารถตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัย

3.2 มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอเพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

3.3 เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

3.4 เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องทั้งของหน่วยงานเองและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

3.5 ติดตาม ตรวจสอบการดำเนินงานและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศและเครือข่ายให้สอดคล้องตามการเปลี่ยนแปลงของโลก

4. องค์ประกอบของนโยบาย

4.1 คำนิยาม

4.2 นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย

- 4.2.1 ระบบสารสนเทศ
- 4.2.2 ระบบเครือข่าย
- 4.2.3 โปรแกรมประยุกต์
- 4.2.4 ระบบปฏิบัติการ
- 4.2.5 ด้านกายภาพ

4.3 นโยบายในการรักษาความมั่นคงปลอดภัยของผู้ใช้งาน

- 4.3.1 แนวปฏิบัติของผู้ใช้งาน
- 4.3.2 ข้อห้ามสำหรับผู้ใช้งาน
- 4.3.3 บทลงโทษเมื่อกระทำผิด

4.4 แผนสำรองข้อมูลสารสนเทศและเตรียมความพร้อมกรณีฉุกเฉิน

- 4.4.1 แผนสำรองข้อมูลเพื่อให้สารสนเทศอยู่ในสภาพพร้อมใช้งาน
- 4.4.2 แผนเตรียมพร้อมกรณีฉุกเฉิน

คำนิยาม

คำนิยามโดยทั่วไปที่ใช้ในนโยบายนี้ ประกอบด้วย

ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Cheif Information Officer: CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศ

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์และเครือข่ายภายในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

การรักษาความมั่นคงปลอดภัย หมายถึงการรักษา ข้อมูล สารสนเทศ และระบบคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร ให้คงไว้ด้วยความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และมีสภาพพร้อมใช้งาน (Availability) โดยจะต้องสามารถตรวจสอบความถูกต้อง (Authenticity) ความรับผิดชอบ (Accountability) ไม่สามารถปฏิเสธความรับผิดชอบ (Non-repudiation) และมีความน่าเชื่อถือ (Reliability)

มาตรฐาน หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

ขั้นตอนการปฏิบัติ หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

แนวปฏิบัติ หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้บริหาร หมายถึง ผู้มีอำนาจบริหารในระดับสูงของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร เช่น ผู้อำนวยการสถาบัน/สำนัก/กอง เป็นต้น

ผู้ใช้งาน หมายถึง บุคคลที่ได้รับอนุญาตให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศขององค์กร โดยมีสิทธิ์และหน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้บริหารของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่ความรับผิดชอบในการดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ เป็นต้น

นักศึกษา หมายถึง นักศึกษาที่กำลังศึกษาอยู่ในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

ศิษย์เก่า หมายถึง นักศึกษาเคยศึกษาอยู่ในมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

อาจารย์ หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานจ้างเหมา ที่ทำงานในสายวิชาการของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างชั่วคราว พนักงานจ้างเหมา ที่ทำงานในสายสนับสนุนของมหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร

หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอกที่มหาวิทยาลัยเทคโนโลยีราชมงคลพระนครอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

ข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ให้ข้อมูลในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

สารสนเทศ หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

ระบบคอมพิวเตอร์ หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

ระบบเครือข่าย หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ขององค์กรได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเตอร์เน็ต เป็นต้น

ระบบแลน และระบบอินทราเน็ต หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

ระบบอินเทอร์เน็ต หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

ระบบเทคโนโลยีสารสนเทศ หมายถึง ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้าง การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิ์ของผู้ใช้งาน หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

สินทรัพย์ หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางภายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าเกี่ยวข้องกับความมั่นคงปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหวและเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้

รหัสผ่าน หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

บัญชีผู้ใช้งานคอมพิวเตอร์ หมายถึง บัญชีผู้ใช้งาน นักศึกษา บุคลากร และบุคคลภายนอก เพื่อใช้ในการตรวจสอบยืนยันตัวตน (Authentication) ก่อนเข้าใช้งานระบบสารสนเทศและเครือข่ายภายในมหาวิทยาลัย

ระบบเครือข่ายเสมือน (Virtual Private Network : VPN) หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเตอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

คำนิยามของประเภทข้อมูล และชั้นความลับ

คำนิยามของประเภทข้อมูล และชั้นความลับ ประกอบด้วย

นิยามประเภทของข้อมูล

ข้อมูลนักศึกษา หมายถึง ข้อมูลที่เกี่ยวข้องกับนักศึกษาทั้งหมด เช่น ประวัติ ข้อมูลส่วนตัว ข้อมูลลงทะเบียน ข้อมูลการวิจัยของนักศึกษาที่ยังไม่เผยแพร่ ผลการเรียน และกิจกรรมนักศึกษา เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

ข้อมูลบุคลากร หมายถึง ข้อมูลที่เกี่ยวข้องกับอาจารย์ และเจ้าหน้าที่ทั้งหมด เช่น ประวัติ ข้อมูลส่วนตัว เงินเดือน ข้อมูลการวิจัยของอาจารย์ที่ยังไม่เผยแพร่ การลา การเลื่อนขั้น และตำแหน่ง เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

ข้อมูลการเงิน หมายถึง ข้อมูลที่เกี่ยวข้องกับการเงิน เช่น งบประมาณ การเงิน บัญชี เบิกจ่าย และพัสดุ เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

ข้อมูลการบริหาร หมายถึง ข้อมูลที่เกี่ยวข้องกับการบริหารมหาวิทยาลัย นโยบาย โครงการ และการดำเนินงานต่าง ๆ ที่ยังไม่ควรเปิดเผยในขณะนี้ เช่น ร่างนโยบายที่อยู่ระหว่างการจัดทำ หนังสือแต่งตั้งคณะทำงาน ร่างหนังสือบันทึกข้อตกลง เป็นต้น จัดเป็นข้อมูลที่เป็นความลับ

ข้อมูลสาธารณะ หมายถึง ข้อมูลที่สามารถเผยแพร่ได้โดยไม่ก่อให้เกิดความเสียหาย และอาจจะช่วยในการส่งเสริมภาพลักษณ์ของมหาวิทยาลัย

นิยามชั้นความลับของข้อมูล

ข้อมูลความลับ หมายถึง ข้อมูลในระบบคอมพิวเตอร์ของมหาวิทยาลัยที่เมื่อถูกเผยแพร่ออกไปแล้วก่อให้เกิดความเสียหายหรือเสียประโยชน์ต่อมหาวิทยาลัย หรือเกิดความเสียหายหรือเสียประโยชน์ต่อบุคคลใดบุคคลหนึ่ง

นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรฐานในการควมคุมและรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย จากการเข้าถึงของผู้ใช้งานที่ถูกต้องตามบทบาทหน้าที่หรือภารกิจที่ได้รับมอบหมาย

2. นโยบายการเข้าถึงหรือควบคุมการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย

ในการควมคุมและรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศและเครือข่าย สามารถแบ่งออกเป็น 5 ด้าน ประกอบด้วย

2.1 ระบบสารสนเทศ

2.2 ระบบเครือข่าย

2.3 โปรแกรมประยุกต์

2.4 ระบบปฏิบัติการ

2.5 ด้านกายภาพ

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

1. วัตถุประสงค์

1.1 เพื่อควบคุมการเข้าถึง ระบบคอมพิวเตอร์ ข้อมูล หรืออุปกรณ์ต่าง ๆ โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

1.2 เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์และการมอบอำนาจของหน่วยงานที่รับผิดชอบ

1.3 เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจ สามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2. แนวปฏิบัติ

แนวปฏิบัติในการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ เป็นแนวปฏิบัติที่ระบุถึงแนวทางในภาพรวมในการควบคุมการเข้าใช้งานของผู้ใช้ที่มีหน้าที่รับผิดชอบต่อระบบคอมพิวเตอร์ ข้อมูล หรืออุปกรณ์ต่าง ๆ ดังนี้

2.1 ผู้ใช้งานภายใน

2.1.1 ระบบสารสนเทศใด ๆ ภายในมหาวิทยาลัย จะต้องมีผู้รับผิดชอบ เจ้าของ หรือผู้ดูแลระบบ ที่จะต้องทำหน้าที่ในการรักษาความมั่นคงปลอดภัยและกำหนดสิทธิ์การเข้าถึงให้แก่ผู้ใช้งานตามภารกิจ หรือตามความรับผิดชอบที่ได้รับมอบหมายอย่างเหมาะสม

2.1.2 ผู้ใช้งานที่ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงระบบสารสนเทศนั้น ๆ ได้ โดยจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่ปลอดภัย น่าเชื่อถือและเหมาะสมก่อนการเข้าใช้งานระบบสารสนเทศ

2.1.3 ผู้ใช้งานที่ได้รับสิทธิ์เข้าถึงระบบสารสนเทศ จะต้องได้รับมอบสิทธิ์ที่อยู่ในขอบเขตที่ตรงกับภาระหน้าที่ของผู้ใช้งานแต่ละคนและจะต้องไม่มอบสิทธิ์ที่มากกว่าภาระหน้าที่ความรับผิดชอบ (Authorization)

2.1.4 ในกรณีที่ผู้ใช้งานเข้าใช้งานระบบสารสนเทศที่มีความสำคัญ หรือระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ เช่น ข้อมูลการเงิน ข้อมูลบุคลากร ข้อมูลการบริหารและข้อมูลนักศึกษา จะต้องมีการจำกัดเวลาในการเชื่อมต่อเมื่อไม่มีการใช้งานระยะเวลาหนึ่ง จะต้องถูกบังคับให้ออกจากระบบ

2.1.5 ในกรณีที่เป็นระบบสารสนเทศเฉพาะที่ถูกใช้งานผ่านเครือข่ายภายในเท่านั้น หรือใช้ผ่านระบบอินทราเน็ตจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) และมีกระบวนการเข้ารหัสข้อมูลอีกชั้นหนึ่ง (SSL VPN) เมื่อผู้ใช้เข้าจากเครือข่ายภายนอก

2.1.6 ผู้ใช้งานที่นำคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ ใด ๆ เข้ามาเชื่อมต่อกับระบบสารสนเทศหรือเครือข่ายภายในมหาวิทยาลัย จะต้องเป็นผู้รับผิดชอบผลที่เกิดจากการกระทำผ่านคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ใด ๆ เหล่านั้น

2.2 ผู้ใช้งานภายนอก (ผู้รับเหมาดำเนินการ หรือบุคคลจากหน่วยงานภายนอก)

2.2.1 ในกรณีที่ผู้ใช้งานภายนอกต้องการเข้าถึงหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศที่มีความสำคัญประกอบด้วย ระบบสารสนเทศที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ เช่น ข้อมูลการเงิน ข้อมูลบุคลากร ข้อมูลการบริหารและข้อมูลนักศึกษา จะต้องได้รับสิทธิ์อนุญาตเป็นลายลักษณ์อักษร หรือมีหนังสือสัญญาที่เกี่ยวข้องที่ถูกอนุมัติโดย อธิการบดี คณบดี หรือผู้อำนวยการ ประจำหน่วยงานที่เป็นเจ้าของระบบสารสนเทศนั้น ๆ

2.2.2 ในกรณีที่ผู้ใช้งานภายนอกต้องการเข้าถึงหรือแก้ไขเปลี่ยนแปลงระบบสารสนเทศทั่วไป เช่น เว็บไซต์ อุปกรณ์ต่าง ๆ หรือข้อมูลกล้องวงจรปิด จะต้องได้รับสิทธิ์อนุญาตจากผู้รับผิดชอบ หรือผู้ดูแลระบบ อาจเป็นลายลักษณ์อักษรหรือไม่ขึ้นกับความเหมาะสม และควรมีการบันทึกข้อมูลการเข้าถึงหรือแก้ไขในแต่ละครั้ง

2.2.3 ผู้ใช้งานภายนอกที่ได้รับสิทธิ์เท่านั้น จึงจะสามารถเข้าใช้เครื่องคอมพิวเตอร์ หรืออุปกรณ์ของมหาวิทยาลัยได้ โดยสิทธิ์ที่ได้รับนั้นให้พิจารณาเป็นกรณี ๆ ไป เช่น เมื่อจำเป็นต้องมีการประชุมพูดคุยกับบุคคลจากหน่วยงานภายนอก หรือเมื่อมีการเช่าพื้นที่ห้องอบรมจากหน่วยงานภายนอก โดยกำหนดให้ผู้รับผิดชอบเครื่องคอมพิวเตอร์ หรืออุปกรณ์ของมหาวิทยาลัย เป็นผู้รับผิดชอบในการมอบสิทธิ์แก่ผู้ใช้งานภายนอก

2.2.4 ผู้ใช้งานภายนอกที่ได้รับสิทธิ์เท่านั้น จึงจะสามารถนำคอมพิวเตอร์ส่วนตัว โทรศัพท์ หรืออุปกรณ์ใด ๆ เข้ามาเชื่อมต่อกับระบบสารสนเทศ หรือเครือข่ายภายในมหาวิทยาลัย โดยสิทธิ์ที่ได้รับนั้นให้พิจารณาเป็นกรณี ๆ ไป เช่น เมื่อจำเป็นต้องมีการประชุมพูดคุยกับบุคคลจากหน่วยงานภายนอก หรือเมื่อมีการเช่าพื้นที่ห้องอบรมจากหน่วยงานภายนอก โดยกำหนดให้ผู้รับผิดชอบระบบสารสนเทศ นั้น ๆ เป็นผู้รับผิดชอบในการมอบสิทธิ์แก่ผู้ใช้งานภายนอก

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบเครือข่าย

1. วัตถุประสงค์

1.1 เพื่อควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์แบบมีสายและไร้สายทั้งภายนอกและภายในองค์กรรวมถึงเครือข่ายเสมือน โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

1.2 เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์ และการมอบอำนาจของหน่วยงานที่รับผิดชอบ

1.3 เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

2. แนวทางปฏิบัติ

2.1 ผู้ดูแลระบบ ต้องแบ่งระบบเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มของผู้ใช้งาน เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อให้สามารถควบคุมป้องกันการบุกรุกได้อย่างเป็นระบบ

2.2 หน่วยงาน บริษัทหรือบุคคลภายนอกจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ต้องได้รับอนุญาติจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการสำนักวิทบริการและเทคโนโลยีสารสนเทศ

2.3 ห้ามผู้ใดทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณเครือข่าย (Switch) หรืออุปกรณ์ที่เกี่ยวข้องกับระบบเครือข่ายโดยไม่ได้รับอนุญาติจากผู้ดูแลระบบ (System Administrator)

2.4 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ

2.4.1 ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาติเท่านั้น ต้องมีวิธีการจำกัดเส้นทางเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

2.4.2 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังเครือข่ายอื่นๆ ภายนอกหน่วยงานควรมีการเชื่อมต่ออุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

2.4.3 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System /Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายหน่วยงานในลักษณะที่ผิดปกติ

2.4.4 การเข้าสู่ระบบเครือข่ายภายในหน่วยงานโดยผ่านทางระบบอินเตอร์เน็ตจำเป็นต้องมีการบันทึกเข้า (Login) และมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้บริการ

2.4.5 หมายเลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงานจำเป็นต้องมีการป้องกันมิให้หน่วยงานจากภายนอกที่เชื่อมต่อสามารถมองเห็นได้

2.4.6 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.4.7 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะที่จำเป็น

2.5 มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

2.5.1 ควรเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความถูกต้องครบถ้วน แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้การจัดเก็บ ต้องกำหนดชั้นความลับการเข้าถึงข้อมูลและผู้ดูแลระบบไม่ได้รับอนุญาติในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบเทคโนโลยีสารสนเทศของหน่วยงาน (IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

2.5.2 ควรตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

2.5.3 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกข้อมูลให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

2.6 มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทางดังนี้

2.6.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.6.2 มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

2.6.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลระยะไกลต้องได้รับการอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.6.4 การเข้าสู่ระบบจากระยะไกลของผู้ใช้จากภายนอกหน่วยงาน ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

2.6.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

นโยบายการเข้าถึงหรือควบคุมการใช้งานโปรแกรมประยุกต์

1. วัตถุประสงค์

1.1 เพื่อควบคุมการเข้าถึงโปรแกรมประยุกต์โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

1.2 เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง การกำหนดสิทธิ์เป็นลำดับชั้น ที่สอดคล้องกับภารกิจและความรับผิดชอบของผู้ใช้งานในแต่ละตำแหน่ง

1.3 เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของข้อมูลประเภทต่าง ๆ ที่อยู่ในโปรแกรมประยุกต์

2. แนวปฏิบัติ

2.1 โปรแกรมประยุกต์ใด ๆ ภายในมหาวิทยาลัย จะต้องมีผู้รับผิดชอบ เจ้าของ หรือผู้ดูแลระบบ ที่จะต้องทำหน้าที่ในการรักษาความมั่นคงปลอดภัย และกำหนดสิทธิ์การเข้าถึงให้แก่ผู้ใช้งานตามภารกิจ หรือตามความรับผิดชอบที่ได้รับมอบหมายอย่างเหมาะสม

2.2 ผู้ใช้งานที่ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงโปรแกรมประยุกต์นั้น ๆ ได้ โดยจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่ปลอดภัย น่าเชื่อถือ และเหมาะสมก่อนการเข้าใช้งานโปรแกรมประยุกต์ เช่น การใช้ชื่อผู้ใช้ และรหัสผ่าน

2.3 ผู้ใช้งานที่ได้รับสิทธิ์เข้าถึงโปรแกรมประยุกต์ จะต้องได้รับมอบสิทธิ์ที่อยู่ในขอบเขตที่ตรงกับภาระหน้าที่ของผู้ใช้งานแต่ละคน และจะต้องไม่มอบสิทธิ์ที่มากกว่าภาระหน้าที่ความรับผิดชอบ (Authorization)

2.4 ในกรณีที่ผู้ใช้งานเข้าใช้งานโปรแกรมประยุกต์ที่มีความสำคัญ หรือโปรแกรมประยุกต์ที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ เช่น ข้อมูลการเงิน ข้อมูลบุคลากร ข้อมูลการบริหาร และข้อมูลนักศึกษา จะต้องมีการจำกัดเวลาในการเชื่อมต่อ เมื่อไม่มีการใช้งานระยะเวลาหนึ่ง จะต้องถูกบังคับให้ออกจากระบบ

2.5 ในกรณีที่เป็นโปรแกรมประยุกต์เฉพาะที่ถูกใช้งานผ่านเครือข่ายภายในเท่านั้น หรือใช้ผ่านระบบอินทราเน็ตจะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) และมีกระบวนการเข้ารหัสข้อมูลอีกชั้นหนึ่ง (SSL VPN) เมื่อผู้ใช้เข้าจากเครือข่ายภายนอก

2.6 โปรแกรมประยุกต์ใด ๆ ที่มีความสำคัญ หรือโปรแกรมประยุกต์ที่เกี่ยวข้องกับข้อมูลที่จัดอยู่ในชั้นความลับ จะต้องมีเอกสารควบคุมการเข้าถึงและกำหนดสิทธิ์ที่ระบุหน่วยงานและผู้รับผิดชอบ และการจัดกลุ่มหรือระดับชั้นของการเข้าถึงที่เหมาะสม ชัดเจน โดยคำนึงถึงภารกิจและความรับผิดชอบของผู้ใช้งานไม่ว่าจะเป็นนักศึกษา อาจารย์ หรือเจ้าหน้าที่

2.7 เมื่อมีการเพิ่ม ปรับเปลี่ยน หรือออกจากงานของผู้ปฏิบัติงานในตำแหน่งที่เกี่ยวข้องหรือมีภารกิจกับโปรแกรมประยุกต์ใด ๆ จะต้องมีการเพิ่ม ปรับเปลี่ยน หรือถอดถอนสิทธิ์ของผู้ใช้งานนั้น

2.8 โปรแกรมประยุกต์ใด ๆ ที่มีการแสดงหรือเชื่อมโยงกับฐานข้อมูลที่เป็นความลับ ซึ่งประกอบด้วยข้อมูลการเงิน ข้อมูลบุคลากร และข้อมูลนักศึกษา หน่วยงานที่รับผิดชอบจะต้องมีผู้ดูแล กำหนดข้อปฏิบัติและหลักเกณฑ์สำหรับการเข้าถึงข้อมูลจากหน่วยงานอื่น หรือผู้ใช้งานจากภายนอก

2.9 นโยบายการเข้าถึงหรือควบคุมการใช้งานโปรแกรมประยุกต์ และเอกสารควบคุมการเข้าถึง และกำหนดสิทธิ์ในแต่ละโปรแกรมประยุกต์ จะต้องแสดงให้ผู้ใช้งานรับทราบ

นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบปฏิบัติการ

1. วัตถุประสงค์

1.1 เพื่อควบคุมการเข้าถึงระบบปฏิบัติการหรือคอมพิวเตอร์โดยคำนึงถึงการใช้งานตามภารกิจและความรับผิดชอบของผู้ใช้งาน

1.2 เพื่อกำหนดกฎเกณฑ์และแนวทางที่เกี่ยวกับการใช้งานระบบปฏิบัติการหรือคอมพิวเตอร์ให้มีความมั่นคงปลอดภัย

1.3 เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความรับผิดชอบของตนเองต่อการใช้งานระบบปฏิบัติการ

2. แนวปฏิบัติ

2.1 คอมพิวเตอร์ใด ๆ ที่เป็นของมหาวิทยาลัย จะต้องมีผู้รับผิดชอบในการใช้งานและการเข้าถึงระบบปฏิบัติการ ให้เป็นไปตามภารกิจ หรือตามความรับผิดชอบที่ได้รับมอบหมายอย่างเหมาะสม

2.2 ระบบปฏิบัติการใด ๆ ที่มีการเข้าถึงหรือใช้งานข้อมูลที่เป็นความลับ หรือมีการติดตั้งโปรแกรมประยุกต์ที่เชื่อมต่อกับข้อมูลที่เป็นความลับ จะต้องมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่ปลอดภัย น่าเชื่อถือ และเหมาะสมก่อนการเข้าใช้งานโปรแกรมประยุกต์ เช่น การใช้ชื่อผู้ใช้และรหัสผ่าน

2.3 ระบบปฏิบัติการใด ๆ ที่มีการเข้าถึงหรือใช้งานข้อมูลที่เป็นความลับ หรือมีการติดตั้งโปรแกรมประยุกต์ที่เชื่อมต่อกับข้อมูลที่เป็นความลับ จะต้องมีการจำกัดเวลาในการเชื่อมต่อ เมื่อไม่มีการใช้งานระยะเวลาหนึ่งจะต้องถูกบังคับให้ออกจากระบบ

2.4 ผู้ใช้งานจะต้องรับผิดชอบในคอมพิวเตอร์ในความดูแลของตนเองในการเข้าถึงและใช้งานระบบปฏิบัติงานโดยผู้ใช้งานที่ได้รับสิทธิ์เท่านั้นจึงจะสามารถเข้าถึงระบบปฏิบัติการได้ ควรจะมีกระบวนการตรวจสอบยืนยันตัวตนของผู้ใช้งาน (Authentication) ที่ปลอดภัย น่าเชื่อถือ และเหมาะสมก่อนการเข้าใช้งานระบบปฏิบัติการ เช่น การใช้ชื่อผู้ใช้ และรหัสผ่าน

2.5 เมื่อมีการเพิ่ม ปรับเปลี่ยน หรือออกจากงานของผู้ใช้งาน จะต้องมีการทบทวนผู้รับผิดชอบในเครื่องคอมพิวเตอร์ใหม่ จะต้องมีการเพิ่ม ปรับเปลี่ยน หรือถอดถอนสิทธิ์ของผู้ใช้งานนั้นในคอมพิวเตอร์ดังกล่าว

2.6 ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน โปรแกรมประยุกต์ และโปรแกรมอรรถประโยชน์ใด ๆ บนเครื่องคอมพิวเตอร์ที่ไม่เกี่ยวข้องกับงานในภารกิจ หรือหน้าที่ความรับผิดชอบของผู้ใช้งาน

2.7 ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งาน โปรแกรมประยุกต์ หรือโปรแกรมอรรถประโยชน์ใด ๆ บนเครื่องคอมพิวเตอร์ที่ละเมิดลิขสิทธิ์ หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลที่ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

2.8 ห้ามไม่ให้ผู้ใช้งานจัดเก็บ ข้อมูลที่ผิดกฎหมาย สิ่งที่ละเมิดลิขสิทธิ์ ข้อมูลหรือรูปภาพที่ไม่เหมาะสมหรือขัดต่อศีลธรรม ลงในคอมพิวเตอร์หรือระบบใด ๆ ของมหาวิทยาลัย หากตรวจพบ ถือว่าเป็นความผิดส่วนบุคคลที่ผู้ใช้งานต้องรับผิดชอบแต่เพียงผู้เดียว

2.9 ห้ามไม่ให้ผู้ใช้งานนำคอมพิวเตอร์ ข้อมูล หรือทรัพยากรใด ๆ ที่เป็นของมหาวิทยาลัยไปใช้ในการหาผลประโยชน์ส่วนตัว หรือผลประโยชน์ทางการค้า หากตรวจพบถือว่าเป็นความผิด โดยให้ผู้บังคับบัญชาเป็นผู้ตัดสินความผิด และบทลงโทษ

2.10 ห้ามไม่ให้ผู้ใช้งานเผยแพร่ หรือเปิดเผย ข้อมูลใด ๆ หรือข้อมูลความลับ ของมหาวิทยาลัย ต่อบุคคลภายนอกหรือที่เป็นสาธารณะ เว้นแต่ข้อมูลนั้นจะเป็นที่ได้มีการเผยแพร่เป็นการทั่วไป หากตรวจพบถือว่าเป็นความผิด โดยให้ผู้บังคับบัญชาเป็นผู้ตัดสินความผิด และบทลงโทษ

2.11 นโยบายการเข้าถึงหรือควบคุมการใช้งานระบบปฏิบัติการจะต้องแสดงให้ผู้ใช้งานรับทราบ

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพ

1. วัตถุประสงค์

เพื่อกำหนดเป็นมาตรฐานในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าที่จำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

2. แนวทางปฏิบัติ

2.1 ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโลยีสารสเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่าย เป็นต้น

2.2 ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศ

2.3 ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออก พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ

2.4 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาเชื่อมต่อเพื่อใช้งานจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานระบบเครือข่าย และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายให้รับผิดชอบงานนั้นๆ ลงนามรับรอง

นโยบายในการรักษาความมั่นคงปลอดภัยของผู้ใช้งาน

1. วัตถุประสงค์

เพื่อเป็นแนวทางให้ผู้ใช้งานได้รับทราบแนวปฏิบัติ และกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบกำหนดไว้ เพื่อให้การใช้งานเทคโนโลยีสารสนเทศเป็นไปอย่างปลอดภัย และมีประสิทธิภาพ

2. การบริหารจัดการบัญชีผู้ใช้งาน

2.1 นักศึกษา นักศึกษาจะได้รับบัญชีผู้ใช้งานคอมพิวเตอร์ โดยชื่อผู้ใช้งานจะเป็นรหัสนักศึกษา และรหัสผ่านจะเป็นหมายเลขประจำตัวประชาชน และเมื่อนักศึกษาสำเร็จการศึกษา ลาออก พ้นสภาพการเป็นนักศึกษา หรือเสียชีวิต บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน

2.2 นักศึกษาแลกเปลี่ยน นักศึกษาจะได้รับบัญชีผู้ใช้งานคอมพิวเตอร์ชั่วคราวที่มีกำหนดอายุการใช้งาน หลังจากที่คณะต้นสังกัดมีหนังสือขออนุญาตการใช้งานเป็นลายลักษณ์อักษร

2.3 ศิษย์เก่า เมื่อนักศึกษาสำเร็จการศึกษา บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน

2.4 บุคลากรใหม่ สามารถลงทะเบียนรับบัญชีผู้ใช้งานคอมพิวเตอร์ได้ หลังจากต้นสังกัดทำหนังสือรายงานตัวไปยังกองบริหารงานบุคคล เมื่อบุคลากรลาออก ไล่ออก เกษียณ หรือเสียชีวิตบัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน

2.5 บุคลากรเดิมเปลี่ยนตำแหน่ง เมื่อมีการเปลี่ยนตำแหน่ง หรือมีการย้ายหน่วยงานโดยมีการลาออกจากตำแหน่งเดิมหรือหน่วยงานเดิม บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกระงับการใช้งาน และจะสามารถใช้งานได้หลังจากต้นสังกัด ทำหนังสือรายงานตัวไปยังกองบริหารงานบุคคล เมื่อบุคลากรลาออก ไล่ออก เกษียณ หรือเสียชีวิต บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน

2.6 บุคลากรจ้างพิเศษ

2.6.1 บุคลากรจ้างพิเศษ ที่เป็นบุคลากรสายวิชาการ หรือผู้บริหารของมหาวิทยาลัย เช่น อาจารย์พิเศษ จะได้รับบัญชีผู้ใช้งานคอมพิวเตอร์แบบพิเศษ ที่สามารถเข้าใช้งานเครือข่ายอินเตอร์เน็ตและระบบสารสนเทศของมหาวิทยาลัยได้ โดยต้องมีหนังสือการขออนุณาตการใช้งานจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร เมื่อสิ้นสุดสัญญาจ้าง บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน

2.6.2 บุคลากรจ้างพิเศษ ที่เป็นบุคลากรสายสนับสนุน จะได้รับบัญชีผู้ใช้งานคอมพิวเตอร์แบบชั่วคราวที่มีการกำหนดอายุการใช้งาน โดยต้องมีหนังสือการขออนุณาตการใช้งานจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร สามารถใช้งานเครือข่ายอินเตอร์เน็ตของมหาวิทยาลัยได้

2.7 บุคลากรเกษียณอายุราชการ บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกปิดการใช้งาน ยกเว้นในกรณีผู้บริหารที่มีการต่ออายุราชการ จะเปิดใช้งานต่อจนสิ้นสุดวาระการดำรงตำแหน่ง

2.8 ผู้ใช้งานชั่วคราว ใช้สำหรับบุคคลภายนอกที่ได้รับสิทธิ์ให้ใช้งานเครือข่ายอินเตอร์เน็ตของมหาวิทยาลัย เช่น บุคลากรภายนอกที่มาติดต่องาน หรือเข้าร่วมอบรม จะได้รับบัญชีผู้ใช้งานที่มีการกำหนดอายุการใช้งาน โดยต้องมีหนังสือการขออนุณาตการใช้งานจากหน่วยงานต้นสังกัดเป็นลายลักษณ์อักษร

3. แนวปฏิบัติของผู้ใช้งาน

3.1 ผู้ใช้งานที่เป็นบุคลากรใหม่ สามารถลงทะเบียนรับบัญชีผู้ใช้งานคอมพิวเตอร์ได้ หลังจากต้นสังกัดส่งหนังสือรายงานตัวไปยังกองบริหารงานบุคคล

3.2 ผู้ใช้งานที่เป็นบุคลากร เมื่อมีการเปลี่ยนตำแหน่ง หรือมีการย้ายหน่วยงานโดยมีการลาออกจากตำแหน่งเดิมหรือหน่วยงานเดิม บัญชีผู้ใช้งานคอมพิวเตอร์จะถูกระงับการใช้งาน และจะสามารถใช้งานได้หลังจากต้นสังกัดทำหนังสือรายงานตัวไปยังกองบริหารงานบุคคล

3.3 ผู้ใช้งานควรกำหนดรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษรหรือมากกว่านั้น ซึ่งประกอบไปด้วยตัวเลข (numerical character) ตัวอักษร (alphabet) และตัวอักษรพิเศษ (special character)

3.4 ผู้ใช้งานควรเปลี่ยรหัสผ่านทุก 3- 6 เดือน หรือเมื่อมีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

3.5 ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่าน เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

3.6 ผู้ใช้งานภายในมหาวิทยาลัยต้องแสดงตัวตน ด้วยชื่อผู้ใช้งานทุกครั้งผ่านซอฟต์แวร์ควบคุม เพื่อระบุตัวตนจุดเชื่อมต่อ ของอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย

3.7 ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของหน่วยงานร่วมกัน

3.8 ผู้ใช้งานควรตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งาน ผู้ใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

3.9 ผู้ใช้งานควรทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.10 ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์ดังกล่าว เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

3.11 ผู้ใช้งานมีหน้าที่รับผิดชอบต่อสินทรัพย์ที่ส่วนงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยรายการสินทรัพย์ที่ผู้ใช้งานต้องรับผิดชอบ การรับคืนทรัพย์สินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

3.12 เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

3.13 บรรดาข้อมูล ไฟล์ ซอฟท์แวร์ หรอสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

3.14 ในการใช้อีเมล (email) ของมหาวิทยาลัย ผู้ใช้งานต้องใช้เพื่อการติดต่องานเท่านั้น ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญในหัวข้ออีเมล และเมื่อจบการใช้งานควรลงชื่อออกจากระบบทุกครั้งเพื่อป้องกันบุคคลอื่นเข้าใช้งาน

3.15 ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

3.16 เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

4. ข้อห้ามสำหรับผู้ใช้งาน

4.1 ห้ามผู้ใช้งานใช้ทรัพย์สินของส่วนงาน เพื่อการรบกวน ก่อนให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัย

4.2 ห้ามผู้ใช้งานเข้าถึงข้อมูลหรือระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผยโดยมิชอบในประการที่น่าจะเกิดความเสียหายต่อผู้อื่น

4.3 ห้ามผู้ใช้งานกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของส่วนงานต้องหยุดชะงัก

4.4 ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์ หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงาน หรือผู้ดูแลระบบที่ได้รับมอบหมาย

4.5 ห้ามผู้ใช้งานกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบการใช้งานหรือรับรู้รหัสผ่านส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อใช้ทรัพยากรก็ตาม

4.6 ห้ามผู้ใช้งานติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของมหาวิทยาลัยโดยไม่ได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูและระบบ

4.7 ห้ามผู้ใช้งานกระทำด้วยประการใด ๆ โดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวางหรือรบกวนจนไม่สามารถทำงานได้ตามปกติได้

4.8 ห้ามผู้ใช้งานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงที่มาของการส่งข้อมูลดังกล่าวอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

4.9 ห้ามผู้ใช้งานกระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศชาติ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือการบริการสาธารณะหรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

4.10 ห้ามผู้ใช้งานจำหน่ายหรือเผยแพร่โปรแกรมที่จัดขึ้นโดยเฉพาะ เพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม พ.ร.บ.คอมพิวเตอร์

4.11 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์ที่อาจกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักรหรือมีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

4.12 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมหรือเป็นเท็จไม่ว่าทั้งหมดหรือบางส่วนโดยที่น่าจะเกิดความเสียหายแก่ผู้อื่น

4.13 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือซึ่งข้อมูลอันเป็นเท็จ โดยประมาณการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

4.14 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ อันเป็นความผิดที่เกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

4.15 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะลามกและข้อมูลคอมพิวเตอร์นั้นประชาชนทั่วไปอาจเข้าถึงได้

4.16 ห้ามผู้ใช้งานนำเข้าหรือเผยแพร่หรือส่งต่อสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการใด ๆ ทั้งนี้ โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง

4.17 ห้ามผู้ใช้งานคัดลอก หรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

4.18 ห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่ฝ่ายเดียว

4.19 ห้ามผู้ใช้งานเข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาติจากผู้ดูแลระบบ

4.20 ห้ามผู้ใช้งานนำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าต่อเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

5. บทลงโทษเมื่อกระทำผิด

ความเสียหายใด ๆ อันเป็นความผิดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2560 และ/หรือ กฎหมายอื่นใดที่กำหนดความผิดเกี่ยวกับการใช้งานคอมพิวเตอร์และการใช้งานเครือข่ายอินเทอร์เน็ต หากผู้ใช้งานฝ่าฝืนเงื่อนไขตามข้อกำหนดนี้มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับหรือยกเลิกการให้บริการโดยทันที และผู้ใช้งานจะต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นจากกรณีดังกล่าวแต่เพียงผู้เดียว

ประกาศ ณ วันที่ 15 เดือนมีนาคม พ.ศ. 2562

พิจารณาเห็นชอบดำเนินการ

(นายธนาวุฒิ นิลมณี)
ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลพระนคร
Chief information officer (CIO)