นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยราชภัฏสวนสุนันทา

1. วัตถุประสงค์และขอบเขต

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสวนสุนันทาหรือต่อไปนี้เรียกว่า “มหาวิทยาลัย” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ มหาวิทยาลัยราชภัฏสวนสุนันทาจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) วิธีปฏิบัติ/ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีมาตรการป้องกันภัยคุกคามต่างๆ โดยมีวัตถุประสงค์ ดังต่อไปนี้

1.1 การจัดทำนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้เกิดความเชื่อมั่นและให้มีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 กำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร อ้างอิงตามมาตรฐาน ISO/IEC 27001 และมีการปรับปรุงอย่างต่อเนื่อง

1.3 นโยบายนี้จะต้องทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในมหาวิทยาลัยได้รับทราบและเจ้าหน้าที่ทุกคนจะต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ และวิธีปฏิบัติ/ขั้นตอนปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย สำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 นโยบายนี้ต้องมีการดำเนินการตรวจสอบและประเมินนโยบาย โดยมีการทบทวนอย่างน้อย ปีละ 1 ครั้ง หรือตามที่ระบุไว้ในเอกสาร “การตรวจสอบประเมินนโยบาย”

2. องค์ประกอบของนโยบาย

2.1 คำนิยาม

2.2 การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

2.3 การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ ในส่วนการบริหารจัดการด้านความมั่นคงปลอดภัยของระบบสารสนเทศทั้งภายในและภายนอกหน่วยงานหรือองค์กร

2.4 การบริหารจัดการทรัพย์สินสารสนเทศ

2.5 การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

2.6 การสร้างความมั่นคงปลอดภัยด้านทางกายภาพและสภาพแวดล้อม

2.7 การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

2.8 การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

2.9 การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

2.10 การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

2.11 การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กรเพื่อให้มีความต่อเนื่อง

2.12 การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการหลักเกณฑ์หรือกระบวนการใดๆ รวมทั้งข้อกำหนดด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

องค์ประกอบของนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย แต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน(Standard) แนวทางปฏิบัติ (Guideline) และ วิธีปฏิบัติ/ขั้นตอนปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย เพื่อที่จะทำให้มหาวิทยาลัยมีมาตรการ ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน บุคลากร ของมหาวิทยาลัย ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย

นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยฉบับนี้ จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ซึ่งเจ้าหน้าที่ของมหาวิทยาลัยและหน่วยงานภายนอกจะต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

- **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยราชภัฏสวนสุนันทา
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย
- **กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร** หมายถึง กลุ่มงานข้อมูลสารสนเทศและการสื่อสาร เป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย
- **หัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสาร** หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐาน การควบคุมดูแลการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** (Access Control) หมายถึง การอนุญาต การกำหนดสิทธิ หรือมอบอำนาจให้ผู้ใช้งาน หรือผู้ที่เกี่ยวข้อง เข้าถึงหรือใช้เครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ
- **ความมั่นคงปลอดภัยสารสนเทศ** (Information Security) หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อ (Reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** (Information Security event) หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่ได้แสดงให้เห็นเป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** (Information Security Incident) หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
- **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งมหาวิทยาลัยกำหนดไว้ ดังนี้
  - **ผู้บริหาร** หมายถึง ผู้มีอำนาจบริหารในระดับสูงของมหาวิทยาลัย เช่น หัวหน้าหน่วยงานราชการ เป็นต้น
  - **ผู้ดูแลระบบ** (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์

- **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการของมหาวิทยาลัย

❖ **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของมหาวิทยาลัย

❖ **สินทรัพย์** หมายถึง ข้อมูล ระบบข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟท์แวร์ที่มีลิขสิทธิ เป็นต้น

❖ **การเข้าถึงหรือการควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

❖ **หน่วยงานภายนอก** หมายถึง บุคคล มหาวิทยาลัยหรือหน่วยงานภายนอก ที่มหาวิทยาลัยราชภัฏสวนสุนันทาอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของหน่วยงาน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

❖ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

❖ **สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

❖ **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

❖ **ระบบเครือข่าย** (Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศและการสื่อสารต่างๆ ของมหาวิทยาลัยได้ เช่น ระบบ LAN, ระบบ Intranet, ระบบ Internet เป็นต้น

❖ **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

❖ **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

- **พื้นที่ทำงานทั่วไป** (General working area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพา (Notebook) ที่ประจำโต๊ะทำงาน
- **พื้นที่ทำงานของผู้ดูแลระบบ** (System administrator area)
- **พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศและการสื่อสารหรือระบบเครือข่าย** (IT equipment or network area)

- **พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์** (Data storage area)
- **พื้นที่ใช้งานระบบเครือข่ายไร้สาย** (Wireless LAN coverage area)

❖ **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

❖ **จดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

❖ **รหัสผ่าน** (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศและการสื่อสาร

❖ **ชุดคำสั่งไม่พึงประสงค์** (Malicious Code) หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลงหรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

❖ **มาตรฐาน** (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

❖ **วิธีปฏิบัติ / ขั้นตอนปฏิบัติ** (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นรายการหรือเป็นลำดับ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

❖ **แนวปฏิบัติ** (Guideline) หมายถึง หมายถึงแนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

หมวดที่ 1
การสร้างความมั่นคงปลอดภัยด้านบริหารจัดการ

1. วัตถุประสงค์

เพื่ออธิบายถึงจุดประสงค์และขอบเขตของนโยบายความมั่นคงปลอดภัยสารสนเทศในภาพรวม โดยรวมถึงความรับผิดชอบในการดูแลและปรับปรุงนโยบาย

2 แนวทางการควบคุม

2.1 จัดทำนโยบายความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของมหาวิทยาลัยเป็นลายลักษณ์อักษรและเผยแพร่ให้หน่วยงานและบุคคลากรที่เกี่ยวข้องทราบ

2.2 จัดให้มีการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันอย่างสม่ำเสมอ อย่างน้อย ปีละ 1 ครั้ง เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงในอนาคต ที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยทางด้านสารสนเทศของมหาวิทยาลัย

2.3 ผู้บริหาร พนักงาน และลูกจ้างรวมถึงบุคคลภายนอกที่เกี่ยวข้องกับข้อมูล ต้องทำความเข้าใจยอมรับและปฏิบัติตามนโยบายความมั่นคงปลอดภัยสารสนเทศ

2.4 หากข้อยกเว้นของนโยบายนั้น มีผลกระทบต่อความมั่นคงปลอดภัยที่มีอยู่เดิม ต้องมีการสร้างมาตรการควบคุมชดเชยขึ้นมารองรับสำหรับข้อยกเว้นดังกล่าว เพื่อให้มั่นใจได้ว่าความเสี่ยงที่เหลืออยู่ในระดับที่สามารถยอมรับได้

หมวดที่ 2
การจัดโครงสร้างด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

1. วัตถุประสงค์

ในการจัดการความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบนั้น มหาวิทยาลัยจำเป็นต้องมีการจัดโครงสร้างของหน่วยงานภายในที่เกี่ยวกับความมั่นคงปลอดภัยสารสนเทศอย่างเหมาะสม ตั้งแต่ระดับบริหารจนถึงหน่วยงานในระดับปฏิบัติการและรวมถึงการกำหนดบทบาทและหน้าที่ที่มีต่อข้อมูลของผู้ที่เกี่ยวข้องในฐานะต่าง ๆ ตลอดจนความเข้าใจและตระหนักถึงหน้าที่ด้านความมั่นคงปลอดภัยข้อมูล

2 แนวทางการควบคุม

2.1 ผู้บริหารให้ความสำคัญและให้การสนับสนุนต่อการบริหารจัดการทางด้านความมั่นคงปลอดภัยสารสนเทศ โดยอนุมัติให้มีการจัดตั้งคณะทำงานความมั่นคงปลอดภัยสารสนเทศ

2.2 ผู้บริหารทุกหน่วยงาน มีหน้าที่ในการสนับสนุนและประสานงานในการประกาศใช้นโยบายความมั่นคงปลอดภัย เพื่อให้มีความร่วมมือและถือปฏิบัติทั่วทั้งมหาวิทยาลัย

2.3 มหาวิทยาลัยต้องกำหนดให้มีการจัดทำรายละเอียดสำหรับติดต่อประสานงานกับหน่วยงานภายนอกที่เกี่ยวกับความมั่นคงปลอดภัย รวมถึงต้องปรับปรุงข้อมูลหน่วยงานในการติดต่อดังกล่าวให้มีความถูกต้องและทันสมัยอยู่เสมอ

2.4 หน่วยงานหรือบุคคลภายนอกที่เกี่ยวข้องในการใช้ข้อมูลของมหาวิทยาลัยต้องมีความรับผิดชอบต่อการปฏิบัติตามข้อกำหนดความมั่นคงปลอดภัยสารสนเทศที่เกี่ยวข้อง เช่น นโยบาย มาตรฐานหรือคำสั่ง เป็นต้น

หมวดที่ 3
การบริหารจัดการทรัพย์สินสารสนเทศ

1. วัตถุประสงค์

ในการที่จะดูแลรักษาและปกป้องทรัพย์สินของมหาวิทยาลัยได้อย่างเหมาะสมนั้น มหาวิทยาลัยควรทราบถึงการมีอยู่ของทรัพย์สิน และควรกำหนดให้มีเจ้าของทรัพย์สินเพื่อรับผิดชอบในทรัพย์สินนั้น โดยที่เจ้าของทรัพย์สินอาจมอบหมายให้ผู้อื่นดูแลและควบคุมทรัพย์สินแทน อย่างไรก็ดี เจ้าของทรัพย์สินยังคงเป็น ผู้ที่รับผิดชอบสูงสุดในทรัพย์สินดังกล่าว

2 แนวทางการควบคุม

2.1 หน่วยงานของมหาวิทยาลัยที่เกี่ยวข้องกับข้อมูล จะต้องดำเนินการจัดทำบัญชีทรัพย์สินที่เกี่ยวข้องกับข้อมูลของมหาวิทยาลัยทรัพย์สินที่เกี่ยวข้องกับข้อมูล

2.2 ผู้ดูแลทรัพย์สินต้องตรวจทาน และปรับปรุงบัญชีทรัพย์สินอย่างสม่ำเสมอ อย่างน้อยปีละครั้งโดยบัญชีทรัพย์สินจะต้องมีรายละเอียดที่เพียงพอ

2.3 ในการจัดทำทะเบียนทรัพย์สิน จะต้องกำหนดเจ้าของทรัพย์สินที่มีหน้าที่รับผิดชอบในการรักษาทรัพย์สินนั้น สำหรับในกรณีที่เป็นทรัพย์สินด้านข้อมูล ซึ่งอาจมีเจ้าของข้อมูลได้หลายคน ผู้บริหารระดับสูงขึ้นไป ต้องมอบหมายความรับผิดชอบความเป็นเจ้าของข้อมูลให้กับบุคคลที่ใช้หรือเกี่ยวข้องกับข้อมูลนั้นมากที่สุด

2.4 ข้อมูลเกี่ยวกับบัญชีทรัพย์สินถือว่าเป็นข้อมูลลับที่อาจอนุญาตให้เปิดเผย หรือเข้าใช้งานได้เฉพาะบุคคลที่เกี่ยวข้องและมีความจำเป็นต้องทราบเท่านั้น

2.5 ผู้ใช้งาน พนักงาน ลูกจ้าง หน่วยงานภายนอกต้องยินยอมทำตามข้อกำหนดในการใช้งานข้อมูลและทรัพย์สินสารสนเทศ ซึ่งรวมถึงการใช้งานอินเทอร์เน็ตและจดหมายอิเล็กทรอนิกส์ (E-mail)

2.6 มหาวิทยาลัยจะต้องกำหนดเกณฑ์ในการจัดลำดับชั้นของข้อมูล เพื่อให้ข้อมูลได้ถูกจัดลำดับชั้นและได้รับการป้องกันอย่างเหมาะสมตามแนวทางการจัดการข้อมูลในแต่ละลำดับชั้น

หมวดที่ 4
การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากร

1. วัตถุประสงค์

หลักการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคล ตั้งแต่การรับเข้าทำงานจนถึงการเลิกจ้างทั้งบุคลากรที่เป็นพนักงานและลูกจ้าง มีส่วนสำคัญที่ช่วยลดความเสี่ยงด้านบุคลากร เนื่องจากสารสนเทศอยู่ในรูปแบบที่หลากหลาย ทำให้การควบคุมความมั่นคงปลอดภัยของสารสนเทศโดยระบบอย่างเดียวไม่อาจเกิดประสิทธิผลเต็มที่ ดังนั้น กระบวนการจัดการด้านทรัพยากรบุคคล จึงมีความจำเป็นในการช่วยทำให้สารสนเทศมีความมั่นคงปลอดภัย

2 แนวทางการควบคุม

2.1 พนักงานและลูกจ้างทุกคนมีบทบาทรับผิดชอบในการรักษาความมั่นคงปลอดภัยสารสนเทศ รวมถึงการปฏิบัติตามนโยบายและระเบียบปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ

2.2 ในกรณีที่พนักงานหรือลูกจ้างมีหน้าที่เกี่ยวข้องกับข้อมูลที่มีความสำคัญหรือความลับ ต้องมีการกำหนดหน้าที่และความรับผิดชอบด้านความมั่นคงปลอดภัยสารสนเทศที่มีลักษณะเฉพาะกับหน้าที่งานนั้นในคำอธิบายหน้าที่งาน

2.3 หน่วยงานด้านบริหารงานบุคคลต้องตรวจสอบประวัติของบุคคลก่อนที่จะทำการว่าจ้าง เช่น หลักฐานการศึกษา บุคคลอ้างอิง ประวัติการทำงานจากหน่วยงานต้นสังกัดเดิม และเอกสารที่ทางราชการออกให้ เป็นต้น

2.4 หน่วยงานด้านบริหารงานบุคคลและหน่วยงานต้นสังกัดของพนักงานและลูกจ้าง ต้องจัดการอบรมให้ความรู้ในการทำงานกับพนักงานและลูกจ้างอย่างสม่ำเสมอ เพื่อเพิ่มเติมความรู้และเพิ่มประสิทธิภาพในการทำงานให้กับพนักงาน

2.5 หน่วยงานด้านบริหารงานบุคคลและหน่วยงานที่เกี่ยวข้อง ต้องร่วมกันกำหนดขั้นตอนการปฏิบัติของพนักงานที่ออกเมื่อสิ้นสุดการจ้างงาน

หมวดที่ 5
การสร้างความมั่นคงปลอดภัยด้านทางกายภาพและสภาพแวดล้อม

1. วัตถุประสงค์

หลักการด้านความมั่นคงปลอดภัยที่เกี่ยวข้องกับกระบวนการจัดการทรัพยากรบุคคล ตั้งแต่การรับเข้าทำงานจนถึงการเลิกจ้างทั้งบุคลากรที่เป็นพนักงานและลูกจ้าง มีส่วนสำคัญที่ช่วยลดความเสี่ยงด้านบุคลากร เนื่องจากสารสนเทศอยู่ในรูปแบบที่หลากหลาย ทำให้การควบคุมความมั่นคงปลอดภัยของสารสนเทศโดยระบบอย่างเดียวไม่อาจเกิดประสิทธิผลเต็มที่ ดังนั้น กระบวนการจัดการด้านทรัพยากรบุคคล จึงมีความจำเป็นในการช่วยทำให้สารสนเทศมีความมั่นคงปลอดภัย

2 แนวทางการควบคุม

2.1 มหาวิทยาลัยต้องมีการจัดระดับความสำคัญของพื้นที่ในอาคารสำนักงาน และกำหนดให้มีพื้นที่ควบคุมโดยใช้การประเมินความเสี่ยง ซึ่งการจัดทำการประเมินความเสี่ยงในพื้นที่อาคารสำนักงานเพื่อกำหนดหาพื้นที่ควบคุมความมั่นคงปลอดภัย (Secure Area) และหามาตรการการควบคุมที่เหมาะสมกับพื้นที่ดังกล่าว

2.2 จะต้องแบ่งแยกพื้นที่จัดวางระบบเทคโนโลยีสารสนเทศและการสื่อสารทางกายภาพให้ชัดเจน เช่น พื้นที่ของระบบงานที่ให้บริการ (Production) พื้นที่ของส่วนพัฒนาระบบงาน (Development) เป็นต้น

2.3 จะต้องมีการกำหนดสิทธิผู้เข้าออกห้องศูนย์ปฏิบัติการเครือข่าย โดยจะต้องได้รับการอนุมัติจากหัวหน้ากลุ่มงานข้อมูลสารสนเทศและการสื่อสารเป็นลายลักษณ์อักษร และจัดทำทะเบียนผู้มีสิทธิเข้าพื้นที่ดังกล่าว

2.4 ต้องจัดทำระบบเก็บบันทึกการเข้าออกศูนย์ปฏิบัติการเครือข่ายตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

2.5 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำอาจมีความจำเป็นต้องเข้าออกศูนย์ปฏิบัติการเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

2.6 การเข้าถึงศูนย์ปฏิบัติการเครือข่ายและห้องคอมพิวเตอร์ ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

2.7 จัดทำแนวปฏิบัติสำหรับบุคคลภายนอกที่จำเป็นต้องเข้าพื้นที่ห้องศูนย์ปฏิบัติการเครือข่าย

หมวดที่ 5
การบริหารจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

1. วัตถุประสงค์

เพื่อทำให้เกิดการปฏิบัติงานด้านระบบประมวลผลที่มีความมั่นคงปลอดภัยและถูกต้อง มหาวิทยาลัยควรต้องมีการกำหนดหน้าที่ความรับผิดชอบ และกระบวนการด้านการจัดการและปฏิบัติงานของระบบประมวลผลที่ชัดเจน ควรพิจารณาถึงการแบ่งแยกหน้าที่ที่เหมาะสมควบคู่ไปกับความมีประสิทธิภาพและประสิทธิผลของการปฏิบัติงาน นอกจากกระบวนการทำงานปกติแล้วควรมีการกำหนดขั้นตอนการปฏิบัติเมื่อเกิดเหตุการณ์กระทบความมั่นคงปลอดภัยขึ้นในระบบประมวลผล

2. แนวทางการควบคุม

2.1 มหาวิทยาลัยต้องมีจัดทำขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับระบบงานสารสนเทศเป็นลายลักษณ์อักษร

2.2 ระบบสารสนเทศและระบบเครือข่ายที่ใช้งานจริงของมหาวิทยาลัย จะต้องมีระเบียบปฏิบัติในการควบคุมการเปลี่ยนแปลงของระบบ

2.3 การให้บริการโดยหน่วยงานภายนอก ต้องระบุข้อตกลงในการจัดการความมั่นคงปลอดภัย รายละเอียดบริการและรูปแบบของการบริหารจัดการ

2.4 มหาวิทยาลัยต้องมีการวางแผนและกำหนดสิ่งที่จำเป็นในการได้รับบริการ (Service Level Agreement: SLA) เช่น ข้อมูล, กระบวนการ, คู่มือ, อุปกรณ์ประมวลผล เป็นต้น และต้องมั่นใจว่าการส่งมอบบริการจากหน่วยงานภายนอกเป็นไปอย่างมั่นคงปลอดภัยตลอดการให้บริการ

2.5 ระบบข้อมูลทุกระบบต้องสามารถรองรับการใช้งานตามที่คาดการณ์ไว้ได้ โดยที่หน่วยงานด้านเทคโนโลยีสารสนเทศ มีหน้าที่ประมาณการถึงความจำเป็นทางด้านฮาร์ดแวร์ พื้นที่สำหรับจัดเก็บข้อมูลและระบบ รวมทั้งการเฝ้าสังเกตประสิทธิภาพในการทำงานของระบบ

2.6 ระบบใหม่ที่จะถูกนำมาใช้งานจริงในมหาวิทยาลัย ต้องได้รับการทดสอบในเรื่องของความสามารถในการรองรับการทำงานของระบบนั้น ๆ และระบบนั้น ๆ ควรจะมีประสิทธิภาพเทียบเท่าหรือเหนือกว่าความต้องการทางเทคนิคและความต้องการทางธุรกิจของมหาวิทยาลัย

2.7 เพื่อควบคุม และป้องกันซอฟต์แวร์ และข้อมูล จากโปรแกรมที่ไม่ประสงค์ดีและซอฟต์แวร์อันตรายก่อนการนำซอฟต์แวร์ หรือข้อมูลจากภายนอกมาใช้งานภายในมหาวิทยาลัย ต้องมีการตรวจสอบซอฟต์แวร์ หรือข้อมูลดังกล่าวให้แน่ใจว่าไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

2.8 หน่วยงานผู้ดูแลระบบ ต้องกำหนดให้โปรแกรมค้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย นอกจากนี้ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

2.9 ต้องจัดให้มีระเบียบปฏิบัติที่เป็นเอกสารในการสำรองและกู้ข้อมูลสำหรับข้อมูลของตน และระเบียบปฏิบัติต้องได้รับการอนุมัติจากหัวหน้า หน่วยงานเทคโนโลยีสารสนเทศ

2.10 หน่วยงานผู้ดูแลระบบ ต้องทำการสำรองข้อมูลและเก็บรักษาไว้ตามแนวทางการปฏิบัติการเก็บรักษาข้อมูลอิเล็กทรอนิกส์ของมหาวิทยาลัย รวมทั้งจดหมายอิเล็กทรอนิกส์

2.11 หน่วยงานผู้ดูแลระบบต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบ โดยระบบหลักต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริง แต่ทดสอบบนระบบทดสอบ นอกจากนี้ ผู้ดูแลระบบยังต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์และเก็บรักษาไว้ตามแนวทางการปฏิบัติการเก็บรักษาข้อมูล โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลทางธุรกิจที่สำคัญด้วย

2.12 ในระบบคอมพิวเตอร์ระดับคอมพิวเตอร์ส่วนบุคคล ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลไฟล์ที่สำคัญ

2.13 กำหนดและจัดทำแผนผังแสดงเครือข่ายสื่อสาร (Network Configuration) แสดงถึงข้อมูลเกี่ยวกับอุปกรณ์และคู่สายที่ใช้ในการสื่อสารของเครือข่ายทั้งหมดอย่างชัดเจน

2.14 จัดให้มีการควบคุมการติดตั้งอุปกรณ์สื่อสารให้สอดคล้องกับแผนผังแสดงเครือข่ายสื่อสารที่ได้จัดทำไว้

2.15 มีมาตรการในการควบคุมดูแลสภาพและประเมินประสิทธิภาพการใช้งานของคู่สาย สายสื่อสาร และอุปกรณ์ในเครือข่ายสื่อสาร เพื่อให้พร้อมใช้งานตลอดเวลา

2.16 จัดทำมาตรการเพื่อป้องกันความเสียหายต่อการดำเนินธุรกิจ อันเนื่องมากจากความเสียหายของสื่อบันทึกข้อมูล สื่อบันทึกข้อมูลต่าง ๆ ควรได้รับการควบคุมและจัดการอย่างเหมาะสม ทั้งในเรื่องของการจัดเก็บ การเข้าใช้งาน และการทำลาย

2.17 จัดทำขั้นตอนปฏิบัติ และข้อบังคับในการใช้งานอุปกรณ์ติดต่อสื่อสารอิเล็กทรอนิกส์ สำหรับการแลกเปลี่ยนสารสนเทศ

2.18 การแลกเปลี่ยนข้อมูลและซอฟต์แวร์กับหน่วยงานภายนอก ต้องได้รับอนุญาตจากผู้บริหารและต้องกระทำโดยมีข้อตกลงในการแลกเปลี่ยนดังกล่าว ที่ครอบคลุมรายละเอียดด้านการควบคุมความมั่นคงปลอดภัย ซึ่งได้จากการประเมินความเสี่ยง รวมถึงความรับผิดชอบทั้งของมหาวิทยาลัยและหน่วยงานภายนอกในการแลกเปลี่ยนดังกล่าว

2.19 ผู้ดูแลระบบต้องเฝ้าระวังการใช้งานระบบของผู้ใช้ การเฝ้าสังเกตระบบถือว่าเป็นส่วนหนึ่งของงานการดูแลระบบ อันได้แก่ การติดตามดูแลการใช้งาน ประสิทธิภาพการประมวลผลและการทำงานของระบบการเข้าถึงของผู้ใช้ และความพร้อมในการใช้งานหรือให้บริการของระบบ

2.20 เจ้าของระบบงานต้องกำหนดระยะเวลาของการจัดเก็บบันทึกเหตุการณ์ต่าง ๆ ของระบบโดยพิจารณาจากปัจจัยความเสี่ยงที่เกี่ยวข้อง เช่น ความสำคัญของระบบการประมวลผล มูลค่าของข้อมูล เป็นต้น

2.21 บันทึกเหตุการณ์ต่าง ๆ ต้องได้รับการตรวจสอบเพื่อหาสาเหตุของเหตุต้องสงสัย ซึ่งความถี่ในการตรวจสอบนั้นขึ้นอยู่กับปัจจัยความเสี่ยงที่เกี่ยวข้อง เช่น ความสำคัญของระบบการประมวลผล มูลค่าของข้อมูล ประวัติการใช้งานระบบในทางที่ผิด และการเชื่อมต่อระหว่างระบบ เป็นต้น

หมวดที่ 7
การควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ ระบบสารสนเทศ ข้อมูลสารสนเทศ ข้อมูลอิเล็กทรอนิกส์ และข้อมูลคอมพิวเตอร์

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศ และการสื่อสาร เครือข่ายสื่อสารของมหาวิทยาลัย และป้องกันการบุกรุกผ่านระบบเครือข่ายจาก ผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยได้อย่างถูกต้อง

2. แนวทางการควบคุม

2.1 มหาวิทยาลัยต้องมีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

2.2 มหาวิทยาลัยต้องมีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของมหาวิทยาลัย

2.3 มหาวิทยาลัยจะต้องมีการกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2.4 มหาวิทยาลัยต้องกำหนดการเข้าใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น 2 ส่วน คือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

2.5 มหาวิทยาลัยจะต้องมีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (use access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตะหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

2.6 มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

2.7 มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการเครือข่ายโดยไม่ได้รับอนุญาต

2.8 มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติกรโดยไม่ได้รับอนุญาต

2.9 มีการควบคุมการเข้าถึงระบบงานหรือโปรแกรมประยุกต์ และสารสนเทศ (application and information access control)

หมวดที่ 8
การจัดหาหรือจัดให้มี การพัฒนา และการบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์ ระบบคอมพิวเตอร์ ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

1. วัตถุประสงค์

เพื่อให้มั่นใจได้ว่าการพัฒนาระบบงาน ได้คำนึงถึงความมั่นคงปลอดภัย และการควบคุมที่เพียงพอ จึงจำเป็นต้องมีการกำหนดให้มีการพิจารณาถึงความต้องการด้านความมั่นคงปลอดภัยของระบบงานก่อนที่จะมีการพัฒนาระบบ รวมถึงการกำหนดให้มีการควบคุมภายในระบบงาน เช่น การตรวจสอบความถูกต้องของข้อมูล ตั้งแต่การนำข้อมูลเข้าสู่ระบบการประมวลผล จนกระทั่งการตรวจสอบผลลัพธ์ที่ได้จากระบบ

2. แนวทางการควบคุม

2.1 เจ้าของระบบงาน ต้องกำหนดความต้องการด้านความมั่นคงปลอดภัยของระบบงานก่อนที่จะพัฒนาหรือจัดหาระบบงาน โดยจะต้องจัดทำเป็นเอกสาร ซึ่งถือเป็นส่วนหนึ่งของเอกสารข้อกำหนดในการพัฒนาหรือจัดหาระบบงาน

2.2 โปรแกรมประยุกต์ของมหาวิทยาลัยที่มีการป้อนข้อมูลเข้าสู่ระบบ จะต้องมีการตรวจสอบความถูกต้องของข้อมูลที่ได้รับจากการป้อนข้อมูล ก่อนที่จะนำข้อมูลนั้นไปประมวลผลต่อ

2.3 ในระบบประมวลผลที่สำคัญของมหาวิทยาลัย ต้องมีการตรวจสอบข้อมูลในระบบกับข้อมูลที่เป็นเอกสารเพื่อตรวจหาความผิดพลาดจากการป้อนข้อมูล หรือการลักลอบเปลี่ยนแปลงข้อมูล

2.4 ระบบประมวลผล ต้องออกแบบให้มีความสามารถในการสอบทาน เพื่อตรวจจับกรณีการประมวลผลข้อมูลมีความผิดพลาดหรือเสียหาย

2.5 ระบบประมวลผลที่สำคัญ ต้องมีการตรวจสอบความถูกต้องของการประมวลผลอย่างสม่ำเสมอ

2.6 กำหนดให้มีการตรวจสอบความถูกต้องของข้อมูลผลลัพธ์ที่ได้จากระบบคอมพิวเตอร์ เพื่อมั่นใจว่าข้อมูลมีความถูกต้องสมบูรณ์

2.7 การปรับปรุงแก้ไขระบบงานต่าง ๆ ต้องจัดทำเป็นเอกสารและสามารถติดตามสถานะได้ รวมถึงต้องมีเอกสารสนับสนุน เช่น แผนการทดสอบการปรับปรุงแก้ไขโปรแกรม และผลการทดสอบ

หมวดที่ 9
การบริหารจัดการสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด

1. วัตถุประสงค์

เพื่อป้องกัน และรับมือกับเหตุการณ์ และจุดอ่อน ที่เกี่ยวข้องกับความมั่นคงปลอดภัยต่อระบบสารสนเทศในช่วงระยะเวลาที่เหมาะสม

2. แนวทางการควบคุม

2.1 ผู้ใช้งาน พนักงาน ลูกจ้าง ผู้เกี่ยวข้องจากภายนอกทั้งหมด มีหน้าที่รับผิดชอบในการบำรุงดูแลรักษาระบบสารสนเทศ เมื่อใดก็ตามที่เกิดเหตุการณ์ความมั่นคงปลอดภัยสารสนเทศ ทุกคนต้องรายงานเหตุการณ์ที่เกิดขึ้นให้กับหน่วยงานความมั่นคงปลอดภัยสารสนเทศได้ทราบทันที

2.2 เมื่อเหตุการณ์ผิดปกติที่ส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูลได้ถูกรายงานไปยังบุคคลหรือหน่วยงานที่รับผิดชอบแล้ว หน่วยงานดังกล่าวต้องทำการวิเคราะห์และกำหนดความรุนแรงของเหตุการณ์โดยจำแนกตามระดับความรุนแรงของเหตุการณ์นั้น ๆ

2.3 ในแต่ละระดับความรุนแรงของเหตุการณ์ ต้องมีระเบียบปฏิบัติในการดำเนินการจัดการสำหรับเหตุการณ์ในระดับดังกล่าว

2.4 ผู้ใช้งาน พนักงาน ลูกจ้าง ผู้เกี่ยวข้องจากภายนอกทั้งหมดซึ่งพบจุดอ่อนช่องโหว่ในระบบสารสนเทศจะต้องไม่เปิดเผย เผยแพร่ สนทนาหรือกระทำการใด ๆ อันเป็นการเผยแพร่ต่อผู้อื่น โดยให้ทำการแจ้งต่อหน่วยงานความมั่นคงปลอดภัยสารสนเทศโดยด่วนที่สุด

2.5 ต้องมีการกำหนดหน้าที่สำหรับหน่วยงานความมั่นคงปลอดภัยสารสนเทศ ในการแก้ไขปัญหาด้านความมั่นคงปลอดภัยสารสนเทศ เมื่อเกิดเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย โดยจะต้องได้รับการกำหนดและมอบหมายสิทธิอย่างชัดเจนในการดำเนินการแก้ไขปัญหา

2.6 ทีมงานในการจัดการกับเหตุการณ์กระทบความมั่นคงปลอดภัยสารสนเทศ ที่เกี่ยวข้องกับระบบคอมพิวเตอร์ หรือ CIRT (Computer Incident Response Team) ควรประกอบด้วยตัวแทนจากหน่วยงานต่าง ๆ ซึ่งมีความรู้ทั้งทางด้านระบบธุรกิจ และทางด้านเทคนิคของมหาวิทยาลัย โดยเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ กลุ่มบุคคลเหล่านี้จะมีส่วนร่วมในการแก้ไขปัญหารวมถึงกำหนดมาตรการป้องกันด้านความมั่นคงปลอดภัยสารสนเทศ

2.7 หน่วยงานความมั่นคงปลอดภัยสารสนเทศ ต้องจัดเตรียมรายงานผลการวิเคราะห์ปัญหาความมั่นคงปลอดภัยระบบสารสนเทศและเหตุการณ์ละเมิด

2.8 เมื่อใดก็ตามที่มีหลักฐานบ่งชี้ชัดว่า ระบบสารสนเทศได้ถูกกระทำการละเมิดโดยการกระทำผิดทางคอมพิวเตอร์หรือการสื่อสาร หน่วยงานความมั่นคงปลอดภัยสารสนเทศต้องเริ่มดำเนินการกระบวนการตรวจสอบรวบรวมข้อมูลให้เพียงพอต่อการนำเสนอผู้บริหารเพื่อที่จะใช้ในการดำเนินการขั้นต่อไป และให้มั่นใจว่าจะไม่เกิดเหตุการณ์ซ้ำ

หมวดที่ 10
การบริหารจัดการด้านการบริการหรือการดำเนินงานของหน่วยงานหรือองค์กร เพื่อให้มีความต่อเนื่อง

1. วัตถุประสงค์

เพื่อป้องกันและรับมือกับการหยุดชะงักของการดำเนินธุรกิจ อันเนื่องมาจากภัยคุกคามต่อการทำงานของระบบ ไม่ว่าจะด้วยอุบัติเหตุ ภัยธรรมชาติ หรือจากเหตุการณ์ที่ไม่สามารถคาดการณ์ได้ล่วงหน้า เหตุการณ์ต่าง ๆ

2. แนวทางการควบคุม

2.1 ผู้บริหารหรือหน่วยงานที่เกี่ยวข้องต้องมีการจัดการกระบวนการต่าง ๆ เพื่อพัฒนาและคงไว้ซึ่งความต่อเนื่องทางธุรกิจของมหาวิทยาลัย

2.2 หน่วยงานเจ้าของกระบวนการรวมถึงหน่วยงานเจ้าของระบบงานธุรกิจที่สนับสนุนกระบวนการธุรกิจนั้น ต้องเข้าร่วมในการดำเนินการระบุเหตุการณ์ที่อาจส่งผลกระทบกับกระบวนการทางธุรกิจ ตลอดจนการประเมินความเสี่ยง เพื่อให้ได้มาซึ่งข้อมูลที่มีความถูกต้อง และครบถ้วนในการดำเนินการจัดทำแผนบริหารจัดการความต่อเนื่องในการดำเนินธุรกิจ

2.3 ผู้บริหารต้องสร้างโครงร่างสำหรับแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจสำหรับทุกหน่วยงาน และต้องมีรูปแบบของแผนฯ รวมถึงสื่อให้กับเจ้าของแผนฯ ของแต่ละหน่วยงานทราบในการจัดทำ เพื่อความสอดคล้องกันของแต่ละหน่วยงาน และเพื่อสะดวกในการจัดลำดับความสำคัญของแผนฯ

2.4 แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่าง ๆ ต้องถูกจัดทำขึ้นภายใต้กรอบมาตรฐานของแผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจ

2.5 แผนเพื่อก่อให้เกิดความต่อเนื่องทางธุรกิจต่าง ๆ ต้องถูกจัดทำเพื่อให้ความมั่นใจได้ว่าสามารถทำให้กระบวนการทางธุรกิจดำเนินการต่อได้ภายในระยะเวลาที่กำหนดหลังจากที่มีการหยุดชะงักการให้บริการ หรือหลังประสบภัยต่าง ๆ

2.6 เจ้าของแผนฯมีหน้าที่ปรับปรุงแผนฯ และต้องจัดให้มีการทดสอบแผนฯอย่างสม่ำเสมอ เพื่อทำให้มั่นใจได้ว่าเมื่อเกิดเหตุการณ์ที่กระทบต่อกระบวนการทางธุรกิจแล้ว จะสามารถใช้แผนฯและดำเนินการตามแผนฯ ได้อย่างทันท่วงที

หมวดที่ 11
การตรวจสอบและการประเมินผลการปฏิบัติตามนโยบาย มาตรการ หลักเกณฑ์หรือกระบวนการใดๆ รวมทั้งข้อกำหนด ด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

1. วัตถุประสงค์

เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมาย ที่เกี่ยวข้องกับการดำเนินธุรกิจ การที่มหาวิทยาลัยทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้อง จะสามารถทำให้มหาวิทยาลัยมีความตระหนักถึงความเสี่ยงที่เกิดขึ้นรวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

2. แนวทางการควบคุม

2.1 หน่วยงานด้านกฎหมาย ต้องรวบรวมและจัดทำเป็นเอกสารที่ระบุถึงกฎหมาย กฎระเบียบ พระราชบัญญัติ หรือข้อบังคับตามสัญญาต่าง ๆ ที่มีผลบังคับกับมหาวิทยาลัยทั้งหมด ทั้งนี้รวมถึงข้อบังคับด้านกฎหมายที่เกี่ยวข้องกับระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย

2.2 หน่วยงานที่เกี่ยวข้องในแต่ละระบบสารสนเทศ ต้องรับผิดชอบในการปฏิบัติตามข้อบังคับด้านกฎหมายหรือกฎระเบียบที่เกี่ยวข้อง โดยขอคำปรึกษาจากหน่วยงานด้านกฎหมาย

2.3 การใช้งานซอฟแวร์ของมหาวิทยาลัยจะต้องสอดคล้องตามกฎหมายด้านการป้องกันสิทธิและทรัพย์สินทางปัญญา

2.4 ต้องมีการตรวจสอบการปฏิบัติ ตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยทุกปี ซึ่งการตรวจสอบดังกล่าวในเรื่องใด ๆ จะครอบคลุมถึงการปฏิบัติงานที่สอดคล้องกับนโยบาย มาตรฐานและ ระเบียบปฏิบัติที่เกี่ยวข้องในเรื่องนั้น ๆ ในด้านความมั่นคงปลอดภัยสารสนเทศ

2.5 ผู้บริหาร ต้องกำกับดูแลเพื่อให้มั่นใจว่าพนักงานและลูกจ้างทราบถึงความรับผิดชอบด้านการรักษาความมั่นคงปลอดภัยสารสนเทศ และได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของพนักงานและลูกจ้าง จากการปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยของสารสนเทศ

2.6 หน่วยงานด้านเทคโนโลยีสารสนเทศ ต้องป้องกันไม่ให้ผู้ใช้งานนำอุปกรณ์ประมวลผลสารสนเทศไปใช้ผิดวัตถุประสงค์ หรือโดยไม่ได้รับอนุญาต ซึ่งอุปกรณ์ประมวลผลจะต้องใช้สำหรับธุรกิจของมหาวิทยาลัยเท่านั้น