ประกาศมหาวิทยาลัยราชภัฏนครราชสีมา
เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏนครราชสีมา พ.ศ.๒๕๕๗

ด้วยมีพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ตามมาตรา ๕ ที่หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้ดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และมาตรา ๗ แนวนโยบายและแนวปฏิบัตินี้ให้หน่วยงานของรัฐจัดทำประกาศนั้น จึงเห็นเป็นการสมควรกำหนดนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏนครราชสีมา พ.ศ.๒๕๕๗ ขึ้นโดยออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ ประกาศมหาวิทยาลัยราชภัฏนครราชสีมา เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏนครราชสีมา พ.ศ.๒๕๕๗”

ข้อ ๒ ประกาศนี้มีผลใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ประกอบด้วยเนื้อหา ๒ ส่วน ดังนี้

๓.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีเนื้อหาครอบคลุมตามข้อ ๔

๓.๑ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕ ถึง ๑๒

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ประกอบด้วยเนื้อหา ๒ ส่วน ดังนี้

๔.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

๑ ผู้บริหาร เจ้าหน้าที่ผู้ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๒ นโยบายได้ทำเป็นลายลักษณ์อักษร โดยมีการประกาศให้ผู้ใช้งานได้รับทราบและสามารถเข้าถึงได้โดยการเผยแพร่ผ่านทางเว็บไซต์ของมหาวิทยาลัย

๓ กำหนดให้มีผู้รับผิดชอบตามนโยบายและแนวทางปฏิบัติดังกล่าว

๔ มีการกำหนดให้ปรับปรุงนโยบายและแนวทางปฏิบัติ อย่างน้อยปีละ ๑ ครั้ง

๔.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างทั่วถึง โดยให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งการคุ้มครองข้อมูลส่วนบุคคล

๒ มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศ โดยมีการแยกประเภท

และจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองที่พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานระบบสารสนเทศได้อย่างต่อเนื่อง

๓ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายในการตรวจสอบ ประเมินความเสี่ยง และกำหนดมาตรฐานในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔ การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศ

มีนโยบายในการสร้างความรู้ในการใช้ระบบสารสนเทศ โดยการจัดทำคู่มือการจัดการอบรมเพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศแก่ผู้ใช้งาน

ข้อ ๕ ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (access control) ซึ่งมีเนื้อหา ดังนี้

๕.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๕.๒ มีการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง โดยการกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๕.๓ มีการกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๖ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่อง ความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๖.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒ การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๖.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม

๖.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๖.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๗ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังนี้

๗.๑ การใช้งานรหัสผ่าน (password use) ต้องกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๗.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓ การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) โดยต้องไม่ให้สินทรัพย์สารสนเทศอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๗.๔ การเข้ารหัสของผู้ใช้งานมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔

ข้อ ๘ การควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

๘.๑ การใช้งานบริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๘.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศได้

๘.๓ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) กำหนดวิธีการที่สามารถระบุอุปกรณ์บนเครือข่าย และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๘.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๘.๕ การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๘.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกัน หรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึง

๘.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูล หรือสารสนเทศสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึง หรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๙ การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

๙.๑ การกำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๙.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๙.๓ การบริหารจัดการรหัสผ่าน (password management system) ต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๙.๔ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) จำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิด หรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้

๙.๕ การยุติการใช้งานระบบสารสนเทศ (session time-out) เมื่อว่างเว้นจากการใช้งาน

๙.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) จำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้น สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยง หรือมีความสำคัญสูง

ข้อ ๑๐ ให้มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) ดังนี้

๑๐.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึง หรือเข้าใช้งานของผู้ใช้งาน และบุคลากรฝ่ายสนับสนุน การเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์ หรือแอพพลิเคชั่น โดยต้องสอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑๐.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

๑๐.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๐.๔ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติแผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกหน่วยงาน

ข้อ ๑๑ การจัดทำระบบสำรองของระบบสารสนเทศ ตามแนวทางต่อไปนี้

๑๑.๑ ต้องพิจารณาคัดเลือก และจัดทำระบบสำรองที่เหมาะสม ให้อยู่ในสภาพพร้อมใช้งาน

๑๑.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง และปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๑.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๑.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๑๑.๕ ต้องมีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๒ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดังนี้

๑๒.๑ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๑๒.๒ การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยหน่วยตรวจสอบภายใน (internal auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยของสารสนเทศ

ข้อ ๑๓ การกำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายแก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตาม

นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของมหาวิทยาลัยเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ สิงหาคม พ.ศ. ๒๕๕๗

(รองศาสตราจารย์ ดร.วิเชียร ฝอยพิกุล)
อธิการบดี

เอกสารแนบท้ายประกาศ
เรื่อง ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏนครราชสีมา พ.ศ.๒๕๕๗ ว่าด้วย คำนิยาม

๑ “**มหาวิทยาลัย**” หมายความว่า มหาวิทยาลัยราชภัฏนครราชสีมา
๒ “**การรักษาความมั่นคงปลอดภัย**” หมายความว่า การรักษาความปลอดภัยสำหรับระบบสารสนเทศของมหาวิทยาลัย
๓ “**ผู้ใช้งาน**” หมายความว่า นักศึกษา และ บุคลากรของมหาวิทยาลัย ประกอบด้วย ข้าราชการ พนักงานในสถาบันอุดมศึกษาสังกัดมหาวิทยาลัยราชภัฏนครราชสีมา ลูกจ้างประจำ และ รวมถึงบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบสารสนเทศของมหาวิทยาลัย
๔ “**สิทธิของผู้ใช้งาน**” หมายความว่า สิทธิทั่วไปสิทธิจำเพาะสิทธิพิเศษและสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย
๕ “**สินทรัพย์**” หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านสารสนเทศของมหาวิทยาลัย เช่น เครื่องคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ เป็นต้น
๖ “**การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ**” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือ ใช้งานระบบเครือข่าย หรือ ระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
๗ “**ความมั่นคงปลอดภัยด้านสารสนเทศ**” หมายความว่า ความมั่นคงและความปลอดภัยสำหรับระบบสารสนเทศของมหาวิทยาลัย โดยธำรงไว้ซึ่ง ความลับ (Confidentiality) ความถูกต้องครบถ้วน(Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
๘ “**เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)** ”หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการ หรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือ มาตรการป้องกันที่ล้มเหลว หรือ เหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
๙ “**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด(Information Security Incident)**”หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือ ไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบสารสนเทศของมหาวิทยาลัยถูกบุกรุก และความมั่นคงปลอดภัยถูกคุกคาม
๑๐ “**ระบบคอมพิวเตอร์**” หมายความว่า อุปกรณ์ หรือ ชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
๑๑ “**ระบบเครือข่าย**” หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของมหาวิทยาลัย เช่น ระบบแลน (Lan) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

๑๒ “**ระบบเทคโนโลยีสารสนเทศ (Information Technology System)**” หมายความถึง ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสารซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรมข้อมูลและสารสนเทศ เป็นต้น

๑๓ “**ข้อมูลคอมพิวเตอร์**” หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๔ “**สารสนเทศ(Information)**”หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

๑๕ “**ผู้ดูแลระบบ(System Administrator)**”หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบ ดูแลรักษา หรือจัดการระบบคอมพิวเตอร์ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๑๖ “**จดหมายอิเล็กทรอนิกส์ (E-Mail)**”หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียงที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

๑๗ “**รหัสผ่าน(Password)**”หมายความว่า ตัวอักษร หรืออักขระ หรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูล และระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ

๑๘ “**บัญชีผู้ใช้บริการ(Account)**”หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์และบริการในระบบเครือข่ายของมหาวิทยาลัย

๑๙ “**โปรแกรมประสงค์ร้าย(Malware)**” หมายความว่า โปรแกรมคอมพิวเตอร์ ชุดคำสั่ง และหรือ ข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวน หรือสร้างความเสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์ หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือ สปายแวร์ (Spyware) หรือ หนอน (Worm) หรือ โทรจัน (Trojan horse) หรือ ฟิชชิง(Phishing) หรือ จดหมายลูกโซ่ (Mass Mailing) เป็นต้น

๒๐ “**ชื่อเครื่องคอมพิวเตอร์(Computer Name)**” หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่าย โดยจะมีชื่อที่ไม่ซ้ำกันทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

๒๑ “**สื่อบันทึกพกพา**” หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึก หรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

๒๒ “**ไบออส(Bios)**”หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนเมนบอร์ดของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนเมนบอร์ด

๒๓ “**การตั้งค่าระบบ(Configuration)**” หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรม หรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

๒๔ “**เลขที่อยู่ไอพี(IP Address)**” หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๒๕ “**แบนด์วิดท์(Bandwidth)**” หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถถ่ายโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

๒๖ “**ชื่อผู้ใช้(Username)**”หมายความว่า ชุดของตัวอักษร หรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๒๗ **“ลงบันทึกเข้า (Login)”**หมายความว่า กระบวนการที่ผู้ใช้บริการต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง

๒๘ **“ลงบันทึกออก (Logout)”**หมายความว่า กระบวนการที่ผู้ใช้บริการทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

๒๙ **“อัพเดท (Update)”**หมายความว่า การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

๓๐ “**ช่องโหว่(Vulnerability)**” หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยอาจเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓๑ **“อุปกรณ์กระจายสัญญาณ(Access Point)”**หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณเครือข่ายไร้สาย

๓๒ **“SSID (Service Set Identifier)”**หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๓๓ “**ค่าโดยปริยาย(Default)**”หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้าและนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้บริการ (USER)

๓๔ **“MAC Address (Media Access Control Address)”**หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ทการ์ดโดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่

๓๕ **“VPN (Virtual Private Network)”**หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ตทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๖ **“การพิสูจน์ยืนยันตัวตน (Authentication)”**หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการ โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

๓๗ **“แผนผังระบบเครือข่าย (Network Diagram)”**หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของหน่วยงาน

๓๘ “**Command Line**” หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

๓๙ “**Firewall Log**” หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์เพื่อตรวจสอบประเภทของการสื่อสารปริมาณการสื่อสารนอกจากนั้นแล้ว ยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในหน่วยงาน

๔๐ “**DOD 5220.22-M**” หมายความว่า การลบข้อมูลอย่างสมบูรณ์ซึ่งได้รับการยอมรับและใช้งานกับกระทรวงกลาโหม ประเทศสหรัฐอเมริกา โดยทำให้ไม่สามารถกู้ไฟล์กลับคืนมาได้

๔๑ **“ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor)”**หมายความว่า ผู้ที่ได้รับมอบหมายจากหน่วยงานให้มีสิทธิในการตรวจสอบระบบสารสนเทศหรือระบบเครือข่ายของหน่วยงาน

๔๒ **“เวลาอ้างอิงสากล (Stratum 0)”**หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากลในประเทศไทย โดยการอ้างอิงกับหน่วยงานมาตรฐาน เช่น กรมอุทกศาสตร์กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ เพื่อให้สอดคล้องกับพระราชบัญญัติว่าการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๔๓ **“ข้อมูลจราจรทางคอมพิวเตอร์ (Log)”**หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

เอกสารแนบท้ายประกาศ
เรื่อง นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏนครราชสีมา ๒๕๕๗

คำนำ

ปัจจุบันเทคโนโลยีสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์เป็นสิ่งสำคัญสำหรับมหาวิทยาลัย เพื่อช่วยอำนวยความสะดวกในการดำเนินงานในด้านต่างๆ อย่างไรก็ตามแม้ว่าเทคโนโลยีสารสนเทศทำให้การเข้าถึงข้อมูลมีความรวดเร็ว และช่วยประหยัดต้นทุนในการดำเนินงาน แต่การที่ระบบเครือข่ายคอมพิวเตอร์ต้องสามารถเชื่อมต่อกับระบบต่างๆ อาทิ การรับส่งจดหมายอิเล็กทรอนิกส์ เว็บไซต์ และอื่นๆ ซึ่งแม้จะมีประโยชน์อย่างมากแต่ในขณะเดียวกันก็มีความเสี่ยงสูงและอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติงานได้เช่นกัน เพราะการใช้งานระบบเครือข่ายคอมพิวเตอร์ทำให้ต้องเปิดประตูเพื่อติดต่อกับภายนอกทำให้มีโอกาสถูกบุกรุกได้มากขึ้น และหลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย การโจมตีทางระบบเครือข่าย การขโมยข้อมูล ซึ่งสิ่งเหล่านี้เป็นการสร้างความเสียหายต่อระบบสารสนเทศและทำให้เสียชื่อเสียง หรือภาพลักษณ์ของมหาวิทยาลัย ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านสารสนเทศจึงจะต้องตระหนักถึงความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้นมหาวิทยาลัยจึงได้แต่งตั้งคณะกรรมการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยขึ้น เพื่อจัดทำนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินงานมีความมั่นคงปลอดภัยเชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

อย่างไรก็ตามการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศเป็นงานที่ต้องได้รับความร่วมมือในการปฏิบัติตามนโยบายและข้อปฏิบัติจากทุกหน่วยงาน รวมทั้งต้องทำอย่างต่อเนื่อง มีการตรวจสอบ และปรับปรุงอย่างสม่ำเสมอเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไป คณะกรรมการฯ จึงหวังเป็นอย่างยิ่งว่า นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้ที่เกี่ยวข้องของมหาวิทยาลัยทุกท่านในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยต่อไป

คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏนครราชสีมา

สารบัญ

หน้า

นโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยราชภัฏนครราชสีมา ๒๕๕๗

๑. หลักการและเหตุผล

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ รวมทั้งจากประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๕ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร เพื่อให้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศจึงได้จัดทำนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อรักษาความมั่นคงปลอดภัยของข้อมูล และระบบสารสนเทศซึ่งเป็นเครื่องมือที่สำคัญในการปฏิบัติงานและการบริหารราชการต่อไป

๒. วัตถุประสงค์

๒.๑ เพื่อให้มีนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ซึ่งเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อกำหนดแนวทางและวิธีการปฏิบัติให้บุคลากรและบุคคลที่ปฏิบัติงานให้กับหน่วยงาน รวมทั้งการยืนยันตัวบุคคล การเข้าถึงและการควบคุมการใช้งานระบบสารสนเทศ

๒.๓ เพื่อให้มีการสำรองข้อมูลสารสนเทศอย่างสม่ำเสมอ และมีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ให้สามารถกู้ระบบกลับคืนมาได้ในระยะเวลาที่เหมาะสม เพื่อให้ใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง และสอดคล้องกับการใช้งานตามภารกิจของมหาวิทยาลัย

๒.๔ เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศอย่างสม่ำเสมอ

๒.๕ เพื่อสร้างความตระหนักถึงความสำคัญของการรักษาความปลอดภัยในการใช้งานระบบสารสนเทศ และส่งเสริมให้เกิดความรู้ความเข้าใจและการให้การอบรมทางด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้แก่บุคลากร และผู้เกี่ยวข้องในการดำเนินงาน

๓. เป้าหมายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจ และนโยบายของมหาวิทยาลัย

๓.๒ กำหนดข้อปฏิบัติ แนวทางแก้ไขตามความเหมาะสม หากมีการละเมิดหรือฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๓.๓. กำกับดูแลการดำเนินงาน เพื่อบริหารจัดการให้ระบบสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๔ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรที่เกี่ยวข้องของมหาวิทยาลัย

๓.๕ ติดตามตรวจสอบการดำเนินงาน และปรับปรุงนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

๓.๖ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ที่รับผิดชอบด้านสารสนเทศของมหาวิทยาลัย เป็นผู้กำกับดูแล เพื่อป้องกันความเสี่ยง หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายแก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง

๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏนครราชสีมา จัดทำขึ้นเพื่อกำหนดแนวทางและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยแบ่งนโยบายออกเป็น ๔ ด้าน ดังต่อไปนี้

ด้านที่ ๑. นโยบายควบคุมการเข้าถึงและใช้งานสารสนเทศ
ด้านที่ ๒. นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ
ด้านที่ ๓. นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
ด้านที่ ๔. นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

ด้านที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานสารสนเทศ

วัตถุประสงค์

เพื่อให้มีการควบคุมการเข้าถึงและการใช้งานสารสนเทศ ตามมาตรา ๕ (๑) ของพระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ มหาวิทยาลัยจึงกำหนดนโยบายและแนวปฏิบัติในการควบคุมการเข้าถึงและการใช้งานสารสนเทศ เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอกที่เข้ามาใช้งาน หรือปฏิบัติงานให้กับหน่วยงานได้รับรู้ และสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของมหาวิทยาลัย (CIO : Chief Information Officer)
๒. สำนักคอมพิวเตอร์
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

- มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์ ThaiCERT ประจำปี ๒๕๕๐

นโยบาย

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

๑.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ให้ดำเนินการโดยคำนึงถึงความมั่นคงปลอดภัยในการใช้งานเป็นสำคัญ โดยจัดทำบัญชีครุภัณฑ์ที่เกี่ยวข้องกับงานสารสนเทศ หรือทะเบียนคุมทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบ หรือ การทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒ กำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงและควบคุมการใช้งานสารสนเทศ เรื่อง การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๑.๓ มีขั้นตอนในการปฏิบัติเพื่อกำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับและการเข้าถึงข้อมูล ตามระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อปฏิบัติ

๑. การควบคุมการเข้าถึงและการใช้งานสารสนเทศ (Access Control)

๑.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ให้ดำเนินการดังนี้

(๑) ให้จัดทำบัญชีครุภัณฑ์ อุปกรณ์ในการประมวลผลข้อมูลในแต่ละหน่วยงานภายใน

(๒) ให้กำหนดผู้ที่ทำหน้าที่รับผิดชอบในการใช้งานครุภัณฑ์ โดยระบุผู้รับผิดชอบครุภัณฑ์ สิทธิในการใช้งานครุภัณฑ์ สถานที่นำไปใช้งาน และอ้างอิงหมายเลขครุภัณฑ์ตามที่งานพัสดุกลางกำหนด

๑.๒ การกำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ

(๑) การกำหนดสิทธิของผู้ใช้งาน ให้กำหนดสิทธิของผู้ใช้งานโดยแบ่งออกเป็น ๕ กลุ่ม คือ

- อ่านอย่างเดียว
- สร้างข้อมูล
- แก้ไขข้อมูล
- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์ในการมอบสิทธิ การระงับสิทธิ การมอบอำนาจ ให้ดำเนินการโดยเป็นไปตามการบริหารจัดการสิทธิของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของหน่วยงานจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์ หรือ ผู้ที่ได้รับมอบหมาย

๑.๓ การควบคุมการใช้ข้อมูล

(๑) การจัดแบ่งประเภทของข้อมูล ให้แบ่งออกเป็น ๒ กลุ่ม คือ

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลงบประมาณ การเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศตามพันธกิจ เช่น ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

(๒) การจัดแบ่งลำดับชั้นความลับของข้อมูล ให้แบ่งออกเป็น ๔ ระดับ คือ

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผย หรือเผยแพร่ทั่วไปได้

(๓) การจัดแบ่งระดับชั้นการเข้าถึงข้อมูล ให้แบ่งออกเป็น ๔ ระดับ คือ

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย
- ระดับชั้นสำหรับผู้ปฏิบัติงาน
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(๔) การกำหนดเวลาการเข้าถึงข้อมูล ให้แบ่งออกเป็น ๒ กลุ่ม คือ

- ระบบงานบริการ (Front Office) สำหรับผู้ใช้งานสามารถเข้าถึงได้ตลอดเวลา

- ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในตามที่หน่วยงานกำหนด

(๕) การกำหนดจำนวนช่องทางการเข้าถึง ให้แบ่งออกเป็น ๒ แบบ คือ

- ช่องทางการใช้งานแบบมีสาย (Wired LAN)
- ช่องทางการใช้งานแบบไร้สาย (Wireless LAN)

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Mission Requirements for Access Control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑) การควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงสารสนเทศ และสิทธิการใช้งานสารสนเทศ ดังนี้

- ระดับชั้นสำหรับผู้บริหาร หรือผู้ที่ได้รับมอบหมาย มีหน้าที่ตรวจสอบความเหมาะสมของการควบคุมการเข้าถึงสารสนเทศ และสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน
- ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย มีหน้าที่ในการควบคุมการเข้าถึงสารสนเทศ และสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน
- ระดับชั้นสำหรับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึก ตรวจสอบ ปรับปรุงและรายงานข้อมูลตามต้องการของมหาวิทยาลัย
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามที่มหาวิทยาลัยกำหนด

(๒) การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

- คณะกรรมการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ เป็นผู้ดำเนินการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย รายงานผลและข้อเสนอต่อมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง เพื่อนำผลไปปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานต่อไป
- หน่วยงานภายในของมหาวิทยาลัย มีหน้าที่รายงานปัญหาและข้อเสนอแนะ โดยมีการตั้งผู้ดูแลระบบประจำหน่วยงานเพื่อเป็นคณะกรรมการประสานงานการใช้งานสารสนเทศ

๒. การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้งาน (User Access Management)

เพื่อควบคุมการเข้าถึงสารสนเทศ ระบบเครือข่าย เฉพาะผู้ที่ได้รับอนุญาต และสามารถตรวจสอบติดตามผู้ใช้งานผ่านระบบพิสูจน์ตัวตน รวมทั้งการกำหนดหลักสูตรในการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

๒.๑ การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

(๑) มีการกำหนดหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) มีการจัดอบรมเพื่อให้ความรู้กับผู้ใช้งาน เรื่องความมั่นคงปลอดภัยด้านสารสนเทศ เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด (Information Security Incident) เพื่อให้เกิดความตระหนักถึงภัยและผลกระทบที่เกิดจากการใช้งานสารสนเทศโดยไม่ระมัดระวัง รวมถึงการกำหนดมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งานของระบบเครือข่าย (User Registration) ให้ครอบคลุมในเรื่องต่อไปนี้

(๑) การจัดทำบัญชีผู้ใช้ (Accounts) เพื่อตรวจสอบสิทธิ และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการทำบัญชีผู้ใช้งานแยกกันระหว่างบุคลากร นักศึกษา ตามหน่วยงานเป็นรายบุคคลไม่ซ้ำซ้อนกัน รวมทั้งการบันทึกและจัดเก็บข้อมูลเพื่อให้ตรวจสอบได้

(๓) กำหนดให้มีการจัดทำเอกสาร หรือ สิ่งที่แสดงเป็นลายลักษณ์อักษรให้กับผู้ใช้งาน (Username)เพื่อให้เข้าใจสิทธิและหน้าที่ที่ต้องรับผิดชอบ

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้ชื่อผู้ใช้งาน (Username) เดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น

๒.๓ มีการบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

ต้องแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้การเข้าถึงและใช้งานสารสนเทศแต่ละกลุ่มเป็นไปตามความเหมาะสม รวมถึงสิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึงและใช้งานสารสนเทศ ดังนี้

(๑) มีกระบวนการในการมอบหมาย หรือกำหนดสิทธิในการใช้งานให้แก่ผู้ใช้งานโดยให้กำหนดกลุ่มผู้ใช้งานออกเป็น ๒ กลุ่ม คือ นักศึกษา และ บุคลากรสายสอนและสายสนับสนุนของมหาวิทยาลัย โดย

- กรณี บุคลากรสายสอนและสายสนับสนุนให้ดำเนินการตรวจสอบการมอบสิทธิ การระงับสิทธิ การมอบอำนาจ โดยกองบริหารงานบุคคล
- กรณี นักศึกษาให้ดำเนินการตรวจสอบดังกล่าว โดยสำนักส่งเสริมวิชาการและงานทะเบียน เพื่อแจ้งสำนักคอมพิวเตอร์ให้ดำเนินการลงทะเบียนผู้ใช้งาน ตามสิทธิต่อไป

(๒) กรณีผู้ใช้งานที่บุคคลภายนอก ซึ่งไม่มีสิทธิในการเข้าถึงและใช้งานสารสนเทศของมหาวิทยาลัยตามข้อ (๑) อาทิ อาจารย์พิเศษ เป็นต้น หากต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการอนุญาตจากอธิการบดี หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษแก่ผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากอธิการบดี หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยมีการกำหนดระยะเวลาใช้งาน และให้ระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๔) มีการจัดเก็บข้อมูลในการมอบหมาย หรือกำหนดสิทธิ

๒.๔ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานผ่านการพิสูจน์ยืนยันตัวตน **(Authentication)** เพื่อเข้าใช้งาน ระบบเทคโนโลยีสารสนเทศ ระบบเครือข่าย ระบบคอมพิวเตอร์ หรือสารสนเทศของหน่วยงาน เช่น การเข้าใช้งานสารสนเทศเพื่อการบริหาร (MIS) การเข้าใช้งาน E-Mail (NRRU MAIL) โดยมีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานต้องดำเนินการ ดังนี้

(๑) มีขั้นตอนสำหรับการปฏิบัติในการบริหารจัดการรหัสผ่าน (User Password) ที่มีความมั่นคงปลอดภัย โดยเมื่อสำนักคอมพิวเตอร์ได้รับแจ้งให้ดำเนินการลงทะเบียนผู้ใช้งาน ตาม ข้อ ๒.๓ แล้วสำนักคอมพิวเตอร์จะได้ส่งมอบ ชื่อผู้ใช้งาน (Username) และ รหัสผ่านชั่วคราว (Temporary Password) สำหรับล็อกอินเข้าใช้งาน เพื่อเปลี่ยนรหัสผ่านให้มีความมั่นคงปลอดภัย

(๒) การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ต้องทำด้วยวิธีการที่ปลอดภัย และถือเป็นความลับ โดยมีการลงนามเพื่อรับรหัสผ่าน

(๓) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษแก่ผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากอธิการบดี หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) โดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(๔) ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตน ห้ามใช้ร่วมกับผู้อื่น ห้ามทำการแจกจ่าย หรือ ให้ผู้อื่นล่วงรู้รหัสผ่าน (Password) ของตนเอง

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้สารสนเทศ และต้องปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก การเปลี่ยนตำแหน่ง การโอนย้าย การสิ้นสุดการจ้าง เป็นต้น โดยมีการดำเนินการดังนี้

(๑) การทบทวนสิทธิการเข้าถึงของผู้ใช้งานสารสนเทศ และการปรับปรุงบัญชีผู้ใช้งานต้องดำเนินการอย่างน้อย ปีละ ๑ ครั้ง

(๒) เมื่อได้รับแจ้งข้อมูลการเปลี่ยนแปลงที่เกิดขึ้นกับผู้ใช้งาน เช่น มีการลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง จบการศึกษา เกษียณอายุราชการ เป็นต้น ต้องมีการทบทวนสิทธิการเข้าถึงของผู้ใช้สารสนเทศ และเพิกถอนสิทธิการเข้าถึงของผู้ใช้งานนั้นๆ

(๓) หลังจากดำเนินการตามข้อ (๒) แล้ว ให้ปรับปรุงบัญชีผู้ใช้งาน และจัดเก็บข้อมูลบัญชีผู้ใช้งานใหม่ให้เป็นปัจจุบัน

๓. การกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อกำหนดหน้าที่รับผิดชอบของผู้ใช้งานให้ตระหนักเรื่องความมั่นคงปลอดภัยในการใช้งานสารสนเทศ รวมทั้งการตรวจสอบติดตามผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผยการล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ โดยต้องมีข้อปฏิบัติ ดังนี้

๓.๑ การใช้งานรหัสผ่าน (User Password)

เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องตั้งรหัสผ่าน (User Password) ให้มีความมั่นคงปลอดภัย (Strong Passwords) ดังนี้

(๑) หลังจากที่ผู้ใช้งานได้รับรหัสผ่านชั่วคราว ตามข้อ ๒.๔ ให้เปลี่ยนรหัสผ่านทันทีเมื่อลงบันทึกเข้า (Login) ใช้งานระบบครั้งแรก

(๒) ต้องกำหนดรหัสผ่านให้มีความมั่นคงปลอดภัย โดยดำเนินการให้มีตัวอักษรจำนวนมากกว่า หรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรภาษาอังกฤษที่เป็นตัวพิมพ์ใหญ่ กับตัวพิมพ์เล็ก หรือ ตัวเลข หรือ สัญลักษณ์เข้าด้วยกัน

(๓) ไม่จดหรือบันทึกรหัสผ่านไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น และต้องไม่กำหนดให้มีการบันทึกรหัสผ่าน (Remember Password) หรือ ระบบเพื่อช่วยจำรหัสผ่าน

(๔) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่น เนื่องจากความจำเป็นในการปฏิบัติงานหลังจากดำเนินการแล้วให้ทำการเปลี่ยนรหัสผ่านใหม่โดยทันที

(๕) ควรมีการเปลี่ยนรหัสผ่านตามเวลาที่เหมาะสม หรือ เปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๓.๒ การกำหนดวิธีการป้องกันอุปกรณ์ประมวลผลสารสนเทศในขณะที่ไม่มีผู้ใช้งาน

เพื่อป้องกันการเข้าถึงอุปกรณ์ประมวลผลสารสนเทศโดยไม่ได้รับอนุญาต การป้องกันการขโมยอุปกรณ์ฯ ให้กำหนดแนวปฏิบัติเพื่อป้องกัน ดังนี้

(๑) มีการกำหนดข้อปฏิบัติในการป้องกันอุปกรณ์คอมพิวเตอร์เพื่อป้องกันการลักขโมย หรือเข้าถึงโดยไม่ได้รับอนุญาต โดยมีการติดตั้งสายล็อคเพื่อการรักษาความปลอดภัยของอุปกรณ์คอมพิวเตอร์ที่ออกแบบเพื่อป้องกันอุปกรณ์คอมพิวเตอร์ เช่น K-Slot ในจอคอมพิวเตอร์เดสก์ทอป เป็นต้น รวมทั้งอาจมีการติดตั้งกล้องวงจรปิดเพื่อตรวจสอบการเข้าออกสถานที่ใช้งาน

(๒) อุปกรณ์และเครื่องคอมพิวเตอร์ขนาดเล็ก เช่น คอมพิวเตอร์โน้ตบุ๊ก ให้จัดเก็บในตู้ที่สามารถล็อกกุญแจได้

(๓) ให้ดำเนินการตั้งรหัสผ่าน (Password) เพื่อป้องกันการเปิดใช้งานอุปกรณ์ฯ เช่น

- การตั้งรหัสผ่าน (Password) เพื่อป้องกันการเข้าถึงไบออส (Bios) ของเครื่องคอมพิวเตอร์
- การตั้งรหัสผ่าน (Password) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการ
- การติดตั้งโปรแกรมเพื่อป้องกันโปรแกรมประสงค์ร้าย (Malware) และอัพเดท (Update) ให้ทันสมัยอยู่เสมอ เพื่อป้องกันช่องโหว่ (Vulnerability) ของอุปกรณ์ฯ

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ โดยกำหนดให้ผู้ใช้งานต้องมีข้อปฏิบัติในการใช้งาน ดังนี้

(๑) มีการกำหนดมาตรการป้องกันทรัพย์สินสารสนเทศของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยสินทรัพย์สารสนเทศที่สำคัญให้อยู่ในสถานการณ์ที่ไม่ปลอดภัย โดยการกำหนด พื้นที่ใช้งานเพื่อป้องกันผู้ที่ไม่เกี่ยวข้องเข้าไปในพื้นที่ใช้งานโดยไม่ได้รับอนุญาต

(๒) มีการกำหนดมาตรการป้องกันการเข้าถึงข้อมูล เอกสาร สื่อบันทึกข้อมูลสารสนเทศ โดยกำหนดข้อปฏิบัติในการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต ดังนี้

๑) การหยุดใช้งานชั่วคราว ต้องกำหนดให้เครื่องคอมพิวเตอร์พักหน้าจอและตั้งรหัสผ่านในการพักหน้าจอ เพื่อให้ผู้ใช้งานต้องพิมพ์รหัสผ่านเพื่อเปิดหน้าจอกลับมาใช้งานใหม่

๒) ต้องทำการบันทึกออก (Logout) จากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๓) สร้างวัฒนธรรมองค์กรให้เกิดความเข้าใจในมาตรการป้องกัน เช่น การเก็บเอกสาร สื่อบันทึกข้อมูลจากโต๊ะทำงาน และเก็บให้ปลอดภัย ก่อนพักหรือเลิกงาน

(๓) มีการกำหนดมาตรการทำลายสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ดังนี้

๑) สื่อบันทึกข้อมูลที่เป็นประเภทจานแม่เหล็ก สื่อบันทึกข้อมูลพกพา ให้ทำการ Format อุปกรณ์ดังกล่าวโดยไม่สามารถเรียกคืนข้อมูลกลับมาได้ ตามมาตรฐาน DOD ๕๒๒๐.๒๒ M

๒) สื่อบันทึกข้อมูลประเภท Optical Disk ทำลายโดยวิธีการหัก หรือ เจาะรู เพื่อไม่สามารถเรียกข้อมูลกลับมาได้

๓.๔ การเข้ารหัสข้อมูล

ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๑) ต้องแสดงหลักฐานเกณฑ์ในการกำหนดเครื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

๒) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ให้ดำเนินการ ดังนี้

๔.๑ การใช้งานระบบเครือข่าย

ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบเครือข่าย เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึง โดยดำเนินการ ดังนี้

๑) มีการป้องกันการเข้าถึงระบบเครือข่ายก่อนใช้งาน ผ่านการพิสูจน์ยืนยันตัวตน

๒) มีการทำแผนผังระบบเครือข่าย (Network Diagram)

๓) มีการกำหนดวิธีการเพื่อควบคุมการเข้าถึงการใช้งานระบบเครือข่ายในรูปแบบต่างๆ ของผู้ใช้งาน เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connection)

ต้องมีข้อปฏิบัติให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย สามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย อาทิ การทำ VPN (Virtual Private Network) ดังนี้

๑) ผู้ใช้งานที่จะเข้าใช้งานระบบเครือข่ายต้องผ่านการพิสูจน์ยืนยันตัวตนก่อนใช้งาน

๒) ให้มีการลงทะเบียนผู้ใช้งานเป็นกรณีเฉพาะ สำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัยที่ต้องการเข้าใช้งานเครือข่ายของมหาวิทยาลัย

๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Network)

ต้องมีกระบวนการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ โดยสามารถใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง ดังนี้

๑) การระบุอุปกรณ์ และการจัดเก็บข้อมูลโดยใช้เลขที่อยู่ไอพี (IP Address) ในการระบุอุปกรณ์

๒) การลงทะเบียน MAC Address (Media Access Control Address) เพื่อแสดงตัวตนและใช้ระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันการเข้าถึง

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑) การปรับเปลี่ยน หรือการเข้าถึงพอร์ตต้องทำหนังสือขออนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษร

๒) ต้องบันทึก และควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

๓) ปิดการใช้งาน หรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้โดยจำกัดระยะเวลาเท่าที่จำเป็นเท่านั้น

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Network)

ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ

๑) เครือข่ายสำหรับกลุ่มผู้ใช้งานภายใน

๒) เครือข่ายสำหรับกลุ่มผู้ใช้งานภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่ใช้งานร่วมกันให้สอดคล้องกับแนวปฏิบัติการการควบคุมการเข้าถึง ดังนี้

๑) กำหนดให้มีการตรวจสอบการเชื่อมต่อเครือข่าย

๒) จำกัดสิทธิของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์การใช้งานตามภารกิจ ดังนี้

๑) ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address Plan)

๒) กำหนดให้มีการเปลี่ยนแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่ายปลายทาง ผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าสู่ระบบจากระยะไกล (Remote Access)

๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบจากภายใน

๒) การเข้าสู่ระบบจากระยะไกล ต้องมีการลงทะเบียนผู้มีสิทธิในการใช้งาน และต้องได้รับการอนุมัติจากผู้อำนวยการสำนักคอมพิวเตอร์

๓) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ให้สิทธิเฉพาะผู้ดูแลระบบเท่านั้น และต้องควบคุมการเข้าสู่ระบบอย่างรัดกุม และทำรายงานแจ้งผู้อำนวยการสำนักคอมพิวเตอร์หลังการใช้งาน

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยต้องกำหนดขั้นตอนในการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยมีการยืนยันตัวตนโดยมีแนวปฏิบัติ ดังนี้

๕.๑ หน้าที่ผู้ดูแลระบบ (System Administrator)

ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์แม่ข่าย และกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งาน

๕.๒ การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มีความปลอดภัย

การเข้าถึงระบบปฏิบัติการจะต้องมีการควบคุมโดยแสดงวิธีการยืนยันตัวตน และดำเนินการให้มีความปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดของระบบ ก่อนการเข้าสู่ระบบจะเสร็จสมบูรณ์

๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓ จำกัดการเชื่อมโยงโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line

๕.๓ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ต้องกำหนดให้มีข้อมูลของผู้เข้าถึงระบบปฏิบัติการเพื่อการยืนยันตัวผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคที่เหมาะสมเพื่อรองรับการยืนยันผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

๑) ให้มีการลงทะเบียนผู้ใช้งานระบบปฏิบัติการเป็นการเฉพาะ โดยต้องมีชื่อผู้ใช้งาน และรหัสผ่าน สำหรับเข้าใช้งาน และกำหนดขั้นตอนทางเทคนิคเฉพาะเพื่อรองรับการยืนยันตัวบุคคลเพิ่มเติม

๒) การอนุญาตให้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกันในการเข้าถึงระบบปฏิบัติการ ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักฯ

๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น RFID หรือ เครื่องอ่านลายนิ้วมือ

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System)

มีระบบบริหารจัดการที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยระบบบริหารจัดการรหัสผ่านจะแจ้งให้ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ และกำหนดให้การตั้งรหัสผ่านมีความมั่นคงปลอดภัย (Strong Passwords) ตามที่ระบุไว้ในข้อ ๓.๑

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ต้องควบคุมการใช้งานโปรแกรมอรรถประโยชน์ ที่จะนำมาใช้กับระบบปฏิบัติการ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้ โดยมีแนวปฏิบัติดังนี้

๑) จำกัดการใช้งาน และกำหนดสิทธิในการใช้โปรแกรมอรรถประโยชน์

๒) กำหนดให้อนุญาตใช้โปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control)

การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศต้องมีการควบคุม ดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่างๆ ของโปรแกรมประยุกต์ หรือแอพพลิเคชั่น โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้โดยมีแนวปฏิบัติดังนี้

๑) ผู้ใช้งานสามารถใช้โปรแกรมประยุกต์หรือแอพพลิเคชั่นตามที่หน่วยงานรับผิดชอบเท่านั้น

๒) ผู้ใช้งานสามารถใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นตามภาระงานที่ได้รับเท่านั้น

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูง

ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูงต่อมหาวิทยาลัย ต้องดำเนินการดังนี้

๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่นๆ แสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกมหาวิทยาลัย (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ มีแนวทางปฏิบัติในการใช้งานดังนี้

๑) ตรวจสอบเครื่องคอมพิวเตอร์ อุปกรณ์และโปรแกรมที่ติดตั้งกับอุปกรณ์ดังกล่าว ว่าอยู่ในสภาพพร้อมใช้งาน หรืออาจเกิดความเสี่ยงในการใช้งานอุปกรณ์

๒) จัดทำเอกสารเพื่อควบคุมการยืมอุปกรณ์ฯ และเมื่อรับคืนต้องตรวจสอบ แก้ไขให้อยู่ในสภาพพร้อมใช้งาน เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์

๓) สร้างวัฒนธรรมในการนำทรัพย์สินของมหาวิทยาลัยไปใช้งาน ผู้ใช้ต้องใช้งานอย่างมีประสิทธิภาพ เพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์

๖.๔ การปฏิบัติงานจากภายนอกมหาวิทยาลัย (Teleworking)

ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติ เพื่อปรับใช้สำหรับการปฏิบัติงานของมหาวิทยาลัยจากภายนอกมหาวิทยาลัย

๑) หน่วยงานที่ต้องปฏิบัติงานจากภายนอกมหาวิทยาลัยต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติ เพื่อควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ

๒) การปฏิบัติงานจากภายนอกมหาวิทยาลัย ต้องได้รับการอนุญาตจากอธิการบดี หรือผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๖.๕ การหมดเวลาในการใช้งานระบบสารสนเทศ (Session Time-out)

เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง ให้ยุติการใช้งานระบบสารสนเทศ โดยดำเนินการดังนี้

๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศของมหาวิทยาลัย (NRRU MIS) เมื่อว่างเว้นจากการใช้งานเป็นเวลาเกิน ๔๕ นาที เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๒) ถ้าไม่มีการใช้งานระบบสารสนเทศของมหาวิทยาลัย (NRRU MIS) ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์ และการเชื่อมต่อเข้าสู่ระบบสารสนเทศโดยทันที

๖.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time)

ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้น

๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้ภายในขอบเขต หรือ ระยะเวลาที่กำหนด เช่น กำหนดให้ใช้งานได้เฉพาะภายในมหาวิทยาลัยเท่านั้น กำหนดให้

ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หรือ กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานปกติของมหาวิทยาลัยเท่านั้น

๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงอันดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และหรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง เช่น ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน เป็นต้น ให้มีการจำกัดการใช้งาน หรือ มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๗ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Lan Access Control)

ผู้ใช้งานที่ต้องการติดตั้งระบบเครือข่ายไร้สาย อุปกรณ์กระจายสัญญาณไร้สาย (Access Point) เพื่อนำมาเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัย ต้องแจ้งสำนักคอมพิวเตอร์ เพื่อมอบหมายผู้ดูแลระบบ (System Administrator) ดำเนินการดังต่อไปนี้

๑) ทำการลงทะเบียนอุปกรณ์ที่จะนำมาใช้เชื่อมต่อระบบเครือข่ายไร้สาย

๒) การควบคุมอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิต ให้มีความมั่นคงปลอดภัยก่อนนำอุปกรณ์นั้นมาใช้งาน

๓) ต้องเปลี่ยนชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายไร้สาย และเลือกใช้ชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดา หรือเจาะรหัสได้โดยง่าย

๔) ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้อำนวยการสำนักทราบโดยทันที

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพ และสภาพแวดล้อม (Physical and Environmental Security)

๘.๑ การกำหนดพื้นที่ที่ต้องรักษาความมั่นคงปลอดภัย

ต้องกำหนดและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน พื้นที่ควบคุมและประกาศให้รับทราบโดยกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศออกเป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) ห้องควบคุมระบบเครือข่าย (Server Room) เป็นต้น

๘.๒ การกำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

การกำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(๑) พื้นที่ทำงานทั่วไป หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ประจำโต๊ะทำงาน หรือห้องเรียน ห้องอบรม ที่ติดตั้งเครื่องคอมพิวเตอร์ เป็นต้น

(๒) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ และ พื้นที่จัดเก็บข้อมูล (Data Storage Area) และห้องควบคุมระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย หรือ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ (System Administrator) หน่วยงานต้องระบุชื่อผู้ปฏิบัติงาน เพื่ออนุญาตให้ผู้ปฏิบัติงานเข้าพื้นที่ทำงาน

๘.๓ การตรวจสอบระบบรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม

การตรวจสอบระบบรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม ที่กำหนดไว้ต้องมีการควบคุม และรักษาความปลอดภัย รวมถึงวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นในสถานการณ์ปัจจุบันอย่างน้อยปีละ ๑ ครั้ง และนำเสนอรายงานต่อผู้บริหารหน่วยงาน

๘.๔ การกำหนดระบบสนับสนุนการทำงานในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

มีระบบสนับสนุนการทำงานในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศที่เพียงพอต่อการใช้งาน โดยให้มีระบบสำรองไฟฟ้า ระบบดับเพลิง ระบบปรับอากาศ ควบคุมความชื้น และให้ติดตั้งกล้องวงจรปิด โดยมีการตรวจสอบ หรือทดสอบระบบสนับสนุนเหล่านั้น อย่างน้อยปีละ ๑ ครั้ง ให้มั่นใจได้ว่า ระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๘.๕ การรักษาความปลอดภัยสายสัญญาณ (Cabling Security)

การตรวจสอบความปลอดภัยสายสัญญาณเครือข่าย และสายเคเบิ้ลอื่นๆ ให้ดำเนินการดังนี้

๑) ให้มีการป้องกันสายสัญญาณเครือข่ายจากการเข้าถึงของบุคคลภายนอก

๒) ให้จัดทำผังสายสัญญาณเครือข่าย และทำป้ายชื่อบนอุปกรณ์ให้รับทราบ

๓) ห้องที่ใช้เป็นจุดเชื่อมต่อสายสัญญาณเครือข่าย อุปกรณ์กระจายสัญญาณประจำอาคาร ต้องมีมาตรการรักษาความปลอดภัย เพื่อป้องกันการเข้าถึงของบุคคลที่ไม่เกี่ยวข้อง

๔) ให้มีการตรวจสอบการทำงานของสายสัญญาณเครือข่าย อย่างน้อยปีละ ๑ ครั้ง และรายงานผลต่อมหาวิทยาลัย

๘.๖ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑) ให้มีการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒) ควบคุมการปฏิบัติงานของผู้ให้บริการภายนอก ที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย รวมทั้งการควบคุมการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้บำรุงรักษาอุปกรณ์จากภายนอก เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์ ประเมินผล และรายงานต่อมหาวิทยาลัย

๘.๗ การนำทรัพย์สินสารสนเทศของมหาวิทยาลัยออกนอกมหาวิทยาลัย (Removal of Property)

กำหนดวิธีการควบคุมการนำอุปกรณ์สารสนเทศออกไปใช้งานนอกมหาวิทยาลัย ดังนี้

๑) การขออนุญาตนำอุปกรณ์สารสนเทศ หรือทรัพย์สินสารสนเทศ ออกไปนอกมหาวิทยาลัย ต้องขออนุญาตตามแบบฟอร์มที่กำหนด และให้หัวหน้าหน่วยงานที่ต้องการนำไปใช้ เป็นผู้ขออนุญาต

๒) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกมหาวิทยาลัย ไม่เกิน ๗ วัน

๓) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบการชำรุดเสียหายของอุปกรณ์

๘.๘ การจัดการอุปกรณ์ที่ใช้งานอยู่นอกมหาวิทยาลัย (Security of Equipment off-premises)

๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์สารสนเทศหรือทรัพย์สินของมหาวิทยาลัยไปใช้งานภายนอกมหาวิทยาลัย เช่น ความปลอดภัยของการขนส่ง และการเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

๒) ไม่ทิ้งอุปกรณ์สารสนเทศหรือทรัพย์สินของมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ

๓) กำหนดผู้รับผิดชอบดูแลอุปกรณ์สารสนเทศหรือทรัพย์สินขณะใช้งานอยู่นอกมหาวิทยาลัย

๘.๙ การกำจัดอุปกรณ์ หรือนำอุปกรณ์กลับมาใช้อีกครั้ง (Secure Disposal or Re-use of Equipment)

๑) การกำจัดอุปกรณ์สารสนเทศหรือนำกลับมาใช้ใหม่ ต้องมีการดำเนินการตรวจสอบและขออนุญาตก่อนดำเนินการตามระเบียบงานพัสดุ

๒) การกำจัดอุปกรณ์สารสนเทศต้องทำลายข้อมูลในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลนั้นได้

๘.๑๐ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศ

๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บ หรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเปลี่ยนแปลงแก้ไขเอกสารนั้น

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ การควบคุมการติดตั้ง หรือปรับปรุงซอฟต์แวร์

การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย เพื่อติดตั้ง หรือปรับปรุง ซอฟต์แวร์ระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่าย ให้ดำเนินการดังนี้

๑) อนุญาตให้ผู้ดูแลระบบที่ได้รับการมอบหมายเท่านั้น เป็นผู้ทำหน้าที่ควบคุมการติดตั้งหรือปรับปรุง ซอฟต์แวร์ระบบสารสนเทศ ในเครื่องคอมพิวเตอร์แม่ข่าย

๒) การติดตั้ง หรือปรับปรุงซอฟต์แวร์ของเครื่องคอมพิวเตอร์แม่ข่ายต้องมีการขออนุมัติก่อนดำเนินการ

๓) กำหนดให้ผู้ดูแลระบบต้องทำการทดสอบระบบสารสนเทศ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ หรือ ซอฟต์แวร์ระบบสารสนเทศที่ต้องการใช้งาน

๔) ไม่ติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่าย กำหนดให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๕) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมและขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศ ในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น

๖) ให้ผู้ดูแลระบบที่เกี่ยวข้องกับระบบสารสนเทศ รายงานการผลการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๙.๒ มาตรการควบคุมช่องโหว่ทางเทคนิค

๑) กำหนดให้มีมาตรการควบคุมช่องโหว่ทางเทคนิค ในการควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย เพื่อใช้บริหารจัดการช่องโหว่ของระบบเหล่านั้น โดยมีการบันทึกข้อมูลดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

- กำหนดมาตรการจัดการกับช่องโหว่ของระบบสารสนเทศอย่างเหมาะสม

๒) มาตรการจัดการกับช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบมีการดำเนินการ ดังนี้

- มีการเฝ้าระวัง และติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศ
- กำหนดให้มีผู้ดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้ง หรือทราบช่องโหว่นั้น

๙.๓ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging)

ต้องการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ เพื่อบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
๓) ข้อมูลวันเวลาที่ออกจากระบบ
๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
๕) ข้อมูลการล๊อกอิน ทั้งที่เสร็จสิ้นและไม่เสร็จสิ้น
๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่เสร็จสิ้นและไม่เสร็จสิ้น
๗) ข้อมูลการตั้งค่าระบบ(Configuration)
๘) ข้อมูลแสดงการใช้งานแอพพลิเคชั่น
๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียนและอ่านไฟล์
๑๐) ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง
๑๑) ข้อมูลโพรโตคอลเครือข่ายที่ใช้
๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
๑๓) แบนด์วิดท์
๑๔) Firewall Log

๑๐. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑๐.๑ การใช้งานสำหรับผู้ใช้งาน

๑) ผู้ใช้งานที่ต้องการใช้งานจดหมายอิเล็กทรอนิคส์ของมหาวิทยาลัย ต้องทำการขออนุญาตเข้าใช้งาน เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

๒) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลอื่นไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่างๆในจดหมายอิเล็กทรอนิกส์นั้น

๓) ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบจดหมายอิเล็กทรอนิกส์ และควรลงชื่อออกจากระบบหลังจากการใช้งาน เพื่อป้องกันบุคคลอื่นเข้าใช้งาน

๑๐.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ใช้งานระบบ(System Administrator)

๑) กำหนดสิทธิเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ให้เหมาะสมกับการใช้บริการ และหน้าที่ความรับผิดชอบของผู้ใช้งาน

๒) มีการทบทวนสิทธิการใช้งานและปรับปรุงบัญชีผู้ใช้งานปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออกหรือเปลี่ยนแปลงตำแหน่ง โอน ย้าย หรือ สิ้นสุดการจ้าง ฯลฯ

๓) ควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (User Access Management) ที่ได้กำหนดไว้

๑๑. การควบคุมการใช้งานระบบอินเทอร์เน็ต (Internet)

๑๑.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อใช้งานระบบอินเทอร์เน็ตให้เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น นอกจากได้รับการอนุมัติจากอธิการบดี หรือ ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO)

๑๑.๒ การใช้จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ต

๑๑.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์ และทำการเข้าสู่เว็บไซท์ที่ไม่เหมาะสม เช่น เว็บไซท์ที่ขัดต่อศีลธรรม เว็บไซท์ที่มีเนื้อหาอันอาจจะกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา พระมหากษัตริย์ เป็นต้น

๑๑.๔ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๑.๕ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ เครือข่ายสังคม ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่เป็นความลับของทางมหาวิทยาลัย ไม่เสนอความคิดเห็น หรือใช้ข้อความยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย

๑๒. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์(Log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์(Log) มีความถูกต้องและสามารถระบุตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

๑๒.๑ จัดเก็บข้อมูลจราจรคอมพิวเตอร์(Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงได้

๑๒.๒ กำหนดให้มีการบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการตรวจสอบ และต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๒.๓ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๒.๔ ต้องตรวจสอบการเทียบเวลาอ้างอิงสากล (Stratum 0)

ด้านที่ ๒
นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยสามารถให้บริการได้อย่างต่อเนื่อง เป็นแนวทางปฏิบัติ และความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัยอย่างเคร่งครัด รวมทั้งสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และการสำรองข้อมูลสารสนเทศ

ผู้รับผิดชอบ

๑.สำนักคอมพิวเตอร์

๒.ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และจัดทำระบบสำรองที่เหมาะสมเพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้งาน

๒. จัดทำ แผนรองรับสถานการณ์ฉุกเฉิน เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุง แผนรองรับสถานการณ์ฉุกเฉิน ดังกล่าวให้สามารถใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๓. กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉิน

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และแผนรองรับสถานการณ์ฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานในมหาวิทยาลัย

ข้อปฏิบัติ

๑. การจัดทำระบบสำรองข้อมูล

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ และการจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑) มีการจัดทำระบบบัญชีระบบสารสนเทศที่มีความสำคัญของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล โดยให้มีการสำรองข้อมูลดังนี้

- กำหนดประเภทของข้อมูลที่ต้องการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม(Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง(Incremental Backup)
- บันทึกข้อมูลของกิจกรรมสำรองข้อมูล ได้แก่ ผู้ดำเนินรายการ วันเวลา ชื่อข้อมูลที่สำรอง
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ และตรวจสอบการกู้คืนข้อมูลจากข้อมูลที่สำรองไว้
- จัดทำ Backup Site เพื่อเก็บข้อมูลสำรอง โดยควรแยกไปที่อาคารอื่นที่มีระยะห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้ในกรณีที่เกิดภัยพิบัติ เช่น ไฟไหม้ น้ำท่วม เป็นต้น

๒. การจัดทำแผนรองรับสถานการณ์ฉุกเฉิน (IT Contingency Plan)

ต้องจัดทำ แผนรองรับสถานการณ์ฉุกเฉิน ที่อาจเกิดขึ้นกับระบบสารสนเทศ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนดังกล่าวให้สามารถใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้เกี่ยวข้อง

๒) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญ และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ปัญหาไฟฟ้า ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือ ปัญหาที่ทำให้ไม่สามารถใช้งานระบบสารสนเทศได้

๓) มีการทบทวนเพื่อปรับปรุงแผนรองรับสถานการณ์ฉุกเฉิน ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๔) การให้ความรู้แก่เจ้าหน้าที่ผู้เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

ด้านที่ ๓

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ รวมทั้งเป็นการป้องกันและลดระดับความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักคอมพิวเตอร์

๒. หน่วยตรวจสอบภายใน (Internal Auditing Unit)

๓. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

-มาตรฐานการรักษาความปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๒.มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง

๓.มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ ๑ ครั้ง ต่อคณะกรรมการบริหารมหาวิทยาลัยเพื่อดำเนินการต่อไป

๔. มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ข้อปฏิบัติ

๑ การตรวจสอบและประเมินความเสี่ยง

มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๒) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน หรือ ผู้ตรวจสอบระบบสารสนเทศจากหน่วยงานภายนอก (External IT Auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยง และระดับความมั่นคงปลอดภัยสารสนเทศ

๒ แนวทางในการตรวจสอบและประเมินความเสี่ยง

มีการกำหนดแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๑) การทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๒) การทบทวนนโยบายและมาตรการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓) มีมาตรการในการตรวจสอบและประเมินระบบสารสนเทศ ดังนี้

- กำหนดให้ผู้ตรวจสอบเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว
- ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลแบบที่ไม่สามารถอ่านอย่างเดียวได้ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้อง ทำลาย หรือลบทันทีที่ตรวจสอบเสร็จ
- ควรกำหนดให้มีการระบุ และจัดสรรทรัพยากรที่จำเป็นต้องใช้ ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
- ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

๓.การรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ

มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ ปีละ ๑ ครั้ง ต่อคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

๔. การแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารเทศ

มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารเทศ โดยเป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ด้านที่ ๔
นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของมหาวิทยาลัย รวมทั้งเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. สำนักคอมพิวเตอร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

-มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. จัดทำแผนการฝึกอบรมทางด้านการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ สำหรับผู้ใช้งาน

๒. จัดทำคู่มือการใช้ระบบสารสนเทศของมหาวิทยาลัยทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์

๓. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย เมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๔. มีการประเมินระดับความรู้ความเข้าใจในการใช้งานระบบสารสนเทศของผู้ใช้งาน

๕. รายงานผลการประเมินระดับความรู้ความเข้าใจในการใช้งานระบบสารสนเทศของผู้ใช้งาน

๖. นำผลการประเมินไปปรับปรุงแผนการการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศสำหรับผู้ใช้งาน

ข้อปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ ทั้งในรูปแบบเอกสาร รูปแบบเอกสารอิเล็กทรอนิกส์และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย

๓. จัดสัมมนาและฝึกอบรมเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน ไม่น้อยกว่าปีละ ๑ ครั้ง หรือ จัดหาวิทยากรที่มีประสบการณ์ด้านการรักษามั่นคงความปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๔. ดำเนินการประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตามประเมินผล และสำรวจความเข้าใจในการใช้งานระบบสารสนเทศของผู้ใช้งาน เพื่อนำไปปรับปรุงแผนการการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศสำหรับผู้ใช้งาน

๖. มีการประเมินระดับความรู้ความเข้าใจในการใช้งานระบบสารสนเทศของผู้ใช้งาน และรายงานผลการประเมินต่อมหาวิทยาลัย