ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบกับพระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ กำหนดให้หน่วยงานของรัฐมีหน้าที่ดำเนินมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และให้การควบคุมการบริหารจัดการ การปฏิบัติงาน การรักษาความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพ มีมาตรฐานในระดับเดียวกัน ตลอดจนสอดคล้องเป็นไปตามพระราชกฤษฎีกาดังกล่าว

อาศัยอำนาจตามความในมาตรา ๒๗ (๑) แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีราชมงคล พ.ศ. ๒๕๔๘ ประกอบกับมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย จึงออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันที่ประกาศเป็นต้นไป

ข้อ ๓ ขอบเขตการดำเนินการ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ และมาตรา ๗ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม (ฉบับที่ ๒) พ.ศ. ๒๕๕๖ กำหนดให้ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร” เพื่อให้การรักษาความมั่นคงปลอดภัยระบบสารสนเทศของมหาวิทยาลัย เป็นไปด้วยความเรียบร้อย

/มีความ...

มีความมั่นคงปลอดภัยและมีประสิทธิภาพ สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องเหมาะสม และเป็นการป้องกันการถูกคุกคามจากผู้ไม่ประสงค์ดีและภัยคุกคามต่าง ๆ มหาวิทยาลัยจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศโดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนการปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและป้องกันภัยคุกคามต่าง ๆ

ข้อ ๔ วัตถุประสงค์

๔.๑ เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมีความมั่นคงปลอดภัยและเชื่อถือได้

๔.๒ เพื่อกำหนดมาตรการ แนวทางปฏิบัติให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยมีการควบคุมการบริหารจัดการ การปฏิบัติงาน การรักษาความมั่นคงปลอดภัยด้านเป็นไปอย่างมีประสิทธิภาพและมีมาตรฐานในระดับเดียวกัน

๔.๓ เพื่อกำหนดความรับผิดชอบ ในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารซึ่งดำรงตำแหน่งผู้บริหารระดับสูงของมหาวิทยาลัยเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น

๔.๔ เพื่อเผยแพร่ให้บุคลากรของมหาวิทยาลัยทุกระดับได้รับทราบ ตระหนักถึงความสำคัญ และถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายให้ทันสมัยอยู่เสมอ

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๒.๑ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

/(๒) ในการ...

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลรวมทั้งระบบชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๕.๒.๒ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ที่ซึ่งไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวัง หรือ รู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๕.๒.๓ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหา ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Desk and Clear Screen Policy) โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

/๕.๒.๔ มีการ...

๕.๒.๔ มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับ

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องมีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๕.๒.๕ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการที่จะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อ เพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๕.๒.๖ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือ แอปพลิเคชันและสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการ

เข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีความควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing WLAN Teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงานโดยใช้ VPN ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานภายนอกหน่วยงาน

๕.๒.๗ ทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ ปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง ปีละ ๑ ครั้ง

๕.๒.๘ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

(๑) ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) ปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยหน่วยตรวจสอบภายใน (Internal Auditing Unit) เพื่อให้หน่วยงานได้ทราบถึงระบบความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖ ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศโดยกำหนดให้ผู้บริหารระดับสูงที่มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยงและเสียหายหรืออันตรายที่เกิดขึ้น

ข้อ ๗ หน่วยงานภายในมหาวิทยาลัยที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

ข้อ ๘ ผู้ใช้งานทุกระดับจะต้องทราบและยึดถือปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยโดยเคร่งครัด เพื่อให้ระบบสารสนเทศมีความมั่นคงและปลอดภัย ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบข้อบังคับ ประกาศ หรือคำสั่งใดของมหาวิทยาลัย และข้อตกลงระหว่างประเทศอย่างเคร่งครัด หากผู้ใช้งานฝ่าฝืน จะต้องถูกลงโทษตามระเบียบ และกฎหมายที่เกี่ยวข้องต่อไป

ข้อ ๙ ให้สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และกำหนดให้ทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐ เพื่อให้บรรลุตามวัตถุประสงค์ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของมหาวิทยาลัยเป็นไปตามเอกสารที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๑๙ เดือน กันยายน พ.ศ. ๒๕๖๖

(ศาสตราจารย์สุวัจน์ ธัญรส)

อธิการบดีมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

เอกสารแนบท้ายประกาศ

แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย พ.ศ. ๒๕๖๖

สารบัญ

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้เกิดการดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัย เชื่อถือได้ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันภัยคุกคามต่าง ๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้องรวมถึงการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่าง ๆ

๒. วัตถุประสงค์และขอบเขต

๒.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย รวมทั้งมีการคุ้มครองข้อมูลส่วนบุคคลอย่างเป็นรูปธรรมทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๒.๒ เพื่อเผยแพร่ให้บุคลากรทุกคนทุกระดับในมหาวิทยาลัยได้รับทราบและต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๓ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้บริหาร บุคลากร ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและตระหนักถึงความสำคัญของข้อมูลส่วนบุคคล สำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

๒.๔ การกำหนดความรับผิดชอบ กรณีระบบคอมพิวเตอร์ ข้อมูลสารสนเทศและข้อมูลส่วนบุคคลเกิดความเสียหายหรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและการคุ้มครองข้อมูลส่วนบุคคล กำหนดให้ผู้บริหารระดับสูงสุด (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๒.๕ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา ๑ ครั้งต่อปีให้มีความทันสมัยอยู่เสมอ

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัยมีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัย

๓.๒ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับทั้งของมหาวิทยาลัยและหน่วยงานที่เกี่ยวข้อง

๓.๓ ติดตามตรวจสอบการดำเนินการและปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๓.๔ กำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๔. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย จัดทำเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การควบคุมและการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัย (information access control)

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

๔. การควบคุมการเข้าถึงระบบเครือข่าย (network access control)

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

๖. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (application and information access control)

๗. การใช้งานอินเทอร์เน็ต

๘. การพัฒนาระบบสารสนเทศ

๙. การใช้งานคอมพิวเตอร์ส่วนบุคคล

๑๐. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

คำนิยาม

๑. **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

๒. **หน่วยงานภายใน** หมายถึง หน่วยงานตามโครงสร้างนอกโครงสร้างมหาวิทยาลัยที่ถูกจัดตั้งขึ้นโดยมีภารกิจและหน้าที่ที่ชัดเจน

๓. **หน่วยงานภายนอก** หมายถึง หน่วยงานเอกชนและหน่วยงานราชการภายนอกที่มหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของหน่วยงาน โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๔. **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

๕. **ผู้พัฒนาระบบ** หมายถึง ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ

๖. **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๗. **ผู้ใช้งาน** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศของมหาวิทยาลัย โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่มหาวิทยาลัยกำหนดไว้ ดังนี้

๗.๑ ผู้บริหาร หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี คณบดี ผู้อำนวยการสำนัก/สถาบัน/กอง และหัวหน้าหน่วยงานภายในมหาวิทยาลัย

๗.๒ ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศ โปรแกรมคอมพิวเตอร์ ฐานข้อมูลคอมพิวเตอร์

๗.๓ บุคลากร หมายถึง ข้าราชการ พนักงานราชการ พนักงานมหาวิทยาลัย ลูกจ้างประจำ ลูกจ้างชั่วคราว และลูกจ้างจ้างเหมาบริการ

๗.๔ นักศึกษา หมายถึง นักศึกษาของมหาวิทยาลัยเทคโนโลยีราชมงคลศรีวิชัย

๗.๕ บุคคลภายนอก หมายถึง เจ้าหน้าที่จากหน่วยงานภายนอกที่ปฏิบัติงานร่วมกับมหาวิทยาลัย

๘. **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๙. **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

๑๐. **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติ เพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

๑๑. **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ควรปฏิบัติเพื่อให้สามารถบรรลุเป้าหมายตามการรักษาความปลอดภัยด้านสารสนเทศ

๑๒. **สิทธิ์ของผู้ใช้งาน** หมายถึง สิทธิ์ทั่วไป สิทธิ์จำเพาะ สิทธิ์พิเศษ และสิทธิ์อื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๑๓. **สินทรัพย์** หมายถึง ข้อมูล สารสนเทศ และสินทรัพย์ด้านระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบสารสนเทศและการสื่อสารของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์หรือสิ่งอื่นใดก็ตามที่มีคุณค่าต่อหน่วยงาน เป็นต้น

๑๔. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานและบุคคลทั่วไป เข้าถึงหรือใช้งานระบบเทคโนโลยีสารสนเทศ อันได้แก่ ระบบเครือข่าย ระบบสารสนเทศ ตลอดจนการกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วย

๑๕. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๑๖. **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

๑๗. **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจจะประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๑๘. **สารสนเทศ (Information)** หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๙. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ทางคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลตามคำสั่งหรือโดยอัตโนมัติ

๒๐. **ระบบเครือข่าย (Network System)** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการรับ-ส่งข้อมูลและสารสนเทศระหว่างระบบคอมพิวเตอร์ต่าง ๆ ของมหาวิทยาลัยได้ เช่น ระบบแลน ระบบอินทราเน็ต ระบบอินเทอร์เน็ต เป็นต้น

๒๐.๑ ระบบแลนและระบบอินทราเน็ต หมายถึง ระบบเครือข่ายภายในหน่วยงานหรือระหว่างหน่วยงานภายในมหาวิทยาลัยเป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารหรือการรับส่งข้อมูลและสารสนเทศภายในมหาวิทยาลัย

๒๐.๒ ระบบอินเทอร์เน็ต หมายถึง ระบบเครือข่ายภายนอกทั่วโลกที่เชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัย

๒๑. **จดหมายอิเล็กทรอนิกส์ (e-Mail)** หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร อักขระ ตัวเลข ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

ด้วยมาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ เกณฑ์วิธีถ่ายโอนไปรษณีย์อย่างง่าย (SMTP) เกณฑ์วิธีการรับไปรษณีย์รุ่นสาม (POP3) และเกณฑ์วิธีการเข้าถึงข้อความอินเทอร์เน็ต (IMAP) เป็นต้น ซึ่งชื่อที่ใช้ในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ประกอบด้วย ๒ ส่วน คือ ชื่อผู้ใช้งานและชื่อโดเมน โดยมีรูปแบบดังนี้ User@rmutsv.ac.th, User@rmutsvmail.com และ User@ms.rmutsv.ac.th

๒๒. **บัญชีผู้ใช้งาน (Username)** หมายถึง บัญชีผู้ใช้งานที่มหาวิทยาลัยออกให้เพื่อใช้พิสูจน์ยืนยันตัวบุคคลในการเข้าใช้งานระบบเครือข่ายหรือระบบสารสนเทศต่าง ๆ ของมหาวิทยาลัย ประกอบด้วยชุดตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เพื่อระบุถึงบุคคลหรือตัวตนของผู้ใช้งาน เพื่อควบคุมการเข้าถึงข้อมูลและระบบเครือข่ายที่มีการกำหนดสิทธิ์การใช้งานไว้

๒๓. **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลในการควบคุมการเข้าถึงข้อมูลและระบบเครือข่าย

๒๔. **การเข้ารหัสลับ (Encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดใช้ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้ได้ตามปกติ

๒๕. **อุปกรณ์จัดเส้นทาง (Router)** หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายที่ทำหน้าที่จัดเส้นทางและการค้นหาเส้นทางเพื่อใช้ในการรับส่งข้อมูลคอมพิวเตอร์ต่อไปยังระบบเครือข่ายอื่น ๆ

๒๖. **การพิสูจน์ตัวจริง (Authentication)** หมายถึง ขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบสารสนเทศ เพื่อรักษาความปลอดภัยในการเข้าใช้ระบบสารสนเทศ โดยใช้ชื่อผู้ใช้และรหัสผ่าน เป็นต้น

๒๗. **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย โดยการทำลาย เปลี่ยนแปลง เพิ่มเติม และทำให้ปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒๘. **สำนักวิทยบริการฯ** หมายถึง สำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นหน่วยงานภายในที่ให้บริการระบบเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ และเครือข่ายภายในมหาวิทยาลัย

๒๙. **ข้อมูล (Data)** หมายถึง ข่าวสาร เอกสาร ข้อเท็จจริงเกี่ยวกับบุคคล สิ่งของหรือเหตุการณ์ที่มีอยู่ในรูปของตัวอักษร อักขระ ตัวเลข ภาษา ภาพ เสียง สัญลักษณ์ต่าง ๆ ที่มีความหมายเฉพาะตัว

๓๐. **ระบบสารสนเทศ (Information System)** หมายถึง ระบบคอมพิวเตอร์ที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ชุดคำสั่งคอมพิวเตอร์ ระบบเครือข่าย ฐานข้อมูลคอมพิวเตอร์ และบุคคลที่เกี่ยวข้อง ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล เปิดเผยและแจกจ่ายข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร

๓๑. **พื้นที่ใช้งานระบบสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานภายในอนุญาตให้มีการใช้งานระบบสารสนเทศ โดยแบ่งเป็น

๓๑.๑ พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

๓๑.๒ พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) หมายถึง พื้นที่ทำงานของผู้ดูแลระบบ เช่น ห้องศูนย์ข้อมูล (Data Center) ห้องปฏิบัติงานของผู้ดูแลระบบ

๓๑.๓ พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area) หมายถึง พื้นที่ที่มีการติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่ายตามอาคารต่าง ๆ เช่น บริเวณพื้นที่การติดตั้งตู้จัดเก็บอุปกรณ์ระบบเครือข่าย เป็นต้น

๓๑.๔ พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) หมายถึง พื้นที่ในการจัดเก็บข้อมูลบนเครื่องคอมพิวเตอร์

๓๑.๕ พื้นที่ใช้งานระบบเครือข่ายไร้สาย (Wireless LAN Coverage Area) หมายถึง พื้นที่ที่สามารถใช้งานระบบเครือข่ายไร้สายที่มหาวิทยาลัยเปิดให้บริการ

๓๒. **ระบบบัญชีผู้ใช้งาน** หมายถึง ระบบสารสนเทศที่ใช้ในการบริหารจัดการเกี่ยวกับบัญชีผู้ใช้งาน ซึ่งมหาวิทยาลัยมอบหมายให้หน่วยงานที่เกี่ยวข้องพัฒนาขึ้น

๓๓. **เหตุการณ์ด้านความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพการบริการของระบบสารสนเทศ หรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่พึงประสงค์ไม่คาดคิด ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน ภัยที่เกิดจากชุดคำสั่งหรือซอฟต์แวร์ ภัยที่เกิดจากไฟไหม้หรือระบบไฟฟ้า และภัยจากน้ำท่วม เป็นต้น

๓๔. **สื่อบันทึกกระเป๋าหิ้วหรือพกพา (Portable Media)** หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูลคอมพิวเตอร์ เช่น แผ่นซีดี แผ่นดิจิทัลอเนกประสงค์หรือดีวีดี หน่วยเก็บข้อมูลแฟลช หน่วยขับแฟลช จานบันทึกแบบแข็งภายนอก เป็นต้น

๓๕. **ผู้ให้บริการภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่มหาวิทยาลัยติดต่อใช้บริการในด้านต่าง ๆ

๓๖. **เจ้าหน้าที่สารสนเทศ** หมายถึง ผู้ที่ได้รับมอบหมายให้ดูแลรับผิดชอบเกี่ยวกับงานด้านสารสนเทศ

๓๗. **ผู้ตรวจสอบระบบสารสนเทศ** หมายถึง ผู้ที่มีความรู้ความเข้าใจในขั้นตอนกระบวนการตรวจสอบระบบสารสนเทศ (IT Audit Technical Know-how) ในระบบที่ต้องเข้าไปตรวจสอบที่ได้รับมอบหมายจากผู้มีอำนาจในองค์กรภายในหรือภายนอกมีหน้าที่ตรวจสอบระบบสารสนเทศเท่านั้น

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงและปลอดภัยที่เกี่ยวข้องกับการควบคุม การกำหนดสิทธิ์ การกำหนดระดับชั้น การกำหนดลำดับชั้น การกำหนดประเภทข้อมูล เวลาที่เข้าถึง และช่องทางที่เข้าถึง รวมทั้งแนวทางในการพัฒนาระบบสารสนเทศและอุปกรณ์ในการประมวลผล เพื่อให้เกิดความชัดเจนและมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักวิทยบริการฯ
๒. ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
๓. หน่วยงานหรือเจ้าของระบบสารสนเทศ
๔. เจ้าของข้อมูล

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (V2.5)

แนวทางปฏิบัติ

๑. การควบคุมและการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัย (information access control)
๑.๑ การกำหนดสิทธิ์เข้าใช้ระบบสารสนเทศของมหาวิทยาลัย ดังนี้
๑.๑.๑ สิทธิ์อ่านอย่างเดียว
๑.๑.๒ สิทธิ์การสร้างข้อมูล
๑.๑.๓ สิทธิ์การป้อนข้อมูล
๑.๑.๔ สิทธิ์การแก้ไขข้อมูล
๑.๑.๕ สิทธิ์การลบข้อมูล
๑.๑.๖ สิทธิ์การจัดการสิทธิ์ผู้ใช้งาน
๑.๑.๗ สิทธิ์การอนุมัติ/อนุญาต
๑.๑.๘ ไม่มีสิทธิ์
๑.๒ การกำหนดประเภทข้อมูลในระบบสารสนเทศของมหาวิทยาลัย ดังนี้
๑.๒.๑ ข้อมูลด้านการให้บริการและประชาสัมพันธ์
๑.๒.๒ ข้อมูลด้านการจัดการและปฏิบัติงาน ได้แก่ บันทึกข้อความ ข้อมูลด้านการเรียนการสอน หลักสูตร การวิจัย และการบริการวิชาการ เป็นต้น

๑.๓ การกำหนดลำดับชั้นของข้อมูลของมหาวิทยาลัย ดังนี้

๑.๓.๑ เปิดเผยได้ หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๓.๒ ส่วนบุคคล หมายถึง ใช้เฉพาะตัวบุคคล บุคลากร หรือหน่วยงานที่ดูแลข้อมูลนั้น

๑.๓.๓ ใช้ภายในเท่านั้น หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในมหาวิทยาลัย

๑.๓.๔ ลับ หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง โดยมีลำดับชั้น ดังนี้

๑.๓.๔.๑ ลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

๑.๓.๔.๒ ลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง

๑.๓.๔.๓ ลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย

๑.๔ การควบคุมระดับชั้นการเข้าถึงให้เหมาะสมตามบทบาทของมหาวิทยาลัย ดังนี้

๑.๔.๑ ระดับผู้บริหาร

๑.๔.๒ ระดับผู้ปฏิบัติงาน

๑.๔.๓ ระดับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๑.๔.๔ ระดับบุคลากร

๑.๔.๕ ระดับนักศึกษา

๑.๔.๖ ระดับบุคคลภายนอก

๑.๕ กำหนดชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

๑.๕.๑ การเข้าถึงสำหรับผู้บริหาร

๑.๕.๒ การเข้าถึงสำหรับผู้ปฏิบัติงาน

๑.๕.๓ การเข้าถึงสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๑.๕.๔ การเข้าถึงสำหรับบุคลากร

๑.๕.๕ การเข้าถึงสำหรับนักศึกษา

๑.๕.๖ การเข้าถึงสำหรับบุคคลภายนอก

๑.๖ การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

๑.๖.๑ ผู้บริหารเข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๑.๖.๒ ผู้ปฏิบัติงานเข้าถึงได้ตามหน้าที่ที่ได้รับมอบหมาย

๑.๖.๓ ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมาย ตามอำนาจหน้าที่

๑.๖.๔ บุคลากรเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

๑.๖.๕ นักศึกษาเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

๑.๖.๖ บุคคลภายนอกเข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้เท่านั้น

๑.๖.๗ การกำหนดสิทธิ์พิเศษสามารถทำได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

๑.๖.๘ การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์หรือหน่วยงานหลักเท่านั้น

๑.๗ เวลาที่เข้าถึง ดังนี้

๑.๗.๑ ระบบงานบริการ (Front Office) สำหรับผู้ใช้งานทั่วไปสามารถเข้าถึงได้ตลอดเวลา

๑.๗.๒ ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานสามารถเข้าถึงได้ ดังนี้

๑.๗.๒.๑ เวลาราชการ ตั้งแต่เวลา ๐๘.๓๐ – ๑๖.๓๐ น.

๑.๗.๒.๒ เวลานอกราชการ ตั้งแต่เวลา ๑๖.๓๑ – ๐๘.๒๙ น.

๑.๗.๒.๓ วันหยุดราชการ ได้แก่ วันเสาร์ วันอาทิตย์ และวันหยุดนักขัตฤกษ์

๑.๗.๒.๔ การเข้าถึงในช่วงเวลาพิเศษ หรือจำเพาะเจาะจง หรือกำหนดจำนวนระยะเวลาการเข้าถึง

๑.๘ ช่องทางการเข้าถึง ดังนี้

๑.๘.๑ ผู้ใช้งานเข้าใช้บริการผ่านระบบอินทราเน็ตของมหาวิทยาลัย ได้ตลอด ๒๔ ชั่วโมง ได้แก่ช่องทาง

๑.๘.๑.๑ ระบบเครือข่ายไร้สาย

๑.๘.๑.๒ ระบบเครือข่ายสายสัญญาณ

๑.๘.๒ ผู้ใช้งานเข้าใช้บริการผ่านระบบอินเทอร์เน็ตของมหาวิทยาลัย สามารถเข้าใช้บริการผ่านระบบเครือข่ายส่วนตัวเสมือน (VPN) ได้ตลอด ๒๔ ชั่วโมง

๑.๘.๓ การประชุมทางไกลสามารถเข้าถึงได้เฉพาะในเวลาราชการและกำหนดเป็นช่วงเวลาเป็นรายครั้ง

๑.๘.๔ การติดต่อด้วยตนเองและการประสานงานผ่านโทรศัพท์ สามารถเข้าถึงได้เฉพาะในเวลาราชการ

๑.๙ การกำหนดการใช้งานตามภารกิจ

มหาวิทยาลัย จัดให้มีการบริการสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศ เพื่อใช้ประโยชน์ตามภารกิจของมหาวิทยาลัย ได้แก่ การเรียนการสอน การวิจัย การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม และการบริหารจัดการ ทั้งนี้การใช้งานตามภารกิจต้องอยู่บนพื้นฐานของการเคารพสิทธิ์และความรู้สึกของบุคคลอื่น และปฏิบัติให้ถูกต้องตามกฎหมาย โดยกำหนดสิทธิ์การเข้าถึง ดังนี้

๑.๙.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

๑.๙.๑.๑ ผู้บริหารจะได้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นผู้บริหาร

๑.๙.๑.๒ บุคลากรจะได้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

๑.๙.๑.๓ นักศึกษาจะได้สิทธิ์ทันทีที่มีสภาพเป็นนักศึกษาและหมดสิทธิ์เมื่อพ้นสภาพนักศึกษา

๑.๙.๑.๔ บุคคลภายนอกจะได้สิทธิ์เมื่อได้รับอนุญาตและเข้าถึงได้เฉพาะระบบและช่วงเวลาที่กำหนดเท่านั้น

๑.๙.๒ ข้อจำกัดในการเข้าถึง

๑.๙.๒.๑ ผู้บริหารเข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

๑.๙.๒.๒ บุคลากรเข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย

๑.๙.๒.๓ นักศึกษาเข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

๑.๙.๒.๔ บุคคลภายนอกเข้าถึงได้ตามที่ได้รับอนุญาต

๑.๑๐ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์

๑.๑๐.๑ จัดทำบัญชีสินทรัพย์หรือทะเบียนสินทรัพย์ เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๑๑ กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามแนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ สร้างความรู้ความเข้าใจแก่ผู้ใช้งานและการกำหนดมาตรการเชิงป้องกัน

๒.๑.๑ มีการประชาสัมพันธ์เกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒ มหาวิทยาลัยต้องพัฒนาระบบบัญชีผู้ใช้งาน โดยมีการอ้างอิงข้อมูลจากฐานข้อมูลบุคลากร และฐานข้อมูลนักศึกษา หรือบัญชีผู้ใช้งานของบุคคลภายนอก

๒.๑.๓ ระบบบัญชีผู้ใช้งานต้องสามารถสร้างบัญชีผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งาน ตั้งรหัสผ่านหรือการแจ้งและเปลี่ยนแปลงรหัสผ่าน สามารถทดสอบการใช้งานได้เป็นอย่างน้อย

๒.๒ การแบ่งกลุ่มบัญชีผู้ใช้งาน มีการแบ่งประเภทบัญชีผู้ใช้งานเป็น ๔ ประเภทดังนี้

๒.๒.๑ บัญชีผู้ใช้งานสำหรับผู้บริหาร

๒.๒.๒ บัญชีผู้ใช้งานสำหรับบุคลากร

๒.๒.๓ บัญชีผู้ใช้งานสำหรับนักศึกษา

๒.๒.๔ บัญชีผู้ใช้งานสำหรับบุคคลภายนอก

๒.๓ การลงทะเบียนบัญชีผู้ใช้งาน (User Registration)

มหาวิทยาลัยจัดให้มีการบริการระบบสารสนเทศเพื่อใช้สำหรับการลงทะเบียนบัญชีผู้ใช้งาน สำหรับนำบัญชีผู้ใช้งานไปใช้เข้าระบบสารสนเทศของมหาวิทยาลัย ผู้ใช้งานสามารถลงทะเบียนผ่านระบบบัญชีผู้ใช้งานได้ตลอดเวลา โดยระบบจะกำหนดและแจ้งบัญชีผู้ใช้งานเป็นชื่อภาษาอังกฤษตามด้วยนามสกุล (ตัวอักษรขึ้นต้น) เช่น ruts.s และรหัสผ่าน มีแนวปฏิบัติดังนี้

๒.๓.๑ สำหรับผู้บริหาร

๒.๓.๑.๑ ผู้บริหารต้องมีข้อมูลครบถ้วนสมบูรณ์ในฐานข้อมูลบุคลากรของมหาวิทยาลัย

๒.๓.๑.๒ ผู้บริหารยื่นคำขอบัญชีผู้ใช้งานผ่านระบบสารสนเทศของมหาวิทยาลัย

๒.๓.๑.๓ แจ้งผลการลงทะเบียนบัญชีผู้ใช้งานผ่านระบบสารสนเทศหรือโทรศัพท์

๒.๓.๒ สำหรับบุคลากร

๒.๓.๒.๑ บุคลากรต้องมีข้อมูลครบถ้วนสมบูรณ์ในฐานข้อมูลบุคลากรของมหาวิทยาลัย

๒.๓.๒.๒ บุคลากรยื่นคำขอบัญชีผู้ใช้งานผ่านระบบสารสนเทศของมหาวิทยาลัย

๒.๓.๒.๓ แจ้งผลการลงทะเบียนบัญชีผู้ใช้งานผ่านระบบสารสนเทศหรือโทรศัพท์

๒.๓.๓ สำหรับนักศึกษา

๒.๓.๓.๑ นักศึกษาใหม่ต้องมีข้อมูลครบถ้วนสมบูรณ์ในฐานข้อมูลนักศึกษาของมหาวิทยาลัย

๒.๓.๓.๒ นักศึกษาสามารถลงทะเบียนบัญชีผู้ใช้งานผ่านระบบสารสนเทศของมหาวิทยาลัย

๒.๓.๓.๓ แจ้งผลการลงทะเบียนบัญชีผู้ใช้งานผ่านระบบสารสนเทศ

๒.๓.๔ สำหรับบุคคลภายนอก

๒.๓.๔.๑ บุคคลภายนอกต้องขออนุมัติเป็นลายลักษณ์อักษรและได้รับอนุมัติจากผู้อำนวยการสำนักวิทยบริการฯ หรือผู้ที่ได้รับมอบหมาย

๒.๔ การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management)

๒.๔.๑ ให้อำนาจกับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายในการระงับหรือเพิกถอนสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ

๒.๔.๒ เมื่อมีการระงับบัญชีผู้ใช้งาน กรณีการขอรับคืนบัญชีผู้ใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษรผ่านต้นสังกัดถึงสำนักวิทยบริการฯ

๒.๔.๓ การเพิกถอนสิทธิ์สำหรับผู้บริหาร กระทำเมื่อผู้บริหารพ้นสภาพการเป็นผู้บริหาร

๒.๔.๔ การเพิกถอนสิทธิ์สำหรับบุคลากร กระทำเมื่อบุคลากรพ้นสภาพการเป็นบุคลากร หน่วยงานแจ้งเปลี่ยนแปลงหน้าที่รับผิดชอบ

๒.๔.๕ การเพิกถอนสิทธิ์สำหรับนักศึกษา กระทำเมื่อนักศึกษาพ้นสภาพการเป็นนักศึกษาหรือลาออกจากการเป็นนักศึกษา

๒.๔.๖ การเพิกถอนสิทธิ์สำหรับบุคคลภายนอก กระทำเมื่อบุคคลภายนอกพ้นระยะเวลาที่กำหนดหรือพ้นระยะเวลาที่ได้รับอนุญาตในการทำภารกิจกับมหาวิทยาลัย

๒.๔.๗ กรณีมีความจำเป็นต้องใช้สิทธิ์พิเศษ ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิ์พิเศษนั้นโดยได้รับความเห็นชอบและอนุมัติจากอธิการบดี หรือผู้ได้รับมอบอำนาจจากอธิการบดี

๒.๔.๗.๑ ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

๒.๔.๗.๒ กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

๒.๔.๗.๓ ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือกรณีที่มีความจำเป็นในการใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๖ เดือน เป็นต้น

๒.๕ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๒.๕.๑ ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานหรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

๒.๕.๒ การส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย โดยส่งผ่านระบบสารสนเทศ

๒.๖ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

๒.๖.๑ ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง

๒.๖.๒ บัญชีผู้ใช้งานจะหมดอายุ ดังนี้

๒.๖.๒.๑ ผู้บริหาร บัญชีผู้ใช้งานหมดอายุเมื่อพ้นสภาพการเป็นผู้บริหารของมหาวิทยาลัย

๒.๖.๒.๒ บุคลากร บัญชีผู้ใช้งานหมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของมหาวิทยาลัย

๒.๖.๒.๓ นักศึกษา บัญชีผู้ใช้งานหมดอายุหลังพ้นสภาพการเป็นนักศึกษา

๒.๖.๒.๔ บุคคลภายนอก บัญชีผู้ใช้งานหมดอายุเมื่อภารกิจเสร็จสิ้น

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑ การใช้งานรหัสผ่าน (Password Use)

๓.๑.๑ ผู้ใช้งานต้องจัดการกับรหัสผ่านให้มีความมั่นคงปลอดภัย

๓.๑.๒ ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกจากระบบบัญชีผู้ใช้งานควรเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

๓.๑.๓ ผู้ใช้งานต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ กับรหัสผ่าน เพื่อให้เกิดความมั่นคงปลอดภัยของระบบสารสนเทศ

๓.๑.๔ ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับและระมัดระวังป้องกันรหัสผ่านไม่ให้รั่วไหลไปยังผู้อื่นและไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ

๓.๑.๕ กำหนดให้รหัสผ่านต้องไม่น้อยกว่า ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษร ตัวเลข หรืออักขระ และอักขระพิเศษเข้าด้วยกัน

๓.๑.๖ ไม่ควรกำหนดรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน (abcdef, 12345) หรือกลุ่มอักขระที่เหมือนกัน (aaaaaa, 11111)

๓.๑.๗ ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่ เป็นต้น

๓.๑.๘ ไม่ใช้รหัสผ่านสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์

๓.๑.๙ ไม่ควรใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านอัตโนมัติ

๓.๑.๑๐ เมื่อมีปัญหาการใช้ชื่อผู้ใช้งานและรหัสผ่าน เช่น ลืมชื่อผู้ใช้งานหรือรหัสผ่านให้ดำเนินการผ่านระบบบัญชีผู้ใช้งานหรือติดต่อผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์

๓.๒.๑ ในกรณีที่ไม่ใช้ระบบสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log Off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบสารสนเทศต่อ และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลควรเปลี่ยนรหัสผ่านทันที

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

๓.๓.๑ จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๓.๓.๒ ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยผู้เป็นเจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

๓.๓.๓ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญผ่านอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๓.๓.๔ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๓.๕ ผู้ใช้งานอาจนำการเข้ารหัสลับมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๓.๓.๖ จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสาร ตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

๓.๓.๗ โปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัยเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน เพราะเป็นการกระทำที่ผิดกฎหมาย

๓.๓.๘ ไม่เก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นส่วนบุคคล

๓.๓.๙ ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

๓.๓.๑๐ ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๓.๓.๑๑ ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้การลบหรือการทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าวต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑ การควบคุมการจัดการระบบเครือข่าย

๔.๑.๑ การใช้งานระบบอินเทอร์เน็ตต้องควบคุมการเข้าใช้โดยผ่านบัญชีผู้ใช้งานระบบสารสนเทศที่เป็นส่วนกลาง

๔.๑.๒ ต้องกำหนดพื้นที่ควบคุมการใช้งานระบบเครือข่าย เพื่อให้ผู้ดูแลระบบสามารถเข้าถึงพื้นที่ใช้งานได้อย่างสะดวกในการปฏิบัติงานระบบเครือข่าย

๔.๑.๓ ห้องควบคุมระบบเครือข่ายต้องอยู่ในห้องที่มีระบบป้องกันการเข้าออก

๔.๑.๔ การเข้าออกห้องควบคุมระบบเครือข่ายต้องได้รับอนุญาตจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๑.๕ การเข้าออกห้องควบคุมระบบเครือข่ายต้องบันทึกการเข้าออก

๔.๑.๖ อุปกรณ์ทางระบบเครือข่ายต้องติดตั้งบริเวณพื้นที่ที่มีความปลอดภัย เพื่อป้องกันอุปกรณ์เสียหายหรือสูญหาย

๔.๑.๗ การใช้งานบริการระบบเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะการบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๑.๘ มหาวิทยาลัยต้องติดตั้งไฟร์วอลล์เพื่อป้องกันทางเข้าออกระบบเครือข่ายจากผู้ไม่หวังดี

๔.๑.๙ การนำอุปกรณ์ระบบเครือข่ายใด ๆ มาเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยต้องได้รับอนุญาตจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๑.๑๐ ต้องควบคุมไม่ให้เปิดบริการระบบเครือข่ายโดยไม่ได้รับอนุญาต

๔.๑.๑๑ ต้องป้องกันการเข้าถึงอุปกรณ์จัดเส้นทางบนระบบเครือข่ายไม่ให้เข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต

๔.๒ การควบคุมการจัดการระบบเครือข่ายไร้สาย

๔.๒.๑ การติดตั้งอุปกรณ์ระบบเครือข่ายไร้สายใด ๆ เพื่อเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัยต้องได้รับอนุญาตและต้องกำหนดค่าปรับแต่งหรือค่าการใช้งานที่เหมาะสมจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๒.๒ อุปกรณ์ทางระบบเครือข่ายไร้สายต้องติดตั้งในพื้นที่ที่มีความปลอดภัย เพื่อป้องกันอุปกรณ์เสียหายหรือสูญหาย

๔.๒.๓ การใช้งานบริการระบบเครือข่ายไร้สายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๒.๔ ต้องควบคุมไม่ให้มีการเปิดให้บริการระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๔.๒.๕ ต้องควบคุมไม่ให้มีการใช้บริการระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๔.๒.๖ การให้บริการระบบเครือข่ายไร้สายจากผู้ให้บริการภายนอกต้องได้รับอนุญาตจากอธิการบดี

๔.๒.๗ การให้บริการระบบเครือข่ายไร้สายจากผู้ให้บริการภายนอกต้องไม่มีผลกระทบต่อนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

๔.๓ การควบคุมการปฏิบัติงานจากภายนอก

๔.๓.๑ การเข้าถึงระบบเครือข่ายจากภายนอกมหาวิทยาลัยต้องกำหนดให้มีการเข้ารหัสในการเชื่อมต่อเพื่อความปลอดภัย

๔.๓.๒ ผู้ใช้งานระบบเครือข่ายที่ปฏิบัติงานจากภายนอกต้องได้รับอนุญาตการเข้าใช้งานระบบเครือข่ายระยะไกลจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๓.๓ ผู้ที่ได้รับอนุญาตให้เข้าใช้งานระบบเครือข่ายระยะไกลต้องรับผิดชอบต่อบัญชีผู้ใช้งานระบบสารสนเทศไม่ให้มีการใช้งานที่ส่อหรือฝ่าฝืนต่อนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

๔.๔ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connections)

๔.๔.๑ มหาวิทยาลัยต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่านเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๔.๔.๒ ผู้ใช้งานที่เข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง ตามช่องทางการเข้าถึงระบบเครือข่ายที่มหาวิทยาลัยกำหนด

๔.๔.๓ ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัยต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

๔.๕ การระบุอุปกรณ์บนระบบเครือข่าย (Equipment Identification in Networks)

๔.๕.๑ ผู้ดูแลระบบต้องทำผังการเชื่อมต่ออุปกรณ์ระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์บนระบบเครือข่ายได้

๔.๕.๒ อุปกรณ์ที่เชื่อมต่อระบบเครือข่ายต้องระบุตำแหน่งที่ตั้งได้ โดยการตรวจสอบจากเลขที่อยู่ไอพี (Internet Protocol: IP Address)

๔.๕.๓ อุปกรณ์ที่นำมาเชื่อมต่อระบบเครือข่ายได้รับเลขที่อยู่ไอพีตามที่กำหนด โดยผู้ดูแลระบบเท่านั้น

๔.๕.๔ เก็บข้อมูลการใช้เลขที่อยู่การควบคุมการเข้าถึงสื่อ (Media Access Control Address: MAC Address) จากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการค่าเลขที่อยู่ไอพีแอดเดรส (DHCP Server)

๔.๖ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบเครือข่าย

๔.๖ ๑ ต้องมีการตรวจสอบและยกเลิกหรือปิดพอร์ต การบริการบนอุปกรณ์ระบบเครือข่ายหรือระบบเครือข่ายไร้สายที่ไม่จำเป็นในการใช้งาน

๔.๖ ๒ บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์ระบบเครือข่ายหรือบริหารจัดการผ่านระบบเครือข่ายจากระยะไกล ต้องได้รับการอนุญาตจากผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

๔.๖ ๓ เมื่อมีการเชื่อมต่อโดยตรงบนตัวอุปกรณ์ต้องกำหนดรหัสผ่านสำหรับการตรวจสอบและปรับแต่งอุปกรณ์ระบบเครือข่าย

๔.๖ ๔ ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากระบบเครือข่ายภายนอกมหาวิทยาลัย

๔.๖ ๕ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔.๗ การแบ่งแยกระบบเครือข่าย (Segregation in Networks)

๔.๗.๑ มหาวิทยาลัยแบ่งแยกระบบเครือข่ายเป็นระบบเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงระบบเครือข่าย

๔.๗.๒ มหาวิทยาลัยจัดแบ่งระบบเครือข่ายภายในและระบบเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบสารสนเทศ

๔.๗.๓ ผู้ดูแลระบบต้องทำผังการเชื่อมต่ออุปกรณ์บนระบบเครือข่ายสายสัญญาณและระบบเครือข่ายไร้สาย เพื่อระบุอุปกรณ์บนระบบเครือข่ายได้

๔.๗.๔ ต้องใช้ไฟร์วอลล์ (Firewall) กั้นหรือแบ่งระบบเครือข่ายภายในและระบบเครือข่ายภายนอก

๔.๗.๕ ต้องใช้เกตเวย์ (Gateway) เพื่อควบคุมการเข้าถึงระบบเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน

๔.๘ การควบคุมการเชื่อมต่อทางระบบเครือข่าย (Network Connection Control)

๔.๘.๑ อนุญาตการเชื่อมต่อเฉพาะเลขที่อยู่ไอพีที่กำหนดให้เท่านั้น

๔.๘.๒ ระบบเครือข่ายที่เชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัย ต้องติดตั้งระบบตรวจจับการบุกรุก

๔.๙ การควบคุมการจัดเส้นทางบนระบบเครือข่าย (Network Routing Control)

๔.๙.๑ การกำหนดการจัดเส้นทางบนระบบเครือข่ายจะต้องจัดการโดยผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้น

๔.๙.๒ การอนุญาตเส้นทางระบบเครือข่ายเฉพาะกลุ่มต้องเป็นเลขที่อยู่ไอพีที่กำหนดเท่านั้น

๔.๙.๓ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในระบบเครือข่าย

๔.๙.๔ ต้องตรวจสอบเลขที่อยู่ไอพีของต้นทางและปลายทาง

๔.๙.๕ ต้องควบคุมการไหลของข้อมูลผ่านระบบเครือข่าย

๔.๙.๖ ต้องกำหนดเส้นทางการไหลของข้อมูลบนระบบเครือข่ายที่สอดคล้องกับการควบคุมเข้าถึงและการใช้งานบริการระบบเครือข่าย

๔.๙.๗ ต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๕.๑ การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๕.๑.๑ สำหรับเครื่องคอมพิวเตอร์ที่เป็นส่วนกลาง เจ้าหน้าที่สารสนเทศต้องติดตั้งโปรแกรมช่วยบริหารจัดการเครื่องคอมพิวเตอร์

๕.๑.๒ สำหรับการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ที่เป็นส่วนกลาง เจ้าหน้าที่สารสนเทศต้องกำหนดชื่อบัญชีผู้ใช้งานและรหัสผ่าน

๕.๑.๓ สำหรับเครื่องคอมพิวเตอร์ที่เป็นส่วนกลางต้องมีการกำหนดระยะเวลาและบันทึกข้อมูลผู้เข้าใช้งาน

๕.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๕.๒.๑ ผู้ใช้งานต้องมีบัญชีผู้ใช้งานและรหัสผ่าน สำหรับเข้าใช้งานระบบปฏิบัติการ

๕.๒.๒ สามารถใช้อุปกรณ์เพิ่มเติมเพื่อควบคุมความปลอดภัย เช่น เครื่องอ่านลายพิมพ์นิ้วมือที่ใช้ สำหรับเครื่องคอมพิวเตอร์แม่ข่าย เป็นต้น

๕.๓ การบริหารจัดการรหัสผ่าน (Password Management System)

๕.๓.๑ สำหรับเครื่องคอมพิวเตอร์ที่เป็นส่วนกลางต้องกำหนดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด เช่น จำนวน ๓ ครั้ง ระบบจะทำการล็อกสิทธิ์การใช้งานจนกว่าเจ้าหน้าที่สารสนเทศจะปลดล็อกถึงจะใช้งานได้

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๕.๔.๑ โปรแกรมที่ติดตั้งบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัยต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมายเท่านั้น

๕.๔.๒ ต้องถอดถอนหรือไม่ติดตั้งโปรแกรมอรรถประโยชน์ (Utility Program) ที่ไม่จำเป็นออกจากระบบปฏิบัติการ

๕.๔.๓ โปรแกรมอรรถประโยชน์ที่มีการพัฒนาโดยใช้บริการภายนอก (Outsource) รหัสต้นฉบับ (Source Code) เมื่อเสร็จสิ้นแล้วต้องเป็นลิขสิทธิ์ของมหาวิทยาลัย

๕.๔.๔ ผู้ดูแลเครื่องคอมพิวเตอร์จะต้องอัปเดตโปรแกรมอรรถประโยชน์ รุ่นล่าสุดให้มีความทันสมัยอยู่เสมอเพื่อความปลอดภัยในการใช้งาน เว้นแต่มีเหตุจำเป็นต้องใช้งานรุ่นเดิม

๕.๕ การยุติการใช้งานระบบสารสนเทศ (Session Timeout)

๕.๕.๑ หากไม่มีการใช้งานระบบเป็นระยะเวลาเกิน ๓๐ นาที ต้องทำการยกเลิกการใช้งานระบบสารสนเทศโดยอัตโนมัติ

๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๕.๖.๑ กำหนดเกณฑ์ระยะเวลาการเชื่อมต่อระบบสารสนเทศที่ใช้บัญชีผู้ใช้งาน (e-Passport) เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดในระยะเวลาที่กำหนดเท่านั้น คือ กำหนดให้ใช้งานได้นานไม่เกิน ๘ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๕.๖.๒ กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูงที่มหาวิทยาลัยเปิดให้บริการต้องจำกัดช่วงระยะเวลาการเชื่อมต่อที่เหมาะสม

๖. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๖.๑.๑ การจำกัดการเข้าถึงของผู้ใช้งาน

๖.๑.๑.๑ เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๖.๑.๑.๒ กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

๖.๑.๑.๓ ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๖.๑.๑.๔ แบ่งกลุ่มผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัย ออกเป็น ๔ กลุ่ม คือ ผู้บริหาร บุคลากร นักศึกษา และบุคคลภายนอก

๖.๑.๑.๕ ระบบสารสนเทศจะต้องมีการจัดทำระบบจัดเก็บสถานะ การเข้าถึง และประวัติการเข้าใช้งาน (Log File)

๖.๑.๑.๖ ระบบสารสนเทศที่มีความสำคัญต้องมีการเข้ารหัสลับการเชื่อมต่อ (SSL Encryption)

๖.๑.๑.๗ การควบคุมผู้รับเหมา (Outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

๑) มีกระบวนการคัดเลือกผู้รับเหมาโดยเฉพาะและต้องกำหนดคุณสมบัติของผู้รับเหมาที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีสำหรับการรับเหมา ทั้งในส่วนของฮาร์ดแวร์และซอฟต์แวร์ รวมถึงระบบที่สนับสนุนการปฏิบัติงาน เพื่อให้ได้ผู้รับเหมาที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาและต้องกำหนดขอบเขตและระดับการรับเหมาอย่างชัดเจน รวมถึงผู้รับเหมาต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

๓) หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาเป็นระยะ ๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาใช้ในการปฏิบัติงาน และเพื่อประเมินประสิทธิภาพของผู้รับเหมาในการกระทำตามข้อกำหนดของหน่วยงาน

๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูลและการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๖.๒ การดูแลระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงาน ดำเนินการดังนี้

๖.๒.๑ ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญต่อองค์กร ต้องแยกออกจากระบบอื่น ๆ

๖.๒.๒ ต้องควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวน

๖.๒.๒.๑ มีห้องปฏิบัติงานแยกเป็นสัดส่วนและต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น ในการเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๖.๒.๒.๒ ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น ๆ

๖.๒.๒.๓ มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญจากผู้ที่ไม่ได้รับอนุญาต

๖.๒.๓ ต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๖.๓.๑ แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ

๖.๓.๑.๑ ต้องล็อกหรือยึดเครื่องให้อยู่กับที่ กรณีที่นำอุปกรณ์ไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๖.๓.๑.๒ ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องคอมพิวเตอร์อัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

๖.๓.๑.๓ ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานเครื่องคอมพิวเตอร์

๖.๓.๑.๔ หลีกเลี่ยงการใช้อุปกรณ์คอมพิวเตอร์ร่วมกับบุคคลอื่น

๖.๓.๑.๕ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลแบบพกพาต่าง ๆ

๖.๓.๑.๖ ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องมีการเข้ารหัสลับข้อมูลทุกครั้ง

๖.๓.๑.๗ เพื่อความปลอดภัยห้ามใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่เป็นอุปกรณ์ปล่อยสัญญาณเครือข่ายไร้สายขณะใช้ระบบเครือข่ายภายในมหาวิทยาลัย

๖.๓.๑.๘ ต้องจัดการกับโปรแกรมไม่พึงประสงค์บนอุปกรณ์คอมพิวเตอร์ เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

๖.๓.๑.๙ มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์เกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

๖.๓.๒ การสำรองข้อมูลและการกู้คืน

๖.๓.๒.๑ ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลของตนเองจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลสำรอง (Backup Media) เช่น แผ่นซีดี แผ่นดิจิทัลอเนกประสงค์หรือดีวีดี หน่วยเก็บข้อมูลแฟลช หน่วยขับแฟลช จานบันทึกแบบแข็งภายนอก เป็นต้น

๖.๓.๒.๒ ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลที่สำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง

๖.๔ การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัยจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๖.๔.๑ ผู้ใช้งานระบบเครือข่ายจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและระบบเครือข่ายของมหาวิทยาลัยต้องทำการพิสูจน์ตัวจริงก่อนเข้าใช้งาน

๖.๔.๒ ผู้ใช้งานต้องไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบสารสนเทศขององค์กรในสถานที่ดังกล่าว

๖.๔.๓ ต้องตรวจสอบอุปกรณ์ให้มีระบบป้องกันไวรัสและกำหนดการใช้งานไฟร์วอลล์อย่างเหมาะสม

๖.๔.๔ ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกล

๗. การใช้งานอินเทอร์เน็ต

๗.๑ ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตให้เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น เช่น ไฟร์วอลล์แทนระบบป้องกันการบุกรุก/ระบบตรวจจับการบุกรุก (Proxy Firewall IPS/IDS) เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น โมเด็มแบบหมุนโทรศัพท์ (Dial-Up Modem) เว้นแต่จะมีเหตุผลความจำเป็นและขออนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ เป็นลายลักษณ์อักษรแล้ว

๗.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่าน เว็บเบราว์เซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บเบราว์เซอร์ติดตั้งอยู่

๗.๓ ผู้ใช้งานไม่ใช้ระบบเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๗.๔ ผู้ใช้งานไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลทีละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

๗.๕ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัย

๗.๖ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๗.๗ ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๗.๘ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๗.๙ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง แพทช์ (Patch) หรือ ฟิคซ์ (Fixes) ต่าง ๆ จากผู้ขายและไม่ละเมิดทรัพย์สินทางปัญญา

๗.๑๐ การเสนอความคิดเห็นผ่านเว็บบอร์ด (Web board) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย และต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๘ การพัฒนาระบบสารสนเทศ

๘.๑ การเข้าถึงระบบสารสนเทศต้องมีการระบุตัวตนผู้ใช้งานโดยผ่านระบบบัญชีผู้ใช้งานระบบสารสนเทศที่เป็นส่วนกลางก่อนเข้าใช้งานเสมอ

๘.๒ ระบบสารสนเทศต้องดูแลโดยผู้ดูแลระบบที่ได้รับอนุญาตจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร และเจ้าของข้อมูลต้องเป็นผู้รับผิดชอบข้อมูลทั้งหมดในระบบสารสนเทศ

๘.๓ เจ้าของระบบสารสนเทศต้องจัดทำเอกสารการพัฒนาระบบอย่างเป็นลายลักษณ์อักษร เช่น ความต้องการของผู้ใช้ (User Requirement) กระแสข้อมูล (Data Flow) พจนานุกรมข้อมูล (Data Dictionary) แผนภาพความสัมพันธ์ของเอนทิตี (Entity Relationship Diagram: ERD)

๘.๔ เจ้าของระบบสารสนเทศต้องจัดทำคู่มือการใช้งานระบบสารสนเทศของหน่วยงาน

๘.๕ คู่มือการใช้งานระบบสารสนเทศจะต้องนำไปไว้บนเว็บไซต์ของระบบสารสนเทศ หรือของหน่วยงานให้มีการดาวน์โหลดเพื่อใช้งานได้ง่าย

๘.๖ เจ้าของระบบสารสนเทศต้องจัดอบรมการใช้งานแก่บุคลากรที่เกี่ยวข้องอย่างน้อย ๓ ปี/๑ ครั้ง

๙ การใช้งานคอมพิวเตอร์ส่วนบุคคล

๙.๑ เครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัยเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้งานต้องใช้เครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่งานของมหาวิทยาลัย

๙.๒ ต้องทำการปิดเครื่องคอมพิวเตอร์ส่วนบุคคลทุกครั้งเมื่อไม่มีการใช้งาน

๙.๓ โปรแกรมที่ได้ติดตั้งลงบนเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัยต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้อง

๙.๔ ต้องติดตั้งและเปิดใช้ระบบป้องกันไวรัสและชุดคำสั่งไม่พึงประสงค์ (Malware) ในเครื่องคอมพิวเตอร์ส่วนบุคคลเสมอ

๙.๕ ไม่ดัดแปลงและแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัยด้วยตนเองจะต้องดำเนินการโดยเจ้าหน้าที่สารสนเทศเท่านั้น

๙.๖ ต้องไม่จัดเก็บข้อมูลที่มีความสำคัญหรือเป็นความลับของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล

๙.๗ ผู้ใช้งานสามารถนำการเข้ารหัสลับมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑๐. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑๐.๑ หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่ายต้องแต่งตั้งผู้มีสิทธิ์ใช้งานและกำหนดจำนวนผู้มีสิทธิ์ในการเข้าถึงระบบปฏิบัติการ

๑๐.๒ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้งานและรหัสผ่านของตัวเองเท่านั้น

๑๐.๓ ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๑๐.๔ ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

๑๐.๕ ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงาน สำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๑๐.๖ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่พึงประสงค์บนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

๑๐.๗ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมไม่พึงประสงค์ ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมไม่พึงประสงค์ การวิเคราะห์ การจัดการ การกู้คืนระบบ จากความเสียหายที่พบ เป็นต้น

๑๐.๘ ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่พึงประสงค์อย่างสม่ำเสมอ

๑๐.๙ ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่พึงประสงค์ เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมีความรู้ ความเข้าใจ และสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่พึงประสงค์ว่าต้องดำเนินการอย่างไร

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองและการกู้ข้อมูลสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการควบคุมและป้องกันในการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการจัดเก็บการสำรองข้อมูล และการเตรียมแผนความพร้อมกรณีฉุกเฉิน เพื่อรองรับแก้ปัญหาในเหตุการณ์ต่าง ๆ

ผู้รับผิดชอบ

๑. สำนักวิทยบริการฯ

๒. ผู้ดูแลระบบและผู้ที่ได้รับมอบหมาย

๓. ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวทางปฏิบัติ

๑. การพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานพร้อมทั้งกำหนดระบบสารสนเทศที่จะทำระบบสำรองและจัดทำแผนและเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองมากขึ้น

๑.๓ จัดเก็บข้อมูลที่สำรองในสื่อเก็บข้อมูลจานบันทึกแบบแข็งภายนอก หรือสื่อข้อมูลสำรอง (Backup Media) โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงชื่อระบบสารสนเทศ วันที่ เวลาที่สำรองข้อมูล และชื่อผู้รับผิดชอบที่ชัดเจน

๑.๔ สื่อจัดเก็บข้อมูลที่จัดเก็บข้อมูลสำรองนั้นต้องไม่จัดเก็บในสถานที่เดียวกับที่ตั้งของระบบสารสนเทศนั้น เพื่อความปลอดภัยในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

๑.๕ กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๑.๖ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๒. การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทำงานแบบอิเล็กทรอนิกส์

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

๒.๑.๑ ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๑.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลด ความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้าใช้ระบบงานได้ เป็นต้น

๒.๑.๓ ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๑.๔ ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๑.๕ ต้องกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการระบบเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

๒.๑.๖ การสร้างความตระหนักหรือให้ความรู้แก่บุคลากรผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน เป็นต้น

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกำหนดหน้าที่และความรับผิดชอบ

๓.๑ ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด ดังนี้

๓.๑.๑ ผู้ดูแลระบบสารสนเทศต้องกำหนดรายละเอียดของโปรแกรมระบบสำรองข้อมูล กู้คืนข้อมูล และทดสอบ เพื่อให้สามารถทำงานได้ตามปกติ

๓.๑.๒ เจ้าหน้าที่ระบบสารสนเทศจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้ตามภารกิจ

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑ ต้องทดสอบสภาพพร้อมใช้งานของระบบ ต่อไปนี้

๔.๑.๑ ระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑.๒ ระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๔.๑.๓ แผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. การกู้คืนข้อมูล (Data Recovery)

๕.๑ จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๕.๒ ตรวจสอบผลการบันทึกสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๕.๓ ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๕.๔ ตรวจสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยเดือนละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑. สำนักวิทยบริการฯ

๒. ผู้ตรวจสอบระบบสารสนเทศ

๓. ผู้ดูแลระบบและผู้ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีเนื้อหา ดังนี้

๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๒. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน (ผู้ตรวจสอบระบบสารสนเทศ) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓. แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๓.๑ ทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๓.๒ ทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๓.๓ ตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ อย่างน้อยปีละ ๑ ครั้ง

๓.๔ มาตรการในการตรวจสอบและประเมินระบบสารสนเทศสำหรับผู้ตรวจสอบระบบสารสนเทศ ดังนี้

๓.๔.๑ กำหนดให้ผู้ตรวจสอบระบบสารสนเทศสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้สิทธิ์แบบอ่านอย่างเดียว

๓.๔.๒ กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาข้อมูลนั้นเพื่อให้ผู้ตรวจสอบระบบสารสนเทศใช้งาน และควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๓.๔.๓ กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

๓.๔.๔ กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบระบบสารสนเทศ และบันทึกข้อมูล (Log File) แสดงการเข้าถึงนั้น รวมถึงวันและเวลาในการเข้าถึงระบบงานที่สำคัญ ๆ

๓.๔.๕ กรณีที่มีเครื่องมือสำหรับการตรวจสอบและประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๓.๕ รายงานผลการประเมินความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง ต่อคณะกรรมการเทคโนโลยีสารสนเทศและการสื่อสาร และรายงานผลต่อคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

ส่วนที่ ๔
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้กับบุคลากร และผู้ที่เกี่ยวข้องทราบ ได้มีความรู้และความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. สำนักวิทยบริการฯ

๒. หน่วยงานภายในและหน่วยงานที่ได้รับมอบหมายในภารกิจต่าง ๆ

๓. ผู้ดูแลระบบและผู้ที่ได้รับมอบหมาย

๔. บุคลากรที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยอาจวิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒. จัดฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการงานสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓. จัดฝึกอบรมงานสารสนเทศของมหาวิทยาลัยอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๔. จัดทำคู่มือการใช้งานสารสนเทศอย่างปลอดภัยและเผยแพร่ตามเว็บไซต์ของหน่วยงาน

๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ การประชาสัมพันธ์ เผยแพร่ผ่านเว็บไซต์ ฯลฯ

๖. ระดมการมีส่วนร่วมและลงสู่ภาคการปฏิบัติด้วยการกำกับติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้