

(ร่าง)

## ประกาศมหาวิทยาลัยนเรศวร

### เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้ประกาศให้หน่วยงานของรัฐจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ.๒๕๕๓ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของมหาวิทยาลัยมีความปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

ฉะนั้น อาศัยอำนาจตามความในมาตรา ๑๗ และมาตรา ๒๐ แห่งพระราชบัญญัติมหาวิทยาลัยนเรศวร พ.ศ.๒๕๓๓ ประกอบมติที่ประชุมคณะกรรมการพิจารณารายละเอียด คุณลักษณะและกำหนดราคากลาง ครุภัณฑ์คอมพิวเตอร์ มหาวิทยาลัยนเรศวร ในคราวประชุมครั้งที่ ๑/๒๕๕๗ เมื่อวันที่ ๑๖ มกราคม ๒๕๕๗ จึงขอออกประกาศไว้ดังนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยนเรศวร เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

บรรดา กฎ ประกาศ คำสั่ง หรือมติอื่นใด ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากประกาศเป็นต้นไป

ข้อ ๓ ในประกาศนี้

๓.๑ “มหาวิทยาลัย” หมายความว่า มหาวิทยาลัยนเรศวร

๓.๒ “ผู้ใช้งาน” หมายความว่า บุคลากร และนิสิตในสังกัดมหาวิทยาลัย หรือบุคคลภายนอกที่ได้รับอนุญาตให้เข้าใช้งานระบบสารสนเทศผ่านระบบเครือข่ายคอมพิวเตอร์ NU-NET

๓.๓ “ผู้ดูแลระบบเครือข่าย” หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ NU-NET

๓.๔ “ผู้ดูแลระบบสารสนเทศ” หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย และฐานข้อมูลของระบบสารสนเทศในด้านต่าง ๆ

๓.๕ “ผู้ดูแลระบบ” หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ดูแลระบบเครือข่ายคอมพิวเตอร์ NU-NET หรือมีหน้าที่ดูแลเครื่องคอมพิวเตอร์แม่ข่าย หรือมีหน้าที่ดูแลฐานข้อมูลของระบบสารสนเทศในด้านต่าง ๆ

๓.๖ “ผู้พัฒนาระบบสารสนเทศ” หมายความว่า บุคลากรในสังกัดมหาวิทยาลัยที่มีหน้าที่ออกแบบ และพัฒนาระบบสารสนเทศตามความต้องการของหน่วยงาน หรือผู้บริหาร

๓.๗ “หน่วยงานเจ้าของข้อมูล” หมายความว่า หน่วยงานในสังกัดมหาวิทยาลัยที่รับผิดชอบโดยตรงในการปรับปรุงข้อมูลในด้านต่าง ๆ เช่น กองบริหารงานบุคคลเป็นเจ้าของข้อมูลเกี่ยวกับบุคลากรของมหาวิทยาลัย กองบริการการศึกษาเป็นเจ้าของข้อมูลเกี่ยวกับนิสิต เป็นต้น

๓.๘ “สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย

๓.๙ “สินทรัพย์” หมายความว่า ทรัพย์สินหรือสิ่งอื่นใดก็ตามที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับมหาวิทยาลัย

๓.๑๐ “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบสิทธิให้ผู้ใช้งานเข้าถึงหรือใช้งานระบบเครือข่ายและระบบสารสนเทศ

๓.๑๑ “ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)” หมายความว่า การดำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิดชอบ (accountability) การห้ามปฏิเสธความรับผิดชอบ (non-repudiation) และความน่าเชื่อถือ (reliability)

๓.๑๒ เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความปลอดภัย

๓.๑๓ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

๓.๑๔ “ระบบเครือข่าย” หมายความว่า ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย NU-NET

๓.๑๕ “ระบบสารสนเทศ” หมายความว่า ระบบงานของหน่วยงานที่ได้นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ และข้อมูลสารสนเทศ มาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนาและควบคุม การติดต่อสื่อสาร เป็นต้น

**ข้อ ๔** การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมตามข้อ ๕

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีเนื้อหาครอบคลุมข้อ ๖

ถึงข้อ ๑๔

**ข้อ ๕** นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร บุคลากรที่ปฏิบัติงานด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการ  
ทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถ  
เข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัย

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบาย เมื่อมีการเปลี่ยนแปลงที่สำคัญซึ่งมีผลต่อ  
การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย

#### ๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่าง  
ทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว  
รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยก  
ประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์  
ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุม  
ความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบ  
คอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรมและ  
เผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

#### ข้อ ๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึง  
การใช้งานและความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่  
เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้น  
ความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

**ข้อ ๗** มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้ผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ จำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริการจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

**ข้อ ๘** มีการกำหนดหน้าที่รับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศมีเนื้อหา ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (clear desk and clear screen policy) โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล เครื่องคอมพิวเตอร์ สารสนเทศ เป็นต้น อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิและต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาลับของทางราชการ พ.ศ. ๒๕๔๔

**ข้อ ๙** มีการควบคุมการเข้าถึงระบบเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตดังนี้

(๑) การใช้บริการระบบเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนระบบเครือข่าย (equipment identification in network) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนระบบเครือข่ายได้ และสามารถยืนยันการเข้าถึงได้

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกระบบเครือข่าย (segregation in network) ต้องทำการแบ่งแยกระบบเครือข่ายสำหรับกลุ่มผู้ใช้งาน

(๖) การควบคุมการเชื่อมต่อทางระบบเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานระบบเครือข่ายที่มีการใช้งานร่วมกัน หรือการเชื่อมต่อระหว่างระบบเครือข่ายจะต้องให้สอดคล้องกับแนวปฏิบัติการควบคุมเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนระบบเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านการไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

**ข้อ ๑๐** มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติที่ต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

**ข้อ ๑๑** มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุน การใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing WLAN teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อป้องกันสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกมหาวิทยาลัย (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกมหาวิทยาลัย

**ข้อ ๑๒** จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการทำงานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

**ข้อ ๑๓** มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้

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

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยสำนักงานตรวจสอบภายใน (internal audit division) หรือโดยผู้ตรวจสอบจากภายนอก (external auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

**ข้อ ๑๔** ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงที่มีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง และความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ .....

(ศาสตราจารย์ ดร.สุจินต์ จินายน)

อธิการบดีมหาวิทยาลัยนเรศวร

เอกสารแนบท้ายประกาศ  
แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ  
ของมหาวิทยาลัยนเรศวร



## สารบัญ

### หน้า

ส่วนที่ ๑	แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ .....	๑
๑.	การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control).....	๑
๒.	การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management).....	๓
๓.	การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities).....	๔
๔.	การควบคุมการเข้าถึงระบบเครือข่าย (network access control) .....	๗
๕.	การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control).....	๙
๖.	การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control).....	๑๑
๗.	การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless lan access control).....	๑๒
๘.	การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security).....	๑๓
๙.	การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย.....	๑๖
๑๐.	การใช้งานเครื่องคอมพิวเตอร์ของมหาวิทยาลัย.....	๑๘
๑๑.	การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ.....	๑๙
๑๒.	การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail) .....	๒๐
๑๓.	การใช้งานระบบอินเทอร์เน็ต (internet) .....	๒๑
๑๔.	การใช้งานเครือข่ายสังคมออนไลน์ (social network).....	๒๑
๑๕.	การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log) .....	๒๒
ส่วนที่ ๒	นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ .....	๒๓
ส่วนที่ ๓	นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ .....	๒๖
ส่วนที่ ๔	นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ .....	๒๘

## ส่วนที่ ๑

### นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

#### วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย
๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

#### ผู้รับผิดชอบ

๑. กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย
๓. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

#### อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

#### แนวทางปฏิบัติ

๑. การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control)
  - ๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน
  - ๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับ การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจนี้
    - (๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น อ่านอย่างเดียว สร้างข้อมูล ป้อนข้อมูล แก้ไขได้ อนุมัติ ไม่มีสิทธิ

- (๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่กำหนดไว้
- (๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายจากหน่วยงานเจ้าของข้อมูล

๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร เช่น ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลบุคลากร เป็นต้น
- ข้อมูลสารสนเทศตามพันธกิจ เช่น ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญมาก
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึง

(๖) การกำหนดจำนวนช่องทางที่สามารถเข้าถึง

๑.๕ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (business requirement for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

- (๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ
- (๒) มีการปรับปรุงให้สอดคล้องกับข้อมูลกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความรู้ความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

- ๒.๑ มีการกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ
- ๒.๒ ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม
- ๒.๓ มีการกำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (user registration) ครอบคลุมในเรื่องต่อไปนี้
  - (๑) จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศและผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
  - (๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
  - (๓) การกำหนดชื่อผู้ใช้งานจะกำหนดจากรหัสประจำตัวนิสิต หรือกำหนดจากชื่อและนามสกุลตัวแรกเป็นภาษาอังกฤษ เป็นต้น
  - (๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่ม ภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น
  - (๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ
  - (๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย
  - (๗) มีการบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
  - (๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการหรือผู้ที่ได้รับมอบหมายจากหน่วยงานเจ้าของข้อมูล
  - (๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เช่น เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง เป็นต้น

๒.๔ มีการบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

- (๑) แสดงกระบวนการในการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
- (๒) มีการกำหนดระดับสิทธิในการเข้าถึงสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน
- (๓) การมอบหมายสิทธิ ต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง
- (๔) มีการบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๕ มีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

- (๑) มีขั้นตอนปฏิบัติสำหรับการตั้งเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
- (๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน
- (๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันทีหลังจากที่ได้รับรหัสผ่าน
- (๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราวแล้ว และควรเปลี่ยนรหัสให้ยากต่อการคาดเดา
- (๕) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน
- (๖) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่
- (๗) ในกรณีมีความจำเป็นให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบโดยมีการกำหนดระยะเวลาใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๖ ทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การลาออก เปลี่ยนตำแหน่ง โอน ย้าย สิ้นสุดการจ้าง เป็นต้น

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติ ดังนี้

๓.๑ มีการกำหนดวิธีการปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่านการใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

- (๑) เปลี่ยนรหัสผ่านชั่วคราว ทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
- (๒) ควรตั้งรหัสผ่านที่ยากต่อการคาดเดา
- (๓) ควรกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลขและอักขระพิเศษเข้าด้วยกัน
- (๔) ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
- (๕) ไม่ตั้งรหัสผ่านจากอักขระที่เรียงกัน หรือกลุ่มเหมือนกัน
- (๖) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านระบบเครือข่ายคอมพิวเตอร์
- (๗) เก็บรักษาบัตรรหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- (๘) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์
- (๙) ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล
- (๑๐) ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
- (๑๑) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
- (๑๒) ควรมีการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนดไว้ หรือเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้
- (๑๓) หลีกเลี่ยงการใช้รหัสผ่านเดิม
- (๑๔) ผู้ดูแลระบบต้องเปลี่ยนรหัสถึงกว่าผู้ใช้งานทั่วไป

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสม

- (๑) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- (๒) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว
- (๓) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

- (๔) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
- (๕) ตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลาไม่เกิด ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
- (๖) ต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ถูกใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแลชั่วคราว

๓.๓ การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสิทธิ์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (clear desk and clear screen policy) โดยต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ เป็นต้น อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

- (๑) มีกำหนดมาตรการป้องกันทรัพย์สินของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานการณ์ที่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ เช่น

- การจัดการบริเวณล้อมรอบ
- การควบคุมการเข้า-ออก
- การจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก
- การวางอุปกรณ์
- ระบบและอุปกรณ์สนับสนุนการทำงาน

- (๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

- (๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

- (๔) มีการกำหนดขอบเขตการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติตามใดๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย
- ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อกเครื่องคอมพิวเตอร์ เมื่อไม่มีผู้ใช้งาน
- ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน
- ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้ โดยไม่ได้รับอนุญาต เช่น กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยใช้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

- (๑) ต้องแสดงหลักฐานเกณฑ์ในการกำหนดเครื่องข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด
- (๒) ต้องแสดงข้อปฏิบัติสำหรับการเข้าถึงข้อมูลลับ หรือข้อมูลที่สำคัญยิ่งยวด

#### ๔. การควบคุมการเข้าถึงระบบเครือข่าย (network access control)

เพื่อป้องกันการเข้าถึงบริการทางระบบเครือข่ายโดยไม่ได้รับอนุญาตดังนี้

๔.๑ การใช้บริการระบบเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

- (๑) มีการกำหนดระบบสารสนเทศที่ต้องมีการควบคุมการเข้าถึง โดยระบบเครือข่าย หรือบริการที่อนุญาตให้มีการใช้งานได้
- (๒) มีข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- (๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย (wireless lan) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าว อย่างน้อยปีละ ๑ ครั้ง

๔.๒ การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (user authentication for external connection) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวตนก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัยสามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

- (๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (identification) ด้วยชื่อผู้ใช้งานทุกครั้ง
- (๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวตน (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน การใช้สมาร์ทการ์ด หรือการใช้ user token ที่ใช้เทคโนโลยี PKI



(๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงาน

(๔) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยจากอินเทอร์เน็ต ให้มีการตรวจสอบผู้ใช้งานด้วย

๔.๓ การระบุอุปกรณ์บนระบบเครือข่าย (equipment identification in network) ต้องมีวิธีการหรือกระบวนการที่สามารถระบุอุปกรณ์บนระบบเครือข่ายได้ และสามารถยืนยันการเข้าถึงได้ ดังนี้

(๑) ให้กำหนดวิธีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์

(๒) มีการควบคุมการใช้งานอย่างเหมาะสม

(๓) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่าย

(๑) แสดงขั้นตอนหรือหลักเกณฑ์ในการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางระบบเครือข่าย

(๒) กำหนดวิธีการป้องกันช่องทางที่ใช้บำรุงรักษาระบบผ่านระบบเครือข่าย

(๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกระบบเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกระบบเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ ระบบ คือ ระบบเครือข่ายสำหรับผู้ใช้งานภายใน และระบบเครือข่ายสำหรับผู้ใช้งานภายนอก

๔.๖ การควบคุมการเชื่อมต่อทางระบบเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานระบบเครือข่ายที่มีการใช้งานร่วมกัน หรือการเชื่อมต่อระหว่างระบบเครือข่าย จะต้องให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อระบบเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่ระบบเครือข่าย

(๓) ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อระบบเครือข่าย

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระบบเครือข่าย และระบบเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่าย โดยไม่ได้รับอนุญาต

๔.๗ การควบคุมการจัดเส้นทางบนระบบเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนระบบเครือข่าย เพื่อให้การเชื่อมต่อของเครื่องคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

- (๑) ควบคุมให้มีการเปิดเผยแผนการใช้หมายเลขไอพี (ip address plan)
- (๒) กำหนดให้มีการแปลงหมายเลขไอพี เพื่อแยกระบบเครือข่ายย่อย
- (๓) กำหนดมาตรการการบังคับใช้เส้นทางบนระบบเครือข่าย สามารถเชื่อมระบบเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการบนระบบเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

- (๑) การเข้าสู่ระบบจากระยะไกล (remote access) สู่อุปกรณ์สารสนเทศและระบบเครือข่ายของมหาวิทยาลัย ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน
- (๒) การเข้าสู่ระบบจากระยะไกล (remote access) ต้องมีการตรวจสอบ เพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน วิธีการเข้ารหัส เป็นต้น
- (๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายได้จากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการหน่วยงานเจ้าของข้อมูลก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด
- (๔) ก่อนกำหนดให้สิทธิในการเข้าสู่ระบบจากระยะไกลผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้อำนวยการหน่วยงานเจ้าของข้อมูลก่อนอย่างเป็นทางการ
- (๕) มีการควบคุมพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น
- (๖) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่วงทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control)

เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต โดยมีแนวปฏิบัติ ดังนี้

๕.๑ ผู้ดูแลระบบเครือข่าย (network system administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (domain control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของมหาวิทยาลัย และกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๕.๒ กำหนดขั้นตอนการปฏิบัติการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

- (๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์
- (๒) ระบบสามารถยุติการเชื่อมต่อเครื่องคอมพิวเตอร์ปลายทางได้ เมื่อพบว่ามีภัยคุกคามคาดการณ์จากเครื่องคอมพิวเตอร์ปลายทาง
- (๓) จำกัดระยะเวลาสำหรับการป้องกันการรหัสผ่าน
- (๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง command line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

- (๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งานและรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย
- (๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งานและรหัสผ่าน ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านเทคนิค
- (๓) สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม เช่น สมาร์ทการ์ด RFID หรือเครื่องอ่านลายนิ้วมือ เป็นต้น

๕.๔ การบริหารจัดการรหัสผ่าน (password management system) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคง

ปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ดำเนินการดังนี้

- (๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรม อรรถประโยชน์
- (๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป
- (๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องการใช้งานเป็นประจำ
- (๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้
- (๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

- (๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็น ระยะเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนด ระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสมเพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต
- (๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ
- (๓) เครื่องคอมพิวเตอร์ปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีกำหนดระยะเวลาให้ ทำการปิดเครื่องคอมพิวเตอร์โดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตาม กำหนด

๕.๗ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้อง จำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

- (๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบ สารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถ ใช้งานได้ ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง เป็นต้น หรือกำหนดให้ใช้งานได้เฉพาะ ช่วงเวลาการทำงานของมหาวิทยาลัยตามปกติเท่านั้น
- (๒) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องคอมพิวเตอร์ปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องคอมพิวเตอร์ปลายทางด้วย

- (๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง ในที่สาธารณะหรือพื้นที่ภายนอกสำนักงาน เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานของผู้ใช้งานและบุคลากรผ่านสนับสนุนการใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือการใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย จะต้องดำเนินการดังนี้

- (๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย
- (๒) มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ
- (๓) มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมในการควบคุมการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๖.๔ การปฏิบัติงานจากภายนอกมหาวิทยาลัย (teleworking) ต้องกำหนดแนวปฏิบัติแผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานจากภายนอกมหาวิทยาลัย

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless lan access control)

๗.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยจะต้องทำการลงทะเบียนกับผู้ดูแลระบบเครือข่าย โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร

๗.๒ ผู้ดูแลระบบเครือข่าย (network system administrator) ต้องดำเนินการดังต่อไปนี้

- (๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งาน การเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการ

ทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบ  
เครือข่ายตามความจำเป็นในการใช้งาน

- (๒) ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
- (๓) ต้องควบคุมสัญญาณของอุปกรณ์ทุกตัวที่ใช้ติดต่อบนเครือข่ายไร้สาย
- (๔) ควรทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้นจากโรงงานผู้ผลิตทันทีที่นำอุปกรณ์  
กระจายสัญญาณ (access point) มาใช้งาน
- (๕) ควรเปลี่ยนค่าบัญชีชื่อผู้ใช้งานและรหัสผ่าน ในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงาน  
ของอุปกรณ์ไร้สายและควรที่จะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อ  
ป้องกันผู้โจมตีไม่ให้อาจเดาหรือเจาะรหัสได้โดยง่าย
- (๖) ต้องกำหนดค่าการรักษาความปลอดภัยของระบบเครือข่ายไร้สายแบบ WEP (wired  
equivalent privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง  
อุปกรณ์กระจายสัญญาณ (access point) เพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น
- (๗) ควรเลือกใช้วิธีการควบคุม MAC Address (media access control address) และชื่อผู้ใช้งาน  
และรหัสผ่านที่มีสิทธิในการเข้าใช้งานในระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์  
ที่มี MAC Address และชื่อผู้ใช้งานและรหัสผ่านตามที่กำหนดให้สามารถเข้าใช้งานระบบ  
เครือข่ายไร้สายได้ไว้เท่านั้น
- (๘) ควรจะมีการติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างระบบเครือข่ายไร้สายและ  
ระบบเครือข่ายภายในมหาวิทยาลัย
- (๙) ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยกับระบบเครือข่ายไร้สายอย่าง  
สม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย  
และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการหรือ  
ผู้ที่ได้รับมอบหมายจากกองบริการเทคโนโลยีสารสนเทศและการสื่อสารทราบโดยทันที

#### ๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (physical and environmental security)

##### ๘.๑ ศูนย์ข้อมูล (data center)

- (๑) ให้กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดพื้นที่ใช้งานระบบ  
สารสนเทศและการสื่อสารให้ชัดเจน กำหนดนโยบายการติดตั้งอุปกรณ์ในศูนย์ข้อมูลและ  
จัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ทราบทั่วกัน โดยการกำหนด  
พื้นที่ดังกล่าวแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือ  
ระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

- (๒) ให้กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร
- (๓) ให้กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร เป็นผู้กำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร
- (๔) หน่วยงานภายในมหาวิทยาลัยที่นำเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ที่ใช้ในการปฏิบัติงานบนระบบเครือข่ายของมหาวิทยาลัย จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งาน และจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาจากผู้อำนวยการกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
- (๕) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบดังนี้ เครื่องกำเนิดกระแสไฟฟ้าสำรอง ระบบปรับอากาศและควบคุมความชื้น เครื่องดับเพลิง และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ
- (๖) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีจากระบบสนับสนุนการทำงานภายในห้องศูนย์ข้อมูล (data center) ทำงานผิดปกติหรือหยุดการทำงาน

#### ๘.๒ การเดินสายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ (cabling security)

- (๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของมหาวิทยาลัยในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้
- (๒) ให้มีการป้องกันสายสัญญาณต่าง ๆ เพื่อป้องกันมิให้เกิดความเสียหาย เช่น การดักจับสัญญาณ การตัดสายสัญญาณ ถูกหนูกัดสายสัญญาณ เป็นต้น
- (๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน
- (๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการเชื่อมต่อสัญญาณผิดเส้น
- (๕) จัดทำฝัງสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง
- (๖) ตู้สื่อสารที่มีสายสัญญาณสื่อสารต่าง ๆ จะต้องปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก
- (๗) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิมสำหรับระบบสารสนเทศที่สำคัญ หรือการเชื่อมต่อระหว่างอุปกรณ์กระจายสัญญาณหลักที่สำคัญ

- (๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจสอบหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

#### ๘.๓ การบำรุงรักษาอุปกรณ์ (equipment maintenance)

- (๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต
- (๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ
- (๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง
- (๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว
- (๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย
- (๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

#### ๘.๔ การนำทรัพย์สินของมหาวิทยาลัยออกนอกมหาวิทยาลัย (removal of property)

- (๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกมหาวิทยาลัย
- (๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกมหาวิทยาลัย
- (๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้นอกมหาวิทยาลัย
- (๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย
- (๕) บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกไปใช้นอกมหาวิทยาลัย เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

#### ๘.๕ การจัดการอุปกรณ์ที่ใช้งานอยู่นอกมหาวิทยาลัย (security of equipment off-premises)

- (๑) กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยออกไปใช้ในางาน เช่น การขนส่ง และการเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น
- (๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ
- (๓) เจ้าหน้าที่ที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

#### ๘.๖ การจำกัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (secure disposal or re-use of equipment)

- (๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว



- (๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๘.๗ การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

- (๑) จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย
- (๒) ให้มีการควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศโดยผู้เป็นเจ้าของระบบนั้น
- (๓) ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนระบบเครือข่ายอินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้นได้

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

- (๑) ให้มีการควบคุมการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย เพื่อป้องกันความเสียหายหรือการหยุดชะงักที่มีต่อระบบสารสนเทศนั้น
- (๒) ให้ผู้ดูแลระบบที่ได้ผ่านการอบรมหรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย
- (๓) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการอนุมัติให้ติดตั้งก่อนดำเนินการ
- (๔) ไม่ควรติดตั้งซอร์สโค้ดคอมไพเลอร์ (compiler) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ
- (๕) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารีสำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย
- (๖) ให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้ อย่างครบถ้วนเพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เช่น ซอฟต์แวร์ระบบปฏิบัติการ และซอฟต์แวร์ที่เป็นตัวระบบสารสนเทศ เป็นต้น
- (๗) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ
- (๘) ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมและขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้นตามระยะเวลาที่เหมาะสม

(๙) ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นทำการพัฒนา

๙.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่มีมหาวิทยาลัยต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๙.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ควรให้มีการควบคุมการพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคลหรือหน่วยงานภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (malware) ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนที่จะดำเนินการติดตั้ง

๙.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

(๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสมโดยทันที

(๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศ ให้ผู้ดูแลระบบสารสนเทศดำเนินการดังนี้

- มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศ รวมทั้งการประสานงาน เพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสาร เพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของมหาวิทยาลัย
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

(๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้ อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๙.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (audit logging) มีการบันทึก พฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

- (๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
- (๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
- (๓) ข้อมูลวันเวลาที่ออกจากระบบ
- (๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
- (๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
- (๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
- (๗) ข้อมูลการเปลี่ยนคอนฟิกูเรชัน (configuration) ของระบบ
- (๘) ข้อมูลแสดงการใช้งานแอปพลิเคชัน
- (๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน หรืออ่านไฟล์ เป็นต้น
- (๑๐) ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง
- (๑๑) ข้อมูลโพรโทคอลระบบเครือข่ายที่ใช้
- (๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
- (๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

## ๑๐. การใช้งานเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

### ๑๐.๑ การใช้งาน

- (๑) เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้งาน ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

- (๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย
- (๓) การติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ควรปรึกษาผู้ดูแลระบบเครือข่ายประจำหน่วยงาน หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับทางมหาวิทยาลัยเท่านั้น
- (๔) การเคลื่อนย้ายเครื่องคอมพิวเตอร์ควรปิดเครื่องก่อนทุกครั้ง และควรใช้ความระมัดระวัง ในขณะที่เคลื่อนย้าย เพื่อป้องกันอันตรายที่อาจเกิดจากการกระแทกกระเทือนหรือทำตกหล่นได้
- (๕) การเปลี่ยนสถานที่ติดตั้งเครื่องคอมพิวเตอร์ จะต้องแจ้งให้เจ้าหน้าที่พัสดุประจำหน่วยงานรับทราบด้วย เพื่อทำบันทึกประวัติการจัดเก็บพัสดุ
- (๖) การส่งซ่อมเครื่องคอมพิวเตอร์ของมหาวิทยาลัย จะต้องแจ้งผู้ดูแลระบบเครือข่ายประจำหน่วยงาน หรืองานบริการคอมพิวเตอร์ กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับทางมหาวิทยาลัย
- (๗) การใช้เครื่องคอมพิวเตอร์เป็นระยะเวลานาน ๆ ควรเลือกใช้งานในบริเวณที่ไม่มีอากาศร้อนจัด เพื่อป้องกันไม่ให้เกิดความเสียหาย
- (๘) ก่อนการใช้งานสื่อบันทึกข้อมูลชนิดต่าง ๆ ต้องมีการตรวจสอบหาไวรัส โดยโปรแกรมป้องกันไวรัสก่อนเสมอ
- (๙) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอของเครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูล
- (๑๐) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนเครื่องคอมพิวเตอร์ที่ใช้งานอยู่
- (๑๑) ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- (๑๒) ไม่ควรวางอาหารหรือเครื่องดื่มใกล้บริเวณเครื่องคอมพิวเตอร์
- (๑๓) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องคอมพิวเตอร์ ขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องคอมพิวเตอร์ทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

#### ๑๐.๒ การสำรองข้อมูลและการกู้คืน

- (๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD, DVD, และ external hard disk เป็นต้น

- (๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (backup media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ
- (๓) ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บนหน่วยจัดเก็บข้อมูล (hard disk) ข้อมูลที่สำคัญควรมีการสำรองข้อมูลเก็บไว้ เพราะหากหน่วยจัดเก็บข้อมูล (hard disk) เสียไป ก็ไม่กระทบต่อการดำเนินงานและสามารถกู้คืนข้อมูลมาใช้ได้

#### ๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

- ๑๑.๑ ผู้ดูแลระบบสารสนเทศ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ
- ๑๑.๒ เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม
- ๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบสารสนเทศต้องกำหนดชื่อผู้ใช้งาน และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล
- ๑๑.๔ การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML encryption เป็นต้น
- ๑๑.๕ ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่น่าเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

#### ๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

##### ๑๒.๑ การใช้งานสำหรับผู้ใช้งาน

- (๑) ผู้ใช้งานที่ต้องการใช้งานจดหมายอิเล็กทรอนิกส์ ของมหาวิทยาลัยต้องทำการกรอกข้อมูลคำขอเข้าใช้งานกับกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อดำเนินการกำหนดสิทธิชื่อผู้ใช้งานรายใหม่
- (๒) ต้องใช้จดหมายอิเล็กทรอนิกส์ ของมหาวิทยาลัย เพื่อการติดต่องานของราชการ
- (๓) ไม่ควรใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- (๔) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

- (๕) ควรหมั่นตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ที่ไม่สำคัญ เพื่อลดปริมาณการใช้พื้นที่ของระบบจดหมายอิเล็กทรอนิกส์ ให้จัดเก็บจดหมายอิเล็กทรอนิกส์เฉพาะส่วนที่สำคัญ
- (๖) ผู้ใช้งานมีหน้าที่ต้องรักษาชื่อผู้ใช้งานและรหัสผ่าน เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง
- (๗) ปฏิบัติตามข้อกำหนดวิธีการปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน (๓.๑) ที่ได้กำหนดไว้อย่างเคร่งครัด

#### ๑๒.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบเครือข่าย (network system administrator)

- (๑) กำหนดการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้งานระบบ และหน้าที่ความรับผิดชอบของผู้ใช้งาน
- (๒) มีการทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น
- (๓) มีการควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

#### ๑๓. การใช้งานระบบอินเทอร์เน็ต (internet)

- ๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นมีเหตุผลความจำเป็นและได้รับการอนุมัติจากผู้อำนวยการหรือผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย
- ๑๓.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บเบราว์เซอร์
- ๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น
- ๑๓.๔ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

๑๓.๕ ผู้ใช้งานต้องระมัดระวังในการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลด การปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดสิทธิ์หรือทรัพย์สินทางปัญญา

๑๓.๖ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับ ของมหาวิทยาลัย ไม่เสนอความคิดเห็นที่จะทำให้เกิดความเสียหายต่อชื่อเสียงของมหาวิทยาลัย หรือใช้ข้อความข่มขู่ ให้อาย ที่จะเป็นการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่น ๆ

๑๓.๗ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้า ใช้งานโดยบุคคลอื่น

#### ๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (social network)

๑๔.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้ เท่านั้น

๑๔.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบต่อมหาวิทยาลัย ผู้ใช้งานต้องแจ้งต่อ กองบริการเทคโนโลยีสารสนเทศและการสื่อสารโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

#### ๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวตนได้ ให้ปฏิบัติ ดังต่อไปนี้

๑๕.๑ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดขึ้น ความลับในการเข้าถึง

๑๕.๒ ห้ามผู้ดูแลระบบเครือข่ายแก้ไขข้อมูลที่เก็บไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของ มหาวิทยาลัย หรือบุคคลที่ได้รับมอบหมายจากมหาวิทยาลัย

๑๕.๓ กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึก การพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๕.๔ ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้น ให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

## ส่วนที่ ๒

### นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

#### วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัย ให้บริการได้อย่างต่อเนื่อง
๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศในการปฏิบัติงานให้กับมหาวิทยาลัยเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

#### ความรับผิดชอบ

๑. กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย
๓. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

#### อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

#### แนวทางปฏิบัติ

๑. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้
  - ๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง
  - ๑.๒ กำหนดให้มีการสำรองข้อมูลระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้
    - (๑) กำหนดประเภทของข้อมูลที่ทำสำรองเก็บไว้ และความถี่ในการสำรองข้อมูล



- (๒) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup) เป็นต้น
- (๓) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ดำเนินการ วัน/เวลา ชื่อข้อมูลสำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- (๔) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกูเรชัน (configuration) ข้อมูลในฐานข้อมูล เป็นต้น
- (๕) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล และเขียนชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- (๖) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับมหาวิทยาลัยควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับมหาวิทยาลัย เช่น ไฟไหม้ น้ำท่วม เป็นต้น
- (๗) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง ที่ใช้จัดเก็บข้อมูลนอกสถานที่
- (๘) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- (๙) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- (๑๐) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามทางต่อไปนี้

- ๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์ โดยมีรายละเอียด ดังนี้
  - (๑) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
  - (๒) มีการประเมินความเสี่ยงสำหรับระบบสำหรับระบบที่มีความสำคัญนั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น
  - (๓) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
  - (๔) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
  - (๕) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการระบบเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(๖) การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้ อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. ต้องการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๔. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๕. มีการทบทวนระบบสารสนเทศ ระบบสำรองข้อมูล และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อ สภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานในมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง

## ส่วนที่ ๓

### นโยบายตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

#### วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
๒. เพื่อเป็นการป้องกันและลดความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ

#### ผู้รับผิดชอบ

๑. กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
๒. สำนักงานตรวจสอบภายใน (internal audit division) หรือผู้ตรวจสอบจากภายนอก (external auditor)
๓. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย
๔. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

#### อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

#### แนวทางปฏิบัติ

๑. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหา ดังนี้
  - ๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง
  - ๑.๒ ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยสำนักงานตรวจสอบภายใน (internal audit division) หรือโดยผู้ตรวจสอบจากภายนอก (external auditor) เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ
๒. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้
  - ๒.๑ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง
  - ๒.๒ มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
  - ๒.๓ มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

๒.๔ มีมาตรการในการตรวจสอบประเมินระบบสารสนเทศ ดังนี้

- (๑) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว
- (๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
- (๓) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
- (๔) ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูล log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ
- (๕) ในกรณีที่เครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

๓. มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง ต่อคณะกรรมการดำเนินงานกองบริการเทคโนโลยีสารสนเทศและการสื่อสาร และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อรับทราบ

๔. มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

## ส่วนที่ ๔

# นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์

### วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย
๒. เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบเครือข่าย และผู้ดูแลระบบสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

### ผู้รับผิดชอบ

๑. กองบริการเทคโนโลยีสารสนเทศและการสื่อสาร
๒. ผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมาย
๓. ผู้ดูแลระบบสารสนเทศที่ได้รับมอบหมาย

### อ้างอิงมาตรฐาน

๑. มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

### แนวทางปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ
๒. จัดทำคู่มือการใช้งานระบบสารสนเทศ และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย
๓. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมของมหาวิทยาลัย
๔. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนา อย่างน้อยปี

- ละ ๑ ครั้ง โดยอาจจัดรวมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดให้ความรู้
๕. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติให้ลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่ายโดยมีการปรับปรุงความรู้อยู่เสมอ
  ๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน