นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสุราษฎร์ธานี พ.ศ.๒๕๖๓

โดย

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

คำนำ

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ มาตรา ๗ และมาตรา ๘ ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา ๓๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากลและตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

มหาวิทยาลัยราชภัฏสุราษฎร์ธานี จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขึ้นเพื่อให้มหาวิทยาลัยราชภัฏสุราษฎร์ธานีมีแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและรักษาความปลอดภัยด้านระบบสารสนเทศ เพื่อให้สอดคล้องตามพระราชกฤษฎีกาดังกล่าว ซึ่งเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติเพื่อให้เกิดความมั่นคงปลอดภัยในการขับเคลื่อนพันธกิจและการให้บริการของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี อีกทั้งยังเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้บริการและผู้มีส่วนเกี่ยวข้องในทุกภาคส่วนและเพื่อสร้างความน่าเชื่อถือให้กับมหาวิทยาลัยราชภัฏสุราษฎร์ธานีต่อไป

มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

กันยายน ๒๕๖๓

สารบัญ

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ในมาตรา ๕ มาตรา ๗ และมาตรา ๘ ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา ๓๕ แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ.๒๕๔๔ ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

มหาวิทยาลัยราชภัฏสุราษฎร์ธานีจึงได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาะสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่นๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ด้วย

๒. วัตถุประสงค์

มหาวิทยาลัยราชภัฏสุราษฎร์ธานีได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ดังต่อไปนี้

๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสุราษฎร์ธานีเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสุราษฎร์ธานีและทำให้การดำเนินงานต่างๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓. เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร คณาจารย์ บุคลากรและนักศึกษา ให้มีความรู้ ความเข้าใจและตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปีอย่างต่อเนื่อง

๒.๕ ให้อธิการบดี ซึ่งดำรงตำแหน่งผู้บริหารระดับสูงของมหาวิทยาลัย (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้น ในกรณีที่ระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๖ นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อมหาวิทยาลัย

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยราชภัฏสุราษฎร์ธานีมีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัย

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับทั้งภายในมหาวิทยาลัยและหน่วยงานที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยราชภัฏสุราษฎร์ธานีจัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้โดยมีรายละเอียด ดังต่อไปนี้

คำนิยาม

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงการใช้งานสารสนเทศ (Information Access Control Policy)

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย (Information Access Control)

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๕. การใช้งานอินเทอร์เน็ต (Use of the Internet)

๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server management)

๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic mail Usage and Control)

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๙. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๑๐. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ให้ใช้งานส่วนรวม (Public Computer Access Control)

๑๑. การควบคุมการเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information System Access Control)

๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)

๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Use of Social Network)

๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองข้อมูลและการกู้คืน (Backup and Recovery Policy)

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ (Verification and Information Risk Assessment Policy)

ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเพื่อที่จะทำให้มหาวิทยาลัยมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัย ช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สิน และเจ้าหน้าที่ของมหาวิทยาลัย ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัยนโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ซึ่งผู้ใช้งาน เจ้าหน้าที่ของมหาวิทยาลัย และหน่วยงานภายนอกต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ประกอบด้วย

(๑) มหาวิทยาลัย หมายถึง มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๒) การรักษาความมั่นคงปลอดภัย หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๓) ผู้บังคับบัญชา หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

(๔) ศูนย์คอมพิวเตอร์และสารสนเทศ หมายถึง ศูนย์คอมพิวเตอร์และสารสนเทศ ภายใต้สังกัดสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๕) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (CIO) หมายถึง ผู้บริหาร/ผู้บริหารระดับสูงที่ได้รับมอบหมายจากอธิการบดีให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยและมีคุณสมบัติตาม มติคณะรัฐมนตรีเมื่อวันที่ ๙ มิถุนายน ๒๕๔๑

(๖) ผู้บริหารศูนย์คอมพิวเตอร์ หมายถึง ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือรองผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ (ศูนย์คอมพิวเตอร์และสารสนเทศ) มหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๗) มาตรฐาน (Standard) หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริงเพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

(๘) วิธีการปฏิบัติ (Procedure) หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

(๙) แนวทางปฏิบัติ (Guideline) หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

(๑๐) ผู้ใช้งาน (User) หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้บริการใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งมหาวิทยาลัยกำหนดไว้ ดังนี้

(๑๐.๑) ผู้บริหาร หมายถึง อธิการบดี รองอธิการบดี คณบดี ผู้อำนวยการสถาบัน สำนัก ศูนย์หรือ หัวหน้าหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะ ผู้ช่วยอธิการบดี รองคณบดี รองผู้อำนวยการสถาบัน สำนัก ศูนย์ หรือรองหัวหน้าหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะ ผู้อำนวยการสำนักงานอธิการบดี ผู้อำนวยการกอง หรือหัวหน้าหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากองตามที่สภามหาวิทยาลัยกำหนด

(๑๐.๒) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูล และผู้พัฒนาระบบสารสนเทศ

(๑๐.๓) เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว สังกัดมหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๑๐.๔) นักศึกษา หมายถึง นักศึกษาของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี

(๑๑) สิทธิของผู้ใช้งาน (User Access Right) หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของคณะ หน่วยงาน หรือ มหาวิทยาลัย

(๑๒) หน่วยงานภายนอก หมายถึง องค์กรหรือหน่วยงานภายนอก ที่มหาวิทยาลัยอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของคณะ หน่วยงาน หรือ มหาวิทยาลัย โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(๑๓) ระบบเทคโนโลยีสารสนเทศ (Information Technology System) หมายถึง ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบดังนี้

(๑๓.๑) ระบบคอมพิวเตอร์ หมายถึง ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware) รวมถึงอุปกรณ์ หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(๑๓.๒) ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System) หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของมหาวิทยาลัยได้ เช่น สายสัญญาณใยแก้วนำแสง (Fiber Optic) ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

- ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในมหาวิทยาลัย
- ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานเข้ากับเครือข่ายอินเตอร์เน็ตทั่วโลก

(๑๓.๓) ข้อมูล (Data) หมายถึง ข้อมูล ข้อมูลส่วนบุคคล ข้อความคำสั่งชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(๑๓.๔) สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

(๑๔) พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace) หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(๑๔.๑) พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

(๑๔.๒) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

(๑๔.๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)

(๑๔.๔) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

(๑๕) เจ้าของข้อมูล หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

(๑๖) สินทรัพย์ หมายถึง ข้อมูลระบบ ข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร หรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(๑๗) จดหมายอิเล็กทรอนิกส์ (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน มาตรฐานที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ ได้แก่ SMTP POP๓ และ IMAP เป็นต้น โดยชื่อที่ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์จะมีรูปแบบซึ่งประกอบไปด้วย ๒ ส่วน ได้แก่ ชื่อผู้ใช้ และชื่อโดเมน เช่น user@sru.ac.th

(๑๘) บัญชีผู้ใช้งาน (Account) หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

(๑๙) รหัสผ่าน (Password) หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูล และระบบเทคโนโลยีสารสนเทศ

(๒๐) ชุดคำสั่งไม่พึงประสงค์ หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(๒๑) ภัยคุกคาม (Threats) หมายถึง เหตุการณ์ต่างๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจส่งผลกระทบ หรือสร้างความเสียหายต่อระบบสารสนเทศของมหาวิทยาลัย

(๒๒) ช่องโหว่ (Vulnerabilities) หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการ ที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของมหาวิทยาลัย

(๒๓) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

(๒๔) ความมั่นคงปลอดภัยด้านสารสนเทศ หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น อาทิ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (nonrepudiation) และความน่าเชื่อถือ (reliability)

(๒๕) เหตุการณ์ด้านความมั่นคงปลอดภัย หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรืออาจสร้างความเสียหายและส่งผลให้

(๒๕.๑) เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบงานสารสนเทศของหน่วยงานเกิดการหยุดชะงัก

(๒๕.๒) เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัย

(๒๕.๓) เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กำหนดไว้

(๒๕.๔) เกิดภาพลักษณ์ที่ไม่ดีต่อมหาวิทยาลัย หรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความพาดพิงถึงมหาวิทยาลัยในเว็บไซต์ภายนอกซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของมหาวิทยาลัย

(๒๖) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของมหาวิทยาลัยสูญเสียการปฏิบัติงาน รวมถึงการให้บริการต่างๆ แต่เพียงบางส่วนหรือทั้งหมด จากการถูกบุกรุกหรือโจมตีทางช่องโหว่ และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่างๆ

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ
(Information Access Control Policy)

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๒. เพื่อให้ผู้ใช้งาน ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่าย ได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชีผู้ใช้สารสนเทศของมหาวิทยาลัยโดยเคร่งครัด

ผู้รับผิดชอบ

๑. ศูนย์คอมพิวเตอร์และสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย (Information Access Control)

๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน

จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๑.๒. กำหนดสิทธิการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย ดังนี้

๑.๒.๑. ไม่มีสิทธิ
๑.๒.๒. อ่านได้อย่างเดียว
๑.๒.๓. สร้างข้อมูล
๑.๒.๔. ป้อนข้อมูล
๑.๒.๕. แก้ไขข้อมูล
๑.๒.๖. ลบข้อมูล
๑.๒.๗. อนุมัติการใช้ข้อมูล

๑.๓. กำหนดประเภทข้อมูลของมหาวิทยาลัยเป็น ๖ ประเภทหลักๆ ดังนี้

๑.๓.๑. ข้อมูลนักศึกษา

๑.๓.๒. ข้อมูลบุคลากร

๑.๓.๓. ข้อมูลการเงินและบัญชี

๑.๓.๔. ข้อมูลทางการศึกษา

๑.๓.๕. ข้อมูลทางการบริหาร

๑.๓.๖. ข้อมูลการจราจรทางคอมพิวเตอร์

๑.๔. กำหนดระดับชั้นความลับของข้อมูลและสารสนเทศของมหาวิทยาลัยเป็น ๔ ระดับดังนี้

๑.๔.๑. ลับ รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๔.๒. ใช้ภายในเท่านั้น เป็นข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในมหาวิทยาลัย

๑.๔.๓. ส่วนบุคคล ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น

๑.๔.๔. เปิดเผยได้เป็นข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๕. เกณฑ์ในการกำหนดชั้นความลับของข้อมูล

๑.๕.๑. ประเภทลับ หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง

๑.๕.๒. ประเภทใช้ภายในเท่านั้น หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในมหาวิทยาลัย

๑.๕.๓. ประเภทส่วนบุคคล หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น

๑.๕.๔. ประเภทเปิดเผยได้หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๖. กำหนดระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัยดังนี้

๑.๖.๑. การเข้าถึงสำหรับผู้บริหาร

๑.๖.๒. การเข้าถึงสำหรับผู้ปฏิบัติงานตามภาระหน้าที่

๑.๖.๓. การเข้าถึงสำหรับผู้ดูแลระบบ

๑.๖.๔. การเข้าถึงระดับบุคคล

๑.๖.๕. การเข้าถึงระดับผู้ใช้งานทั่วไป

๑.๗. เกณฑ์การแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

๑.๗.๑. ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น

๑.๗.๒. ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

๑.๗.๓. ผู้ดูแลระบบ มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่

๑.๗.๔. บุคคล เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้

๑.๗.๕. ผู้ใช้งานทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น

๑.๗.๖. การกำหนดสิทธิพิเศษสามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น

๑.๗.๗. การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิหรือหน่วยงานหลักเท่านั้น

๑.๘. กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัยในแต่ละประเภทดังนี้

๑.๘.๑. ข้อมูลนักศึกษา หน่วยงานหลัก คือ สำนักส่งเสริมวิชาการและงานทะเบียน

๑.๘.๒. ข้อมูลบุคลากร หน่วยงานหลัก คือ กองการเจ้าหน้าที่

๑.๘.๓. ข้อมูลการเงินและบัญชี หน่วยงานหลัก คือ กองคลัง

๑.๘.๔. ข้อมูลทางการศึกษา หน่วยงานหลัก คือ สำนักส่งเสริมวิชาการและงานทะเบียน

๑.๘.๕. ข้อมูลทางการบริหาร ขึ้นอยู่กับหน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลัก

๑.๘.๖. ข้อมูลการจราจรทางคอมพิวเตอร์ หน่วยงานหลัก คือ ศูนย์คอมพิวเตอร์และสารสนเทศ

๑.๘.๗. การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจของมหาวิทยาลัยราชภัฏสุราษฎร์ธานี

๑.๙. การควบคุมการเปลี่ยนแปลง

๑.๙.๑. การเปลี่ยนแปลงใดๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการดังนี้

(๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง

(๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้นๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

(๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

๑.๙.๒. ต้องจัดเก็บซอร์สโค้ดและไลบรารี่ของระบบสารสนเทศทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๑๐. การกำหนดการใช้งานตามภารกิจ

๑.๑๐.๑.การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) นักศึกษา จะให้สิทธิทันทีที่มีสภาพเป็นนักศึกษาและหมดสิทธิเมื่อพ้นสภาพนักศึกษา ไปแล้ว ๙๐ วัน

(๒) บุคลากร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิเมื่อพ้นสภาพการเป็นบุคลากร

(๓) ผู้บริหาร จะให้สิทธิเข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิเมื่อพ้นสภาพการเป็นผู้บริหาร

(๔) บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

๑.๑๐.๒.ข้อจำกัดในการเข้าถึง

(๑) นักศึกษา เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

(๒) บุคลากร เข้าถึงได้ตามสิทธิเบื้องต้นและภารกิจที่ได้รับมอบหมาย

(๓) ผู้บริหาร เข้าถึงตามสิทธิและภารกิจที่ได้รับมอบหมาย

(๔) บุคคลภายนอก เข้าถึงได้ตามที่ได้รับอนุญาต

๑.๑๑. ระยะเวลาการใช้งาน

๑.๑๑.๑. ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศ ผู้ใช้งานจะเข้าถึงและใช้งานได้ดังนี้

(๑) การเข้าถึงในเวลาราชการ ๐๘.๓๐-๑๗.๐๐ น.

(๒) การเข้าถึงนอกเวลาราชการ หลัง ๑๗.๐๐ น. เป็นต้นไป

(๓) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนักขัตฤกษ์

๑.๑๑.๒. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(๑) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญต้องตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ

๑.๑๒. การหมดสิทธิการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๒.๑. บัญชีผู้ใช้หมดอายุ

๑.๑๒.๒. เมื่อมีการเปลี่ยนแปลงสิทธิการเข้าถึง

๑.๑๒.๓. ถูกระงับสิทธิ

๑.๑๓. การทบทวนและตรวจสอบสิทธิการเข้าถึงและการใช้งานข้อมูล สารสนเทศ และระบบสารสนเทศ

๑.๑๓.๑. ทบทวนและตรวจสอบสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ ปีละ ๑ ครั้ง โดยผู้ดูแลระบบพิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามคณะ/หน่วยงานที่ขอสิทธิ จัดส่งรายชื่อนั้นให้กับ

หน่วยงานที่ขอสิทธิเพื่อดำเนินการทบทวนว่า มีรายชื่อที่ลาออกหรือมีการเปลี่ยนแปลงแต่ยังไม่ได้แก้ไขสิทธิการเข้าถึงให้ถูกต้องหรือไม่

๑.๑๓.๒. หน่วยงานผู้ขอสิทธิแจ้งกลับผู้ดูแลระบบเพื่อดำเนินการแก้ไขให้ถูกต้อง

๑.๑๓.๓. หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลงสิทธิให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบทันที

๑.๑๔. ช่องทางการเข้าถึง

๑.๑๔.๑. เครือข่ายภายในมหาวิทยาลัย

๑.๑๔.๒. เครือข่ายภายนอกมหาวิทยาลัย

๑.๑๔.๓. เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑. การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

๒.๑.๑. จัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑.๒. อบรมผู้ใช้งาน เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง

๒.๑.๓. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๒.๒. การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบสารสนเทศของมหาวิทยาลัยจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศของมหาวิทยาลัย ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้งานออกเป็น 4 กลุ่ม ดังต่อไปนี้

๒.๒.๑. ผู้บริหารของมหาวิทยาลัย

๒.๒.๒. บุคลากรของมหาวิทยาลัย อาจารย์พิเศษ นักวิจัย และแขกของหน่วยงาน

๒.๒.๓. นักศึกษาของมหาวิทยาลัย

๒.๒.๔. บุคคลอื่นๆ ที่ มหาวิทยาลัยมอบสิทธิให้

๒.๓. การลงทะเบียนผู้ใช้งาน

๒.๓.๑. นักศึกษา นักศึกษาใหม่ทุกคน ได้รับบัญชีผู้ใช้หลังจากที่สำนักส่งเสริมวิชาการและงานทะเบียนป้อนข้อมูลนักศึกษาเข้าสู่ระบบสารสนเทศนักศึกษา

๒.๓.๒. บุคลากรของมหาวิทยาลัย อาจารย์พิเศษ นักวิจัย และแขกของหน่วยงานศูนย์คอมพิวเตอร์และสารสนเทศ จะสร้างบัญชีบุคลากรใหม่หลังจากที่กองการเจ้าหน้าที่ หรือ คณะ/หน่วยงานป้อนข้อมูลบุคลากรเข้าระบบสารสนเทศบุคลากร หรือดำเนินการตาม ๒.๓.๓. (๑) และ (๒)

๒.๓.๓. กรณีหน่วยงานต้องการบัญชีผู้ใช้เพื่อบริหารจัดการในการให้บริการบุคคลอื่นๆ ให้ดำเนินการดังนี้

(๑) ดาวน์โหลดแบบฟอร์มได้จาก www.arit.sru.ac.th หัวข้อแบบฟอร์มขอใช้บริการต่างๆ กรอกข้อมูลให้ครบถ้วนแล้วนำส่งศูนย์คอมพิวเตอร์และสารสนเทศ

(๒) ศูนย์คอมพิวเตอร์และสารสนเทศจะออกบัญชีผู้ใช้ให้ตามข้อมูลที่หน่วยงานระบุ และแจ้งผู้รับผิดชอบตามอีเมล์ที่ระบุไว้ในแบบฟอร์มหรือส่งข้อความไปยังหมายเลขโทรศัพท์ที่ระบุไว้ในแบบฟอร์ม

(๓) ผู้รับผิดชอบของหน่วยงาน จะต้องรับผิดชอบความเสียหายใดๆ ที่จะเกิดจากการใช้งานบัญชีผู้ใช้ที่ศูนย์คอมพิวเตอร์และสารสนเทศออกให้

(๔) หากต้องการเปลี่ยนแปลงผู้รับผิดชอบบัญชีผู้ใช้ ให้แจ้งศูนย์คอมพิวเตอร์และสารสนเทศเป็นลายลักษณ์อักษรลงนามโดยผู้บริหารของหน่วยงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมบัญชีผู้ใช้และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

(๕) หากต้องการยกเลิกบัญชีผู้ใช้ ให้แจ้งศูนย์คอมพิวเตอร์และสารสนเทศเป็นลายลักษณ์อักษรลงนามโดยผู้บริหารของหน่วยงาน ระบุ ชื่อผู้รับผิดชอบ และจำนวนบัญชีผู้ใช้ที่ต้องการยกเลิก

๒.๓.๔. บุคคลอื่นๆ ที่ มหาวิทยาลัยมอบสิทธิให้ เช่น บุคคลที่ทำงานในหน่วยงานอิสระ บุคคลที่มหาวิทยาลัยมอบสิทธิให้ สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อที่สำนักงานศูนย์คอมพิวเตอร์และสารสนเทศ โดยมีหนังสือรับรองจากผู้บริหารระดับคณะ/หน่วยงานขึ้นไป และแสดงบัตรประจำตัวประชาชน หรือหนังสือเดินทาง พร้อมสำเนาที่รับรองสำเนาถูกต้อง จำนวน ๑ ฉบับ

๒.๔. การจัดการบัญชีผู้ใช้ของมหาวิทยาลัย

๒.๔.๑. การบริหารจัดการบัญชีผู้ใช้สำหรับบุคลากรของมหาวิทยาลัย ดำเนินการโดยผ่านผู้แทนของหน่วยงาน โดยผู้บริหารของหน่วยงานแจ้งชื่อผู้แทนที่จะรับผิดชอบในการดูแลบัญชีผู้ใช้ของบุคลากรในสังกัด เป็นลายลักษณ์อักษรถึงผู้บริหารศูนย์คอมพิวเตอร์ โดยมีรายละเอียด ดังนี้

(๑) ชื่อหน่วยงาน

(๒) ชื่อ-สกุลของผู้แทน

(๓) ชื่อบัญชีผู้ใช้ของผู้แทน

(๔) อีเมล์ของผู้แทน

(๕) หมายเลขโทรศัพท์ของผู้แทน

๒.๔.๒. การเปลี่ยนแปลงผู้แทนของหน่วยงาน ให้แจ้งศูนย์คอมพิวเตอร์และสารสนเทศเป็นลายลักษณ์อักษรลงนามโดยผู้บริหารของหน่วยงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่พร้อมอีเมล์และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

๒.๕. การจัดการสิทธิของผู้ใช้งาน

๒.๕.๑. เมื่อเจ้าหน้าที่ของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิการใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิหรือถอดถอนสิทธิออกจากระบบทันที

๒.๕.๒. การแจ้งขอใช้สิทธิ/เปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(๑) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของหน่วยงานหลัก

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๒.๕.๓. ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒.๕.๔. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องพิจารณาการควบคุมผู้ใช้งานที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอโดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา โดยต้องได้รับความเห็นชอบและอนุมัติจากอธิการบดีหรือผู้ที่ได้รับมอบอำนาจจากอธิการบดี

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งานหรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ต้องเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๒.๖. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๒.๖.๑. ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๒.๖.๒. ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๒.๖.๓. ผู้ดูแลระบบต้องจัดส่งรหัสผ่านให้ผู้ใช้งาน โดยหลีกเลี่ยงการใช้อีเมล์เป็นช่องทางในการส่ง

๒.๖.๔. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราวและต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๒.๖.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

๒.๖.๖. ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอเป็นเวลานาน

๒.๖.๗. กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้งานรายนั้นจะถูกตัดสิทธิการใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๒.๗. การทบทวนสิทธิการเข้าถึง

๒.๗.๑. ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

๒.๗.๒. บัญชีผู้ใช้จะหมดอายุ ดังนี้

(๑) กรณีบุคลากร หมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของมหาวิทยาลัย ยกเว้นผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ตเท่านั้น

(๒) กรณีนักศึกษา หมดอายุหลังพ้นสภาพการเป็นนักศึกษา ๙๐ วัน แต่จะเปลี่ยนสภาพเป็นศิษย์เก่าโดยอัตโนมัติ ซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับเข้าอินเทอร์เน็ต และระบบฐานข้อมูลศิษย์เก่าเท่านั้น

(๓) กรณีที่ไม่ใช่บุคลากรของมหาวิทยาลัย หมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชีหรือเมื่อไม่มีการเข้าใช้งานติดต่อกันเกิน ๓ เดือน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑. การใช้งานบัญชีผู้ใช้และรหัสผ่าน

๓.๑.๑. ผู้ใช้งานต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๓.๑.๒. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๓.๒. การใช้งานรหัสผ่าน

๓.๒.๑. ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน ตามระยะเวลาที่มหาวิทยาลัยกำหนด

๓.๒.๒. ไม่กำหนดรหัสผ่านที่มีส่วนหนึ่งมาจากสิ่งที่สื่อถึงตัวผู้ใช้งาน เช่น ชื่อ นามสกุล ชื่อเล่น ชื่อบิดา ชื่อมารดา ชื่อหน่วยงาน หรือคำศัพท์ที่มีใช้ในพจนานุกรม เป็นต้น ต้องประกอบด้วย ตัวอักษรไม่น้อยกว่า 8 ตัว โดยต้องผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และตัวอักขระพิเศษเข้าด้วยกัน

๓.๒.๓. ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

๓.๒.๔. ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

๓.๒.๕. หลีกเลี่ยงการใช้รหัสผ่านเดียวกับระบบงานต่าง ๆ ที่มีสิทธิใช้งาน

๓.๒.๖. เก็บบัญชีและรหัสผ่านของตนเองไว้เป็นความลับ

๓.๓. การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

๓.๓.๑. ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อกหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๓.๓.๒. ผู้ใช้งานต้องล็อกอุปกรณ์และเครื่องคอมพิวเตอร์ที่สำคัญ เมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแล

๓.๓.๓. ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๓.๔. การจัดวางและการป้องกันอุปกรณ์

๓.๔.๑. จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับอนุญาต

๓.๔.๒. อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๓.๔.๓. ดำเนินการตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๓.๕. การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๓.๕.๑. จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๓.๕.๒. ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศโดยผู้เป็นเจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

๓.๕.๓. มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๓.๕.๔. สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมเพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๓.๕.๕. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๓.๕.๖. จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่นๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

๓.๕.๗. โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย เป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรม และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

๓.๕.๘. ไม่เก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๓.๕.๙. ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

๓.๕.๑๐.ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๓.๕.๑๑.ต้องลบข้อมูลที่ไม่มีการใช้งานตั้งแต่ ๕ ปีขึ้นไปออกจากฐานข้อมูล และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล ทั้งนี้ การลบหรือทำลายข้อมูลอิเล็กทรอนิกส์ดังกล่าวต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติให้ทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูลทุกครั้ง

๓.๖. การป้องกันโปรแกรมไม่ประสงค์ดี

๓.๖.๑. ผู้ใช้งานต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมไม่ประสงค์ดี รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๓.๖.๒. ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๓.๖.๓. ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมไม่ประสงค์ดีก่อนการรับส่งทุกครั้ง

๓.๖.๔. ผู้ใช้งานต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมไม่ประสงค์ดีก่อนการเปิดใช้ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่นไฟล์ที่มีนามสกุล .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe เป็นต้น

๔. การควบคุมการเข้าถึงระบบเครือข่าย (Network Access Control)

๔.๑. การเข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย

๔.๑.๑. การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจะต้องพิสูจน์ตัวตนผู้ใช้งานด้วยบัญชีผู้ใช้ที่มหาวิทยาลัยออกให้

๔.๑.๒. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิที่ได้รับอนุญาตเท่านั้น

๔.๑.๓. การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจากภายนอกต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรฐานการเข้าถึงระบบเครือข่ายมหาวิทยาลัยจากภายใน

๔.๑.๔. เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับศูนย์คอมพิวเตอร์และสารสนเทศ

๔.๑.๕. จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ตอุปกรณ์เครือข่ายตามความจำเป็น

๔.๑.๖. การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๔.๑.๗. การเข้าใช้เครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของมหาวิทยาลัย ต้องขออนุญาตใช้บัญชีชั่วคราวจากมหาวิทยาลัย ซึ่งจะเข้าถึงได้ตามสิทธิที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

๔.๒. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๔.๒.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในมหาวิทยาลัยจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากผู้บริหารศูนย์คอมพิวเตอร์ หรือผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

๔.๒.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สายและได้รับอนุญาตจากผู้ดูแลระบบ

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าเริ่มต้นมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN client และอุปกรณ์กระจายสัญญาณ ด้วยวิธีที่มีประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น

(๗) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

(๘) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่าย

ไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้รายงานต่อผู้บริหารศูนย์คอมพิวเตอร์และสารสนเทศ ทราบโดยทันที

๔.๓. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๔.๓.๑. อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๔.๓.๒. เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L๓

๔.๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๔.๔.๑. ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๔.๔.๒. ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๔.๔.๓. ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกมหาวิทยาลัย แต่ให้เชื่อมต่อผ่านช่องทางที่ปลอดภัยที่มหาวิทยาลัยกำหนด เช่น VPN เป็นต้น

๔.๔.๔. อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๔.๔.๕. ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๔.๔.๖. ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๔.๕. การแบ่งแยกเครือข่าย (segregation in networks)

๔.๕.๑. ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๔.๕.๒. แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่างๆ ของมหาวิทยาลัย

๔.๕.๓. ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

๔.๕.๔. ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงาน ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๔.๖. การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control)

๔.๖.๑. อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๔.๖.๒. ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัย ต้องติดตั้งระบบตรวจจับการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี

๔.๗. การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)

๔.๗.๑. อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๔.๗.๒. มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๔.๗.๓. ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๔.๗.๔. ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๔.๗.๕. ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๔.๗.๖. ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

๔.๘. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connections)

๔.๘.๑. ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๔.๘.๒. ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิในการเข้าใช้บริการแล้วเท่านั้น

๔.๘.๓. ต้องมีระบบตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่าน เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๕. การใช้งานอินเทอร์เน็ต (Use of the Internet)

๕.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ตามสิทธิที่ได้รับ

๕.๒. ห้ามใช้อินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๕.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น

๕.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๕.๕. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๖. การบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server Management)

๖.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๖.๒. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๖.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (time.uni.net.th หรือ clock.nectec.or.th) ที่มหาวิทยาลัยใช้อ้างอิง

๖.๔. เปิดใช้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัย

๖.๕. ต้องปรับปรุงระบบซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่างๆ

๖.๖. ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๖.๗. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

๗. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (Electronic mail Usage and Control)

๗.๑. นักศึกษา ใช้บัญชีผู้ใช้ที่เป็นตัวเลขรหัสนักศึกษา ตามด้วย @student.sru.ac.th โดยรหัสผ่านจะใช้เป็นหมายเลขบัตรประจำตัวประชาชนของนักศึกษาเป็นค่าเริ่มต้นและเมื่อเข้าใช้งานบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ในครั้งแรก ระบบจะบังคับให้นักศึกษาทำการเปลี่ยนรหัสผ่านใหม่ทันที โดยเข้าใช้งานได้ที่ mail.google.com/a/student.sru.ac.th

๗.๒. บุคลากร ดาวน์โหลดแบบฟอร์มจาก arit.sru.ac.th หัวข้อแบบฟอร์มขอใช้บริการต่างๆ (แบบฟอร์มการสมัครใช้อีเมล์มหาวิทยาลัย) กรอกแบบฟอร์มให้ครบถ้วน จากนั้นนำส่งศูนย์คอมพิวเตอร์และสารสนเทศเพื่อลงทะเบียนและเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์(SRU Mail) โดยเข้าใช้งานได้ที่ mail.google.com/a/sru.ac.th

๗.๓. ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ

๗.๔. กรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงบนหัวข้อจดหมายอิเล็กทรอนิกส์

๗.๕. ผู้ใช้งานมีหน้าที่จะต้องรักษาบัญชีผู้ใช้ และรหัสผ่านเป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้องเพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี

๗.๖. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องบันทึกการออกทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

๗.๗. ก่อนส่งต่อ เปิดไฟล์ หรือคลิกลิ้งค์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

๗.๘. ต้องไม่ส่งข้อมูลส่วนบุคคลที่สำคัญ เช่น รหัสผ่าน บัญชีผู้ใช้ หมายเลขประจำตัวประชาชน หมายเลขบัตรเครดิต ฯลฯ ผ่านจดหมายอิเล็กทรอนิกส์

๘. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๘.๑. ผู้ดูแลระบบ (System Administrator)

ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๘.๒. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

๘.๒.๑. ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๘.๒.๒. ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๘.๒.๓. จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๘.๒.๔. จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๘.๓. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๘.๓.๑. ผู้ใช้งานต้องมีบัญชีผู้ใช้และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

๘.๓.๒. สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม โดยใช้สมาร์ทการ์ด RFID หรือเครื่องอ่านลายพิมพ์นิ้วมือ หรือวิธีการอื่นที่มีความปลอดภัย

๘.๔. การบริหารจัดการรหัสผ่าน (Password Management System)

๘.๔.๑. ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อกสิทธิการเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

๘.๔.๒. ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

๘.๔.๓. มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

๘.๔.๔. ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

๘.๔.๕. ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๘.๔.๖. เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๘.๕. การใช้งานโปรแกรมอรรถประโยชน์(Use of System Utilities)

๘.๕.๑. จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๘.๕.๒. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๘.๕.๓. ต้องจัดเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๘.๕.๔. ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๘.๕.๕. โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่องค์กรได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

๘.๕.๖. ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๘.๖. การหมดเวลาใช้งานระบบสารสนเทศ (Session Time-Out)

๘.๖.๑. ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาทีตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๘.๖.๒. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๘.๖.๓. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๘.๗. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time)

๘.๗.๑. กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ไม่เกิน ๓ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของมหาวิทยาลัยเท่านั้น

๘.๗.๒. การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๘.๗.๓. กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๙. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)

๙.๑. หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย ต้องแต่งตั้งผู้มีสิทธิ กำหนดจำนวนผู้มีสิทธิในการเข้าถึงระบบปฏิบัติการ

๙.๒. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๙.๓. ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๙.๔. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๙.๕. ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

๙.๖. ห้ามการติดตั้งซอฟต์แวร์อื่นๆ หรือซอฟต์แวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่มหาวิทยาลัยไม่อนุญาต

๙.๗. ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงานสำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๙.๘. ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมไม่ประสงค์ดีบนเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง

๙.๙. กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมไม่ประสงค์ดี เช่น การรายงานการเกิดขึ้นของโปรแกรมไม่ประสงค์ดี การวิเคราะห์ การจัดการ การกู้คืนระบบจากความเสียหายที่พบ

๙.๑๐.ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมไม่ประสงค์ดีอย่างสม่ำเสมอ

๙.๑๑.ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดี เพื่อให้ผู้ดูแลระบบและผู้ใช้งานมีความรู้ความเข้าใจและสามารถป้องกันตนเองได้และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร

๑๐. การควบคุมการเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ให้ใช้งานส่วนรวม (Public Computer Access Control)

๑๐.๑. ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตนเอง

๑๐.๒. ระบบต้องไม่แสดงรายละเอียดสำคัญก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๑๐.๓. ต้องตั้งค่าระบบให้สามารถยุติการเชื่อมต่อเมื่อพบว่ามีความพยายามคาดเดารหัสผ่าน

๑๐.๔. ระบบจะต้องจำกัดสิทธิผู้ใช้งานในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

๑๑. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)

๑๑.๑. การจำกัดการเข้าถึงสารสนเทศ

๑๑.๑.๑. การจำกัดการเข้าถึงของผู้ใช้งาน

(๑) เข้าได้ตามสิทธิที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดสิทธิการเข้าถึงข้อมูลส่วนบุคคล

(๓) ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๑๑.๑.๒. แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของมหาวิทยาลัย ออกเป็น ๓ กลุ่ม คือ ๑) ผู้ดูแลระบบ ๒) ผู้พัฒนาระบบงาน และ ๓) ผู้ใช้งานระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจนเป็นลายลักษณ์อักษร

๑๑.๑.๓. การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

(๑) ชื่อบัญชีผู้ใช้

(๒) วันเวลาที่เข้าถึงระบบ

(๓) วันเวลาที่ออกจากระบบ

(๔) เหตุการณ์สำคัญที่เกิดขึ้น

(๕) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) แสดงการใช้สิทธิ เช่น สิทธิของผู้ดูแลระบบ

(๘) แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน อ่านไฟล์

(๙) หมายเลขไอพีแอดเดรสที่เข้าถึง

(๑๐)แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

(๑๑)แสดงการหยุดการทำงานของระบบงานที่สำคัญ

๑๑.๑.๔. การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

๑๑.๑.๕. การควบคุมผู้รับเหมา (outsource) กรณีมีการจ้างเหมาบำรุงรักษาดูแล และพัฒนาระบบสารสนเทศ

(๑) มีกระบวนการคัดเลือกผู้รับเหมา โดยต้องกำหนดคุณสมบัติของผู้รับเหมาที่ชัดเจน เช่น ต้องมีประสบการณ์มีลูกค้าอ้างอิงน่าเชื่อถือ หรือ ใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาทั้งในส่วนของฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุนอื่นๆ เพื่อให้ได้ผู้รับเหมาที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

(๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมา โดยต้องกำหนดขอบเขตและระดับการรับเหมาอย่างชัดเจน และผู้รับเหมาต้องนำเสนอรายละเอียดงาน ขอบเขตงานให้ครบถ้วน

(๓) หน่วยงานต้องเข้าไปตรวจสอบรายละเอียดของการปฏิบัติงานของผู้รับเหมาได้ เช่น ร่วมกำหนดวิธีการทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาเป็นระยะๆ ตามที่กำหนดไว้หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาใช้ในการปฏิบัติงานและเพื่อประเมินความสม่ำเสมอของผู้รับเหมาในการดำเนินงานตามข้อกำหนดของหน่วยงาน

(๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน ด้วยวิธีการควบคุมการเข้าถึงแบบเดียวกับบุคคลภายนอก โดยมีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

(๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๑๑.๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบต่อคนกลุ่มใหญ่ หรือระบบที่มีความสำคัญต่อหน่วยงานจะต้องดำเนินการดังนี้

๑๑.๒.๑. ระบบซึ่งไวต่อการรบกวน มีผลกระทบ และมีความสำคัญสูง ได้แก่ ระบบสารสนเทศบุคลากร ระบบสารสนเทศนักศึกษา และระบบสารสนเทศทางการเงิน ต้องแยกออกจากระบบอื่น และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

๑๑.๒.๒. ต้องควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวนโดยเฉพาะ

(๑) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

(๒) ติดตั้งระบบแยกต่างหากจากระบบสารสนเทศอื่น

(๓) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

(๔) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

๑๑.๒.๓. ต้องควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร

๑๑.๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๑.๓.๑. แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ

(๑) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีที่นำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(๔) ไม่ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

(๕) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่างๆ

(๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูลทุกครั้ง

(๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในมหาวิทยาลัย

(๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(๙) มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟล์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

๑๑.๓.๒. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External hard disks) เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๑๑.๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๑.๔.๑. ผู้ใช้งานระบบจากระยะไกล จะต้องได้รับการอนุมัติสิทธิจากผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (Chief Information Officer: CIO) โดยทำการเชื่อมต่อผ่านระบบ Virtual Private Network (VPN) ตามที่มหาวิทยาลัยกำหนด พร้อมทั้งทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

๑๑.๔.๒. ต้องรักษาความปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในองค์กร

๑๑.๔.๓. มีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาตและการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานขององค์กร

๑๑.๔.๔. ต้องกำหนดให้ผู้ใช้งานระบบจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตน รวมทั้งบุคคลอื่น เข้าถึงระบบเทคโนโลยีสารสนเทศขององค์กรในสถานที่ดังกล่าว

๑๑.๔.๕. ต้องตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบสารสนเทศขององค์กรจากระยะไกลมีระบบป้องกันไวรัสและการใช้งานไฟร์วอลล์อย่างเหมาะสม

๑๑.๔.๖. ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้เข้าถึงสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ขององค์กรที่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๒. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)

๑๒.๑. ต้องกำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงาน และมี Log Server ของหน่วยงานสำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของมหาวิทยาลัยเมื่อมีการร้องขอ

๑๒.๒. กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

๑๒.๓. บันทึกการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน และบันทึกรายละเอียดของระบบป้องกันการบุกรุกได้แก่ บันทึกการเข้าออกระบบ ซึ่งประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โปรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๑๒.๔. ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๑๒.๕. กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่างๆ และจำกัดสิทธิการเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๑๓. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)

๑๓.๑. ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม ประกอบด้วย

๑๓.๑.๑. ผู้ดูแลระบบเครือข่าย (system administrator)

๑๓.๑.๒. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (network administrator)

๑๓.๑.๓. ผู้ดูแลระบบสารสนเทศ (application administrator)

๑๓.๒. ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบ ดังนี้

๑๓.๒.๑. ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๑๓.๒.๒. เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนถูกต้องและความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้เว้นแต่ ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

(๒) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(๓) ข้อมูลจราจรทางคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ time.uni.net.th หรือ clock.nectec.or.th

๑๓.๓. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๓.๑. ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที

ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

๑๓.๓.๒. ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๑๓.๓.๓. ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่างๆ ให้เหมาะสม

๑๓.๓.๔. ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๑๓.๓.๕. ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๓.๔. ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

๑๓.๔.๑. ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๑๓.๔.๒. ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๑๓.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

๑๓.๕.๑. ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

๑๓.๕.๒. ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๑๓.๕.๓. ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Use of Social Network)

๑๔.๑. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๑๔.๒. ในการใช้งานเครือข่ายสังคมออนไลน์ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๑๔.๓. ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย

๑๔.๔. หากผู้ใช้งานทราบหรือรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งศูนย์คอมพิวเตอร์และสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๕. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑๕.๑. การจัดการบริเวณแวดล้อมทางกายภาพ

๑๕.๑.๑. กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๑๕.๑.๒. กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๑.๓. ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ

๑๕.๒. การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

๑๕.๒.๑. ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๒. ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๕.๒.๓. มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว

๑๕.๒.๔. ต้องพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้องศูนย์กลางข้อมูล (data center)

๑๕.๒.๕. ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๑๕.๒.๖. มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก

๑๕.๒.๗. ดูแลผู้ที่มาเยือนจนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน และป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

๑๕.๒.๘. ต้องควบคุมหน่วยงานภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๙. สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๑๐. เจ้าหน้าที่ของบริษัท ผู้ได้รับการว่าจ้างหรือผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอดระยะเวลาการปฏิบัติงาน

๑๕.๒.๑๑. ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๕.๒.๑๒. ต้องทบทวนหรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๕.๓. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๑๕.๓.๑. จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๕.๓.๒. จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๑๕.๓.๓. จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในมหาวิทยาลัย

๑๕.๓.๔. ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน

๑๕.๓.๕. ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

๑๕.๔. การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

๑๕.๔.๑. จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๑๕.๔.๒. ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น

๑๕.๔.๓. ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๑๕.๕. การนำทรัพย์สินของมหาวิทยาลัยออกนอกสำนักงาน

๑๕.๕.๑. ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกมหาวิทยาลัย

๑๕.๕.๒. บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกนอกสำนักงาน เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๕.๕.๓. ให้เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยเสมือนเป็นทรัพย์สินของตนเอง

๑๕.๖. ระบบและอุปกรณ์สนับสนุนการทำงาน

๑๕.๖.๑. ต้องสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งาน โดยให้มี

(๑) ระบบสำรองกระแสไฟฟ้า

(๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง

(๓) ระบบระบายอากาศ

(๔) ระบบปรับอากาศและควบคุมความชื้น

(๕) ระบบป้องกันอัคคีภัย

๑๕.๖.๒. ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑๕.๖.๓. ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงาน ทำงานผิดปกติหรือหยุดทำงาน

๑๕.๖.๔. จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองข้อมูลและการกู้คืน (Backup and Recovery Policy)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. ศูนย์คอมพิวเตอร์และสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ของคณะ/หน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ระบบสำรอง (disaster recovery site: DR site)

๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรองและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๑.๒. ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

๑.๒.๑. มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

๑.๒.๒. มีระบบไฟฟ้าสำรอง

๑.๒.๓. มีระบบปรับอากาศและความชื้นที่เหมาะสม

๑.๒.๔. มีระบบป้องกันอัคคีภัย

๑.๒.๕. มีระบบส่องสว่างที่เหมาะสม

๑.๒.๖. มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

๑.๒.๗. มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล (Data Backup)

๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูล และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง

๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๒.๓. กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๒.๔. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานะการทำงานสำเร็จ/ไม่สำเร็จ

๒.๕. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และ ข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ

๒.๖. จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

๒.๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๒.๘. มีแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๘.๑. ต้องกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๘.๒. ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้

๒.๘.๓. ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

๒.๘.๔. ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

๒.๘.๕. ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล (Data Recovery)

๓.๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๓.๒. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๓.๓. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๓.๔. ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑. ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ
(Verification and Information Risk Assessment Policy)

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่างๆ ซึ่งทำให้ระบบสารสนเทศของมหาวิทยาลัยหรือของหน่วยงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

๑. ศูนย์คอมพิวเตอร์และสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. หน่วยตรวจสอบภายใน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. หน่วยงานจะต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ โดยต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศโดยผู้ตรวจสอบภายใน อย่างน้อยปีละ ๑ ครั้ง

๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ดังต่อไปนี้

๒.๑. ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

๒.๒. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

๒.๓. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

๒.๔. ความเสี่ยงที่เกิดจากการลงบันทึกเข้าสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

๒.๕. ความเสี่ยงที่เกิดจากการลักลอบใช้บัญชีผู้ใช้และรหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

๒.๖. ความเสี่ยงที่เกิดจากความเสียหายทางกายภาพ เช่น ไฟไหม้ น้ำท่วม อุปกรณ์สูญหาย เป็นต้น

๓. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

๔. การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

๔.๑. ระดับความน่าจะเป็นที่จะเกิดความเสี่ยงที่ระบุ

๔.๒. ระดับความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

๔.๓. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ

๔.๔. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

๕. ต้องแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบ และประเมินผลงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ ๔
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Awareness Policy)

วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและผู้เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. ศูนย์คอมพิวเตอร์และสารสนเทศ
๒. หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย
๔. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒. อบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓. จัดฝึกอบรมการใช้งานสารสนเทศของมหาวิทยาลัยอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๔. จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เช่น การติดประกาศ ประชาสัมพันธ์แผ่นพับ เผยแพร่ผ่านเว็บไซต์ ฯลฯ

๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้