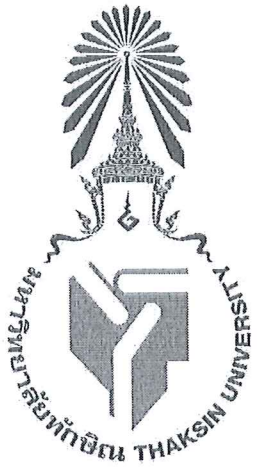

นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยทักษิณ พ.ศ. ๒๕๖๒

สารบัญ

คำนิยามจำกัดความ

๑. **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยทักษิณ

๒. **หน่วยงาน** หมายถึง คณะ ศูนย์ สถาบัน สำนัก วิทยาลัย หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่น ในสังกัดมหาวิทยาลัยทักษิณ

๓. **ผู้ใช้งาน (user)** หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย เจ้าหน้าที่ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหาร และนิสิตของมหาวิทยาลัย รวมถึงบุคคล และ/หรือ หน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และ/หรือ ระบบเครือข่ายของมหาวิทยาลัย

๔. **ชื่อผู้ใช้ (user name)** หมายถึง ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่ได้กำหนดสิทธิ์การใช้งานไว้

๕. **รหัสผ่าน (password)** หมายถึง กลุ่มตัวอักษรหรือตัวเลขหรืออักขระที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูล สารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย

๖. **บัญชีผู้ใช้ (user account)** หมายถึง รายชื่อผู้ใช้และรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

๗. **ระบบคอมพิวเตอร์** หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๘. **อุปกรณ์คอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์ทุกชนิด อุปกรณ์สื่อสารแบบพกพา เช่น สมาร์ทโฟน แท็บเล็ต รวมถึงอุปกรณ์อิเล็กทรอนิกส์ที่ทำหน้าที่ได้เหมือนคอมพิวเตอร์ และอุปกรณ์ที่เชื่อต่อหรือทำงานเป็นส่วนหนึ่งของระบบคอมพิวเตอร์โดยอาจทำหน้าที่เป็นอุปกรณ์สื่อสาร หรือใช้บันทึกข้อมูล เช่น เครื่องพิมพ์ สแกนเนอร์ หน่วยความจำภายนอก โทรศัพท์ กล้องดิจิทัล โทรทัศน์อัจฉริยะ และอุปกรณ์เครือข่ายต่าง ๆ เป็นต้น

๙. **อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่** หมายถึง อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารที่สามารถนำไปติดตั้งนอกสถานที่ได้ และอุปกรณ์คอมพิวเตอร์แบบพกพา เช่น โน้ตบุ๊ค แท็บเล็ต สมาร์ทโฟน เป็นต้น

๑๐. **ข้อมูล (data)** หมายถึง ข้อเท็จจริงที่เป็นตัวเลข ข้อความ ภาพ เสียง วีดีโอ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ รวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าธุรกรรมทางอิเล็กทรอนิกส์

๑๑. **สารสนเทศ (information)** หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น

๑๒. **ระบบสารสนเทศ (information system)** หมายถึง ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ ระบบคอมพิวเตอร์ ทั้งฮาร์ดแวร์ ซอฟต์แวร์ ระบบเครือข่าย ฐานข้อมูล ผู้พัฒนาระบบ ผู้ใช้งานระบบ พนักงานที่เกี่ยวข้อง และผู้เชี่ยวชาญในสาขา ทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม

๑๓. **ระบบเทคโนโลยีสารสนเทศ** หมายถึง เครื่องคอมพิวเตอร์ ระบบงาน เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เครือข่าย และ/หรือ ระบบหรืออุปกรณ์สนับสนุนการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

๑๔. **การเข้าถึง** หมายถึง การอนุญาต หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงระบบสารสนเทศและระบบเครือข่าย

๑๕. **การควบคุมการใช้งาน** หมายถึง การกำหนดสิทธิ์ในการเข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย

๑๖. **การพิสูจน์ยืนยันตัวตน (authentication)** หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใจระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ โดยทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้งาน และรหัสผ่าน

๑๗. **ลงบันทึกการเข้า (login)** หมายถึง กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามเงื่อนไขที่ตั้งไว้เพื่อเข้าใช้ระบบคอมพิวเตอร์หรือระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้งาน และรหัสผ่านให้ถูกต้อง

๑๘. **ลงบันทึกการออก (logout)** หมายถึง กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่าย

๑๙. **การเข้ารหัส (encryption)** หมายถึง การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๐. **ผู้ดูแลระบบ (system administrator)** หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหารให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๒๑. **สื่อบันทึกข้อมูล** หมายถึง สื่อทั้งที่เป็นอิเล็กทรอนิกส์และไม่เป็นอิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, Flash Drive, Handy Drive, Thumb Drive, Hard Drive, Portable Hard Drive, โทรศัพท์มือถือ กล้องถ่ายรูปดิจิตอล กล้องวีดีโอ หรือเครื่องบันทึกเสียง เป็นต้น

๒๒. **จดหมายอิเล็กทรอนิกส์ อีเมล (electronic mail, e-mail)** หมายถึง ระบบรับส่งข้อมูลอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีสารสนเทศ ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพนิ่ง ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

๒๓. **อัพเดท (update)** หมายถึง ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่าง ๆ ของระบบสารสนเทศให้ทันสมัยอยู่เสมอ

๒๔. **ช่องโหว่ (vulnerability)** หมายถึง ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๕. VPN (Virtual Private Network) หมายถึง เครือข่ายส่วนตัวเสมือน โดยในการส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะ แล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๒๖. **อุปกรณ์กระจายสัญญาณ (Access Point)** หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

๒๗. SSID (Service Set Identifier) หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๒๘. WEP (Wire Equivalent Privacy) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

๒๙. WPA (Wi-Fi Protected Access) หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP

๓๐. MAC Address (Media Access Control Address) หมายถึง หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขที่จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

๓๑. **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๓๒. **เครือข่าย** หมายถึง โครงข่ายคอมพิวเตอร์ที่เชื่อมโยงคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ต่าง ๆ เข้าด้วยกัน ซึ่งทำให้การสื่อสารข้อมูลระหว่างคอมพิวเตอร์และอุปกรณ์คอมพิวเตอร์ทั้งที่อยู่ภายในและภายนอกองค์กรสามารถติดต่อสื่อสารและแลกเปลี่ยนข้อมูลกันได้ โครงข่ายนี้โดยพื้นฐานประกอบด้วยโครงข่ายสำหรับการติดต่อสื่อสารภายในองค์กร และโครงข่ายบนอินเทอร์เน็ต ซึ่งทำให้คอมพิวเตอร์ภายในองค์กรหนึ่งสามารถติดต่อสื่อสารกับคอมพิวเตอร์ขององค์กรหนึ่งได้

๓๓. **อินเทอร์เน็ต (Internet)** หมายถึง เครือข่ายของคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกันโดยอาศัยเครือข่ายโทรคมนาคมเป็นตัวเชื่อมโยง

๓๔. **แผนผังระบบเครือข่าย** หมายถึง แผนผังหรือแผนภาพที่แสดงรูปแบบการวางอุปกรณ์เครือข่ายในระบบเครือข่ายที่แสดงการเชื่อมโยง เพื่อให้เห็นเส้นทางการไหลเวียนของข้อมูลในเครือข่าย

๓๕. **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง เวลา วันที่ ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๓๖. **หมายเลขไอพีแอดเดรส (IP Address)** หมายถึง ตัวเลขประจำเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่ายที่เชื่อมต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)

๓๗. TSU iPass หมายถึง บัญชีผู้ใช้ที่มหาวิทยาลัยออกให้เพื่อใช้สำหรับการพิสูจน์ยืนยันตัวตนในการเข้าใช้งานเครือข่ายและระบบสารสนเทศต่าง ๆ ของมหาวิทยาลัย

๓๘. **เครือข่ายสังคมออนไลน์ (Social Network)** หมายถึง เว็บไซต์หรือแอพพลิเคชันที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ

๓๙. **ระบบสำรอง (Disaster Recovery Site : DR Site)** หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วย ฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

ความเป็นมา

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่าง ๆ มีความมั่นคงปลอดภัย เชื่อถือได้ มหาวิทยาลัยทักษิณ ได้กำหนดแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณเป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่าง ๆ และการปฏิบัติตามเจตนารมณ์ของพระราชกฤษฎีกาดังกล่าวได้อย่างถูกต้องและเหมาสม รวมถึงยังได้เตรียมความพร้อมตามกฎหมายและประกาศด้านเทคโนโลยีสารสนเทศอื่น ๆ ที่เกี่ยวข้อง และการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ด้วย

๒. วัตถุประสงค์

มหาวิทยาลัยทักษิณ ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มีวัตถุประสงค์ดังต่อไปนี้

๒.๑ เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยทักษิณ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒ เพื่อให้เกิดความเชื่อมั่นด้านความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยทักษิณ และทำให้ดำเนินงานต่าง ๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓ เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหาร เจ้าหน้าที่ทุกระดับ นิสิต และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร มีความรู้ความเข้าใจและตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔ เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. เป้าหมาย

เป้าหมายในการจัดทำแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย-ทักษิณ มีรายละเอียดดังต่อไปนี้

๓.๑ ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัย

๓.๒ เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

๓.๓ เผยแพร่ความรู้ความเข้าใจเพื่อสร้างความตระหนักให้บุคลากรและผู้เกี่ยวข้องทุกระดับ ทั้งของมหาวิทยาลัยเอง และหน่วยงานที่เกี่ยวข้อง

๓.๔ ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงที่เกิดขึ้น

๔. องค์ประกอบของนโยบาย

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมหาวิทยาลัยทักษิณจัดทำขึ้นเพื่อกำหนดแนวทางและวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ส่วนที่ ๑ นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๑. การบริหารจัดการการเข้าถึงข้อมูลสารสนเทศมหาวิทยาลัย (Information Access Management)
๒. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๓. การควบคุมการเข้าถึงระบบเครือข่าย และระบบอินเทอร์เน็ต (Network and Internet Access Control)
๔. การบริหารจัดการและการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
๕. การบริหารจัดการและการเข้าถึงของเครื่องคอมพิวเตอร์
๖. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์
๗. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (Application and Information Access Control)
๘. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)
๙. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)
๑๐. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)
๑๑. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองสารสนเทศ (Backup Policy)

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ (Investigate and Risk Assessment Policy)

ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

ส่วนที่ ๑
นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๒. เพื่อให้ผู้ใช้ ผู้ดูแลระบบ และผู้เกี่ยวข้องทุกฝ่ายได้รับรู้ เข้าใจขั้นตอนและปฏิบัติตามแนวทางบริหารจัดการบัญชี ผู้ใช้สารสนเทศของมหาวิทยาลัยและถือปฏิบัติโดยเคร่งครัด รวมทั้งสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใจงานระบบเทคโนโลยีสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

ผู้รับผิดชอบ

๑. สำนักคอมพิวเตอร์

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การบริหารจัดการการเข้าถึงข้อมูลสารสนเทศมหาวิทยาลัย (Information Access Management)

๑.๑ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย ดังนี้

๑.๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน เพื่อจำแนกกลุ่มทรัพยากรของระบบหรือการทำงาน โดยกำหนดกลุ่มผู้ใช้งานและสิทธิ์ของกลุ่มผู้ใช้งาน

๑.๑.๒ ห้ามผู้ไม่มีสิทธิ์เข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล หากไม่ได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบ

๑.๒ กำหนดสิทธิ์การเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย ดังนี้

๑.๒.๑ ไม่มีสิทธิ์

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 ๘ ประเภทหลักๆ ดังนี้

๑.๓.๑ ข้อมูลนิสิต

๑.๓.๒ ข้อมูลบุคลากร

๑.๓.๓ ข้อมูลการเงินและบัญชี
๑.๓.๔ ข้อมูลทางการศึกษา
๑.๓.๕ ข้อมูลทางการวิจัย และบริการวิชาการ
๑.๓.๖ ข้อมูลทางด้านศิลปวัฒนธรรม
๑.๓.๗ ข้อมูลทางการบริหาร
๑.๓.๘ ข้อมูลการจราจรทางคอมพิวเตอร์

๑.๔ การกำหนดชั้นความลับของข้อมูล

๑.๔.๑ ประเภทลับ หมายถึง ข้อมูลที่รู้เฉพาะผู้ที่เป็นเจ้าของหรือผู้ที่มีหน้าที่เกี่ยวข้องโดยตรง
๑.๔.๒ ประเภทใช้ภายในเท่านั้น หมายถึง ข้อมูลที่สื่อสารกันในกลุ่มย่อยหรือระหว่างคณะ/หน่วยงาน หรือข้อมูลที่เผยแพร่เฉพาะภายในมหาวิทยาลัย
๑.๔.๓ ประเภทส่วนบุคคล หมายถึง ข้อมูลที่ใช้เฉพาะตัวบุคคล เจ้าหน้าที่ หรือหน่วยงานที่ดูแลข้อมูลนั้น
๑.๔.๔ ประเภทเปิดเผยได้ หมายถึง ข้อมูลที่เปิดเผยได้ทั้งภายในและภายนอกมหาวิทยาลัย

๑.๕ การจัดแบ่งระดับชั้นการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัย

๑.๕.๑ ผู้บริหาร เข้าถึงได้ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในหน่วยงานนั้น
๑.๕.๒ ผู้ปฏิบัติงาน เข้าถึงได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย
๑.๕.๓ ผู้ดูแลระบบ มีสิทธิ์ในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่
๑.๕.๔ บุคลากร เข้าถึงได้เฉพาะข้อมูลส่วนบุคคลของตนเองและเข้าถึงข้อมูลตามที่ได้รับมอบหมายตามอำนาจหน้าที่
๑.๕.๕ ผู้ใช้ทั่วไป เข้าถึงได้เฉพาะข้อมูลที่ได้รับอนุญาตให้เข้าถึงได้ และสามารถดู เขียน แก้ไข และลบข้อมูลเฉพาะที่ตนเองสร้างขึ้นเท่านั้น
๑.๕.๖ การกำหนดสิทธิ์พิเศษ สามารถดำเนินการได้เมื่อได้รับอนุมัติจากผู้มีอำนาจหรือเจ้าของข้อมูลเท่านั้น
๑.๕.๗ การมอบอำนาจในการเข้าถึงสามารถดำเนินการได้เมื่อได้รับความยินยอมจากเจ้าของสิทธิ์หรือหน่วยงานหลักเท่านั้น

๑.๖ กำหนดให้มีหน่วยงานหลักหรือหน่วยงานเจ้าภาพในการอนุญาตการเข้าถึงข้อมูลและสารสนเทศของมหาวิทยาลัยในแต่ละประเภท ดังนี้

๑.๖.๑ ข้อมูลนิสิต หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลนิสิต
๑.๖.๒ ข้อมูลบุคลากร หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลบุคลากร
๑.๖.๓ ข้อมูลการเงินและบัญชี หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลการเงินและบัญชี
๑.๖.๔ ข้อมูลทางการศึกษา หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลทางการศึกษา

๑.๖.๕ ข้อมูลทางการวิจัย และบริการวิชาการ หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลทางการวิจัย และบริการวิชาการ

๑.๖.๖ ข้อมูลทางด้านศิลปวัฒนธรรม หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลทางด้านศิลปวัฒนธรรม

๑.๖.๗ ข้อมูลทางการบริหาร หน่วยงานหลักคือ หน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักดูแลข้อมูลทางการบริหาร

๑.๖.๘ ข้อมูลการจราจรทางคอมพิวเตอร์ หน่วยงานหลักคือ สำนักคอมพิวเตอร์และหน่วยงานที่ให้บริการระบบสารสนเทศ

๑.๖.๙ การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจของมหาวิทยาลัยทักษิณ

๑.๗ การควบคุมการเปลี่ยนแปลง

๑.๗.๑ การเปลี่ยนแปลงใด ๆ ที่อาจส่งผลกระทบต่อข้อมูลและสารสนเทศที่ใช้งานอยู่ให้ดำเนินการดังนี้

(๑) พิจารณาวางแผนดำเนินการเปลี่ยนแปลง รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ในการเปลี่ยนแปลง กรณีที่ผลกระทบจากการเปลี่ยนแปลงอาจส่งผลต่อข้อมูลและสารสนเทศที่อยู่ในระดับชั้นที่มีความสำคัญสูง แผนการดำเนินการเปลี่ยนแปลงจะต้องได้รับความเห็นชอบจากหน่วยงานที่มหาวิทยาลัยมอบหมายเป็นหน่วยงานหลักให้ดูแลข้อมูลและสารสนเทศ

(๒) แจ้งให้ผู้ที่เกี่ยวข้องได้รับทราบเกี่ยวกับการเปลี่ยนแปลงนั้น ๆ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการเตรียมความพร้อมก่อนที่จะดำเนินการเปลี่ยนแปลง

(๓) ต้องตรวจสอบความสมบูรณ์ของข้อมูลและสารสนเทศภายหลังจากที่มีการเปลี่ยนแปลง

๑.๗.๒ ต้องจัดเก็บซอร์สโค้ตและไลบรารี่ของระบบสารสนเทศ ทั้งเวอร์ชั่นปัจจุบันและเวอร์ชั่นเก่าไว้ในสถานที่ที่มีความมั่นคงปลอดภัย เพื่อให้สามารถนำกลับมาใช้ได้เมื่อจำเป็น

๑.๘ การกำหนดการใช้งานตามภารกิจ

๑.๘.๑ การควบคุมการเข้าถึงระบบสารสนเทศ

(๑) นิสิต จะให้สิทธิ์ทันทีที่มีสภาพเป็นนิสิตและหมดสิทธิ์เมื่อพ้นสภาพนิสิตไปแล้ว ๙๐ วัน

(๒) บุคลากร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นบุคลากร

(๓) ผู้บริหาร จะให้สิทธิ์เข้าถึงตามภาระหน้าที่ที่ได้รับมอบหมายและหมดสิทธิ์เมื่อพ้นสภาพการเป็นผู้บริหาร

(๔) ผู้เกษียณอายุ ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

(๕) ศิษย์เก่า ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

(๖) บุคคลภายนอก ได้รับอนุญาตเฉพาะระบบและช่วงเวลาที่กำหนด

๑.๘.๒ ข้อจำกัดในการเข้าถึง

(๑) นิสิต เข้าถึงได้เฉพาะระบบที่ได้รับอนุญาต

(๒) บุคลากร เข้าถึงได้ตามสิทธิ์เบื้องต้นและภารกิจที่ได้รับมอบหมาย

(๓) ผู้บริหาร เข้าถึงตามสิทธิ์และภารกิจที่ได้รับมอบหมาย

(๔) ผู้เกษียณอายุ เข้าถึงได้ตามที่ได้รับอนุญาต

(๕) ศิษย์เก่า เข้าถึงได้ตามที่ได้รับอนุญาต

(๖) บุคคลทั่วไป เข้าถึงได้ตามที่ได้รับอนุญาต

๑.๙ ระยะเวลาการใช้งาน

๑.๙.๑ ระยะเวลาการเข้าถึงและการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศของผู้ใช้ จะเข้าถึงและใช้งานได้ดังนี้

(๑) การเข้าถึงในเวลาราชการ ๐๘.๐๐-๑๗.๐๐ น.

(๒) การเข้าถึงนอกเวลาราชการ หลัง ๑๗.๐๐ น. เป็นต้นไป

(๓) การเข้าถึงในช่วงวันหยุดราชการและวันหยุดนขัตฤกษ์

๑.๙.๒ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ

(๑) กำหนดให้ระบบสารสนเทศที่มีความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญต้องตัดและหมดเวลาการใช้งานที่สั้นขึ้นเพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

(๒) ต้องจำกัดช่วงระยะเวลาการเชื่อมต่อสำหรับระบบสารสนเทศความเสี่ยงสูงหรือระบบที่มีข้อมูลสำคัญ

๑.๑๐ การหมดสิทธิ์การเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๐.๑ บัญชีผู้ใช้หมดอายุ

๑.๑๐.๒ เมื่อมีการเปลี่ยนแปลงสิทธิ์การเข้าถึง

๑.๑๐.๓ ถูกระงับสิทธิ์

๑.๑๑ การทบทวนและตรวจสอบการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศ

๑.๑๑.๑ ทบทวนและตรวจสอบสิทธิ์การเข้าถึงและใช้งานระบบสารสนเทศปีละ ๑ ครั้ง

๑.๑๑.๒ หน่วยงานที่เป็นเจ้าของระบบสารสนเทศต้องตรวจสอบคุณสมบัติและสิทธิ์ของผู้ใช้อย่างสม่ำเสมอ หากมีการเปลี่ยนแปลงจะต้องดำเนินการเปลี่ยนแปลง สิทธิ์ให้สอดคล้องกับระดับชั้นการเข้าถึงและการใช้งานระบบทันที

๑.๑๒ ช่องทางการเข้าถึง

๑.๑๒.๑ เครือข่ายภายในมหาวิทยาลัย

๑.๑๒.๒ เครือข่ายภายนอกมหาวิทยาลัย

๑.๑๒.๓ เข้าถึงโดยผ่านระบบที่จัดไว้ให้

๑.๑๓ การสร้างความรู้ความเข้าใจให้แก่ผู้ใช้งาน

๑.๑๓.๑ ต้องจัดทำหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๑๓.๒ อบรมผู้ใช้ เพื่อให้สามารถใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศได้อย่างถูกต้อง รวมถึงให้ตระหนักและเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศโดยไม่ระมัดระวัง

๑.๑๓.๓ ประชาสัมพันธ์ผ่านช่องทางต่าง ๆ เพื่อให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

๑.๑๔ การแบ่งกลุ่มบัญชีผู้ใช้

บัญชีผู้ใช้ระบบสารสนเทศของมหาวิทยาลัยจัดทำขึ้นเพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศ และระบบสารสนเทศของมหาวิทยาลัย ต้องระบุชื่อบัญชีผู้ใช้แยกเป็นรายบุคคลที่ไม่ซ้ำซ้อนกัน โดยแบ่งกลุ่มผู้ใช้ออกเป็น ๔ กลุ่ม คือ

๑.๑๔.๑ นิสิตของมหาวิทยาลัย

๑.๑๔.๒ บุคลากรของมหาวิทยาลัย อาจารย์พิเศษ ลูกจ้างจ้างเหมา และแขกของหน่วยงาน

๑.๑๔.๓ ลูกค้า

๑.๑๔.๔ บุคคลอื่นๆ ที่มหาวิทยาลัยมอบสิทธิ์ให้

๑.๑๕ การลงทะเบียนผู้ใช้

๑.๑๕.๑ นิสิตของมหาวิทยาลัย ได้รับบัญชีผู้ใช้โดยอัตโนมัติทันทีที่งานทะเบียนนิสิตและบริการการศึกษา ป้อนข้อมูลนิสิตเข้าสู่ระบบสารสนเทศ

๑.๑๕.๒ บุคลากรของมหาวิทยาลัย ที่ฝ่ายบริหารกลางและทรัพยากรบุคคลบันทึกประวัติลงในฐานข้อมูลบุคลากร สามารถได้รับบัญชีผู้ใช้โดยการลงทะเบียนผ่านระบบ ipass.tsu.ac.th

๑.๑๕.๓ อาจารย์พิเศษ ลูกจ้างจ้างเหมาของหน่วยงาน แขกของหน่วยงาน และบุคคลอื่นๆ ที่มหาวิทยาลัยมอบสิทธิ์ให้ ต้องการบัญชีผู้ใช้เพื่อบริหารจัดการในการให้บริการ ดำเนินการดังนี้

(๑) ดาวน์โหลดแบบฟอร์มได้จาก ipass.tsu.ac.th หัวข้อแบบฟอร์มขอบัญชีผู้ใช้กรอกข้อมูลให้ครบถ้วนส่งสำนักคอมพิวเตอร์

(๒) สำนักคอมพิวเตอร์จะออกบัญชีผู้ใช้ให้ตามคำร้องขอใช้บริการที่ผ่านการพิจารณาจากหน่วยงานผู้รับผิดชอบ และส่งกลับไปยังหน่วยงานเป็นเอกสารปกปิด

(๓) หน่วยงานและผู้ใช้ที่ร้องของบัญชีผู้ใช้ จะต้องรับผิดชอบความเสียหายใดๆ ที่จะเกิดจากการใช้งานบัญชีผู้ใช้ที่สำนักคอมพิวเตอร์ออกให้

(๔) หากต้องการเปลี่ยนแปลงผู้รับผิดชอบบัญชีผู้ใช้ ให้แจ้งสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษร ลงนามโดยผู้บริหารของหน่วยงาน ระบุผู้รับผิดชอบเดิม และชื่อผู้รับผิดชอบใหม่ พร้อมบัญชีผู้ใช้และหมายเลขโทรศัพท์ที่ติดต่อได้ของผู้รับผิดชอบใหม่

(๕) หากต้องการยกเลิกบัญชีผู้ใช้ ให้แจ้งสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษรลงนาม โดยผู้บริหารของหน่วยงาน ระบุชื่อผู้รับผิดชอบ และจำนวนบัญชีผู้ใช้ที่ต้องการยกเลิก

๑.๑๖ การจัดการสิทธิ์ของผู้ใช้งาน

๑.๑๖.๑ เมื่อเจ้าหน้าที่ของหน่วยงานลาออกหรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

๑.๑๖.๒ การแจ้งขอใช้สิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลและสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร ระบุเหตุผล และความจำเป็น

(๑) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของหน่วยงานหลัก

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) หน่วยงานหลักสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๑.๑๖.๓ ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๑.๑๖.๔ กรณีมีความจำเป็นต้องใช้สิทธิ์พิเศษกับผู้ใช้ ต้องพิจารณาการควบคุมผู้ใช้ที่มีสิทธิ์พิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา โดยต้องได้รับความเห็นชอบและอนุมัติจากอธิการบดีหรือผู้ที่ได้รับมอบอำนาจจากอธิการบดี

(๑) ควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้ต้องควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๒) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๓) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัดตามเงื่อนไขที่กำหนด

๑.๑๗ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

๑.๑๗.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนการปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

๑.๑๗.๒ ผู้ดูแลระบบต้องกำหนดรหัสผ่านชั่วคราว โดยกำหนดรหัสผ่านให้มีความยากต่อการเดาโดยผู้อื่นและกำหนดรหัสผ่านที่แตกต่างกัน

๑.๑๗.๓ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีหลังจากที่ได้รับรหัสผ่านชั่วคราว และต้องเปลี่ยนรหัสผ่านที่มีความยากต่อการคาดเดา

๑.๑๗.๔ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านเป็นระยะหรือทุกครั้งที่มีการแจ้งเตือนหรือบังคับให้เปลี่ยนรหัสผ่านจากผู้ดูแลระบบ

๑.๑๗.๕ ผู้ใช้งานต้องลงบันทึกการออกจากระบบทันที เมื่อเลิกใช้งานระบบหรือไม่อยู่หน้าจอ เป็นเวลานาน

๑.๑๗.๖ กรณีผู้ดูแลระบบตรวจพบว่ารหัสผ่านของผู้ใช้งานไม่มีความปลอดภัย หรือตรวจสอบได้ว่าถูกนำไปใช้โดยผู้อื่น ผู้ใช้รายงานนั้นจะถูกตัดสิทธิ์การใช้งานชั่วคราวจนกว่าจะดำเนินการเปลี่ยนรหัสผ่านเป็นที่เรียบร้อย

๑.๑๘ การทบทวนสิทธิ์การเข้าถึง

๑.๑๘.๑ ต้องมีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง และทบทวนทุกครั้งที่มีการโอนย้ายหรือปรับเปลี่ยนหน้าที่ความรับผิดชอบของบุคลากร

๑.๑๘.๒ บัญชีผู้ใช้จะหมดอายุ ดังนี้

(๑) กรณีบุคลากรหมดอายุเมื่อพ้นสภาพการเป็นบุคลากรของมหาวิทยาลัย ยกเว้นผู้เกษียณอายุราชการซึ่งสามารถใช้ชื่อบัญชีและรหัสผ่านสำหรับระบบที่ได้รับอนุญาตเท่านั้น

(๒) กรณีนิสิตพ้นสภาพเนื่องจากสำเร็จการศึกษาถือว่าเป็นศิษย์เก่าโดยอัตโนมัติ สามารถลงทะเบียนเพื่อยืนยันข้อมูลการเป็นศิษย์เก่าในระบบฐานข้อมูลศิษย์เก่า และกรณีอื่นๆ เช่น พ้นสภาพ ถูกไล่ออก ไม่ถือเป็นศิษย์เก่า

(๓) กรณีที่ไม่ใช่บุคลากรของมหาวิทยาลัย มีอายุการใช้งานตามช่วงเวลาที่กำหนด

๒. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๒.๑ การใช้งานบัญชีผู้ใช้และรหัสผ่าน

๒.๑.๑ ผู้ใช้ต้องทำการป้องกัน ดูแล รักษาข้อมูลบัญชีผู้ใช้และรหัสผ่าน โดยผู้ใช้แต่ละคนต้องมีบัญชีชื่อผู้ใช้ของตนเอง และห้ามทำการเผยแพร่แจกจ่ายหรือทำให้ผู้อื่นล่วงรู้รหัสผ่าน

๒.๑.๒ ผู้ใช้ต้องเปลี่ยนรหัสผ่านทันทีเมื่อสงสัยว่ารหัสผ่านอาจถูกเปิดเผยหรือล่วงรู้

๒.๒ การป้องกันอุปกรณ์ขณะไม่มีผู้ใช้งาน

๒.๒.๑ ผู้ดูแลระบบต้องสร้างความตระหนักเพื่อให้ผู้ใช้งานเข้าใจมาตรการป้องกันที่กำหนดไว้

๒.๒.๒ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่านเพื่อเข้าใช้งาน

๒.๒.๓ ผู้ใช้งานต้องล็อคอุปกรณ์คอมพิวเตอร์ เครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเมื่อไม่ได้ใช้งานหรือต้องปล่อยทิ้งโดยไม่ได้ดูแล

๒.๒.๔ ผู้ใช้งานต้องออกจากระบบเทคโนโลยีสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๒.๒.๕ ผู้ใช้งานอุปกรณ์ไอทีส่วนบุคคล เช่น โทรศัพท์มือถือ เครื่องคอมพิวเตอร์พกพา ต้องเปิดใช้ระบบป้องกันการเข้าถึงของอุปกรณ์ไอทีนั้น เพื่อป้องกันการใช้งานโดยบุคคลอื่น

๒.๓ การจัดวางและการป้องกันอุปกรณ์

๒.๓.๑ จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการสูญหายหรือใช้งานโดยไม่ได้รับอนุญาต

๒.๓.๒ อุปกรณ์ที่มีความสำคัญให้แยกเก็บไว้ในพื้นที่ที่มีความมั่นคงปลอดภัย

๒.๓.๓ ต้องตรวจสอบ สอดส่อง และดูแลสภาพแวดล้อมภายในบริเวณหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายใน เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว เช่น การตรวจสอบระดับอุณหภูมิ ความชื้น ว่าอยู่ในระดับปกติหรือไม่

๒.๓.๔ ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสมเพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก โดยการหันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ซึ่งไม่มีสิทธิ์สามารถมองเห็นหน้าจอนั้นได้

๒.๔ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

๒.๔.๑ จัดเก็บเอกสาร ข้อมูล สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศไว้ในสถานที่มั่นคงปลอดภัย

๒.๔.๒ ต้องควบคุมการเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ โดยเป็นเจ้าของหรือผู้ได้รับมอบหมายเป็นลายลักษณ์อักษรเท่านั้น

๒.๔.๓ มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญได้

๒.๔.๔ สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมเพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒.๔.๕ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ

๒.๔.๖ จัดทำแนวทางสำหรับจัดเก็บ การทำลาย และระยะเวลาการจัดเก็บสำหรับข้อมูลหรือเอกสารตอบโต้ และแนวทางต้องสอดคล้องกับกฎหมาย ระเบียบข้อบังคับหรือข้อกำหนดอื่นๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

๒.๔.๗ โปรแกรมต่างๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย เป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

๒.๔.๘ ไม่เก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๒.๔.๙ ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูล ก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

๒.๔.๑๐ ต้องลบหรือฟอร์แมต (Format) ข้อมูลที่บันทึกอยู่ในอุปกรณ์ที่ใช้ในการบันทึกข้อมูลก่อนทำลายหรือเปลี่ยนทดแทนหรือจำหน่ายอุปกรณ์

๒.๔.๑๑ ต้องสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

๒.๕ การป้องกันโปรแกรมประสงค์ร้าย

๒.๕.๑ ผู้ใช้ต้องติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดโปรแกรมประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๕.๒ ต้องทำการปรับปรุงระบบปฏิบัติการ เว็บเบราว์เซอร์ และโปรแกรมต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

๒.๕.๓ ในการรับส่งข้อมูลคอมพิวเตอร์หรือสารสนเทศ ผ่านทางระบบเครือข่าย และผ่านทางสื่อบันทึกข้อมูลทุกชนิด ผู้ใช้ต้องทำการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้ายก่อนการรับส่งทุกครั้ง

๒.๕.๔ ผู้ใช้ต้องตรวจสอบไฟล์ โดยใช้โปรแกรมป้องกันโปรแกรมประสงค์ร้าย ก่อนการเปิดใช้ไฟล์ที่สามารถประมวลผลได้ (Executable file) เช่น ไฟล์ที่มีนามสกุล exe, .com, .bat, .vbs, .scr, .pif, .hat, .doc, .docx, .xls, .xlsx เป็นต้น

๓. การควบคุมการเข้าถึงระบบเครือข่าย และระบบอินเทอร์เน็ต (Network and Internet Access Control)

๓.๑ การเข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย

๓.๑.๑ การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจะต้องพิสูจน์ตัวตนผู้ใช้ด้วยบัญชีผู้ใช้ที่มหาวิทยาลัยออกให้

๓.๑.๒ ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๓.๑.๓ การเข้าถึงระบบเครือข่ายของมหาวิทยาลัยจากภายนอกต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และต้องกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นเป็นพิเศษจากมาตรฐานการเข้าถึงระบบเครือข่ายของมหาวิทยาลัย

๓.๑.๔ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องที่ต้องการให้เข้าถึงได้จากอินเทอร์เน็ตจะต้องลงทะเบียนกับสำนักคอมพิวเตอร์

๓.๑.๕ จำกัดการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน รวมทั้งตรวจสอบเปิดปิดพอร์ตอุปกรณ์เครือข่ายตามความจำเป็น

๓.๑.๖ การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่าย ต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๑.๗ การเข้าถึงเครือข่ายของบุคคลที่ไม่มีบัญชีผู้ใช้ของมหาวิทยาลัย ต้องขออนุญาตใช้บัญชีชั่วคราวจากมหาวิทยาลัย ซึ่งจะเข้าถึงได้ตามสิทธิ์ที่ได้รับอนุญาตและจะต้องพิสูจน์ตัวตนด้วยบัญชีชั่วคราวนั้น

๓.๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๓.๒.๑ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในมหาวิทยาลัยจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์หรือผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

๓.๒.๒ ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๒) ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (access point) ทุกตัวที่นำมาใช้ในระบบเครือข่ายไร้สาย

(๓) ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณเพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งาน และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ต้องทำการเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่าปริยายมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) ต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖) ต้องเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณด้วยวิธีที่มีความประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูล และทำให้ปลอดภัยมากขึ้น

(๗) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

(๘) ต้องใช้ซอฟแวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยทันทีการ

๓.๓ การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

๓.๓.๑ อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

๓.๓.๒ เก็บข้อมูลการใช้ MAC Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L3

๓.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ

๓.๔.๑ ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

๓.๔.๒ ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับแต่งอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

๓.๔.๓ ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกมหาวิทยาลัย แต่ให้เชื่อมต่อ ผ่านช่องทางที่ปลอดภัยที่มหาวิทยาลัยกำหนด เช่น VPN เป็นต้น

๓.๔.๔ อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

๓.๔.๕ ต้องปิดพอร์ตหรือปิดบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๓.๔.๖ ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๓.๕ การแบ่งแยกเครือข่าย (Segregation in Networks)

๓.๕.๑ ต้องจัดทำแผนผังระบบเครือข่าย ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๓.๕.๒ แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้ และระบบงานต่าง ๆ ของมหาวิทยาลัย

๓.๕.๓ ต้องใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

๓.๕.๔ ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายทั้งจากภายในและภายนอกหน่วยงานซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๓.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

๓.๖.๑ อนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๓.๖.๒ อนุญาตการเชื่อมต่อสาย UTP (Unshielded Twisted Pair) ที่มีการต่อหัวสายตามมาตรฐาน EIA/TIA 568B เท่านั้น และมีการทดสอบค่าต่าง เช่น ค่าอัตราการลดทอนสัญญาณ ค่า Near End Crosstalk และค่า ARC

๓.๖.๓ ระบบเครือข่ายที่เชื่อมต่อไปยังเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัย ต้องติดตั้งระบบตรวจจับการบุกรุก และต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย

๓.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

๓.๗.๑ อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

๓.๗.๒ มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย

๓.๗.๓ ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๓.๗.๔ ต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

๓.๗.๕ ต้องกำหนดเส้นทางการไหลของข้อมูลบนเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้งานบริการเครือข่าย

๓.๗.๖ ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

๓.๘ การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External connections)

๓.๘.๑ ผู้ใช้งานจะเข้าใช้งานระบบต้องแสดงตัวตนด้วยชื่อผู้ใช้งานทุกครั้ง

๓.๘.๒ ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน ต้องเป็นผู้ที่ได้รับสิทธิ์ในการเข้าใช้บริการแล้วเท่านั้น

๓.๘.๓ ต้องมีระบบตรวจสอบลงบันทึกผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยจะต้องมีวิธีการยืนยันตัวตนด้วยการป้อนชื่อผู้ใช้งานและรหัสผ่านเพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๓.๙ การใช้งานอินเทอร์เน็ต (use of the Internet)

๓.๙.๑ ผู้ใช้ต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้ตามสิทธิ์ที่ได้รับ

๓.๙.๒ ห้ามใช้อินเทอร์เน็ตมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล

๓.๙.๓ ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย เป็นต้น

๓.๙.๔ ผู้ใช้ต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๓.๙.๕ ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๔. การบริหารจัดการและการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๔.๑ กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๔.๒ มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๔.๓ ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (time.tsu.ac.th หรือ time.pt.tsu.ac.th) ที่มหาวิทยาลัยใช้อ้างอิง

๔.๔ เปิดให้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัยด้วย

๔.๕ ต้องปรับปรุงระบบซอฟแวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่าง ๆ

๔.๖ ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๔.๗ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

๔.๘ หัวหน้าหน่วยงานที่เป็นเจ้าของเครื่องแม่ข่าย ต้องแต่งตั้งผู้มีสิทธิ์ และกำหนดจำนวนผู้มีสิทธิ์ในการเข้าถึงระบบปฏิบัติการ

๔.๙ ผู้ใช้ต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๔.๑๐ ต้องไม่แสดงรายละเอียดสำคัญของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๔.๑๑ ผู้ดูแลระบบต้องยุติการให้บริการทันที ในกรณีตรวจพบว่ามีการใช้งานที่ผิดปกติ หรือไม่ปลอดภัย

๔.๑๒ ห้ามการติดตั้งของซอฟต์แวร์อื่นๆ หรือซอฟแวร์ที่ได้มาจากแหล่งภายนอก รวมทั้งการใช้ไฟล์อื่นที่มหาวิทยาลัยไม่อนุญาต

๔.๑๓ ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องตรวจสอบซอฟต์แวร์หรือข้อมูลในระบบงาน สำคัญอย่างสม่ำเสมอ เพื่อป้องกันการติดตั้งซอฟต์แวร์หรือข้อมูลในระบบงานนั้นโดยไม่ได้รับอนุญาต

๔.๑๔ ติดตั้งซอฟต์แวร์เพื่อป้องกันโปรแกรมประสงค์ร้ายบนเครื่องแม่ข่ายทุกเครื่อง

๔.๑๕ กำหนดหน้าที่ความรับผิดชอบและขั้นตอนปฏิบัติ สำหรับการจัดการกับโปรแกรมประสงค์ร้าย ได้แก่ การรายงานการเกิดขึ้นของโปรแกรมประสงค์ร้าย การวิเคราะห์ การจัดการ การกู้คืน ระบบจากความเสียหายที่พบ เป็นต้น

๔.๑๖ ต้องติดตามข้อมูลข่าวสารเกี่ยวกับโปรแกรมประสงค์ร้ายอย่างสม่ำเสมอ

๔.๑๗ ต้องสร้างความตระหนักเกี่ยวกับโปรแกรมประสงค์ร้าย เพื่อให้ผู้ดูแลระบบและผู้ใช้มีความรู้ความเข้าใจ และสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมประสงค์ร้ายว่าต้องดำเนินการอย่างไร

๕. การบริหารจัดการและการเข้าถึงของเครื่องคอมพิวเตอร์

๕.๑ ผู้ดูแลระบบเครื่องคอมพิวเตอร์ (System Administrator)

๕.๑.๑ ต้องกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๕.๒ การเข้าถึงเครื่องคอมพิวเตอร์ที่หน่วยงานจัดไว้ใช้งาน

๕.๒.๑ ผู้ใช้งานต้องยืนยันตัวตนในการเข้าใช้ระบบปฏิบัติการด้วยบัญชีผู้ใช้และรหัสผ่านของตัวเอง

๕.๒.๒ ระบบต้องไม่แสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๕.๒.๓ ระบบจะต้องจำกัดสิทธิ์ผู้ใช้ในการติดตั้ง เปลี่ยนแปลง หรือลบโปรแกรมหรือข้อมูลบนเครื่อง

๕.๓ ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

๕.๓.๑ ผู้ใช้ ต้องมีชื่อผู้ใช้และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศของมหาวิทยาลัย

๕.๓.๒ สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม โดยใช้สมาร์ทการ์ด RFID หรือเครื่องอ่านลายพิมพ์นิ้วมือ หรือวิธีการอื่นที่มีความปลอดภัย

๕.๔ การบริหารจัดการรหัสผ่าน (Password Management System)

๕.๔.๑ ไม่แสดงข้อมูลรหัสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

๕.๔.๒ เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๕.๕ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

๕.๕.๑ จำกัดสิทธิ์การเข้าถึง และกำหนดสิทธิ์อย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๕.๕.๒ จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๕.๕.๓ ต้องถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๕.๔ โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

๕.๕.๕ ห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๕.๖ การหมดเวลาและจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Session time-Out and Limitation of Connection)

๕.๖.๑ ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็น เวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบ เมื่อว่างเว้นจากการใช้งานให้สั้นลง หรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๕.๖.๒ กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง เป็นต้น และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานตามปกติของมหาวิทยาลัยเท่านั้น

๕.๖.๓ การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๕.๖.๔ กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือ ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

๖. การใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์

๖.๑ บุคลากรและนิสิต จะได้สิทธิ์การใช้บัญชีจดหมายอิเล็กทรอนิกส์ ตามที่มหาวิทยาลัยกำหนดตั้งแต่เริ่มมีสถานะเป็นบุคลากรหรือนิสิต

๖.๒ ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ

๖.๓ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ห้ามระบุสาระสำคัญของข้อมูลลงบนหัวข้อจดหมายอิเล็กทรอนิกส์

๖.๔ ผู้ใช้มีหน้าที่รักษาชื่อผู้ใช้งานและรหัสผ่านเป็นความลับไม่ให้รั่วไหล เพื่อป้องกันการใช้งานโดยผู้ไม่ประสงค์ดี

๖.๕ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ต้องออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์ของตน

๖.๖ เพื่อป้องกันความเสียหายที่จะเกิดกับระบบของมหาวิทยาลัย ระบบจดหมายอิเล็กทรอนิกส์จะต้องควบคุมจำนวนจดหมายที่ผู้ใช้สามารถส่งได้ ไม่ให้เกินจำนวนที่กำหนดภายในระยะเวลาหนึ่งหากมีความพยายามที่จะส่งจดหมายจำนวนมาก ระบบจะปิดกั้นการส่งโดยอัตโนมัติ

๖.๗ ก่อนส่งต่อ เปิดไฟล์หรือคลิกลิ้งค์ที่แนบมา ต้องตรวจสอบให้แน่ใจก่อนว่าไม่ใช่จดหมายหลอกลวง

๖.๘ มีระบบอัตโนมัติสำหรับตรวจสอบรูปแบบอีเมลผิดปกติทั้งขาเข้าและขาออก

๗. การเข้าถึงโปรแกรมประยุกต์และระบบสารสนเทศ (application and information access control)

๗.๑ การจำกัดการเข้าถึงสารสนเทศ

๗.๑.๑ การจำกัดการเข้าถึงของผู้ใช้งาน

(๑) เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

(๓) ต้องออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

๗.๑.๒ แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศของมหาวิทยาลัย ออกเป็น ๓ กลุ่ม คือ ผู้ดูแลระบบ ผู้พัฒนาระบบงาน และผู้ใช้ระบบ โดยกำหนดหน้าที่รับผิดชอบอย่างชัดเจน เป็นลายลักษณ์อักษร

๗.๑.๓ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งานและการเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

(๑) ชื่อบัญชีผู้ใช้

(๒) วันเวลาที่เข้าถึงระบบ

(๓) วันเวลาที่ออกจากระบบ

(๔) เหตุการณ์สำคัญที่เกิดขึ้น

(๕) บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

(๖) แสดงการใช้สิทธิ์ เช่น สิทธิ์ของผู้ดูแลระบบ

(๗) หมายเลขไอพีแอดเดรสที่เข้าถึง

(๘) แสดงการหยุดทำงานของระบบป้องกันการบุกรุก

๗.๑.๔ การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML, Encryption เป็นต้น

๗.๒ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๒.๑ แนวปฏิบัติสำหรับการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของทางราชการ

(๑) ต้องล็อคหรือยึดเครื่องให้อยู่กับที่กรณีที่นำเครื่องไปใช้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๒) ต้องเปิดใช้ระบบล็อคหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งานและในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อคหน้าจอทุกครั้ง

(๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(๔) ไม่ใช้อุปกรณ์คอมพิวเตอร์แบบพกพาร่วมกับบุคคลอื่น

(๕) ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูลทุกครั้ง

(๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในมหาวิทยาลัย

(๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์คอมพิวเตอร์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

๗.๓.๒ การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้ต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลสำรอง (backup media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก เป็นต้น

(๒) ผู้ใช้มีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๘. การบริหารจัดการระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log Management)

๘.๑ กำหนดผู้รักษาข้อมูลจราจรคอมพิวเตอร์ประจำหน่วยงาน และมี Log Server ของหน่วยงานสำหรับรวบรวมข้อมูลจราจรคอมพิวเตอร์ที่พร้อมส่งมอบให้ผู้รักษาข้อมูลจราจรคอมพิวเตอร์ของมหาวิทยาลัยเมื่อมีการร้องขอ

๘.๒ กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของหน่วยงาน

๘.๓ บันทึกการทำงานของคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้และบันทึกรายละเอียดของระบบป้องกันการบุกรุก ได้แก่ บันทึกการเข้าออกระบบ ซึ่งประกอบด้วย บัญชีผู้ใช้ หมายเลขไอพีแอดเดรสต้นทาง หมายเลขไอพีแอดเดรสปลายทาง โปรโตคอล และหมายเลขพอร์ต เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้ตามที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

๘.๔ ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้อย่างสม่ำเสมอ

๘.๕ กำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลง หรือทำลาย ข้อมูลจราจรคอมพิวเตอร์ต่างๆ และจำกัดสิทธิ์การเข้าถึงข้อมูลจราจรคอมพิวเตอร์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๙. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)

๙.๑ ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

๙.๑.๑ ผู้ดูแลระบบเครือข่าย (Network Administrator)

๙.๑.๒ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (Server Administrator)

๙.๑.๓ ผู้ดูแลระบบสารสนเทศ (Application Administrator)

๙.๒ ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

๙.๒.๑ ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

๙.๒.๒ เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็น เพื่อให้สามารถระบุตัวตนผู้ใช้นับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัยดังต่อไปนี้

(๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนถูกต้องและความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงานหรือบุคคลที่หน่วยงานมอบหมาย

(๒) ข้อมูลจราจรคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้เป็นรายบุคคลได้

(๓) ข้อมูลจราจรคอมพิวเตอร์ต้องบันทึกอ้างอิงเวลากับ time.tsu.ac.th หรือ time.pt.tsu.ac.th

๙.๓ ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

๙.๓.๑ ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้ที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้ผู้นั้นให้ยุติการกระทำในทันที และในกรณีจำเป็น เพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้ทันที

๙.๓.๒ ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

๙.๓.๓ ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมประสงค์ร้ายต่าง ๆ ให้เหมาะสม

๙.๓.๔ ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๙.๓.๕ ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๙.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

๙.๔.๑ ดูแลรักษาและปรับปรุงบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๙.๔.๒ ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้อง และเป็นปัจจุบันอยู่เสมอ

๙.๕ หลักธรรมาภิบาลของผู้ดูแลระบบ

๙.๕.๑ ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้โดยไม่มีเหตุผลอันสมควร

๙.๕.๒ ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

๙.๕.๓ ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผย ให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๑๐. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๐.๑ การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของทางราชการเป็นสำคัญ

๑๐.๒ ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย

๑๐.๓ การใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้ต้องไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย

๑๐.๔ หากผู้ใช้งานพบว่า การใช้งานเครือข่ายสังคมออนไลน์ไม่เหมาะสมหรือมีผลกระทบกับมหาวิทยาลัยต้องแจ้งสำนักคอมพิวเตอร์โดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๑. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๑๑.๑ การจัดการบริเวณแวดล้อมทางกายภาพ

๑๑.๑.๑ กำหนดระดับความสำคัญของพื้นที่หรือการจำแนกพื้นที่ใช้งาน

๑๑.๑.๒ กำหนดระบบป้องกันการบุกรุกที่ติดตั้งให้ครอบคลุมพื้นที่หรือบริเวณที่มีความสำคัญ

๑๑.๑.๓ ดำเนินการทดสอบระบบป้องกันการบุกรุกทางกายภาพอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังใช้งานได้ตามปกติ

๑๑.๒ การควบคุมการเข้า-ออกพื้นที่ทางกายภาพ

๑๑.๒.๑ ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๑.๒.๒ ต้องควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

๑๑.๒.๓ มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงพื้นที่ดังกล่าว

๑๑.๒.๔ ต้องพิสูจน์ตัวตน เช่น การใช้สแกนนิ้วมือ การใช้รหัสผ่าน เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ เช่น ห้อง Data Center ห้อง Network Center

๑๑.๒.๕ ต้องบันทึกวันและเวลาเข้า-ออก ของผู้ที่มาเยือน และจัดเก็บบันทึกไว้เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

๑๑.๒.๖ มีบันทึกรายการอุปกรณ์ที่นำเข้า-ออก

๑๑.๒.๗ ต้องดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติการในพื้นที่หรือบริเวณที่มีความสำคัญ จนกระทั่งเสร็จสิ้นภารกิจ เพื่อป้องกันการสูญหายของทรัพย์สิน และป้องกันการเข้าถึงพื้นที่ส่วนอื่นที่ไม่ได้รับอนุญาต

๑๑.๒.๘ ต้องควบคุมบุคคลภายนอกในการนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานมาปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๑.๒.๙ สร้างความตระหนักให้ผู้ที่มาเยือนจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

๑๑.๒.๑๐ เจ้าหน้าที่ของบริษัทผู้ได้รับการว่าจ้าง/ผู้ที่มาเยือน ต้องติดบัตรให้เห็นชัดตลอดระยะเวลาการทำงาน

๑๑.๒.๑๑ ต้องทบทวน หรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างสม่ำเสมอ

๑๑.๓ การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก

๑๑.๓.๑ จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๑๑.๓.๒ จำกัดบุคคลซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

๑๑.๓.๓ จัดพื้นที่หรือบริเวณที่ส่งมอบไว้ในบริเวณต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่นๆ ภายในมหาวิทยาลัย

๑๑.๓.๔ ให้ตรวจสอบผลิตภัณฑ์ที่เป็นอันตรายก่อนที่จะโอนย้ายไปยังพื้นที่ใช้งาน

๑๑.๓.๕ ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

๑๑.๔ การสร้างความมั่นคงปลอดภัยสำหรับเอกสารระบบ

๑๑.๔.๑ จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

๑๑.๔.๒ ต้องควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศเฉพาะผู้เกี่ยวข้องเท่านั้น

๑๑.๔.๓ ควบคุมการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนเครือข่ายสาธารณะ เช่น อินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

๑๑.๕ การนำทรัพย์สินของมหาวิทยาลัยออกนอกสำนักงาน

๑๑.๕.๑ ต้องขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินออกนอกมหาวิทยาลัย

๑๑.๕.๒ บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกนอกสำนักงาน เพื่อใช้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๑.๕.๓ ต้องรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยเสมือนเป็นทรัพย์สินของตนเอง

๑๑.๖ ระบบและอุปกรณ์สนับสนุนการทำงาน

๑๑.๖.๑ เพื่อให้การทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยทำงานได้อย่างต่อเนื่อง มีเสถียรภาพ มีประสิทธิภาพ และใช้งานได้คุ้มค่า ต้องสร้างสภาพแวดล้อมและมีอุปกรณ์สนับสนุนการทำงานดังนี้

(๑) ระบบปรับอากาศและควบคุมความชื้น

(๒) ระบบสำรองกระแสไฟฟ้า (UPS)

(๓) เครื่องกำเนิดกระแสไฟฟ้า

(๔) ระบบป้องกันอัคคีภัย

๑๑.๖.๒ ต้องตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑๑.๖.๓ ติดตั้งระบบเสียงเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดทำงาน

๑๑.๖.๔ จัดทำแผนผังแสดงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ผู้เกี่ยวข้องรับทราบ

ส่วนที่ ๒
นโยบายการจัดทำระบบสำรองสารสนเทศ (Backup Policy)

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีสภาพพร้อมใช้และให้บริการได้อย่างต่อเนื่อง
๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสารสนเทศ การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลคอมพิวเตอร์แม่ข่าย และผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหา ต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. สำนักคอมพิวเตอร์
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของคณะ/หน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ระบบสำรอง (Disaster Recovery Site : DR Site)

๑.๑ จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรอง และทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง
๑.๒ ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุมดังนี้
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 สถานการณ์ทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๒.๕ ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

๒.๖ จัดเก็บอุปกรณ์สำรองไว้ในระบบสำรอง

๒.๗ ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๒.๘ มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

๒.๘.๑ ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

๒.๘.๒ ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

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 ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูล และแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ
(Investigate and Risk Assessment)

วัตถุประสงค์

เพื่อให้ผู้เกี่ยวข้องทุกฝ่ายได้รับทราบถึงหน้าที่ ความรับผิดชอบ และความจำเป็นในการประเมินความเสี่ยงสารสนเทศ เพื่อหาแนวทางป้องกันภัยคุกคามและการโจมตีต่างๆ ซึ่งจะให้ระบบสารสนเทศของมหาวิทยาลัยหรือของหน่วยงานมีความปลอดภัยและมีความพร้อมใช้งานอยู่เสมอ

ผู้รับผิดชอบ

๑. สำนักคอมพิวเตอร์
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. หน่วยตรวจสอบภายใน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. หน่วยงานต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศโดยผู้ตรวจสอบภายในอย่างน้อยปีละ ๑ ครั้ง
๒. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ดังต่อไปนี้
   ๒.๑ ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต
   ๒.๒ ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต
   ๒.๓ ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดจากการขัดข้องระหว่างการใช้งาน
   ๒.๔ ความเสี่ยงที่เกิดจากการลักลอบใช้บัญชีผู้ใช้ และรหัสผ่านของผู้อื่นโดยได้ไม่ได้รับอนุญาต
   ๒.๕ 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 และเพื่อป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้

ผู้รับผิดชอบ

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

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. ต้องกำหนดหลักสูตรการฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ โดยอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายกับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒. ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๓. จัดฝึกอบรมการใช้งานสารสนเทศของมหาวิทยาลัยอย่างสม่ำเสมอ หรือทุกครั้งที่มีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

๔. จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และเผยแพร่ทางเว็บไซต์ของหน่วยงาน

๕. ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย ซึ่งมีการเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

๖. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติ ด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้

ส่วนที่ ๕
แผนสำรองสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan)
มหาวิทยาลัยทักษิณ

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศซึ่งจัดเก็บไว้ที่ห้องศูนย์กลางข้อมูล (Data Center) ถือเป็นทรัพย์สินทางการบริหารสำคัญของมหาวิทยาลัยทักษิณ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนด้านบริหาร การจัดการเรียนการสอน การวิจัย และการให้บริการวิชาการ ดังนั้นเพื่อป้องกันปัจจัยจากภายนอกและปัจจัยจากภายในมากระทบ และทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งอุปกรณ์ต่าง ๆ เกิดความเสียหายได้ มหาวิทยาลัยทักษิณจึงได้จัดทำแผนป้องกันปัญหาระบบเทคโนโลยีสารสนเทศจากเหตุการณ์ฉุกเฉิน (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลระบบ ป้องกัน และแก้ไขปัญหาที่อาจกระทบต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณ

๒. วัตถุประสงค์

๒.๑ เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลระบบรักษาความปลอดภัย
ด้านเทคโนโลยีสารสนเทศ

๒.๒ เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณ ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔ เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณ

๓. เหตุภัยพิบัติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยทักษิณ ซึ่งสามารถจำแนกประเภทของภัยได้ดังนี้

๓.๑ ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องศูนย์กลางข้อมูล (Data Center) และห้องศูนย์ระบบเครือข่าย (Network Center) ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๓.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓.๓ ระบบสื่อสารของห้องศูนย์กลางข้อมูลที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๓.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๓.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

๓.๖ ไวรัสคอมพิวเตอร์

๓.๗ ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๓.๘ ระบบเทคโนโลยีสารสนเทศหลักหลักเสียหาย หรือข้อมูลถูกทำลาย

๔. แนวทางการป้องกันและแก้ไขความเสียหายจากภัยพิบัติ

๔.๑ ภัยธรรมชาติ

ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของห้องศูนย์กลางข้อมูล ได้แก่ อัคคีภัย อุทกภัย และการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๔.๑.๑ การป้องกันอัคคีภัย

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน

(๒) จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากรทุกคนอย่างน้อยปีละ ๑ ครั้ง

(๓) จัดทำระบบดับเพลิงอัตโนมัติสำหรับห้องศูนย์กลางข้อมูล

๔.๑.๒ การป้องกันอุทกภัย ความชื้น และอุณหภูมิที่ไม่เหมาะสม

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น และติดตั้งระบบอัตโนมัติตรวจสอบการทำงานตลอด ๒๔ ชั่วโมง

(๒) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๔.๒ การโจรกรรมอุปกรณ์ส่วนของการจัดเก็บและให้บริการข้อมูล

๔.๒.๑ ควบคุมการเข้าออกห้องศูนย์กลางข้อมูล โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป

๔.๒.๒ จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยลายนิ้วมือ (Finger Scan)

๔.๒.๓ มีเวรเฝ้าระวังและตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

๔.๒.๔ ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๓ ระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๔.๓.๑ ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา

๔.๓.๒ ต้องจัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้ในกรณีที่ระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

๔.๔ กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๔.๔.๑ มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๒๐ นาที

๔.๔.๒ เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาให้บริการ ตรวจสอบการทำงานของระบบทุกวัน และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในภาพพร้อมใช้งานอย่างน้อยเดือนละ ๑ ครั้ง

๔.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

๔.๕.๑ ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบตลอดเวลา

๔.๕.๒ จัดเวรเฝ้าระวังระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือมีความถี่ในการเรียกใช้งานผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกัน

๔.๕.๓ ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และปรับปรุงอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๔.๕.๔ กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต

๔.๕.๕ ป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรส (IP address) โดยการกรองแพ็คเกทที่มาจากภายนอก

๔.๖ ไวรัสคอมพิวเตอร์

๔.๖.๑ ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๔.๖.๒ ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่าง ๆ

๔.๖.๓ ใช้ความระมัดระวังในการเปิดอีเมล เช่น ไม่เปิดอีเมลที่ไม่ทราบแหล่งที่มา หรือลบอีเมลทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔.๖.๔ ระมัดระวังการดาวน์โหลดไฟล์ต่าง ๆ จากอินเทอร์เน็ต

๔.๗ ระบบเสียหายจากภัยสงครามหรือเหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากภัยดังกล่าวเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ สามารถป้องกันได้โดยการจัดทำศูนย์กลางข้อมูลสำรองนอกอาคารสำนักคอมพิวเตอร์ และมีระบบสำรองข้อมูลโดยแยกสถานที่จัดเก็บมากกว่า ๑ ที่ หากความเสียหายกับข้อมูลก็จะสามารถนำข้อมูลที่มีในศูนย์กลางข้อมูลสำรองหรือข้อมูลในระบบสำรองที่จัดเก็บไว้มาใช้แทนได้ทันที

๔.๘ ระบบบริการหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๔.๘.๑ สำรองข้อมูลอัตโนมัติโดยเครื่องคอมพิวเตอร์แม่ข่ายจะสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน โดยเครื่องจะบันทึกประวัติการทำงานไว้ทุกวัน และเครื่องดังกล่าวจะกระจายข้อมูลที่สำรองไว้ไปยังฮาร์ดิสก์ภายนอก (External Harddisk) และเครื่องคอมพิวเตอร์แม่ข่ายสำรองข้อมูลกลางที่สำนักคอมพิวเตอร์ วิทยาเขตพัทลุง

๔.๘.๒ ทดสอบกู้คืนข้อมูลและฐานข้อมูลที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๑ ครั้ง

๔.๘.๓ บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสียหายของข้อมูล

๔.๙ การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

๔.๙.๑ มีระบบยืนยันตัวตน เพื่อตรวจสอบสิทธิก่อนเข้าใช้อินเทอร์เน็ตหรือใช้งานระบบเครือข่ายตามอำนาจหน้าที่และความรับผิดชอบ

๔.๙.๒ กำหนดมาตรการควบคุมการเข้าออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

๔.๙.๓ หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในห้องศูนย์กลางข้อมูล จะต้องให้เจ้าหน้าที่ดูแลศูนย์กลางข้อมูลเป็นผู้รับผิดชอบนำเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกมีการติดตั้งระบบสแกนลายนิ้วมือ และติดตั้งกล้องวงจรปิดเพื่อป้องกันการโจรกรรม

๔.๙.๔ ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ต สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ได้โดยเปิดใช้งานตลอดเวลา

๔.๙.๕ มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กรเพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกันต่อไป

๕. การกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ต้องอยู่ในสภาพพร้อมให้บริการได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเกิดความเสียหายหรือหยุดทำงานต้องดำเนินการดังนี้

๕.๑ ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่น ๆ ที่เกี่ยวข้อง

๕.๒ จัดหาอุปกรณ์หรือชิ้นส่วนเพื่อทดแทน

๕.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

๕.๔ นำข้อมูลจากสื่อบันทึกข้อมูลสำรองหรือจากระบบสำรองข้อมูลกลับมาใช้งานโดยเร็วภายใน ๔๘ ชั่วโมง

๖. ผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน่วยงานต้องจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้นดังนี้

๖.๑ ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบได้แก่

๖.๑.๑ ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO)

๖.๑.๒ ผู้บริหารเทคโนโลยีระดับสูงสุดของหน่วยงาน (Chief Information Officer:CIO)

๖.๑.๓ ผู้อำนวยการสำนักคอมพิวเตอร์

๖.๒ ระดับปฏิบัติ

๖.๒.๑ ทีมบริการเครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่

(๑) บริหารจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายให้อยู่ในสภาพพร้อมใช้งานและกู้คืนเมื่อเครื่องไม่ทำงาน

(๒) เฝ้าระวังการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

(๓) ดูแลการสำรองและกู้คืนข้อมูลและฐานข้อมูลจากความเสียหายให้กลับมาใช้งานตามปกติ

(๔) ทดสอบการกู้คืนข้อมูลในระบบสำรองข้อมูล เพื่อทดสอบว่าข้อมูลที่สำรองไว้สามารถนำกลับมาใช้งานได้เมื่อจำเป็น

(๕) บำรุงรักษาและทดสอบการกู้คืนระบบสำรองข้อมูล เพื่อให้ระบบมีความพร้อมใช้อยู่เสมอ

๖.๒.๒ ทีมบริการระบบเครือข่ายและสื่อสาร

(๑) เฝ้าระวังการทำงานของระบบเครือข่ายและสื่อสารให้ทำงานได้ตลอดเวลาที่เปิดบริการ

(๒) บำรุงรักษาและกู้คืนระบบเครือข่ายและสื่อสารให้ทำงานได้ปกติ

(๓) ค้นหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์

(๔) จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบสื่อสาร ระบบปรับอากาศ ให้พร้อมใช้งาน

(๕) บำรุงรักษาศูนย์กลางข้อมูลเป็นประจำทุกเดือน เพื่อให้ศูนย์กลางข้อมูลอยู่ในสภาพพร้อมใช้งานอยู่เสมอ

๖.๒.๓ ทีมไฟฟ้า

(๑) ติดตั้งระบบดับเพลิงอัตโนมัติในห้องศูนย์กลางข้อมูล (Data Center) และห้องศูนย์กลางระบบเครือข่าย (Network Center)

(๒) ดูแลและบำรุงรักษาระบบไฟฟ้า ระบบปรับอากาศ การควบคุมความชื้นห้องศูนย์กลางข้อมูลที่อาคารสำนักคอมพิวเตอร์

(๓) ดูแลระบบแจ้งเตือนระบบไฟฟ้าขัดข้องนอกเวลาราชการ เพื่อให้เจ้าหน้าที่ผู้รับผิดชอบสามารถเข้าไปแก้ไขปัญหาได้อย่างรวดเร็ว

(๔) ตรวจสอบและเตรียมน้ำมันสำรองสำหรับเครื่องกำเนิดไฟฟ้า เพื่อให้เครื่องพร้อมใช้งานเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๕) รับผิดชอบการเปิดเครื่องกำเนิดไฟฟ้าเมื่อเกิดเหตุไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๖) เฝ้าระวังระบบไฟฟ้า

๗. การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามที่ระบุอย่างน้อยปีละ ๑ ครั้ง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบ ให้ผู้อำนวยการสำนักคอมพิวเตอร์ทราบเป็นประจำทุกเดือน และส่งผ่านผู้บริหารเทคโนโลยีระดับสูงสุดของหน่วยงาน (Chief Information Officer: CIO) ทราบ เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer: CEO) ทราบ และหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบทันที