เอกสารแนบท้าย
นโยบายและแนวปฏิบัติการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์

กันยายน ๒๕๖๗

สารบัญ

นโยบายและแนวปฏิบัติการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่าย
ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์

หลักการและขอบเขต

ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์เป็นหน่วยงานที่ให้บริการโครงสร้างพื้นฐานดิจิทัลและการสื่อสาร ที่ทันสมัยและมีประสิทธิภาพ มุ่งมั่นที่จะเป็นศูนย์กลางในการสนับสนุนการดำเนินงานของมหาวิทยาลัยในยุคดิจิทัล พัฒนาและส่งมอบโซลูชันด้านดิจิทัลที่ตอบโจทย์ความต้องการของทุกภาคส่วน ดังนั้น อาศัยพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๖๐ (ฉบับที่ ๒) พระราชบัญญัติการรักษาความมั่นคงปลอดภัยไซเบอร์ พ.ศ. ๒๕๖๒ พระราชบัญญัติการบริหารงานและการให้บริการภาครัฐผ่านระบบดิจิทัล พ.ศ.๒๕๖๒ และกฎหมายรองที่เกี่ยวข้อง ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์จึงจัดทำแนวปฏิบัติการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่าย โดยแบ่งหมวดหมู่ ดังนี้

หมวด ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม

หมวด ๒ บริหารการจัดการด้านการสื่อสารและการดำเนินงานของระบบเครือข่าย ระบบงานคอมพิวเตอร์ และระบบสารสนเทศ

หมวด ๓ การควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ

ผู้เกี่ยวข้อง

เอกสารนี้ประกาศใช้กับผู้มีส่วนได้ส่วนเสียที่เกี่ยวข้องกับการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่ายศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์ รวมถึงผู้เกี่ยวข้องอื่น ๆ ที่ไม่ได้ระบุไว้ในเอกสารฉบับนี้

คำนิยาม

คำศัพท์	ความหมาย
มหาวิทยาลัย	มหาวิทยาลัยวลัยลักษณ์
หน่วยงาน	หน่วยงานของมหาวิทยาลัยวลัยลักษณ์ ได้แก่ สำนักงานอธิการบดี สำนักวิชา วิทยาลัย ศูนย์ สถาบัน ส่วนงาน หรือหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าหน่วยงานดังกล่าว
หน่วยงานภายนอก	หน่วยงานอื่นซึ่งมิใช่หน่วยงานของมหาวิทยาลัยวลัยลักษณ์ และให้หมายความรวมถึงบุคคลหรือคณะบุคคลภายนอกที่มหาวิทยาลัยวลัยลักษณ์ติดต่อด้วย
ศูนย์เทคโนโลยีดิจิทัล	ศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์
ผู้บริหาร	ผู้บริหารที่เกี่ยวข้องกับการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่ายตามคณะกรรมการ/คณะทำงานที่เกี่ยวข้อง
ผู้บังคับบัญชา	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

คำศัพท์	ความหมาย
หัวหน้าหน่วยงาน	ผู้บังคับบัญชาของหน่วยงานภายในมหาวิทยาลัยวลัยลักษณ์ ได้แก่ คณบดี ผู้อำนวยการสถาบัน ผู้อำนวยการศูนย์ หัวหน้าส่วน หรือหัวหน้างานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่า และให้หมายความรวมถึงผู้ที่ได้รับมอบอำนาจเป็นลายลักษณ์อักษรจากอธิการบดีมหาวิทยาลัยวลัยลักษณ์ด้วย
เจ้าหน้าที่	พนักงาน และลูกจ้างของมหาวิทยาลัยวลัยลักษณ์ และให้หมายความรวมถึงพนักงานตามสัญญาจ้างด้วย
นักศึกษา	นักศึกษาของมหาวิทยาลัยวลัยลักษณ์
ผู้ใช้งาน	พนักงานและนักศึกษาของมหาวิทยาลัย และให้หมายความรวมถึงบุคคลที่ได้รับคำสั่งจากมหาวิทยาลัย หรือมหาวิทยาลัยมอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ หรือบุคคลภายนอกที่เข้ามาติดต่อกับมหาวิทยาลัยวลัยลักษณ์
หน่วยงานภายนอก	หน่วยงานอื่นซึ่งมิใช่หน่วยงานของมหาวิทยาลัย และให้หมายความรวมถึงบุคคลหรือคณะบุคคลภายนอกที่มหาวิทยาลัยติดต่อด้วย
ผู้ดูแลระบบ (System Administrator)	เจ้าหน้าที่ที่ได้รับมอบหมาย จากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบและเครือข่ายคอมพิวเตอร์ ระบบแม่ข่ายหรือระบบสารสนเทศ ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่าย คอมพิวเตอร์ เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างประจำ และลูกจ้างชั่วคราว ของมหาวิทยาลัย
บุคคลภายนอก	ผู้รับจ้าง เจ้าหน้าที่ของหน่วยงานภายนอกอื่น ๆ ทั้งที่เป็นหน่วยงานราชการและเอกชน รวมถึงประชาชนทั่วไปที่ใช้บริการระบบสารสนเทศของมหาวิทยาลัย
ข้อมูล (Data)	สิ่งที่สื่อความหมายให้รู้เรื่องราวข้อเท็จจริงหรือเรื่องอื่นใด ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเอง หรือโดยผ่านวิธีการใด ๆ และ ไม่ว่าจะได้จัดทำไว้ในรูปของเอกสารแฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ภาพถ่ายดาวเทียม ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ เครื่องมือตรวจวัด การสำรวจระยะไกล หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้
สารสนเทศ (Information)	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้งานสามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจ และอื่น ๆ

คำศัพท์	ความหมาย
ระบบสารสนเทศ (Information System)	ระบบงานที่นำเทคโนโลยีมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งประกอบด้วยเทคโนโลยีคอมพิวเตอร์และ เทคโนโลยีการสื่อสารโทรคมนาคม ได้แก่ ระบบคอมพิวเตอร์ (Computer System) ระบบเครือข่าย (Network System) ซอฟต์แวร์ (Software) ข้อมูล (Data) และสารสนเทศ (Information) เป็นต้น
ทรัพย์สิน (Asset)	สิ่งที่มีคุณค่าหรือมูลค่าต่อหน่วยงานและเป็นทรัพย์สินที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่หน่วยงานเป็นเจ้าของ เช่า ว่าจ้าง พัฒนา หรือจัดซื้อ โดยแบ่งแยกออกเป็นประเภทต่าง ๆ ได้แก่ สารสนเทศ (Information) ซอฟต์แวร์ (Software) ทรัพย์สินที่มีรูปร่าง (Physical Asset) บริการสาธารณูปโภคพื้นฐาน (Service) และบุคลากร (People)
ระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Information Technology System)”	ระบบงานของหน่วยงานที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วย ในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อลื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น
ระบบเครือข่าย (Network System)	ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลระหว่างระบบเทคโนโลยีสารสนเทศและ การสื่อสารต่าง ๆ ของหน่วยงานได้ เช่น ระบบแลน (Lan) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น
ระบบคอมพิวเตอร์ (Computer System)	อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือ ชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
ระบบอินเทอร์เน็ต (Internet)	ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบ เครือข่ายคอมพิวเตอร์ต่าง ๆ ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก
จดหมายอิเล็กทรอนิกส์ (e-mail)	ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์ และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง
ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address)	ชุดอักขระที่ระบุเฉพาะเจาะจงถึงตำแหน่งที่อยู่ของตู้ไปรษณีย์ของผู้ที่ใช้จดหมายอิเล็กทรอนิกส์ ซึ่งจะประกอบด้วยชื่อของบุคคล ได้แก่ First name ตามด้วยสัญลักษณ์จุดทศนิยม (.) ตามด้ายตัวอักษร ๒ ตัวแรกของนามสกุลและตามสัญลักษณ์ @ และชื่อของโดเมน (Domain Name) ได้แก่ username.it@wu.ac.th

คำศัพท์	ความหมาย
รหัสผ่าน (Password)	เครื่องมือรักษาความปลอดภัยที่ประกอบด้วยชุดของตัวอักษร ซึ่งใช้ตรวจสอบสิทธิในการเข้าถึงระบบแก่ผู้ใช้แต่ละคน เพื่อแสดงรับรองความถูกต้องแท้จริง (Authentication) ของผู้ใช้
ชุดคำสั่งไม่พึงประสงค์ (Malicious Code)	ชุดคำสั่งที่มีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือเพิ่มเติมขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
ช่องโหว่ (Vulnerability)	ช่องทางของระบบซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่า หรือเหตุการณ์ที่ไม่พึงประสงค์ที่ทำให้ระบบสารสนเทศไม่ สามารถทำงานได้ตามวัตถุประสงค์
มัลแวร์ (Malware)	โปรแกรมคอมพิวเตอร์สร้างขึ้นมาเพื่อให้เกิดความเสียหายหรือ รบกวนการทำงานของระบบทำให้ข้อมูลรั่วไหลเปิดช่องให้มีผู้บุกรุกเข้ามาหรือสร้างความเดือดร้อนรำคาญ ได้แก่ ไวรัสคอมพิวเตอร์ (Computer Virus) หนอมคอมพิวเตอร์ (Computer Worm) ม้าโทรจัน (Trojan Horse) โปรแกรมเข้ารหัสไฟล์คอมพิวเตอร์เพื่อเรียกค่าไถ่ (Ransomware) เป็นต้น

การเผยแพร่และทบทวน

เอกสารแนบท้ายนโยบายและแนวปฏิบัติการใช้งานทรัพยากรคอมพิวเตอร์และเครือข่ายศูนย์เทคโนโลยีดิจิทัล มหาวิทยาลัยวลัยลักษณ์นี้ จะต้องเผยแพร่โดยการแจ้งเวียนเพื่อให้พนักงานและนักศึกษาได้รับทราบและถือปฏิบัติ โดยเมื่อเริ่มนำไปใช้ในระยะแรกสามารถทบทวนได้บ่อยครั้งเป็นรายไตรมาสเพื่อให้เหมาะสมกับบริบทการปฏิบัติงานจริง และควรมีการทบทวนเป็นประจำ อย่างน้อยปีละ ๑ (หนึ่ง) ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ หรือตามที่ศูนย์เทคโนโลยีดิจิทัลเห็นสมควร

หมวด ๑ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสภาพแวดล้อม

เพื่อควบคุมและป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาตของสินทรัพย์ของมหาวิทยาลัย ไม่ให้เกิดการสูญหาย ถูกขโมย เกิดความเสียหาย เกิดการก่อกวนหรือแทรกแซง ป้องกันการถูกเปิดเผย โดยไม่ได้รับอนุญาตของสินทรัพย์ของมหาวิทยาลัย และป้องกันไม่ให้กิจกรรมการดำเนินงานต่าง ๆ ของมหาวิทยาลัย เกิดการติดขัดหรือหยุดชะงัก

แนวทางปฏิบัติการรักษาความมั่นคงปลอดภัยด้านศูนย์ข้อมูล

๑) มาตรฐานของศูนย์ข้อมูล (Data Center) และศูนย์ข้อมูลสำรอง (Disaster Recovery)

๑.๑) หน่วยงานต้องกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้ชัดเจนและจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานโดยการกำหนดพื้นที่ดังกล่าวแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย

๑.๒) หน่วยงานต้องมีการบริหารจัดการพื้นที่สำหรับการส่งมอบครุภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศที่จัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ที่ไม่ได้รับอนุญาต

๑.๓) หน่วยงานต้องกำหนดสิทธิให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วนประกอบด้วย

(๑) จัดทำเอกสาร “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

(๒) จัดทำเอกสาร “บันทึกการเข้าออกพื้นที่” เพื่อทำการบันทึกการเข้าออกพื้นที่ที่ใช้งานและกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้าออกดังกล่าว

(๓) จัดให้มีเจ้าหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร อย่างสม่ำเสมอ

(๔) ต้องมีการทบทวนปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงข้อมูลที่เกี่ยวข้องกับสิทธิการเข้าออกพื้นที่ เช่น การโอน โยกย้าย ลาออก หรือสิ้นสุดการจ้าง

๑.๔) หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายในมหาวิทยาลัย จะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบดูแลพื้นที่

๑.๕) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งาน โดยให้มีระบบดับเพลิง ระบบปรับอากาศและควบคุมความชื้น และให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างสม่ำเสมอ โดยให้มั่นใจว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

๑.๖) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องเครื่องทำงานผิดปกติหรือหยุดการทำงาน

๒) การควบคุมการเข้าออกศูนย์ข้อมูลและศูนย์สำรองข้อมูล

๒.๑) ต้องมีการบริหารจัดการพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นสัดส่วนชัดเจน เช่น พื้นที่ควบคุมส่วนระบบเครือข่าย (Network Zone) พื้นที่ควบคุมพิเศษส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึง หรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

๒.๒) หัวหน้าฝ่ายหรือหัวหน้างาน ต้องอนุมัติสิทธิในการเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้กับผู้รับผิดชอบพื้นที่ และมีการบันทึกเอกสาร “บันทึกการเข้าออกพื้นที่”

๒.๓) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ อาจมีความจำเป็นต้องเข้าออกพื้นที่ต้องมีการขอสิทธิเข้าออกศูนย์ข้อมูลและศูนย์สำรองข้อมูล โดยจัดทำบันทึกข้อความผ่านระบบ DOMS เสนอผู้บังคับบัญชาต้นสังกัดรับทราบและพิจารณาอนุมัติตามลำดับขั้น และต้องได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับภารกิจและหน้าที่รับผิดชอบในการปฏิบัติงานภายในหน่วยงาน

๒.๔) ผู้ดูแลระบบและผู้รับผิดชอบพื้นที่ต้องยืนยันตัวตนด้วยระบบการสแกนลายนิ้วมือหรือระบบการสแกนหน้าหรือรหัสผ่าน

๒.๕) การเข้าออกพื้นที่ต้องมีการควบคุมอย่างรัดกุม มีการบันทึกข้อมูลการเข้าออกพื้นที่ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๒.๖) ผู้ติดต่อหรือบุคคลภายนอกต้องมีเอกสารขอเข้าปฏิบัติงานและได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร และมีการมอบหมายผู้ดูแลระบบหรือผู้รับผิดชอบพื้นที่ตามลำดับการบังคับบัญชา

๒.๗) ผู้ติดต่อหรือบุคคลภายนอกสามารถนำผู้ติดตามเข้ามาช่วยงานได้ไม่เกินครั้งละ ๒ คน โดยทุกคนต้องแสดงบัตรที่ใช้ระบุตัวตนที่ออกโดยส่วนราชการ ต่อผู้ดูแลระบบหรือผู้รับผิดชอบพื้นที่ และมีการลงบันทึกข้อมูลบัตรใน “บันทึกการเข้าออกพื้นที่”

๒.๘) ผู้ติดต่อหรือบุคคลภายนอกที่จะเข้าปฏิบัติงาน หรือนำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงาน จะต้องลงบันทึกรายการอุปกรณ์ในเอกสาร "บันทึกการเข้าออกพื้นที่" ให้ถูกต้องชัดเจนโดยผู้ดูแลหรือผู้รับผิดชอบพื้นที่

๒.๙) การเข้าพื้นที่ของผู้ติดต่อหรือบุคคลภายนอก ต้องอยู่ภายใต้ความรับผิดชอบของผู้ดูแลระบบหรือผู้รับผิดชอบพื้นที่ที่ได้รับมอบหมายตามเอกสารขอเข้าปฏิบัติงาน

๒.๑๐) ผู้ดูแลระบบหรือผู้รับผิดชอบพื้นที่ต้องตรวจสอบความถูกต้องของข้อมูลใน "บันทึกการเข้าออกพื้นที่" เป็นประจำทุกเดือน

๒.๑๑) หัวหน้าฝ่ายหรือหัวหน้างาน ต้องทบทวนการมอบหมายสิทธิผู้ดูแลระบบหรือผู้รับผิดชอบพื้นที่ให้มีความถูกต้องเหมาะสมอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น การย้าย โอน ลาออก หรือสิ้นสุดสัญญาจ้าง

๓) การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ

๓.๑) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ หรือมีการป้องกันโดยวิธีอื่นที่เหมาะสม เพื่อป้องกันการตัดสายสัญญาณทำให้เกิดความเสียหาย หรือการดักจับข้อมูลโดยผู้ที่มิได้รับอนุญาต

๓.๒) สายไฟต้องแยกจากสายสื่อสารในระยะที่เหมาะสม เพื่อป้องกันการรบกวนของสัญญาณ

๓.๓) ติดป้ายชี้บ่งสายสัญญาณและบนอุปกรณ์ต่าง ๆ เพื่อป้องกันการต่อสัญญาณผิดเส้น

๓.๔) จัดทำแผนผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

๓.๕) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

๓.๖) พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ Coaxial Cable สำหรับระบบสารสนเทศที่สำคัญ

๓.๗) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดีสำหรับสายไฟเบอร์ออฟติก

๔) การบำรุงรักษาอุปกรณ์

๔.๑) วางแผนการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลา และต้องมีการซ่อมบำรุงอย่างทันท่วงทีตามความสำคัญของระบบ

๔.๒) บันทึกประวัติการบำรุงรักษาและซ่อมบำรุงอุปกรณ์ทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง โดยมีรายละเอียด ดังนี้ วันที่บำรุงรักษาและซ่อมบำรุง รายการอุปกรณ์ สถานะของอุปกรณ์ ปัญหาที่พบและการแก้ไข ผู้ดำเนินการบำรุงรักษาและซ่อมบำรุงพร้อมลงลายมือชื่อ

๔.๓) ถ้ามีการจัดจ้างหน่วยงานหรือผู้ให้บริการภายนอก เพื่อบำรุงรักษาและซ่อมบำรุงอุปกรณ์หน่วยงานภายในที่จัดจ้างต้องจัดให้มีสัญญาหรือข้อตกลงการจ้าง โดยต้องกำหนดระยะเวลา ขอบเขต และระดับการให้บริการอย่างชัดเจน

๔.๔) ควบคุมดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย ในกรณีที่ต้องเข้าปฏิบัติงานในพื้นที่ ผู้ดูแลระบบหรือผู้รับผิดชอบการซ่อมบำรุงอุปกรณ์จะต้องอยู่ในพื้นที่ทุกครั้ง

๔.๕) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างหรือผู้ให้บริการภายนอกที่เข้ามาบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๕) ข้อกำหนดด้านความมั่นคงปลอดภัยของอุปกรณ์

๕.๑) ความมั่นคงปลอดภัยของอุปกรณ์

(๑) ต้องจัดมาตรการป้องกันอุปกรณ์ของสำนักงานเพื่อหลีกเลี่ยงความเสี่ยงจากภัยคุกคามทางกายภาพและอันตรายต่าง ๆ รวมถึงความเสี่ยงในการเข้าถึงอุปกรณ์โดยไม่ได้รับอนุญาต และต้องมีการควบคุมการเข้าออกในบริเวณพื้นที่

(๒) อุปกรณ์ที่มีความสำคัญต่อระบบสารสนเทศ ต้องได้รับการปิดล็อกและป้องกันการเข้าถึง

(๓) ต้องมีกลไกการป้องกันการล้มเหลวของระบบและอุปกรณ์สนับสนุนต่าง ๆ ได้แก่ ระบบไฟฟ้า ระบบไฟฟ้าสำรอง ระบบน้ำประปา ระบบตรวจจับและดับเพลิง และระบบควบคุมอุณหภูมิ และความชื้น

(๔) ต้องกำหนดให้มีการบำรุงรักษาอุปกรณ์ต่าง ๆ อย่างสม่ำเสมอ เพื่อให้อุปกรณ์ทำงานได้อย่างต่อเนื่องและอยู่ในสภาพที่มีความสมบูรณ์ต่อการใช้งาน เป็นไปตามมาตรฐานหรือคุณสมบัติของอุปกรณ์แต่ละระบบ ตามระยะเวลาและขั้นตอนที่อุปกรณ์แต่ละประเภทกำหนดหรือตามแผนการบำรุงรักษาระบบคอมพิวเตอร์นั้น ๆ

(๕) ต้องกำหนดให้มีวิธีการในการทำลายอุปกรณ์ที่มีข้อมูลสำคัญเก็บไว้ เช่น ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น ทั้งนี้ เพื่อป้องกันการรั่วไหลหรือการเปิดเผยข้อมูลดังกล่าว

๕.๒) การปฏิบัติในการเคลื่อนย้ายทรัพย์สินสารสนเทศ เข้า-ออก นอกพื้นที่

(๑) การนำทรัพย์สินสารสนเทศ เข้า-ออก นอกพื้นที่ จะต้องได้รับการอนุมัติจากหัวหน้าหน่วยงาน หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานก่อนทุกครั้ง

(๒) กรณีที่มีการนำทรัพย์สินสารสนเทศของมหาวิทยาลัยไปปฏิบัติงานภายนอกพื้นที่ เช่น ที่บ้าน หรือที่สาธารณะ เป็นต้น ผู้ใช้งานจะต้องปกปิดทรัพย์สินสารสนเทศให้เป็นความลับและไม่เปิดเผยแก่บุคคลภายนอก พร้อมทั้งต้องดูแลรักษาทรัพย์สินสารสนเทศให้มีความปลอดภัยตลอดเวลา

(๓) กรณีที่มีการนำทรัพย์สินสารสนเทศกลับเข้ามาใช้ภายในพื้นที่ จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดมัลแวร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งาน ให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัย

๕.๓) การปฏิบัติในการเคลื่อนย้ายทรัพย์สินสารสนเทศเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

(๑) ต้องมีการควบคุม ดูแล การเข้าออกในบริเวณพื้นที่โดยให้ผ่านเข้าออก เฉพาะผู้ที่มีสิทธิหรือผู้ที่ได้รับอนุญาตเท่านั้น

(๒) การนำทรัพย์สินสารสนเทศเข้าออกศูนย์ข้อมูล จะต้องได้รับการอนุมัติจากหัวหน้าหน่วยงาน หรือเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าหน่วยงานก่อนทุกครั้ง

(๓) กรณีที่มีการนำทรัพย์สินสารสนเทศกลับเข้ามาในห้องศูนย์ข้อมูล จะต้องมีการตรวจสอบโปรแกรมป้องกันและกำจัดมัลแวร์ให้เป็นปัจจุบัน รวมทั้งสื่อต่าง ๆ ที่จะนำกลับเข้ามาใช้งานให้ปลอดภัยก่อนการเชื่อมต่อกับระบบเครือข่ายของมหาวิทยาลัย

หมวด ๒ บริหารการจัดการด้านการสื่อสารและการดำเนินงานของระบบเทคโนโลยีสารสนเทศ

เพื่อให้การดำเนินงานที่เกี่ยวข้องกับอุปกรณ์ประมวลผลสารสนเทศเป็นไปอย่างถูกต้องและปลอดภัย รักษาระดับความมั่นคงปลอดภัยของการปฏิบัติหน้าที่ให้เป็นไปตามข้อตกลง ลดความเสี่ยงจากการล้มเหลวของระบบ ป้องกันซอฟต์แวร์และสารสนเทศให้ปลอดภัยจากการถูกทำลาย โดยชุดคำสั่งไม่พึงประสงค์ ป้องกันสารสนเทศบนเครือข่ายและโครงสร้างพื้นฐานที่สนับสนุนการทำงานของเครือข่าย ป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สิน โดยไม่ได้รับอนุญาต โดยประกอบด้วยนโยบายการดำเนินงาน ดังต่อไปนี้

๒.๑ นโยบายความมั่นคงปลอดภัยด้านเครือข่าย

วัตถุประสงค์

นโยบายนี้กำหนดขึ้นเพื่อให้การใช้งานระบบครือข่ายเป็นไปอย่างถูกต้องและปลอดภัย จึงจำเป็นต้องมีการบริหารจัดการเครือข่ายของหน่วยงาน ให้มีความมั่นคงปลอดภัยด้านความถูกต้อง การเก็บรักษา เป็นความลับ และความพร้อมในการใช้งาน นโยบายดังกล่าวนี้มีผลบังคับใช้กับ “ผู้ดูแลระบบ” หรือผู้รับผิดชอบของหน่วยงานภายในและหน่วยงานภายนอกที่ขออนุญาตใช้งานระบบเครือข่าย

แนวปฏิบัติความมั่นคงปลอดภัยด้านเครือข่ายสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) การกำหนดหน้าที่ความรับผิดชอบและวิธีการปฏิบัติงาน (Operational Procedures and Responsibilities)

๑.๑) หัวหน้าฝ่ายหรือหัวหน้างานต้องจัดทำคู่มือและขั้นตอนการปฏิบัติงานของระบบเทคโนโลยีสารสนเทศ ในส่วนของการใช้อุปกรณ์เครือข่าย พร้อมแบ่งหน้าที่ความรับผิดชอบในการดำเนินงานในส่วนที่เกี่ยวกับระบบสารสนเทศและเครือข่ายที่หน่วยงานนั้น ๆ รับผิดชอบ

๑.๒) ในกรณีที่มีการเปลี่ยนแปลงแก้ไขการใช้อุปกรณ์เครือข่ายของระบบเทคโนโลยีสารสนเทศ หน่วยงานที่ดูแลระบบเทคโนโลยีสารสนเทศนั้นต้องทำการบันทึกรายละเอียดการเปลี่ยนแปลงแก้ไขข้อมูลที่สำคัญและแจ้งให้หน่วยงานอื่น ๆ ที่เกี่ยวข้องทราบ

๑.๓) หัวหน้าฝ่ายหรือหัวหน้างานที่เป็นเจ้าของระบบเทคโนโลยีสารสนเทศ ต้องจัดทำแผนรับมือเหตุการณ์ด้านความมั่นคงปลอดภัย และดำเนินการตรวจสอบผู้ไม่ประสงค์ดี

๑.๔) หัวหน้าฝ่ายหรือหัวหน้างานที่เป็นเจ้าของระบบเทคโนโลยีสารสนเทศ ต้องแยกเครื่องคอมพิวเตอร์ที่ใช้ในการพัฒนาระบบสารสนเทศออกจากเครื่องที่ทำงานจริงหรือเครื่องให้บริการ

๑.๕) ในกรณีที่มีการบริหารจัดการระบบเทคโนโลยีสารสนเทศจากเครือข่ายภายนอก หน่วยงานที่รับผิดชอบต้องปฏิบัติตามการควบคุมการเข้าถึงเครือข่าย โดยควบคุมให้ใช้งานหรือเข้าถึงระบบตามสิทธิของผู้ใช้งานที่ได้รับ และตรวจสอบการใช้งานอย่างสม่ำเสมอ

๒) การบริหารจัดการเครือข่าย (Network Management)

ผู้ดูแลระบบต้องบริหารจัดการความมั่นคงปลอดภัยในเครือข่าย ซึ่งมีแนวทางปฏิบัติดังนี้

๒.๑) ระบบเครือข่ายภายใน อุปกรณ์ที่ทำหน้าที่เชื่อมโยงกับระบบเครือข่าย เพื่อการทำงานภายใน ได้แก่ Router หรือ Switch มีข้อปฏิบัติดังนี้

(๑) อุปกรณ์ที่ทำหน้าที่ขยายการเชื่อมต่อเครือข่าย ต้องปิด Service Port ที่ ไม่จำเป็น และในการส่งข้อมูลการทำงานของอุปกรณ์เครือข่ายจะต้องไม่ใช้ค่าเริ่มต้นได้แก่ Default Community, Default Username และ Default Password

(๒) การเชื่อมต่อเครือข่ายเพื่อใช้งานระบบต่าง ๆ จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร

(๓) ผู้ดูแลระบบจะต้องมีแผนดำเนินการบำรุงรักษาและปรับปรุงเครือข่าย เพื่อให้สามารถใช้งานได้ดีอยู่เสมอ

(๔) ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบ หรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

(๕) ผู้ดูแลระบบมีหน้าที่ในการติดตั้งอุปกรณ์ซอฟต์แวร์ระบบการเข้ารหัส ข้อมูลอัตโนมัติหรือระบบอื่นใดที่เกี่ยวข้องกับเครือข่ายคอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

(๖) ผู้ดูแลระบบจะต้องไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลที่รับหรือส่งผ่านเครือข่ายคอมพิวเตอร์ ซึ่งตนไม่มีสิทธิในการเข้าถึงข้อมูลนั้น

๒.๒) อุปกรณ์ Server ที่เชื่อมต่อกับระบบเครือข่ายเพื่อการทำงานภายในหน่วยงานมีข้อปฏิบัติดังนี้

(๑) ผู้ดูแลระบบต้องเปลี่ยนค่าบัญชีผู้ใช้งานและรหัสผ่านที่ถูกกำหนดมาตั้งแต่เริ่มต้น (Default Username/Default Password)

(๒) ต้องทำ Hardening และบันทึกการทำ Configuration Set up ของอุปกรณ์ Server

(๓) ต้องเปิด Port ที่จำเป็นเท่านั้น ส่วน Port ที่ไม่ใช้งานต้องปิดทั้งหมด

(๔) ต้องบันทึกการติดตั้ง Service Patch ทุกครั้ง

(๕) ต้องไม่เปิดเผย OS Version, Service Port, IP Address และ Service Patch Version ให้บุคคลที่ไม่เกี่ยวข้องทราบ

(๖) เมื่อ Logon เพื่อใช้งาน Server ผ่าน Console แล้วเมื่อเลิกใช้งานจะต้อง Logoff User นั้นโดยทันที

(๗) ผู้ดูแลระบบจะต้องสำรองข้อมูลและระบบปฏิบัติการอย่างน้อยเดือนละ ๑ ครั้ง และทดสอบการสำรองข้อมูลอย่างน้อยปีละ ๒ ครั้ง โดยต้องสอดคล้องกับความสำคัญของระบบ

๓) การป้องกันการใช้งานเครือข่าย

๓.๑) ห้ามนำอุปกรณ์เครือข่ายมาติดตั้งกับระบบเครือข่าย โดยได้ไม่รับอนุญาตจากศูนย์เทคโนโลยีดิจิทัล

๓.๒) ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย ได้แก่ การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่าย

๓.๓) ห้ามผู้ใช้งานเครือข่ายกระทำการใด ๆ ที่รบกวนระบบเครือข่าย ได้แก่ การเปิดใช้งาน Service DHCP เพื่อเชื่อมต่อเข้ากับระบบเครือข่าย

๓.๔) ตรวจสอบการเชื่อมต่อเครือข่ายและจำกัดสิทธิ์ รวมถึงความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

๓.๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่ายจากระยะไกล โดยไม่ได้รับอนุญาต โดยมีการควบคุมการเข้าถึงพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และเปิดใช้บริการ (Service) ที่จำเป็นเท่านั้น เช่น SSH SFTP และ Ping เป็นต้น รวมถึงมีการดูแลตรวจสอบการเปิดให้บริการอยู่เสมอ

๔) การป้องกันซอฟต์แวร์และสารสนเทศของหน่วยงาน ให้ปลอดภัยจากการถูกทำลายจากซอฟต์แวร์ที่ไม่ประสงค์ดี (Protection Against Malicious Software) ให้ปฏิบัติตามนโยบายการใช้งานระบบป้องกันไวรัสและมัลแวร์สำหรับระบบงานคอมพิวเตอร์

๕) การวางแผนและการตรวจรับทรัพยากรสารสนเทศ (System Planning and Acceptance) หน่วยงานต้องมีการวางแผนกำหนดความต้องการทรัพยากรสารสนเทศ พร้อมกำหนดคุณลักษณะ จัดทำแผนจัดซื้อจัดหา เกณฑ์การตรวจรับทรัพยากรสารสนเทศ และแผนการบำรุงรักษา ล่วงหน้าอย่างน้อย ๒ ปีงบประมาณ

๒.๒ นโยบายการใช้งานอินเทอร์เน็ต

วัตถุประสงค์

นโยบายนี้ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานอินเทอร์เน็ตของมหาวิทยาลัย การรักษาข้อมูลและทรัพยากรต่าง ๆ ของหน่วยงานให้มีความมั่นคงปลอดภัย

แนวปฏิบัติการใช้งานอินเทอร์เน็ตสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ผู้ดูแลระบบหรือผู้รับผิดชอบต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยจัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น และแจ้งให้ผู้ใช้งานทราบ

๒) ผู้ดูแลระบบหรือผู้รับผิดชอบต้องเฝ้าระวังและตรวจสอบผู้ใช้งานไม่ให้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Fiber Optic หรือ ADSL ยกเว้นมีเหตุผลความจำเป็นและได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร

แนวปฏิบัติการใช้งานอินเทอร์เน็ตสำหรับผู้ใช้งาน

๑) การรับ/ส่งข้อมูลคอมพิวเตอร์ผ่านระบบเครือข่ายอินเทอร์เน็ตจะต้องมีการตรวจสอบไวรัสหรือมัลแวร์ โดยโปรแกรมป้องกันไวรัสและมัลแวร์ก่อนการรับ/ส่งข้อมูลทุกครั้ง

๒) ห้ามใช้เครือข่ายอินเทอร์เน็ต เพื่อประโยชน์ทางธุรกิจส่วนตัว หรือเข้าถึงเว็บไซต์ที่มีเนื้อหาไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม สังคม หรือความมั่นคงของประเทศ

๓) ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อรักษาประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย

๔) ห้ามเผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

๕) ห้ามเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัย ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๖) ห้ามนำเข้าข้อมูลคอมพิวเตอร์ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามกอนาจาร และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

๗) ห้ามนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๘) ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๙) ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดเพื่อปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๐) การเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย การทำลายความสัมพันธ์กับบุคคลอื่นของหน่วยงานอื่น

๑๑) หลังจากใช้งานอินเทอร์เน็ต ให้ทำการปิดเว็บเบราว์เซอร์และลงชื่อออกการใช้งานระบบต่าง ๆ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๓ นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์

วัตถุประสงค์

นโยบายนี้ ได้ถูกจัดทำขึ้นเพื่อช่วยให้ผู้ใช้งานรับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ให้มีการป้องกันการเข้าถึงหรือการเปลี่ยนแปลงแก้ไขข้อความ ในจดหมายอิเล็กทรอนิกส์โดยไม่ได้รับอนุญาต การรักษาข้อมูลและทรัพยากรต่าง ๆ ของมหาวิทยาลัย ให้มีความมั่นคงปลอดภัย

แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ผู้ดูแลระบบหรือผู้รับผิดชอบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ ให้เหมาะสมกับการเข้าใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงต้องแจ้งให้ผู้เกี่ยวข้องทราบ

๒) ผู้ดูแลระบบหรือผู้รับผิดชอบต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์

๓) สำหรับผู้ใช้งานรายใหม่จะต้องกำหนดรหัสผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์ เมื่อมีการเข้าสู่ระบบในครั้งแรก

๔) ผู้ดูแลระบบหรือผู้รับผิดชอบต้องมีมาตรการการกำหนดรหัสผ่านที่ดี (Good Password) โดยรหัสผ่านจะต้องมีทั้ง ตัวอักษร ตัวเลข และสัญลักษณ์พิเศษประสมกัน และกำหนดความยาวของรหัสผ่านอย่างน้อย ๘ ตัวอักษรเพื่อความปลอดภัย

๕) รหัสผ่านจดหมายอิเล็กทรอนิกส์ ขณะใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านโดยตรง แต่ต้องแสดงในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “X” หรือ “๐” ในการพิมพ์แต่ละตัวอักษร

๖) ผู้ดูแลระบบต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ ต้องมีการลงชื่อออกจากหน้าจอตัดการใช้งาน เมื่อผู้ใช้งานไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ ๖๐ นาที และต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้งเมื่อต้องการใช้งานต่อ

แนวทางปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์สำหรับผู้ใช้งาน

๑) ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์ และควรมีการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๒) ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ด้วยความระมัดระวังเพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยหรือละเมิดลิขสิทธิ์ สร้างความน่ารำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย

๓) ผู้ใช้งานต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่ได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์และให้ถือว่าเจ้าของเป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๔) ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อการทำงานของมหาวิทยาลัยเท่านั้น

๕) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๖) ผู้ใช้งานต้องตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนเปิด และต้องตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสและมัลแวร์ เพื่อป้องกันการเปิดไฟล์ที่เป็น Executable File เช่น .exe, .com เป็นต้น

๗) ผู้ใช้งานไม่ควรเปิดหรือส่งจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๘) ผู้ใช้งานต้องใช้ข้อความที่สุภาพในการรับ-ส่งจดหมายอิเล็กทรอนิกส์ หลีกเลี่ยงการใช้ข้อความที่ไม่เหมาะสม ที่อาจทำให้เสียชื่อเสียงของมหาวิทยาลัย หรือเกิดความแตกแยกระหว่างหน่วยงาน

๙) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๑๐) ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

๑๑) ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

๒.๔ นโยบายความมั่นคงปลอดภัยของการตรวจจับการบุกรุก (IDS/IPS policy)

วัตถุประสงค์

นโยบายการติดตั้งระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากรระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในมหาวิทยาลัย ให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

แนวทางปฏิบัติความมั่นคงปลอดภัยของการตรวจจับการบุกรุกสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ระบบตรวจสอบการบุกรุกต้องครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของศูนย์ข้อมูลหลักและศูนย์ข้อมูลสำรอง

๒) ระบบที่สามารถเข้าถึงได้จากระบบอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบตรวจสอบการบุกรุก

๓) ระบบใน DMZ (Demilitarized Zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการ ก่อนการติดตั้งและเปิดให้บริการ

๔) โฮสต์และเครือข่ายทั้งหมดที่มีการส่งผ่านระบบตรวจสอบการบุกรุก ต้องมีการตรวจสอบและอัปเดต Patch/Signature อย่างสม่ำเสมอ และต้องมีการบันทึกผลการตรวจสอบ รวมถึงต้องมีการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และการเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

๕) ระบบตรวจสอบการบุกรุก จะทำงานภายใต้กฎควบคุมพื้นฐานของ Firewall ที่ใช้ในการเข้าถึงเครือข่ายของระบบเครื่องแม่ข่ายที่มีการติดตั้งจะต้องมีการตรวจสอบข้อมูลประจำวัน

๖) พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุก การโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ จะต้องมีการรายงานให้หัวหน้าฝ่ายหรือหัวหน้างานทราบทันทีที่ตรวจพบ

๗) หากตรวจพบเหตุการณ์หรือพฤติกรรมที่น่าสงสัย หรือระบบการทำงานที่ผิดปกติ จะต้องรายงานให้หัวหน้าฝ่ายหรือหัวหน้างานทราบทันที

๘) การตรวจสอบการบุกรุก จะต้องเก็บบันทึกข้อมูลให้สืบค้นย้อนหลังได้ไม่น้อยกว่า ๙๐ วัน

๙) ศูนย์เทคโนโลยีดิจิทัลมีสิทธิ์ยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์หรือเครื่องแม่ข่ายที่มีพฤติกรรมเสี่ยงต่อการบุกรุก โดยไม่ต้องมีการแจ้งผู้ใช้งานทราบล่วงหน้า

๑๐) ผู้ที่พยายามกระทำการอันใดที่เป็นการละเมิดนโยบาย การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศ จะถูกระงับการใช้งานเครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมาย ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของมหาวิทยาลัย จะต้องถูกดำเนินคดีตามขั้นตอน

๒.๕ นโยบายการใช้งานเครื่องคอมพิวเตอร์พกพา

วัตถุประสงค์

เพื่อควบคุมดูแลการนำเครื่องคอมพิวเตอร์พกพาไปปฏิบัติงาน และเพื่อเป็นการป้องกันข้อมูล และอุปกรณ์ของมหาวิทยาลัยให้มีความมั่นคงปลอดภัย “ผู้ใช้งาน” จึงต้องรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งาน การบำรุงรักษา และสิ่งที่ต้องหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์พกพาให้มีความมั่นคงปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องเชื่อถือได้ (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

แนวทางปฏิบัติในการใช้งานเครื่องคอมพิวเตอร์พกพาสำหรับผู้ใช้งาน

๑) การใช้งานเครื่องคอมพิวเตอร์พกพา มีแนวทางปฏิบัติ ดังนี้

๑.๑) เครื่องคอมพิวเตอร์พกพาของมหาวิทยาลัย เป็นสินทรัพย์ของมหาวิทยาลัย ดังนั้นผู้ใช้งานต้องมีความระมัดระวัง และใช้เพื่องานของมหาวิทยาลัยเท่านั้น

๑.๒) โปรแกรมที่ติดตั้งต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย และต้องไม่คัดลอกหรือกระทำการอย่างใดอย่างหนึ่ง ที่เป็นการละเมิดลิขสิทธิ์หรือผิดกฎหมาย

๑.๓) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์พกพาตรวจซ่อมจะต้องดำเนินการโดยหน่วยงานเจ้าของอุปกรณ์ที่ได้รับมาตั้งแต่ต้น

๑.๔) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

๑.๕) ผู้ใช้งานห้ามดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของเครื่องคอมพิวเตอร์พกพา และรักษาสภาพของเครื่องคอมพิวเตอร์พกพาให้มีสภาพเดิม ยกเว้นที่ได้รับอนุญาตจากหัวหน้าฝ่ายหรือหัวหน้าหน่วยงาน

๑.๖) ผู้ใช้งานหลีกเลี่ยงการใส่เครื่องคอมพิวเตอร์พกพาในกระเป๋าที่เสี่ยงต่อการถูกกดทับหรือโยนทิ้ง

๑.๗) ห้ามใช้งานเครื่องคอมพิวเตอร์พกพาในสภาพอากาศร้อนจัดเป็นเวลานาน ควรปิดเครื่องเพื่อพักก่อนใช้งานใหม่

๑.๘) หลีกเลี่ยงการวางเครื่องคอมพิวเตอร์พกพาใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูง เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ

๑.๙) การเช็ดทำความสะอาดหน้าจอควรทำอย่างเบามือและเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพื่อป้องกันรอยขีดข่วน

๒) ความปลอดภัยทางด้านกายภาพ มีแนวทางปฏิบัติ ดังนี้

๒.๑) ผู้ใช้งานต้องรับผิดชอบในการป้องกันการสูญหาย และไม่วางเครื่องทิ้งไว้ในสถานที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๒.๒) ห้ามเก็บหรือใช้งานเครื่องคอมพิวเตอร์พกพาในสถานที่ที่มีความร้อน ความชื้น หรือฝุ่นละอองสูง และต้องระวังป้องกันการตกกระแทก

๒.๓) ห้ามเปลี่ยนแปลงหรือแก้ไขส่วนประกอบย่อย (Sub Components) ภายในเครื่อง รวมถึงอุปกรณ์สำรองไฟฟ้า

๓) การควบคุมการเข้าถึงระบบปฏิบัติการและการใช้รหัสผ่าน (Password) มีแนวทางปฏิบัติ ดังนี้

๓.๑) ผู้ใช้งานต้องกำหนดรหัสผ่านของเครื่องคอมพิวเตอร์พกพา

๓.๒) ผู้ใช้งานต้องลงชื่อออกจากระบบทันทีเมื่อเลิกใช้งานเครื่องคอมพิวเตอร์พกพาที่เชื่อมต่อกับระบบเครือข่าย

๓.๓) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Login) และรหัสผ่าน (Password) ในการใช้งานอุปกรณ์เชื่อมต่อเครือข่าย

๔) การป้องกันจากไวรัสและมัลแวร์ มีแนวทางปฏิบัติ ดังนี้

๔.๑) ผู้ใช้งานต้องปรับปรุง (Update) ระบบปฏิบัติการ และโปรแกรมใช้งานอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ที่เกิดขึ้นจากซอฟต์แวร์ และเป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

๔.๒) หากพบหรือสงสัยว่าเครื่องคอมพิวเตอร์พกพาติดไวรัสและมัลแวร์ ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของไวรัสและมัลแวร์ ไปยังเครื่องคอมพิวเตอร์อื่น ๆ ได้

๕) การสำรองและกู้คืนข้อมูล มีแนวทางปฏิบัติ ดังนี้

๕.๑) ผู้ใช้งานต้องสำรองข้อมูลจากเครื่องคอมพิวเตอร์พกพา โดยวิธีการและสื่อ (Media) ต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

๕.๒) ผู้ใช้งานต้องเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลข้อมูล

๕.๓) การเคลื่อนย้ายสื่อสำรองข้อมูลออกนอกสถานที่จะต้องมีการป้องกันการเข้าถึงข้อมูลอย่างมั่นคงปลอดภัย

๖) การบำรุงรักษาเครื่องคอมพิวเตอร์พกพา มีแนวทางปฏิบัติ ดังนี้

๖.๑) เครื่องคอมพิวเตอร์พกพาจะต้องขึ้นทะเบียนครุภัณฑ์ เพื่อความสะดวกในการตรวจสอบและการบำรุงรักษา

๖.๒) มหาวิทยาลัยจะให้บริการเฉพาะเครื่องคอมพิวเตอร์พกพาที่ขึ้นทะเบียนครุภัณฑ์แล้วหรืออยู่ระหว่างการส่งมอบเท่านั้น

๖.๓) หากเครื่องคอมพิวเตอร์พกพาเกิดการชำรุดเสียหาย ไม่สามารถใช้งานได้ทั้งด้านซอฟต์แวร์หรือฮาร์ดแวร์ ผู้ใช้งานมีหน้าที่จะต้องแจ้งให้หน่วยงานที่รับผิดชอบรับทราบเพื่อดำเนินการแก้ไขต่อไป

๖.๔) หากเครื่องคอมพิวเตอร์พกพาอยู่ในสัญญาหรือระยะเวลาการรับประกันเกิดการชำรุดเสียหาย หน่วยงานที่รับผิดชอบมีหน้าที่ติดต่อคู่สัญญาหรือผู้แทนจำหน่าย เพื่อดำเนินการตรวจซ่อมตามที่ระบุในสัญญา

๖.๕) หากเครื่องคอมพิวเตอร์พกพาอยู่นอกเหนือหรือพ้นระยะเวลาการรับประกัน ศูนย์เทคโนโลยีดิจิทัลมีหน้าที่ซ่อมแซมในเบื้องต้น และดำเนินการในส่วนที่เกี่ยวข้องต่อไป

๒.๖ นโยบายการจัดการสื่อที่ใช้ในการบันทึกข้อมูล

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อบริหารการจัดการสื่อที่ใช้ในการบันทึกข้อมูล เช่น ป้องกันการเปิดเผยข้อมูล การเปลี่ยนแปลงแก้ไข การลบหรือการทำลาย โดยไม่ได้รับอนุญาต

แนวทางปฏิบัติในการจัดการสื่อที่ใช้ในการบันทึกข้อมูลสำหรับผู้ใช้งาน

๑) การบริหารจัดการสื่อบันทึกข้อมูลที่สามารถเคลื่อนที่ย้ายได้ (Management of Removable Media) มีแนวทางปฏิบัติดังนี้

๑.๑) ข้อมูลที่มีชั้นความลับต้องกำหนดให้ถูกทำลายเมื่อไม่มีการใช้งานแล้ว โดยต้องมั่นใจว่าข้อมูลไม่สามารถกู้คืนได้ ก่อนที่จะนำสื่อบันทึกข้อมูลออกไปจากมหาวิทยาลัย

๑.๒) หากจำเป็นต้องนำสื่อบันทึกข้อมูลออกไปภายนอกมหาวิทยาลัย ต้องได้รับการอนุมัติจากหน่วยงานที่เกี่ยวข้อง และต้องบันทึกการโยกย้าย เพื่อใช้ในการตรวจสอบ

๑.๓) สื่อบันทึกข้อมูลทั้งหมดจะต้องถูกจัดเก็บอย่างปลอดภัย อยู่ในสภาพแวดล้อมที่ไม่เป็นอันตรายต่อสื่อบันทึกข้อมูล ได้แก่ อุณหภูมิหรือความชื้นที่เหมาะสมตามข้อกำหนดของผู้ผลิต

๑.๔) การจัดเก็บสื่อบันทึกข้อมูลที่สำคัญ ต้องมีการป้องกันการรั่วไหลหรือเปิดเผยข้อมูล ได้แก่ การติดป้ายชื่ออย่างชัดเจน และกำหนดผู้มีสิทธิ์ในการใช้งาน

๑.๕) หากข้อมูลที่ต้องการจัดเก็บมีอายุการจัดเก็บยาวนานกว่าอายุการใช้งานของสื่อบันทึกข้อมูล ต้องจัดเก็บข้อมูลไว้ที่แหล่งอื่นเพื่อป้องกันการสูญหาย

๑.๖) ต้องจัดทำทะเบียนบันทึกข้อมูลของสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ เพื่อลดโอกาสการสูญหายของข้อมูล

๑.๗) การใช้งานตัวอ่านสื่อบันทึกข้อมูลที่สามารถเคลื่อนย้ายได้ ต้องใช้เพื่อวัตถุประสงค์ของหน่วยงานเท่านั้น และต้องมีเอกสารกำหนดอำนาจในการใช้งานเป็นลายลักษณอักษรอย่างชัดเจน

๒) การกำจัดสื่อบันทึกข้อมูล (Disposal of Media)

๒.๑) สื่อบันทึกข้อมูลที่ไม่มีความจำเป็นต้องใช้งานอีก ต้องถูกทำลายด้วยวิธีการที่ปลอดภัย เพื่อป้องกันการรั่วไหลของข้อมูล เช่น การเผา การแยกชิ้นส่วนเป็นชิ้นเล็ก ๆ หรือลบข้อมูลด้วยโปรแกรมที่มหาวิทยาลัยรับรอง

๒.๒) กระบวนการกำจัดสื่อบันทึกข้อมูลต้องระบุวิธีการอย่างชัดเจน เพื่อความปลอดภัยของข้อมูลตามแนวทางความมั่นคงปลอดภัยของอุปกรณ์

๒.๓) ต้องรวบรวมสื่อบันทึกข้อมูลที่ไม่ต้องการแล้วกำจัดพร้อมกันด้วยวิธีการที่ปลอดภัย

๒.๔) ในกรณีที่ใช้บริการกำจัดสื่อและเอกสารจากหน่วยงานภายนอก ต้องเลือกหน่วยงานที่มีการควบคุมและมีประสบการณ์ที่ดี

๒.๕) ต้องมีการบันทึกกระบวนการกำจัดสื่อบันทึกข้อมูลเพื่อใช้ในการตรวจส

๒.๖) หากเป็นสื่อบันทึกข้อมูลส่วนบุคคล กระบวนการในการทำลายให้ดำเนินการตาม พรบ. คุ้มครองข้อมูลส่วนบุคคล พ.ศ. ๒๕๖๒ มาตรา ๓๓ และ ๓๗

หมายเหตุ : ข้อมูลที่ไม่มีความสำคัญเมื่อมีการรวบรวมเป็นจำนวนมาก ๆ อาจจะกลายเป็นข้อมูลที่มีความสำคัญได้ ดังนั้นในการกำจัดต้องคำนึงถึงข้อมูลที่มีการรวบรวมไว้ด้วย

๒.๗ นโยบายการใช้งานระบบป้องกันไวรัสและมัลแวร์สำหรับระบบงานคอมพิวเตอร์

วัตถุประสงค์

นโยบายนี้จัดทำขึ้นเพื่อป้องกันและลดความเสี่ยงจากการติดไวรัสและมัลแวร์ในเครื่องคอมพิวเตอร์ (PC) เครื่องคอมพิวเตอร์พกพา (Notebook) และเครื่องแม่ข่าย (Server) ของมหาวิทยาลัย โดยมีเป้าหมายในการเสริมสร้างความปลอดภัยและความเสถียรในการทำงานของระบบเทคโนโลยีสารสนเทศภายในมหาวิทยาลัย

แนวทางปฏิบัติในการใช้งานระบบป้องกันไวรัสและมัลแวร์สำหรับระบบงานคอมพิวเตอร์สำหรับผู้ใช้งาน

๑) ศูนย์เทคโนโลยีดิจิทัลเป็นผู้จัดหาระบบป้องกันไวรัสและมัลแวร์สำหรับเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์พกพา เครื่องแม่ข่ายที่เป็นทรัพย์สินของมหาวิทยาลัย โดยมีหลักพิจารณาให้ความสำคัญ (High Priority) ดังนี้

๑.๑) เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพาที่ต้องใช้ทำงานร่วมกับระบบงานที่สำคัญหรือระบบสารสนเทศที่มีข้อมูลความลับของหน่วยงาน ได้แก่ ERP, HR เป็นต้น

๑.๒) เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพา ที่ใช้ทำงานกับข้อมูลสำคัญ หรือข้อมูลอันเป็นความลับของหน่วยงานได้แก่ การจัดทำข้อกำหนด การทำร่างสัญญาทางกฎหมาย การทำงานด้านบัญชี/การเงิน เป็นต้น

๑.๓) เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพา ที่ใช้ควบคุมระบบงานสำคัญ (System Management) ของหน่วยงาน

๑.๔) เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพาของผู้บริหารระดับต้นขึ้นไป

๑.๕) เครื่องคอมพิวเตอร์ หรือเครื่องคอมพิวเตอร์พกพา ที่ใช้พัฒนาซอฟท์แวร์ หรือใช้ทำงาน System Administration หรือ Network Administration

๑.๖) เครื่องคอมพิวเตอร์หรือเครื่องคอมพิวเตอร์พกพา ของผู้ใช้งานที่ต้องทำหน้าที่ติดต่อกับหน่วยงานภายนอก หรือที่ต้องเชื่อมต่อกับทั้งอินทราเน็ต และอินเทอร์เน็ต เพื่อประโยชน์ทางราชการหรือภาพลักษณ์ของหน่วยงาน

๒) กำหนดให้ศูนย์เทคโนโลยีดิจิทัลร่วมกับหน่วยงานที่เกี่ยวข้อง เป็นผู้ประสานงานและดำเนินการที่เกี่ยวข้อง ได้แก่

๒.๑) แจ้งเวียนให้หน่วยงานภายในมหาวิทยาลัยรับทราบในช่องทางที่เหมาะสม

๒.๒) ศูนย์เทคโนโลยีดิจิทัลเป็นผู้รับผิดชอบดูแลบำรุงรักษา การอัพเดท Patch ปิดช่องโหว่ในระบบป้องกันไวรัสและมัลแวร์ เสนองบประมาณ ปรับเพิ่มลด จำนวนลิขสิทธิ์อนุญาตหรือจำกัดการใช้งานของผู้ใช้งาน และดำเนินการในส่วนที่เกี่ยวข้อง

๒.๓) ศูนย์เทคโนโลยีดิจิทัลดำเนินการอัพเดท Virus Signature ให้เป็นไปอย่างอัตโนมัติ และตั้งค่าของระบบป้องกันไวรัสและมัลแวร์ให้สามารถใช้งานได้อย่างมีประสิทธิภาพ

๒.๔) ศูนย์เทคโนโลยีดิจิทัลจะต้องปฏิบัติตามนโยบายเกี่ยวกับการใช้งานระบบป้องกันไวรัสและมัลแวร์ภายในเครือข่าย

๒.๕) มหาวิทยาลัยจะไม่อนุญาตให้ใช้งานระบบป้องกันไวรัสและมัลแวร์ที่ละเมิดลิขสิทธิ์

๓) กรณีที่หน่วยงานต้องการใช้ระบบป้องกันไวรัสและมัลแวร์กับระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์แม่ข่าย หรืออุปกรณ์อื่นที่ไม่ใช่เครื่องคอมพิวเตอร์และเครื่องคอมพิวเตอร์พกพา ให้ขออนุญาตต่อศูนย์เทคโนโลยีดิจิทัล เพื่อพิจารณาเป็นรายกรณีไป

๔) กรณีตรวจพบว่าผู้ใช้งาน หรือหน่วยงานไม่ปฏิบัติตามนโยบายการใช้งานระบบป้องกันไวรัสและมัลแวร์สำหรับเครื่องคอมพิวเตอร์ ศูนย์เทคโนโลยีดิจิทัลสามารถเข้าตรวจสอบสาเหตุ และแจ้งผลการตรวจสอบให้หัวหน้าฝ่ายหรือหัวหน้างาน และผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลทราบต่อไป

หมวด ๓ การควบคุมการเข้าถึงและการใช้งานระบบเทคโนโลยีสารสนเทศ

เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต ป้องกันการเปิดเผย หรือการขโมยสารสนเทศและอุปกรณ์ประมวลผลสารสนเทศ สร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์สื่อสารประเภทพกพาและการปฏิบัติงานจากภายนอกมหาวิทยาลัย

๓.๑ การควบคุมการเข้าถึงระบบเครือข่าย

วัตถุประสงค์

นโยบายนี้เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลและทรัพยากรเครือข่าย โดยกำหนดมาตรการในการควบคุม ตรวจสอบ และจำกัดการเข้าถึงระบบให้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น ทั้งนี้เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การรั่วไหลของข้อมูลที่เป็นความลับ และความเสียหายที่อาจเกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย ตลอดจนเพื่อให้มั่นใจว่าการใช้งานระบบเป็นไปอย่างเหมาะสม มีประสิทธิภาพ และสอดคล้องกับกฎหมายและระเบียบที่เกี่ยวข้อง

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ออกแบบระบบเครือข่ายตามกลุ่มของบริการและตามกลุ่มของผู้ใช้งาน โดยอย่างน้อยต้องแบ่งแยกเครือข่ายภายในกับภายนอก ได้แก่

๑.๑) เครือข่ายภายใน (Internal Network) สำหรับผู้ใช้งานภายในมหาวิทยาลัย

๑.๒) เครือข่ายภายนอก (External Network) สำหรับผู้ใช้งานทั่วไป (Guest User)

๒) จัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่ระบุขอบเขตและอุปกรณ์ต่าง ๆ อย่างชัดเจน พร้อมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

๓) กำหนดสิทธิให้แก่ผู้ใช้งาน เพื่อให้ใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๔) กำหนดเส้นทางบังคับบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่ายให้แก่ผู้ใช้งาน

๕) กำหนดบุคคลที่รับผิดชอบการปรับปรุงค่า Parameter ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ อย่างชัดเจน โดยมีการทบทวนอย่างน้อยปีละ ๑ ครั้ง และต้องแจ้งบุคคลที่เกี่ยวข้องทุกครั้งที่มีการเปลี่ยนแปลง

๖) ระบบเครือข่ายที่เชื่อมต่อกับเครือข่ายภายนอกต้องผ่านอุปกรณ์ป้องกันการบุกรุก เช่น Firewall และต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware)

๗) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการเข้าถึงที่ผิดปกติและการแก้ไขเปลี่ยนแปลงโดยบุคคลที่ไม่มีอำนาจ

๘) มีระบบป้องกันไม่ให้บุคคลภายนอกมองเห็น IP Address ภายใน เพื่อป้องกันการเข้าถึงข้อมูลโครงสร้างของเครือข่าย

แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายสำหรับผู้ใช้งาน

๑) ต้องลงทะเบียนผู้ใช้งาน ก่อนใช้งานระบบเครือข่าย

๒) การเข้าสู่ระบบเครือข่ายทุกครั้ง ต้องลงชื่อเข้าใช้งาน (Login) และพิสูจน์ยืนยันตัวตน (Authentication) เพื่อความปลอดภัย

๓) การเชื่อมต่อเครือข่ายจากภายนอกหรือการใช้งาน VPN ทุกครั้ง ต้องระบุชื่อผู้ใช้งานและรหัสผ่าน

๔) การติดตั้งและเชื่อมต่ออุปกรณ์เครือข่ายหรือเครื่องแม่ข่ายใด ๆ กับระบบเครือข่ายของมหาวิทยาลัย ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษรและปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

๕) การใช้เครื่องมือตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของมหาวิทยาลัย โดยการกำหนดสิทธิของผู้ใช้ให้เหมาะสมกับหน้าที่และความรับผิดชอบ รวมถึงการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนและได้รับอนุญาตจากผู้ดูแลระบบ เพื่อรักษาความมั่นคงปลอดภัยในการใช้งานเครือข่ายไร้สายของมหาวิทยาลัย

แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายไร้สายสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ต้องกำหนดสิทธิการเข้าถึงของผู้ใช้ให้เหมาะสมกับหน้าที่ความรับผิดชอบ และทบทวนสิทธิอย่างน้อยปีละ ๑ ครั้ง หากมีการเปลี่ยนแปลงต้องแจ้งให้ผู้เกี่ยวข้องทราบ

๒) ต้องกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณไร้สาย (Access point) ให้เหมาะสม เพื่อจำกัดบริเวณที่จำเป็นต้องใช้งานและป้องกันการโจมตีจากภายนอก

๓) ต้องปรับระดับสัญญาณให้เหมาะสมกับพื้นที่ใช้งาน และตรวจสอบให้แน่ใจว่าสัญญาณครอบคลุมพื้นที่ที่ต้องการใช้งาน

๔) เมื่อเริ่มใช้งานอุปกรณ์กระจายสัญญาณไร้สาย ผู้ดูแลระบบต้องเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดมาจากผู้ผลิตทันที

๕) ต้องเปลี่ยนค่าชื่อผู้ใช้และรหัสผ่านที่ใช้ในการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณไร้สาย โดยเลือกใช้รหัสผ่านที่มีความปลอดภัยเพื่อป้องกันการโจมตี

๖) ต้องมีการตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเป็นประจำ พร้อมทั้งบันทึกและตรวจสอบเหตุการณ์ที่น่าสงสัย

แนวปฏิบัติการควบคุมการเข้าถึงเครือข่ายไร้สายสำหรับผู้ใช้งาน

๑) ต้องลงทะเบียนผู้ใช้งาน ก่อนใช้งานระบบเครือข่ายไร้สาย

๒) การเข้าสู่ระบบเครือข่ายทุกครั้ง ต้องลงชื่อเข้าใช้งาน (Login) และพิสูจน์ยืนยันตัวตน (Authentication) เพื่อความปลอดภัย

๓) การติดตั้งและเชื่อมต่ออุปกรณ์กระจายสัญญาณไร้สายกับระบบเครือข่ายของมหาวิทยาลัย ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร และปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยไซเบอร์

๔) การใช้เครื่องมือตรวจสอบระบบเครือข่ายไร้สายต้องได้รับการอนุมัติและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๓.๓ การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย

วัตถุประสงค์

เพื่อให้การติดตั้ง การกำหนดค่า และการบริหารจัดการอุปกรณ์ป้องกันเครือข่าย (Firewall) เป็นไปอย่างมีประสิทธิภาพและปลอดภัย และจำกัดการเข้าถึงเฉพาะผู้ที่ได้รับมอบหมายอย่างชัดเจน นอกจากนี้ ยังมีการกำหนดนโยบายในการใช้พอร์ตเชื่อมต่อเครือข่ายเฉพาะที่จำเป็น เพื่อป้องกันการใช้งานที่ไม่เหมาะสมหรือเป็นภัยต่อเครือข่าย หากต้องการใช้พอร์ตอื่น ต้องได้รับอนุญาตอย่างเป็นลายลักษณ์อักษร

แนวปฏิบัติการควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่ายสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) ศูนย์เทคโนโลยีดิจิทัลมีหน้าที่รับผิดชอบในการติดตั้ง กำหนดค่า และบริหารจัดการ อุปกรณ์ป้องกันเครือข่ายหลัก (Firewall) ที่เชื่อมต่อกับเครือข่ายภายนอก

๒) กำหนดให้เข้าถึงอุปกรณ์ป้องกันเครือข่ายเฉพาะผู้ที่ได้รับมอบหมายเท่านั้น

๓) กำหนดนโยบาย (Policy Firewall) ให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ เฉพาะการใช้พอร์ตเชื่อมต่อที่จำเป็นต่อการใช้งานเท่านั้น หากต้องการใช้พอร์ตอื่นเพิ่มเติม ต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีดิจิทัลเป็นลายลักษณ์อักษร

๓.๔ การควบคุมการเข้าถึงระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์เพื่องานสำนักงาน

วัตถุประสงค์

เพื่อรักษาความปลอดภัยของข้อมูล ลดความเสี่ยงจากการเข้าถึงโดยไม่ได้รับอนุญาต ป้องกันการละเมิดการใช้งานที่ไม่เหมาะสม และสนับสนุนการทำงานของผู้ใช้งานให้เป็นไปอย่างมีประสิทธิภาพ รวมทั้งเป็นการปฏิบัติตามมาตรฐานที่เกี่ยวข้องแนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการสำหรับผู้ใช้งาน

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการสำหรับเครื่องคอมพิวเตอร์เพื่องานสำนักงานเพื่อเข้าใช้งาน

๑) ต้องยกเลิกบัญชีผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกรหัสผู้ใช้งานที่ได้ถูกกำหนดค่าเริ่มต้นจากการติดตั้งระบบทันทีที่ได้รับเครื่องคอมพิวเตอร์

๒) ต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

๓) ต้องตั้งค่าการใช้งานภาพพักหน้าจอและล็อกหน้าจอเมื่อไม่มีการใช้งาน

๔) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer เช่น Bit Torrent หรือโปรแกรมที่มีความเสี่ยงโดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีดิจิทัล

๕) ห้ามติดตั้งหรือใช้งานซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ หากมีการละเมิดผู้ใช้งานต้องรับผิดชอบส่วนบุคคล

๖) ห้ามใช้ทรัพยากรของมหาวิทยาลัยเพื่อประโยชน์อื่นใดที่ไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

๓.๕ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อให้มั่นใจว่าการดำเนินการในระบบสารสนเทศเป็นไปอย่างถูกต้องและมีประสิทธิภาพ นอกจากนี้ยังช่วยในการตรวจสอบและติดตามการใช้งาน เพื่อสนับสนุนการปฏิบัติตามกฎหมาย ข้อบังคับ และมาตรฐานด้านความปลอดภัยข้อมูลที่เกี่ยวข้อง

แนวปฏิบัติการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศสำหรับผู้ดูแลระบบหรือผู้รับผิดชอบ

๑) สร้างบัญชีผู้ใช้งาน (Username) สำหรับการเข้าถึงระบบสารสนเทศ ควบคุมและบริหารจัดการ รวมทั้งดูแลรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๒) กำหนดสิทธิและบริหารจัดการการเข้าถึงระบบสารสนเทศให้กับผู้ใช้งาน ทบทวนสิทธิ์และบัญชีผู้ใช้งานอย่างสม่ำเสมอเพื่อให้แน่ใจว่าสิทธิ์ที่กำหนดยังคงมีความเหมาะสม

๓) กำหนดให้ระบบสารสนเทศมีการบันทึกประวัติการใช้งาน (Logs)

๔) กำหนดประเภทของข้อมูล ลำดับความสำคัญ ลำดับชั้นความลับ การเข้าถึง และช่องทางการเข้าถึงระบบสารสนเทศ

๕) การกำหนดเวลาใช้งานระบบสารสนเทศ (Session Time-out) ให้ดำเนินการ ดังนี้

๕.๑) กำหนดให้ระบบมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน โดยให้ใช้งานได้ภายในช่วงเวลาที่กำหนดเท่านั้น

๕.๒) สำหรับระบบที่มีความสำคัญสูงหรือใช้งานในสถานที่เสี่ยง ควรกำหนดเวลาการเชื่อมต่อให้สั้นลงเพื่อความปลอดภัย

๖) การสำรองข้อมูล (Backup)

๖.๑) จัดลำดับความสำคัญในการสำรองข้อมูลของระบบสารสนเทศ

(๑) ระบบแอปพลิเคชันและฐานข้อมูลที่มีความสำคัญจะต้องสำรองข้อมูลทุกวัน

(๒) ระบบแอปพลิเคชันและฐานข้อมูลทั่วไปจะสำรองข้อมูลเดือนละครั้ง

๖.๒) กำหนดความถี่และรูปแบบการสำรองข้อมูลให้เหมาะสม

(๑) ระบบที่มีความสำคัญจะสำรองข้อมูลแบบเต็มทุกวันศุกร์ และสำรองข้อมูลแบบส่วนเพิ่มทุกวัน

(๒) ระบบทั่วไปจะสำรองข้อมูลแบบเต็มเดือนละครั้ง

๖.๓) เก็บข้อมูลสำรองในสื่อที่แตกต่างกัน เช่น เก็บข้อมูลสำรองในสื่อที่แตกต่างกันอย่างน้อย ๒ ที่ เช่น ฮาร์ดดิสก์หรือเทป

๖.๔) ตรวจสอบและทดสอบการกู้คืนข้อมูล โดยดำเนินการอย่างน้อยปีละ ๒ ครั้ง (ทุก ๖ เดือน) เพื่อเพิ่มความมั่นใจในความพร้อมใช้งานของข้อมูลสำรอง

๖.๕) กำหนดระยะเวลาการเก็บรักษาข้อมูลสำรอง โดยพิจารณาตามระบบที่สำคัญอย่างน้อย ๖๐ วัน

๖.๖) รักษาความปลอดภัยของข้อมูลสำรอง ต้องจำกัดการเข้าถึงข้อมูลสำรองเฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

๖.๗) กำหนดผู้รับผิดชอบในการดำเนินการสำรองข้อมูลและกู้คืนข้อมูล ต้องระบุชื่อและตำแหน่งของผู้รับผิดชอบหลักและผู้รับผิดชอบสำรอง

๖.๘) จัดทำเอกสารและรายงานเกี่ยวกับการสำรองข้อมูล โดยสามารถตรวจสอบได้และส่งผลลัพธ์เป็นระบบอัตโนมัติมาให้ผู้สำรองข้อมูลที่ระบุไว้ในข้อ ๖.๗

แนวปฏิบัติการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศสำหรับผู้ใช้งาน

๑) ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศตามสิทธิที่ได้รับ

๒) ต้องแสดงตัวตนผ่านชื่อผู้ใช้งานและรหัสผ่านที่ได้รับการตรวจสอบและยืนยันก่อนเข้าถึงระบบสารสนเทศ

๓) ผู้ใช้งานที่ไม่มีการใช้งานเกินระยะเวลาที่กำหนดจะถูกยุติการเข้าถึงระบบโดยอัตโนมัติ

๔) บุคคลภายนอกที่ต้องการเข้าถึงระบบสารสนเทศ ต้องได้รับอนุญาตจากหน่วยงานเจ้าของระบบสารสนเทศเป็นลายลักษณ์อักษร โดยแจ้งเหตุผลความจำเป็นสำหรับการปฏิบัติงาน และต้องรักษาความลับทางราชการ ในกรณีที่เกิดความเสียหายต้องรับผิดชอบต่อค่าเสียหายที่เกิดจากการเข้าถึงตามที่เจ้าของระบบกำหนด