ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก (Information Security Policy)

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก เป็นไปอย่างเหมาะสมมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้องได้ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้นต่อไป

อาศัยอำนาจตามความในมาตรา ๗ วรรคหนึ่ง แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่บัดนี้ เป็นต้นไป

ข้อ ๓. บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ให้ใช้ประกาศนี้แทน

ข้อ ๔. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก มีวัตถุประสงค์ ดังต่อไปนี้

๔.๑ เพื่อให้เกิดความเชื่อมั่นและมีความมั่นคงปลอดภัยในการใช้งานด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ทำให้ดำเนินงานได้อย่างมีประสิทธิภาพและประสิทธิผล

๔.๒ เพื่อเผยแพร่ประกาศนโยบายและข้อปฏิบัติให้บุคลากรทุกระดับในหน่วยงานสังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก และผู้ที่เกี่ยวข้องทั้งหมดได้รับทราบ เข้าถึง เข้าใจและถือปฏิบัติตามนโยบายและแนวปฏิบัติอย่างเคร่งครัด

๔.๓ เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีการปฏิบัติให้ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ตระหนักถึงความสำคัญของการรักษาความมั่นคงในการใช้งานด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด โดยจะต้องมีการทบทวนนโยบายปีละหนึ่งครั้ง

ข้อ ๕. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก กำหนดประเด็นสำคัญดังต่อไปนี้

๕.๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

๕.๑.๑ การเข้าถึง...

๕.๑.๑ การเข้าถึงระบบสารสนเทศ ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงกำหนดสิทธิ์ เพื่อให้ผู้ใช้งานในทุกระดับได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

๕.๑.๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศและป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ต้องกำหนดให้มีการลงทะเบียนผู้ใช้งาน ตรวจสอบบัญชีผู้ใช้งานอนุมัติและกำหนดรหัสผ่านการลงทะเบียนผู้ใช้งาน เพื่อให้ผู้ใช้งานที่มีสิทธิ์เท่านั้นที่สามารถเข้าใช้ระบบสารสนเทศได้ และต้องเก็บบันทึกข้อมูลการเข้าถึงและข้อมูลจราจรทางคอมพิวเตอร์ตลอดจนบริหารจัดการสิทธิ์การเข้าถึงข้อมูลให้เหมาะสมตามระดับชั้นความลับของผู้ใช้งาน ต้องมีการทบทวนสิทธิ์การใช้งานและตรวจสอบการละเมิดความปลอดภัยเสมอ

๕.๑.๓ การควบคุมการเข้าถึงเครือข่าย เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตต้องกำหนดสิทธิ์ในการเข้าถึงเครือข่ายให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์สำหรับใช้งานอินเทอร์เน็ต โดยผ่านระบบรักษาความปลอดภัยตามที่มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกจัดสรรไว้ และมีการออกแบบระบบเครือข่ายโดยแบ่งเขต (Zone) การใช้งาน เพื่อทำให้การควบคุมและป้องกันภัยคุกคามได้อย่างเป็นระบบและมีประสิทธิภาพ

๕.๑.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาตต้องกำหนดให้ผู้ที่จะเข้าใช้งานต้องลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งานและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่านก่อนการเข้าใช้งานต้องกำหนดระยะเวลา เพื่อยุติการใช้งานเมื่อว่างเว้นจากการใช้งาน และจำกัดระยะเวลาในการเชื่อมต่อระบบสารสนเทศตลอดจนกำหนดมาตรการในการใช้งานโปรแกรมอรรถประโยชน์ต่าง ๆ เพื่อไม่ให้เป็นการละเมิดลิขสิทธิ์และป้องกันโปรแกรมไม่ประสงค์ดีต่าง ๆ

๕.๑.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์และแอปพลิเคชันต้องกำหนดสิทธิ์การเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญ โปรแกรมประยุกต์หรือแอปพลิเคชันต่าง ๆ รวมถึงจดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) และระบบงานต่าง ๆ โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่ และต้องได้รับความเห็นชอบจากหัวหน้าหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๕.๒ การจัดทำระบบสำรองข้อมูล เพื่อให้ระบบสารสนเทศของหน่วยงานสามารถให้บริการได้อย่างต่อเนื่อง และมีเสถียรภาพต้องจัดทำระบบสารสนเทศและระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน โดยคัดเลือกระบบสารสนเทศที่สำคัญ เรียงลำดับความจำเป็นมากไปน้อย พร้อมทั้งกำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ในการสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์อย่างน้อยปีละหนึ่งครั้ง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๕.๓ ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยจัดให้มีการตรวจสอบจากผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละหนึ่งครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๖. กรณี...

ข้อ ๖. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดของหน่วยงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๗. ให้ถือปฏิบัติตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ตามที่แนบท้ายประกาศนี้

ประกาศ ณ วันที่ ๒๙ เดือน กันยายน พ.ศ. ๒๕๖๖

(รองศาสตราจารย์ฤกษ์ชัย ฟูประทีปศิริ)
อธิการดีมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

RMUTTO
www.rmutto.ac.th ราชมงคลตะวันออก

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก (Information Security Policy)

จัดทำโดย : สำนักวิทยบริการและเทคโลโลยีสารสนเทศ

คำนำ

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ในมาตราหน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2543 ที่กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก มีแนวทางปฏิบัติในการควบคุมการปฏิบัติงานและรักษาความปลอดภัยด้านระบบสารสนเทศ และเพื่อให้สอดคล้องตามพระราชกฤษฎีกาดังกล่าว ซึ่งประกอบด้วยแนวนโยบายและแนวปฏิบัติต่าง ๆ ซึ่งเป็นสิ่งสำคัญที่ผู้ปฏิบัติงานต้องถือปฏิบัติ เพื่อให้เกิดความมั่นคงปลอดภัยในการขับเคลื่อนพันธกิจและการให้บริการของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก อีกทั้งยังเป็นการสร้างความเชื่อมั่นให้กับผู้ใช้บริการ และผู้มีส่วนเกี่ยวข้องในทุกภาคส่วนทั้งภายในและภายนอกมหาวิทยาลัยและเพื่อสร้างความน่าเชื่อถือให้กับมหาวิทยาลัยต่อไป

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

กันยายน 2566

สารบัญ

เรื่อง **หน้า**

สารบัญ (ต่อ)

เรื่อง **หน้า**

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก
(Information Security Policy)

1. วัตถุประสงค์และขอบเขต

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 ในมาตรา 4 และมาตรา 7 ซึ่งออกโดยอาศัยอำนาจตามความในมาตรา 34 วรรคหนึ่งแห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2549 อันเป็นกฎหมายที่มีบทบัญญัติบางประการเกี่ยวกับการจำกัดสิทธิและเสรีภาพของบุคคล ซึ่งมาตรา 29 ประกอบกับมาตรา 4 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย (ฉบับชั่วคราว) พ.ศ. 2549 ได้กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2543 กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร

เพื่อให้การรักษาความปลอดภัยระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก หรือต่อไปนี้เรียกว่า “มหาวิทยาลัย” เป็นไปด้วยความเรียบร้อย มีความมั่นคงปลอดภัย และมีประสิทธิภาพ สามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องเหมาะสมและเป็นการป้องกันการถูกคุกคามจากผู้ไม่ประสงค์ดี และภัยคุกคามต่าง ๆ มหาวิทยาลัย จึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ โดยกำหนดให้มีมาตรฐาน (Standard) แนวปฏิบัติ (Guideline) ขั้นตอนปฏิบัติ (Procedure) ให้ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ และป้องกันภัยคุกคามต่าง ๆ โดยมีวัตถุประสงค์ดังต่อไปนี้

1.1 เพื่อให้เกิดความเชื่อมั่นและมีระบบการรักษาความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศของมหาวิทยาลัยให้สามารถดำเนินงานไปได้อย่างมีประสิทธิภาพและประสิทธิผล

1.2 เพื่อให้มหาวิทยาลัยมีการกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ โดยอ้างอิงตามมาตรฐาน ISO/IEC 27001 Annex A และรายละเอียดวิธีปฏิบัติทางเทคนิคจาก ISO/IEC 17799:2004 รวมทั้งมีการปรับปรุงอย่างต่อเนื่อง

1.3 เพื่อเผยแพร่ให้เจ้าหน้าที่ทุกระดับในมหาวิทยาลัยได้รับทราบและเจ้าหน้าที่ทุกคนต้องถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

1.4 เพื่อกำหนดมาตรฐานแนวทางปฏิบัติให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานให้กับมหาวิทยาลัยได้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยสำหรับการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

1.5 ให้อธิการบดี ซึ่งดำรงตำแหน่งผู้บริหารระดับสูงของมหาวิทยาลัย (CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นในกรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความ

เสียหายหรืออันตรายใด ๆ แก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1.6 นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา 1 ครั้งต่อปี

2. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ 1 นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environment Security Policy)

ส่วนที่ 2 นโยบายการควบคุมการเข้า-ออกห้องปฏิบัติการระบบเครือข่าย (Network System Operation Room Policy)

ส่วนที่ 3 นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร (Access Control Policy)

ส่วนที่ 4 นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ (Third Party Access Control Policy)

ส่วนที่ 5 นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย (Network Access Control)

ส่วนที่ 6 นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

ส่วนที่ 7 นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application Information Access Control)

ส่วนที่ 8 นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล (Use of Personal Computer Policy)

ส่วนที่ 9 นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Use of Notebook Computer Policy)

ส่วนที่ 10 นโยบายการใช้งานอินเทอร์เน็ต (Internet Security Policy)

ส่วนที่ 11 นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Policy)

ส่วนที่ 12 ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์ (Terms of Use and Disclaimer)

ส่วนที่ 13 นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

ส่วนที่ 14 นโยบายป้องกันไวรัส และซอฟต์แวร์ที่ไม่ประสงค์ดี (Virus and Malicious Software Protection Policy)

ส่วนที่ 15 นโยบายป้องกันระบบเครือข่ายและตรวจจับการบุกรุก (Firewall & IPS Policy)

ส่วนที่ 16 นโยบายการสำรองและกู้คืนข้อมูล (Backup and Recovery Policy)

ส่วนที่ 17 นโยบายด้านการปฏิบัติตามข้อบังคับ (Compliance Policy)

ส่วนที่ 18 นโยบายการสอบทานการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษา ความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ 19 นโยบายการและแนวปฏิบัติในการใช้สื่อสังคมออนไลน์ (Social Network Policy)

ส่วนที่ 20 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Awareness Policy)

องค์ประกอบของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยแต่ละส่วนที่กล่าวข้างต้นจะประกอบด้วยวัตถุประสงค์ รายละเอียดของมาตรฐาน (Standard) แนวทางปฏิบัติ (Guideline) และขั้นตอนวิธีการปฏิบัติ (Procedure) ในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อที่จะทำให้มหาวิทยาลัยมีมาตรการในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารอยู่ในระดับที่ปลอดภัยช่วยลดความเสียหายต่อการดำเนินงาน ทรัพย์สินและเจ้าหน้าที่ของมหาวิทยาลัย ทำให้สามารถดำเนินงานได้อย่างมั่นคงปลอดภัย นโยบายการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย ซึ่งผู้ใช้งานเจ้าหน้าที่ของมหาวิทยาลัยและหน่วยงานภายนอกต้องปฏิบัติตามอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศนี้ ประกอบด้วย

(1) **มหาวิทยาลัย** หมายถึง มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(2) **การรักษาความมั่นคงปลอดภัย** หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(3) **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย

(4) **สำนักวิทยบริการ** หมายถึง สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(5) **ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (CIO)** หมายถึง ผู้บริหาร/ผู้บริหารระดับสูง ที่ได้รับมอบหมายจากอธิการบดีให้ดูแลรับผิดชอบด้านเทคโนโลยีสารสนเทศ และการสื่อสารของมหาวิทยาลัยและมีคุณสมบัติตามมติคณะรัฐมนตรี เมื่อวันที่ 9 มิถุนายน 2541

(6) **ผู้อำนวยการสำนักวิทยบริการ** หมายถึง ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(7) **มาตรฐาน (Standard)** หมายถึง บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์หรือเป้าหมาย

(8) **วิธีการปฏิบัติ (Procedure)** หมายถึง รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์

(9) **แนวทางปฏิบัติ (Guideline)** หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

(10) **ผู้ใช้งาน (User)** หมายถึง บุคคลที่ได้รับอนุญาต (Authorized user) ให้สามารถเข้าใช้บริการ ใช้งานบริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่งมหาวิทยาลัยกำหนดไว้ ดังนี้

(10.1) ผู้บริหาร หมายถึง อธิการบดี รองอธิการบดี คณบดี ผู้อำนวยการสถาบัน สำนัก ศูนย์ หรือหัวหน้าหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่าคณะ ผู้ช่วยอธิการบดี รองคณบดี รองผู้อำนวยการสถาบัน ผู้อำนวยการสำนักงานอธิการบดี ผู้อำนวยการสำนักงานวิทยาเขต ผู้อำนวยการสำนักงานเขตพื้นที่ ผู้อำนวยการกอง หรือหัวหน้าหน่วยงานที่เรียกชื่ออย่างอื่นที่มีฐานะเทียบเท่ากองตามที่สภามหาวิทยาลัยกำหนด

(10.2) ผู้ดูแลระบบ (System Administrator) หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์แม่ข่ายระบบเครือข่ายคอมพิวเตอร์ ระบบฐานข้อมูล และผู้พัฒนาระบบสารสนเทศ

(10.3) เจ้าหน้าที่ หมายถึง ข้าราชการ พนักงานในสถาบันอุดมศึกษา พนักงานราชการ พนักงานตามภารกิจ ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างโครงการ ผู้ปฏิบัติงาน สังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(10.4) นักศึกษา หมายถึง นักศึกษามหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

(11) **สิทธิของผู้ใช้งาน (User Access Right)** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของคณะ หน่วยงาน หรือมหาวิทยาลัย

(12) **หน่วยงานภายนอก** หมายถึง องค์กรหรือหน่วยงานภายนอกที่มหาวิทยาลัยอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของคณะ หน่วยงาน หรือมหาวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่ และต้องรับผิดชอบในการรักษาความลับของข้อมูล

(13) **ระบบเทคโนโลยีสารสนเทศ (Information Technology System)** หมายถึง ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์มาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุน การให้บริการ การพัฒนา และควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบดังนี้

(13.1) ระบบคอมพิวเตอร์ หมายถึง ฮาร์ดแวร์ (Hardware) ซอฟต์แวร์ (Software) และบุคลากรทางคอมพิวเตอร์ (Peopleware) รวมถึงอุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่งหรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

(13.2) ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System) ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของมหาวิทยาลัยได้ เช่น สายสัญญาณใยแก้วนำแสง (Fiber Optic) ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

O ระบบ LAN และระบบ Intranet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกันเป็นเครือข่ายที่มีจุดประสงค์ เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในมหาวิทยาลัย

O ระบบ Internet หมายถึง ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ของหน่วยงานเข้ากับเครือข่ายอินเทอร์เน็ตทั่วโลก

(13.3) ข้อมูล (Data) หมายถึง ข้อมูล ข้อมูลส่วนบุคคล ข้อความคำสั่งชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

(13.4) สารสนเทศ (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความหรือภาพกราฟฟิกที่ผู้ใช้สามารถเข้าใจได้ง่ายและสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

(14) **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ (Information System Workspace)** หมายถึง พื้นที่ที่หน่วยงานอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

O พื้นที่ทำงานทั่วไป (General Working Area) หมายถึง พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคลและคอมพิวเตอร์พกพาที่ประจำโต๊ะทำงาน

O พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area)

O พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย (IT Equipment or Network Area)

O พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

(15) **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

(16) **สินทรัพย์** หมายถึง ข้อมูลระบบ ข้อมูลและทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารหรือสิ่งใดก็ตามที่มีคุณค่าของหน่วยงาน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

(17) **จดหมายอิเล็กทรอนิกส์ (E-mail)** หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน มาตรฐาน,ที่ใช้ในการรับ-ส่งข้อมูลชนิดนี้ได้แก่ SMTP POP3 และ IMAP เป็นต้นโดยชื่อที่ใช้ในการรับส่งจดหมายอิเล็กทรอนิกส์ จะมีรูปแบบซึ่งประกอบไปด้วย 2 ส่วน คือ ชื่อผู้ใช้ และชื่อโดเมน เช่น user@rmutto.ac.th หรือ user@office.rmutto.ac.th เป็นต้น

(18) **บัญชีผู้ใช้งาน (Account)** หมายถึง บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

(19) **รหัสผ่าน (Password)** หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

(20) **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ขัดข้องหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

(21) **ภัยคุกคาม (Threats)** หมายถึง เหตุการณ์ต่าง ๆ ที่เป็นไปได้หรือเหตุการณ์ที่ไม่พึงประสงค์ซึ่งอาจส่งผลกระทบหรือสร้างความเสียหายต่อระบบสารสนเทศของมหาวิทยาลัย

(22) **ช่องโหว่ (Vulnerabilities)** หมายถึง จุดอ่อนของทรัพย์สินหรือมาตรการที่เป็นช่องทางเกิดปัจจัยเสี่ยงจากภัยคุกคามที่มีผลกระทบต่อทรัพย์สินหรือต่อระบบสารสนเทศของมหาวิทยาลัย

(23) **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึง โดยมิชอบเอาไว้ด้วยก็ได้

(24) **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น อาทิ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

(25) **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยหรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อนหรืออาจสร้างความเสียหายและส่งผลให้

O เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการปฏิบัติงานสำคัญ เช่น ระบบงานสารสนเทศของหน่วยเกิดการหยุดชะงัก เป็นต้น

O เป็นการละเมิดนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัย

O เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่าง ๆ ที่กำหนดไว้

O เกิดภาพลักษณ์ที่ไม่ดีต่อมหาวิทยาลัย หรือทำให้สูญเสียชื่อเสียง เช่น การไปโพสต์ข้อความพาดพิงถึงมหาวิทยาลัยในเว็บไซต์ภายนอก ซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของมหาวิทยาลัย เป็นต้น

O เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ที่เป็นจุดอ่อนจำเป็นต้องได้รับรายงานจากผู้ใช้งาน เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสมได้ผลและทันกาล

(26) **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง เหตุบกพร่องหรือเหตุละเมิดด้านความมั่นคงปลอดภัย ซึ่งอาจทำให้ระบบของมหาวิทยาลัยสูญเสียการปฏิบัติงานรวมถึงการให้บริการต่าง ๆ แต่เพียงบางส่วนหรือทั้งหมดจากการถูกบุกรุกหรือโจมตีทางช่องโหว่และความมั่นคงปลอดภัยถูกคุกคามจากภัยคุกคามรูปแบบต่าง ๆ

ส่วนที่ 1
นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security Policy)

1. วัตถุประสงค์

กำหนดเป็นมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศข้อมูลซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้และหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของของมหาวิทยาลัย

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 แผนกอาคารสถานที่

2.3 คณะ/หน่วยงาน

2.4 ผู้ดูแลระบบ /เจ้าหน้าที่ ที่ได้รับมอบหมาย

3. การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)

3.1 ภายในมหาวิทยาลัยควรมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่าง ๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

3.2 จัดให้มีเวรยามรักษาอาคารและห้องปฏิบัติการระบบเครือข่ายและอุปกรณ์เชื่อมโยงเครือข่ายภายในอาคาร เพื่อป้องกันการแอบลักลอบเข้าสู่พื้นที่ปฏิบัติงานภายใน เพื่อการลักลอบก่อวินาศกรรม การโจรกรรม หรือการทำลายอุปกรณ์ ระบบประมวลผล ระบบฐานข้อมูล และระบบเครือข่ายคอมพิวเตอร์

3.3 ผู้บริหารควรกำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area)

3.4 ผู้บริหารต้องกำหนดสิทธิ์ให้กับเจ้าหน้าที่ให้สามารถมีสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน ประกอบด้วย

3.4.1 จัดทำ “ทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศ

3.4.2 ทำการบันทึกการเข้า-ออกพื้นที่ใช้งาน และกำหนดผู้มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออกดังกล่าว โดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออกพื้นที่”

3.4.3 จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศเป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิ์เข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารอย่างน้อยปีละ 1 ครั้ง

3.5 มีการจัดสภาพแวดล้อมทางกายภาพ เพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในคณะ/หน่วยงาน

3.6 มีการประเมินความเสี่ยงทางกายภาพและกำหนดมาตรการลดความเสี่ยง

3.7 ผนังล้อมรอบของสำนักงานหรือพื้นที่ที่มีระบบเทคโนโลยีสารสนเทศอยู่ภายในควรสร้างเป็นผนังทึบ

3.8 ประตูหรือทางเข้าสำนักงาน หรืออาคารออกแบบ เพื่อป้องกันการบุกรุกทางกายภาพ

3.9 ประตูหรือทางเข้าของห้องปฏิบัติการระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

3.10 เจ้าหน้าที่ที่ปฏิบัติงานภายในคณะ/หน่วยงาน ต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอภายหลังเลิกงาน และนอกเวลาราชการ

3.11 มีการจัดระบบการรักษาความปลอดภัย โดยมีพนักงานรักษาความปลอดภัย (รปภ.) และควรมีการติดตั้งกล้องวงจรปิดภายใน และภายนอกอาคาร ประตูทางเข้า เพื่อควบคุมการเข้าถึงของบุคคลภายนอก

3.12 ประตูหนี ไฟและผนังในบริเวณข้างเคียงต้องมีการก่อสร้างให้มีความทนทานต่อความร้อนอย่างเพียงพอ

3.13 ต้องมีการดำเนินการตรวจสอบ หรือทดสอบประตูหนีไฟเพื่อให้มีความทนทานเพียงพอและสอดคล้องกับกฎหมาย ระเบียบ และข้อบังคับต่าง ๆ ที่มหาวิทยาลัยต้องปฏิบัติตาม

3.14 ต้องป้องกันการบุกรุกของบุคคลภายนอก ซึ่งอาจเข้า-ออกอาคารโดยผ่านทางประตูหนีไฟ

3.15 ต้องมีการตรวจสอบประตูหนีไฟอย่างสม่ำเสมอ เพื่อดูว่ายังใช้งานได้ตามปกติ

3.16 เจ้าหน้าที่ของมหาวิทยาลัยต้องปิดประตู หน้าต่างให้ล็อคอยู่เสมอภายหลังเลิกงาน

3.17 ประตูและหน้าต่างในบริเวณชั้น 1 ของพื้นที่ที่มีความสำคัญควรมีการป้องกันการถูกทุบแตกเพื่อป้องกันการบุกรุกเข้ามาภายในอาคาร

4. การควบคุมการเข้า-ออก อาคาร สถานที่ (Physical Entry Controls)

4.1 จัดทำเอกสารระบุสิทธิ์ของผู้ใช้และ“หน่วยงานภายนอก” ในการเข้าถึงสถานที่โดยแบ่งแยกได้ดังนี้

4.1.1 มหาวิทยาลัยต้องกำหนดสิทธิ์ผู้ใช้ที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้า-ออก ในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

4.1.2 รณรงค์หรือออกกฎให้เจ้าหน้าที่ของมหาวิทยาลัยแขวนบัตรพนักงาน เพื่อใช้ระบุตัวตนก่อนเข้าอาคารหรือสถานที่สำคัญของหน่วยงาน

4.1.3 การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอกหรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์ม การเข้า-ออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

4.1.4 บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในมหาวิทยาลัย

4.1.5 กรณีที่บุคคลภายนอกหรือผู้ติดต่อต้องการนำอุปกรณ์ต่าง ๆ คอมพิวเตอร์ส่วนบุคคล หรือคอมพิวเตอร์พกพา สมาร์ทโฟน หรืออุปกรณ์เครือข่ายเข้าบริเวณอาคาร เจ้าหน้าที่รักษาความปลอดภัยจะต้องลงบันทึกในแบบฟอร์มการเข้า-ออกในรายการอุปกรณ์ที่นำเข้ามาให้ถูกต้อง

4.1.6 กรณีที่บุคคลภายนอกเข้ามาติดต่อเจ้าหน้าที่จะต้องลงชื่ออนุญาตการเข้า-ออกในแบบฟอร์มการเข้า-ออกให้ถูกต้อง

4.1.7 บุคคลภายนอกหรือผู้ติดต่อต้องคืนแบบฟอร์มการเข้า-ออกและบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และรปภ. ต้องตรวจสอบผู้ติดต่ออุปกรณ์ พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

4.2 ผู้เข้าจะได้รับสิทธิ์ให้เข้า-ออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

4.3 หากมีบุคคลอื่นใดที่ไม่ใช่ผู้ใช้ขอเข้าพื้นที่โดยมิได้ขอสิทธิ์ในการเข้าพื้นที่นั้นไว้เป็นการล่วงหน้าคณะ/หน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต ทั้งนี้จะต้องแสดงบัตรประจำตัวที่มหาวิทยาลัยออกให้โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการขอเข้า-ออกไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

5. การรักษาความมั่นคงปลอดภัยสำหรับสำนักงาน ห้องทำงานและทรัพย์สินอื่น ๆ (Securing Office Room And Facilities)

5.1 เจ้าหน้าที่ทุกคนต้องปฏิบัติการป้องกันทรัพย์สิน

5.2 เจ้าหน้าที่ต้องออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

5.3 ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย หากจัดเก็บในตู้เอกสารต้องมีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของราชการ

5.4 ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งานและป้องกันตู้หรือบริเวณที่ใช้ในการรับ-ส่งเอกสารไปรษณีย์ เพื่อความปลอดภัยของข้อมูล

5.5 ต้องไม่ให้ผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์คอมพิวเตอร์ต่าง ๆ เช่น เครื่องคอมพิวเตอร์ กล้องดิจิตอล เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

5.6 นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

6. การจัดบริเวณสำหรับการเข้าถึงหรือการส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and Loading Areas)

6.1 จำกัดการเข้าถึงพื้นที่หรือบริเวณที่มีการส่งมอบหรือขนถ่ายผลิตภัณฑ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

6.2 จำกัดเจ้าหน้าที่ ซึ่งสามารถเข้าถึงพื้นที่หรือบริเวณส่งมอบนั้น

6.3 ควรจัดพื้นที่หรือบริเวณส่งมอบไว้ในบริเวณต่างหาก เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายใน คณะ/หน่วยงาน

6.4 ต้องตรวจสอบวัสดุหรือปัจจัยการผลิตที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

6.5 กำหนดให้มีการลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอก โดยให้สอดคล้องกับระเบียบพัสดุหรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สิน

7. การจัดวางและการป้องกันอุปกรณ์ (Equipment Siting and Protection)

7.1 ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสมเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ของเจ้าหน้าที่ในคณะ/หน่วยงาน/สำนักงานให้น้อยที่สุด

7.2 ต้องจัดวางระบบเทคโนโลยีสารสนเทศในตำแหน่งที่เหมาะสม เพื่อหลีกเลี่ยงการมองเห็นข้อมูลสำคัญจากบุคคลภายนอก โดยการทันหน้าจอเข้ามาภายในโดยไม่ให้บุคคลผู้ ซึ่งไม่มีสิทธิ์สามารถมองเห็นหน้าจอนั้นได้

7.3 ต้องแยกเก็บอุปกรณ์ที่มีความสำคัญไว้ต่างหากอีกพื้นที่หนึ่ง เพื่อดูแลความมั่นคงปลอดภัย

7.4 ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ห้องปฏิบัติการระบบเครือข่าย/ระบบคอมพิวเตอร์/ระบบคอมพิวเตอร์แม่ข่าย

7.5 ดำเนินการตรวจสอบ สอดส่อง ระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์/อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์/ระบบคอมพิวเตอร์ แม่ข่าย เพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

7.6 มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน หรือไฟฟ้ากระชาก

8. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

8.1 ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยที่เพียงพอต่อความต้องการใช้งาน ได้แก่ ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้า ระดับกระแสไฟฟ้า ระบบยูพิเอส เครื่องกำเนิดกระแสไฟฟ้าสำรอง เป็นต้น และต้องมีการตรวจสอบหรือทดสอบ ระบบสนับสนุนดังกล่าวอย่างสม่ำเสมอ เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

8.2 ต้องมีการใช้ระบบสำรองกระแสไฟฟ้า (UPS) กับระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันอุปกรณ์ไฟฟ้าเสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้าและต้องทดสอบระบบสำรองกระแสไฟฟ้าอย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

8.3 ต้องมีเครื่องกำเนิดกระแสไฟฟ้าสำรอง เพื่อจ่ายไฟเมื่อกระแสไฟฟ้าหลักเกิดการหยุดชะงักเป็นระยะเวลายาวนาน และต้องจัดเตรียมน้ำมันเชื้อเพลิงสำรองอย่างเพียงพอสำหรับเครื่องกำเนิดกระแสไฟฟ้าสำรองเอาไว้ใช้งานในช่วงเกิดเหตุฉุกเฉิน

8.4 ต้องมีระบบไฟส่องสว่างฉุกเฉิน เพื่อรองรับในกรณีที่กระแสไฟฟ้าหลักเกิดขัดข้อง

8.5 ต้องมีระบบจ่ายน้ำที่เพียงพอสำหรับระบบปรับอากาศที่ต้องใช้น้ำในการทำงาน

8.6 ต้องมีระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนภายในห้องเครื่องทำงานผิดปกติหรือหยุดทำงาน

8.7 ต้องมีระบบสายสื่อสารสำรองซึ่งเชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ต และ/หรือผู้ให้บริการโทรคมนาคม เพื่อใช้เป็นเส้นทางสำรอง

9. การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (Cabling Security)

9.1 หลีกเสี่ยงการเดินสายสัญญาณเครือข่ายของหน่วยงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

9.2 ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณหรือการดัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

9.3 ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซง รบกวนของสัญญาณซึ่งกันและกัน

9.4 ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

9.5 จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

9.6 ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

9.7 พิจารณาใช้งานสายไฟเบอร์ออฟติก แทนสายสัญญาณสื่อสารแบบเดิมสำหรับระบบสารสนเทศที่สำคัญ

9.8 ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

10. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

10.1 ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต หรือตามระยะเวลาที่กำหนดไวในสัญญาซ่อมบำรุงรักษาอุปกรณ์ระหว่างมหาวิทยาลัยและผู้ประกอบการ

10.2 ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

10.3 จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

10.4 จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

10.5 ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในหน่วยงาน

10.6 จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

11. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment Off-Premises)

11.1 กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์

11.2 ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

11.3 เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

12. การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่อีกครั้ง (Secure Disposal or re-use Of Equipment)

12.1 ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการเปลี่ยน หรือทดแทนอุปกรณ์

12.2 ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการทำลายหรือจำหน่าย

12.3 ต้องทำการฟอร์แมต (Format) ฮาร์ดดิสก์ เพื่อป้องกันการกู้คืนข้อมูลในฮาร์ดดิสก์ โดยการใช้วิธีแบบเขียนทับซ้ำจำนวน 1 ครั้ง ตามมาตรฐาน NIST 800-88 สำหรับข้อมูลที่มีความลับระดับต่ำหรือแบบเขียนทับซ้ำจำนวน 3 ครั้ง ตามมาตรฐาน DoD 5220.22-M สำหรับข้อมูลที่มีความลับระดับปานกลางหรือแบบเขียนทับซ้ำจำนวน 7 ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

12.4 ควรลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ 5 ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

12.5 ต้องได้รับความเห็นชอบจากผู้มีอำนาจอนุมัติในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

12.6 มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ มีวิธีการดังนี้

12.6.1 ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการเปลี่ยน หรือทดแทนอุปกรณ์

12.6.2 ต้องทำการลบข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการทำลาย หรือจำหน่าย

12.6.3 ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในแผ่น CD/DVD ใช้วิธีการย่อยทำลายแผ่น CD/DVD

12.6.4 ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในเทป DDS, DAT, LTO จะต้องทำการลบข้อมูลทั้งม้วนเทป (Erase) ผ่าน Tape Device ก่อนการทำลายม้วนเทป

12.6.5 ข้อมูลอิเล็กทรอนิกส์ที่จัดเก็บในฮาร์ดดิสก์ (Hard Disk) หรือ Memory Devices แบบ USB, Flash drive, SD cards ให้ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD 5220-22M ของกระทรวงกลาโหมสหรัฐอเมริกาว่าด้วยการลบข้อมูลในฮาร์ดดิสก์ ดังนี้

12.6.5.1 ใช้ซอฟต์แวร์ Disk Wipe (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hard Disk หรือ Memory Devices โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php

12.6.5.2 ใช้ซอฟต์แวร์ Eraser (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล โดยสามารถดาวน์โหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php

13. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

13.1 ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกมหาวิทยาลัย/คณะ/หน่วยงาน

13.2 กำหนดผู้มีอำนาจในการเคลื่อนย้าย หรือนำอุปกรณ์ออกนอกมหาวิทยาลัย/คณะ/ หน่วยงาน

13.3 กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกมหาวิทยาลัย/คณะ/หน่วยงาน

13.4 เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

13.5 บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ส่วนที่ 2
นโยบายการควบคุมการเข้า-ออกห้องปฏิบัติการระบบเครือข่าย
(Network System Operation Room Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศที่สำคัญซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของมหาวิทยาลัย โดยมีการกำหนดกระบวนการควบคุมการเข้า-ออก ที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้า-ออก ห้องปฏิบัติการระบบเครือข่าย

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ /เจ้าหน้าที่ที่ได้รับมอบหมาย

3. คำจำกัดความของผู้เกี่ยวข้อง

3.1 ผู้ดูแลระบบ หมายถึง เจ้าหน้าที่ทุกคนที่ทำงานเกี่ยวข้องโดยตรงกับงานปฏิบัติการและบำรุงดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารภายในห้องปฏิบัติการระบบเครือข่าย

3.2 เจ้าหน้าที่ หมายถึง เจ้าหน้าที่ที่มีสิทธิในการเข้า-ออก สถานที่ อาคาร ห้อง ตามที่กำหนดในทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่

3.3 ผู้ติดต่อจากหน่วยงานภายนอก หมายถึง บุคคลจากหน่วยงานภายนอกที่มาทำการติดต่อขอเข้าถึงหรือใช้ข้อมูลหรือทรัพย์สินต่าง ๆ ของห้องปฏิบัติการระบบเครือข่าย

4. บทบาทและความรับผิดชอบ

4.1 ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

4.1.1 อนุมัติสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

4.1.2 อนุมัติกระบวนการควบคุมการเข้า-ออก ห้องปฏิบัติการระบบเครือข่าย

4.2 คณบดี /ผู้อำนวยการ /หัวหน้าหน่วยงาน

4.2.1 อนุมัติสิทธิเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ ของคณะ/ หน่วยงาน

4.2.2 อนุมัติกระบวนการควบคุมการเข้า-ออก ห้องปฏิบัติการระบบเครือข่ายของ คณะ/หน่วยงาน

4.3 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่าย

4.3.1 ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องปฏิบัติการระบบเครือข่ายให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องปฏิบัติการระบบเครือข่ายอย่างเคร่งครัด

4.3.2 ตรวจสอบให้มั่นใจว่าบุคคลที่ได้ผ่านเข้า-ออกห้องปฏิบัติการระบบเครือข่ายต้องติดบัตรผู้ติดต่อ (Visitor) หรือบัตรประจำตัวของมหาวิทยาลัยเท่านั้น

5. แนวปฏิบัติการควบคุมการเข้า-ออกห้องปฏิบัติการระบบเครือข่าย

5.1 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่ายและเจ้าหน้าที่มหาวิทยาลัย มีแนวทางปฏิบัติ ดังนี้

5.1.1 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่าย ควรจัดระบบเทคโนโลยีสารสนเทศให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone) เป็นต้น เพื่อสะดวกในการปฏิบัติงานและยังทำให้การควบคุมการเข้าถึงหรือเข้าใช้งานอุปกรณ์คอมพิวเตอร์สำคัญต่าง ๆ มีประสิทธิภาพมากขึ้น

5.1.2 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่าย ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้องปฏิบัติการระบบเครือข่าย โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้า-ออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

5.1.3 สิทธิในการเข้า-ออกห้องปฏิบัติการระบบเครือข่ายของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องปฏิบัติการระบบเครือข่าย

5.1.4 เจ้าหน้าที่ทุกคนต้องได้รับอนุญาต/ทำบัตรผ่าน/Key Card/Finger Scan เพื่อใช้ในการเข้า-ออกห้องควบคุมระบบเครือข่ายคอมพิวเตอร์

5.1.5 ต้องจัดทำระบบเก็บบันทึกการเข้า-ออกห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

5.1.6 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำอาจมีความจำเป็นต้องเข้า-ออกห้องปฏิบัติการระบบเครือข่ายต้องมีการควบคุมอย่างรัดกุม

5.1.7 การเข้าถึงห้องปฏิบัติการระบบเครือข่าย ต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่” และต้องตรวจสอบให้มั่นใจว่าบุคคลที่ผ่านเข้า-ออกทุกคนต้องกรอกแบบฟอร์มดังกล่าว

5.1.8 กรณีผู้ติดต่อจากหน่วยงานภายนอก มีความจำเป็นต้องเข้าห้องปฏิบัติการระบบเครือข่าย เจ้าหน้าที่ผู้รับผิดชอบจะต้องเป็นผู้นำพาเข้าไป และคอยสอดส่องกำกับดูแลตลอดการปฏิบัติงาน

5.2 ผู้ติดต่อจากหน่วยงานภายนอก มีแนวทางปฏิบัติ ดังนี้

5.2.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการแลกบัตรที่ใช้ระบุตัวตน เช่น บัตรประจำตัวประชาชน หรือใบอนุญาตขับขี่กับเจ้าหน้าที่รักษาความปลอดภัย เพื่อรับบัตรผู้ติดต่อ “Visitor” แล้วทำการลงบันทึกข้อมูลในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “บันทึกการเข้า-ออกพื้นที่”

5.2.2 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในห้องปฏิบัติการระบบเครือข่ายจะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออก ตามที่ระบุไวในเอกสาร “บันทึกการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

5.2.3 ผู้ติดต่อจากหน่วยงานภายนอกต้องติดบัตรผ่านตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในห้องปฏิบัติการระบบเครือข่าย/สำนักวิทยบริการฯ

5.2.4 พื้นที่ที่ผู้ติดต่อจากหน่วยงานภายนอก สามารถเข้าได้ตามที่ระบุไว้ในแบบฟอร์มการขออนุญาตเข้า-ออก และต้องมีเจ้าหน้าที่คอยสอดส่องดูแลตลอดเวลา

5.2.5 ผู้ติดต่อจากหน่วยงานภายนอกต้องคืนบัตรผู้ติดต่อกับเจ้าหน้าที่รักษาความปลอดภัย ซึ่งเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบการคืนบัตรและตรวจสอบแบบฟอร์มการขออนุญาตเข้า-ออก ว่ามีเจ้าหน้าที่ลงนามอนุญาตแล้วทุกครั้ง

5.2.6 เจ้าหน้าที่รักษาความปลอดภัย ต้องตรวจสอบรายการอุปกรณ์ที่ลงบันทึกไว้ในแบบฟอร์มการขออนุญาตเข้า-ออก และตรวจสอบอุปกรณ์ที่นำออกมาให้ถูกต้อง

5.2.7 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกและแบบฟอร์มการขออนุญาตเข้า-ออก กับเจ้าหน้าที่รักษาความปลอดภัยเป็นประจำทุกเดือน

ส่วนที่ 3
นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร
(Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศให้หยุดชะงักและทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 คณะ/หน่วยงาน
2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

3. ข้อกำหนดเกี่ยวกับประเภทข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

3.1 ประเภทข้อมูลของมหาวิทยาลัย แบ่งได้ดังนี้
3.1.1 ข้อมูลสารสนเทศด้านการบริหารจัดการ
- นโยบาย
- ยุทธศาสตร์
- ข้อมูลข้อมูลคำรับรองการปฏิบัติราชการ
- ข้อมูลส่วนบุคคล
- ข้อมูลงบประมาณการเงินและบัญชี

3.1.2 ข้อมูลสารสนเทศด้านการจัดการและปฏิบัติงาน
- ข้อมูลการดำเนินงานตามภารกิจของมหาวิทยาลัย
- ข้อมูลกฎ ระเบียบ คำสั่ง
- ข้อมูลการติดต่อสื่อสารภายในมหาวิทยาลัย
- ข้อมูลติดตามการดำเนินงานตามภารกิจของมหาวิทยาลัย
- ข้อมูลติดตามการใช้จ่ายงบประมาณ
- ข้อมูลรายงานผลการปฏิบัติงาน

3.1.3 ข้อมูลสารสนเทศด้านการให้บริการ
- ข้อมูลทะเบียนนิสิต นักศึกษา
- ข้อมูลใบอนุญาตและใบรับรอง
- ข้อมูลวิชาการและองค์ความรู้
- ข้อมูลด้านการวิจัย

3.2 ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล

ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

3.2.1 การกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสารกำหนดไว้ 3 ระดับ ได้แก่ ลับ ลับมาก ลับที่สุด และมีการกำหนดความรับผิดชอบให้แก่ผู้มีอำนาจกำหนดชั้นความลับ เป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

3.2.2 การควบคุมเอกสาร โดยกำหนดให้มีมาตรการควบคุมต่าง ๆ คือ การจัดทำทะเบียน การตรวจสอบ การจัดทำเอกสาร การสำเนาและการแปล การโอน การส่งและการรับ การเก็บรักษา การยืม การทำลาย การปฏิบัติในเวลาฉุกเฉิน เวลาสูญหาย รวมถึงการเปิดเผยข้อมูลในเอกสาร

3.3 เวลาที่ได้เข้าถึง (Walk in)

3.3.1 การเข้าถึงสารสนเทศในเวลาราชการ (08.30 – 16.30 น.)

3.3.2 การเข้าถึงสารสนเทศนอกเวลาราชการ (นอกช่วงเวลา 08.30 – 16.30 น.)

3.3.3 การเข้าถึงสารสนเทศในช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

3.3.4 การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึงระยะเวลาการเข้าถึง ได้แก่

- 1-3 รัน
- 1 สัปดาห์
- 1 เดือน
- 3 เดือน
- ครึ่งปีงบประมาณ
- ตามเวลาที่ร้องขอ

3.4 ช่องทางการเข้าถึง

3.4.1 ติดต่อด้วยตนเอง (เข้าถึงได้ในเวลาราชการ)

3.4.2 เคาน์เตอร์บริการ (เข้าถึงได้ในเวลาราชการ)

3.4.3 โทรศัพท์หรือโทรสาร (เข้าถึงได้ในเวลาราชการ)

3.4.4 หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในเวลาราชการ)

3.4.5 ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

3.4.6 ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

3.4.7 ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

3.4.8 เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

3.4.9 การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ และในช่วงเวลาพิเศษเป็นรายครั้ง)

4. แนวปฏิบัติในการควบคุมการเข้าถึงระบบ

4.1 สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศที่สำคัญต้องมีการควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

4.2 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทุก 6 เดือนเป็นอย่างน้อย ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

4.3 ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

4.4 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

4.5 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

5. แนวปฏิบัติการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.1 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ได้แก่ ผู้ใช้ในการขออนุญาตเข้าระบบงานนั้นจะต้องมีการทำเป็นเอกสาร เพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

5.2 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความ จำเป็นขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

5.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

6. แนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้

6.1 การลงทะเบียนเจ้าหน้าที่ใหม่ของมหาวิทยาลัย

6.1.1 จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งานสำหรับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย

6.1.2 ผู้ดูแลระบบต้องตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิ์จากเจ้าของระบบสำหรับการใช้งานระบบสารสนเทศและบริการอย่างถูกต้อง จะต้องมีการอนุมัติรับรองการได้สิทธิ์จากผู้บริหารอย่างชัดเจน

6.1.3 ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

6.1.4 ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัย

6.1.5 ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้ เพื่อแสดงถึงสิทธิและ หน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากที่ได้ทำความเข้าใจแล้ว

6.1.6 ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

6.1.7 การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

6.1.8 การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.8.1 เจ้าหน้าที่ใหม่ของมหาวิทยาลัยกรอกข้อมูลคำขอใช้บริการลงแบบฟอร์มลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.1.8.2 ยื่นคำขอกับเจ้าหน้าที่ของสำนักวิทยบริการฯ ที่ได้รับมอบหมาย เพื่อขออนุมัติจากผู้อำนวยการสำนักวิทยบริการฯ

6.2 การบริหารจัดการสิทธิ์ผู้ใช้งาน (User Management)

6.2.1 ผู้ดูแลระบบตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมดพร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบลายเซ็นของบุคคลผู้มีสิทธิ์อนุญาตในการลงทะเบียน ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

6.2.2 ผู้ดูแลระบบต้องตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

6.2.3 ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารแก่ผู้ใช้โดยให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

6.2.4 ผู้ดูแลระบบต้องกำหนดระดับสิทธิ์ในการเข้าถึงที่เหมาะสมสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

6.2.5 ผู้ดูแลระบบต้องมอบหมายสิทธิ์ให้มีความสอดคล้องกับแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

6.2.6 ผู้ดูแลระบบต้องจัดเก็บการมอบหมายสิทธิ์ให้แก่ผู้ใช้งาน

6.2.7 กรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิ์พิเศษที่ได้รับด้วยว่าการเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

6.2.8 ผู้ใช้บริการต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

6.2.9 การแจ้งยกเลิกสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศ

6.2.9.1 หัวหน้างานหรือผู้บังคับบัญชากรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการสำนักวิทยบริการฯ

6.2.9.2 ผู้ดูแลระบบยกเลิกสิทธิ์การใช้งานระบบตามคำขอในแบบฟอร์ม และลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

6.2.9.3 กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะที่เกี่ยวกับการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษรรวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

6.3 การบริหารจัดการรหัสผ่าน (Password Management)

6.3.1 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

6.3.2 ระบบบริหารจัดการรหัสผ่านต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเองและมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่ที่ตั้ง

6.3.3 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น โดยกำหนดไม่ให้ใช้ชื่อ นามสกุล วันเกิด หมายเลขโทรศัพท์ คำจากพจนานุกรม

6.3.4 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ 6 เดือน

6.3.5 ระบบบริหารจัดการรหัสผ่านต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

6.3.6 ระบบบริหารจัดการรหัสผ่านต้องสามารถระบุข้อผิดพลาดในการตั้งรหัสผ่านของผู้ใช้งานได้

6.3.7 ระบบบริหารจัดการรหัสผ่านต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน โดยต้องให้แสดงเป็นเครื่องหมายจุดหรือดอกจัน หรือสัญลักษณ์อื่น ๆ บนหน้าจอ

6.3.8 ระบบบริหารจัดการรหัสผ่านต้องมีการจัดเก็บรหัสผ่านเดิมที่ผู้ใช้งานเคยตั้งไปแล้วเพื่อตรวจสอบไม่ให้นำกลับมาใช้ใหม่ตามระยะเวลาที่เหมาะสม

6.3.9 การจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานจะต้องแยกต่างหากจากข้อมูลของระบบงาน

6.3.10 ระบบบริหารจัดการรหัสผ่านต้องป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้และ/หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากการเข้ารหัส ข้อมูล การคำนวณผลรวม (Hash) เพื่อซ่อนข้อมูลไว้

6.4 การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

6.4.1 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานระยะเวลาในการเข้าถึงช่องทางในการเข้าถึง รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

6.4.1.1 ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบงาน

6.4.1.2 ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

6.4.1.3 ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

6.4.1.4 การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะต้องได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

6.4.1.5 ต้องกำหนดการเปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

6.4.1.6 ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

6.4.2 ผู้ใช้สามารถนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 มีแนวปฏิบัติ ดังนี้

6.4.2.1 การประเมินความเสี่ยง เพื่อระบุระดับความสำคัญและระดับความลับที่เหมาะสมสำหรับข้อมูลที่จำเป็นต้องป้องกัน

6.4.2.2 กำหนดหลักการทั่วไปสำหรับการป้องกันข้อมูล โดยใช้การเข้ารหัสข้อมูล

6.4.2.3 การจัดเก็บ Username และ Password ของระบบสารสนเทศลงในฐานข้อมูลใด ๆ จะต้องทำการเข้ารหัสด้วย MD5 เป็นอย่างน้อยใน Field ของ Password ก่อนบันทึกลงในฐานข้อมูลทุกครั้ง

6.4.2.4 ต้องมีการเชื่อมต่อโดยการเข้ารหัส SSL ผ่านโปรโตคอล https สำหรับระบบสารสนเทศแบบ web application เพื่อเป็นการเข้ารหัสข้อมูลที่ส่งระหว่างบราวเซอร์ และเว็บเซิร์ฟเวอร์

6.4.2.5 กำหนดช่องทางการรับ-ส่งข้อมูลสำคัญหรือข้อมูลลับที่เหมาะสมกับมหาวิทยาลัยสำหรับช่องทาง ดังต่อไปนี้

- ระบบการสื่อสารข้อมูล ซึ่งรวมถึง LAN และอินเทอร์เน็ต
- เครือข่ายไร้สายและอุปกรณ์เครือข่ายไร้สาย
- สื่อบันทึกข้อมูลที่สามารถถอดแยกได้ (จากตัวเครื่องคอมพิวเตอร์)

6.4.2.6 กำหนดวิธีการในการบริหารจัดการและการใช้งานกุญแจสำหรับการเข้ารหัสข้อมูล ดังนี้

- วิธีการป้องกันกุญแจที่ใช้สำหรับการเข้ารหัสข้อมูล
- วิธีการกู้คืนข้อมูลที่ถูกเข้ารหัสไว้ในกรณ์ที่กุญแจเกิดการสูญหายหรือถูกทำให้เสียหาย
- บทบาทและผู้มีหน้าที่รับผิดชอบที่เกี่ยวข้องกับการเข้ารหัสข้อมูล ประกอบด้วย ผู้ทำหน้าที่ควบคุมและดูแลกุญแจ การสร้างกุญแจ ผู้ทำหน้าที่ทำลาย ผู้ใช้งาน ผู้ทำหน้าที่ จัดการกรณีกุญแจเกิดการสูญหาย

6.4.2.7 ระบุข้อมูลเกี่ยวกับการเข้ารหัสข้อมูลที่เป็นความลับหรือวิธีการรักษาความลับของข้อมูล ดังนี้

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ด้วยการใช้การเข้ารหัสข้อมูลตามมาตรฐานที่มหาวิทยาลัยกำหนด

- ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งาน โดยการกำหนดรหัสผ่านสำหรับไฟล์ที่มีการใช้งาน

- ต้องแสดงชั้นความลับบนไฟล์ข้อมูลลับ และแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

6.4.2.8 ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายของมหาวิทยาลัย เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้

6.4.2.9 ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

6.4.2.10 ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

6.4.2.11 ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

6.4.3 เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิ์ในการเข้าถึงข้อมูลอย่างน้อยปีละ 4 ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิ์ต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

6.5 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

6.5.1 ผู้ดูแลระบบต้องกำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งาน หรือใช้ระบบการกำหนดรหัสผ่านอัตโนมัติ

6.5.2 ผู้ดูแลระบบมีการกำหนดระยะเวลาการเปลี่ยนรหัสผ่าน โดยพิจารณาจากลำดับชั้นความลับของข้อมูลหรือความสำคัญตามภารกิจ และรหัสผ่านที่กำหนดใหม่ ต้องไม่ซ้ำกับรหัสผ่านเดิม

6.5.3 ผู้ใช้งานที่ได้รับรหัสผ่านในครั้งแรกหรือได้รับรหัสผ่านใหม่ ควรเปลี่ยนรหัสผ่านที่ได้รับโดยทันที

6.5.4 ผู้ใช้งานต้องกำหนดรหัสผ่านและเปลี่ยนรหัสผ่านของตนเองในการใช้งานตามหลักเกณฑ์ ซึ่งผู้ดูแลระบบกำหนด และต้องยินยอมให้ผู้ดูแลระบบดำเนินการใด ๆ เพื่อให้เกิดความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

6.5.5 ผู้ใช้งานต้องเก็บรักษารหัสผ่านให้เป็นความลับ และระมัดระวังป้องกันรหัสผ่านของตนเองในการใช้งานไม่ให้รั่วไหลไปยังผู้อื่นและไม่มอบให้ผู้อื่นนำไปใช้ไม่ว่าด้วยเหตุใด ๆ ทั้งสิ้น เว้นแต่กรณี ผู้ใช้งานที่มีอำนาจอนุมัติใด ๆ ในระบบเทคโนโลยีสารสนเทศไม่สามารถปฏิบัติราชการ อันจะเป็นเหตุให้ระบบ เทคโนโลยีสารสนเทศไม่สามารถดำเนินการต่อไปได้ให้แต่งตั้งผู้ปฏิบัติงานแทนในช่วงเวลาดังกล่าว เพื่อใช้เป็น หลักฐานในการตรวจสอบการใช้สิทธิ และหลังจากผู้ปฏิบัติงานแทนดำเนินการเรียบร้อยแล้วให้ผู้ใช้งาน ซึ่งเป็น เจ้าของรหัสผ่านทำการเปลี่ยนรหัสผ่านโดยทันที

6.5.6 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ใหญ่ ตัวพิมพ์เล็ก ตัวเลข และสัญลักษณ์เข้าด้วยกัน)

6.5.7 ไม่ควรกำหนดรหัสผ่านอย่างเป็นแบบแผน เช่น “abcdef” “aaaaaa” “12345”

6.5.8 ไม่ควรกำหนดรหัสผ่านที่เกี่ยวข้องกับผู้ใช้งาน เช่น ชื่อสกุล วัน เดือน ปีเกิด ที่อยู่

6.5.9 ไม่ควรกำหนดรหัสผ่านเป็นคำศัพท์ที่อยู่ในพจนานุกรม

6.5.10 กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ไม่เกิน 3 ครั้ง

6.5.11 ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

6.5.12 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ

6.5.13 ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

6.5.14 ในกรณีที่ไม่ใช้ระบบเทคโนโลยีสารสนเทศ ให้ผู้ใช้งานออกจากระบบ (Log off) ทันที เพื่อป้องกันบุคคลอื่นมาใช้ระบบเทคโนโลยีสารสนเทศต่อเนื่อง และหากสงสัยว่ารหัสผ่านเกิดการรั่วไหลต้องเปลี่ยนรหัสผ่านทันที

6.5.15 เมื่อผู้ใช้งานมีปัญหาในการลืมชื่อผู้ใช้งานและรหัสผ่านให้ติดต่อผู้ดูแลระบบ เพื่อดำเนินการรีเซ็ตชื่อผู้ใช้งานหรือรหัสผ่าน

6.5.16 ในกรณีการส่งมอบรหัสผ่านให้กับผู้ใช้งานแบบเอกสารต้องเป็นไปอย่างปลอดภัยโดยใส่ซองปิดผนึกและประทับตรา “ลับ” และส่งไปยังผู้ใช้งานและแนบเอกสาร “แนวปฏิบัติสำหรับการบริหารจัดการชื่อผู้ใช้งานและรหัสผ่าน” รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตาม ระเบียบดังกล่าวโดยเคร่งครัด

6.6 การใช้งานรหัสผ่าน (Password Use)

6.6.1 ผู้ใช้ต้องเก็บรหัสผ่านไว้เป็นความสับ

6.6.2 ผู้ใช้ต้องเปลี่ยนแปลงรหัสผ่านชั่วคราวทันทีที่เข้าใช้งานเป็นครั้งแรก

6.6.3 ผู้ใช้งานต้องจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย โดยหลีกเลี่ยงการบันทึกรหัสผ่านลงในกระดาษในแฟ้มข้อมูลหรือในอุปกรณ์พกพาต่าง ๆ นอกจากว่าจะเป็นการบันทึกอย่างปลอดภัยและวิธีการในการบันทึกได้รับการอนุมัติแล้ว

6.6.4 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านอย่างสม่ำเสมออย่างน้อยตามช่วงเวลาที่กำหนด หรืออย่างน้อยทุก ๆ 6 เดือน หรือขึ้นอยู่กับจำนวนการเข้าถึงระบบ (รหัสผ่านสำหรับผู้ใช้ที่ได้สิทธิ์พิเศษต้องได้รับการเปลี่ยนแปลงบ่อยกว่าปกติ)

6.6.5 ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

6.6.6 ผู้ใช้งานต้องตั้งรหัสผ่านที่มีความยาวอย่างน้อย 8 ตัวอักษรซึ่งเป็นจำนวนขั้นต่ำกำหนดไว้

6.6.7 ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

6.6.8 ผู้ใช้งานไม่ควรตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม

6.6.9 ผู้ใช้งานควรหลีกเลี่ยงการตั้งรหัสผ่านที่ไม่มีคำซ้ำหรือตัวอักษรซ้ำ ไม่ควรเป็นตัวเลขทั้งหมดหรือไม่ควรเป็นตัวอักษรทั้งหมด

6.6.10 ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

6.6.11 ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

6.6.12 ผู้ใช้งานไม่ควรกำหนดให้ทำการบันทึกรหัสผ่าน หรือกระบวนการ Login อัตโนมัติที่จดจำรหัสผ่านของตนเองไว้ เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลัง

6.6.13 ผู้ใช้งานไม่ควรใช้รหัสผ่านร่วมกับผู้อื่น

6.6.14 ไม่ใช้รหัสผ่านเดียวกันในกรณีใช้ในการปฏิบัติงานและในกรณีใช้ส่วนตัว

6.6.15 ผู้ใช้งานควรหลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ใช้งาน

6.7 การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of user access right)

6.7.1 สิทธิ์การเข้าถึงข้อมูลของผู้ใช้ต้องได้รับการพิจารณาทบทวนอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนดทุก ๆ 6 เดือน และทุกครั้งที่มีการปรับเปลี่ยนการย้ายหน่วยงานการเลื่อนตำแหน่งงาน เปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง

6.7.2 สิทธิ์การเข้าถึงข้อมูลต้องได้รับการทบทวนและจัดสรรใหม่เมื่อมีการโยกย้ายเจ้าหน้าภายในคณะ/หน่วยงาน/มหาวิทยาลัย

6.7.3 การให้อำนาจสำหรับสิทธิ์การเข้าถึงพิเศษ ต้องมีการทบทวนอย่างน้อย ทุก 3 เดือน

6.7.4 การจัดสรรสิทธิ์พิเศษต้องได้รับการตรวจสอบอย่างสม่ำเสมอตามช่วงระยะเวลาที่กำหนด เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิ์พิเศษกับผู้ใช้ที่ไม่ได้รับมอบอำนาจ

6.7.5 ความเปลี่ยนแปลงของผู้ใช้ที่ได้รับสิทธิ์พิเศษต้องถูกบันทึก เพื่อการทบทวน

6.8 การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานดูแล (Unattended user equipment)

6.8.1 ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศระบบงานเครื่องคอมพิวเตอร์ที่ใช้งานหรือเครื่องคอมพิวเตอร์พกพา โดยทันทีเมื่อเสร็จสิ้นงาน

6.8.2 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

6.8.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User name และ Password ทุกครั้ง

6.8.4 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งานประมาณ 4 - 15 นาที หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

6.8.5 มีการจำกัดระยะเวลาในการป้อนรหัสผ่าน และหากผู้ใช้งานป้อนรหัสผ่านผิดเกิน 3 ครั้ง ระบบจะทำการล็อคสิทธิ์การเข้าถึงของผู้ใช้งานทำให้ผู้ใช้งานรายนั้นไม่สามารถเข้าถึงระบบปฏิบัติการได้อีกจนกว่าผู้ดูแลระบบจะดำเนินการปลดล็อคให้

6.8.6 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

6.8.7 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันที เมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

6.8.8 ผู้ใช้งานต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแล ชั่วคราว

7. แนวปฏิบัติการเข้าถึงระบบเครือข่าย (Network access control)

7.1 ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศที่มีการใช้งานกลุ่มของผู้ใช้ และกลุ่มของระบบสารสนเทศ เช่น โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เป็นต้น เพื่อทำให้การควบคุมและป้องกันการบุกรุกสามารถทำได้อย่างเป็นระบบ

7.2 การเข้าสู่ระบบเครือข่ายภายในของมหาวิทยาลัย โดยผ่านทางอินเทอร์เน็ตหรืออินทราเน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักวิทยบริการฯ ก่อนที่จะสามารถใช้งานได้ในทุกกรณี

7.3 ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

7.4 ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

7.5 ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

7.6 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละครั้ง นอกจากนี้การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

7.7 ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกมหาวิทยาลัยควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกหรือโปรแกรมในการทำ Packet Filtering เช่น การใช้ Firewall หรือ Hardware อื่น ๆ รวมทั้งต้องมีความสามารถในการตรวจมัลแวร์ (Malware) ด้วย

7.8 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

7.9 การเข้าสู่ระบบงานเครือข่ายภายในมหาวิทยาลัย โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการลงชื่อเข้าใช้งาน (Login) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

7.10 IP Address ภายในของระบบงานเครือข่ายภายในของมหาวิทยาลัยจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

7.11 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

7.12 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

7.13 การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักวิทยบริการฯ เท่านั้น

8. แนวปฏิบัติการบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

8.1 ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

8.2 ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

8.3 ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ Telnet Ftp หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้ว ต้องมีมาตรการป้องกันเพิ่มเติมด้วย

8.4 ควรดำเนินการติดตั้งอัพเดตระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น Web Server เป็นต้น

8.5 ควรมีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

8.6 การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการ โดยเจ้าหน้าที่สำนักวิทยบริการฯ เท่านั้น

9. แนวปฏิบัติการบริหารจัดการการบันทึกและตรวจสอบ

9.1 ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่ายบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบบันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้ อย่างน้อย 3 เดือน โดยในการบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (audit logging) ควรมีการบันทึกพฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

(1) ข้อมูลชื่อบัญชีผู้ใช้งาน
(2) ข้อมูลวันเวลาที่เข้าถึงระบบ
(3) ข้อมูลวันเวลาที่ออกจากระบบ
(4) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
(5) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
(6) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
(7) ข้อมูลการเปลี่ยนคอนฟิเกูเรชั่นของระบบ
(8) ข้อมูลแสดงการใช้งานแอพพลิเคชั่น
(9) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำการเปิด ปิด เขียน อ่านไฟล์
(10) ข้อมูลไอพีแอดเดรสที่เข้าถึง
(11) ข้อมูลโปรโตคอลเครือข่ายที่ใช้
(12) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
(13) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

9.2 ต้องจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของมหาวิทยาลัย เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้งานและต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้องตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 และประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. 2550 และเพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ให้ปฏิบัติดังต่อไปนี้

(1) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

(2) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (IT auditor) หรือบุคคลที่หน่วยงานมอบหมาย

(3) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

9.3 ควรมีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

9.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

10. แนวปฏิบัติการควบคุมการเข้าใช้งานระบบจากภายนอกสำนักวิทยบริการฯ

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกโดยมีแนวทางปฏิบัติ ดังนี้

10.1 การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยก่อให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของมหาวิทยาลัยการควบคุมบุคคลที่เข้าสู่ระบบของมหาวิทยาลัยจากระยะไกล จึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

10.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักวิทยบริการฯ ก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

10.3 ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

10.4 ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

10.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิด Port และ Modem ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็นช่องทางดังกล่าวควรตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

11. แนวปฏิบัติการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication For External Connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

11.1 ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

11.2 ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ดหรือการใช้ USB token ที่มีความสามารถ PKI

11.3 ต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบสารสนเทศของหน่วยงานอย่างน้อย 1 วิธี

11.4 ผู้ใช้งานที่ทำการเชื่อมต่อจากภายนอกมหาวิทยาลัยต้องทำการเข้ารหัสข้อมูลในการเข้าถึงระบบพิสูจน์ตัวตนจากระยะไกลผ่านระบบ VPN (Virtual Private Network) ของมหาวิทยาลัย

11.5 การเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ตให้มีการตรวจสอบผู้ใช้งานด้วย

12. การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear desk and clear screen policy)

ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูลและแฟ้มข้อมูล เครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วง ระบบสารสนเทศและข้อมูลสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานมีแนวทางปฏิบัติ ดังนี้

12.1 ผู้ใช้งานต้องป้องกันทรัพย์สินของมหาวิทยาลัยและควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย โดยให้ครอบคลุมเรื่องต่าง ๆ ประกอบด้วย

- การจัดทำบริเวณล้อมรอบ (Physical Security Perimeter)
- การควบคุมการเข้าออกพื้นที่ (Physical Entry Control)
- การจัดบริเวณสำหรับการเข้าถึง และส่งมอบผลิตภัณฑ์โดยบุคคลภายนอก (Public Access Delivery and loading area)
- การจัดวางและการป้องกันอุปกรณ์ (Equipment sitting and protection)
- ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

12.2 การป้องกันต้องมีความสอดคล้องกับเรื่องต่าง ๆ ดังนี้

- แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ
- กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ
- วัฒนธรรมองค์กร

12.3 ต้องมีการป้องกันเครื่องคอมพิวเตอร์หรือระบบงานของมหาวิทยาลัยก่อนเข้าใช้งาน โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสม

12.4 ต้องมีการกำหนดขอบเขตของการป้องกัน ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใด ๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย

- จัดเก็บเอกสาร ข้อมูลในการทำงาน ข้อมูลสำคัญหรือลับหรือสื่อบันทึกข้อมูลไว้ในสถานที่ที่มีความปลอดภัยภายหลังจากใช้งานเสร็จ

- ลงชื่อออกจากระบบทันทีเมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

- ล็อคเครื่องคอมพิวเตอร์เมื่อไม่ได้ใช้งาน

- ป้องกันเครื่องโทรสารที่ใช้ในการติดต่อสื่อสารหรือล่งข้อมูลสำคัญเมื่อไม่มีผู้ใช้งาน

- ป้องกันตู้ หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

- นำเอกสารสำคัญหรือลับออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

- ในกรณีที่ต้องการนำทรัพย์สินสารสนเทศต่าง ๆ เช่น เอกสาร สื่อบันทึก คอมพิวเตอร์ หรือสารสนเทศออกจากคณะ/หน่วยงาน/มหาวิทยาลัย ต้องขออนุมัติจากผู้บังคับบัญชา ก่อนทุกครั้ง

12.5 ผู้ดูแลระบบต้องจัดทำบัญชีทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสาร โดยระบุผู้รับผิดชอบในทรัพย์สินอย่างชัดเจน

12.6 ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่ใช้สำหรับการให้บริการระบบคอมพิวเตอร์และระบบเครือข่ายหลักของมหาวิทยาลัย เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้หรือสูญหาย

12.7 ผู้ดูแลระบบต้องเก็บรักษาอุปกรณ์ของระบบคอมพิวเตอร์และระบบเครือข่ายในพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารและอนุญาตให้เข้าถึงได้เฉพาะผู้ดูแลระบบเท่านั้น

ส่วนที่ 4
นโยบายการควบคุมหน่วยงานภายนอกเข้าถึงระบบเทคโนโลยีสารสนเทศ
(Third Party Access Control Policy)

1. วัตถุประสงค์

การใช้บริการจากหน่วยภายนอกอาจก่อให้เกิดความเสี่ยงได้ เช่น ความเสี่ยงต่อการเข้าถึงข้อมูล ความเสี่ยงต่อการถูกแก้ไขข้อมูลอย่างไม่ถูกต้อง และการประมวลผลของระบบงานโดยไม่ได้รับอนุญาต เป็นต้น เพื่อให้การควบคุมหน่วยงานภายนอกที่มีการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยให้เป็นไปอย่างมั่นคงปลอดภัยและกำหนดแนวทางในการคัดเลือกควบคุมการปฏิบัติงานของหน่วยงานภายนอก เช่น การพัฒนาระบบการใช้บริการของที่ปรึกษา การใช้บริการด้านระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก เป็นต้น

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ /เจ้าหน้าที่ที่ได้รับมอบหมาย

3. แนวปฏิบัติทั่วไป

3.1 ผู้อำนวยการสำนักวิทยบริการฯ ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหลักหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

3.2 คณบดี/ผู้อำนวยการ/หัวหน้าหน่วยงาน ต้องกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศหลักหรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศของคณะ/หน่วยงานได้

3.3 หน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากมหาวิทยาลัย/คณะ/หน่วยงานของมหาวิทยาลัย โดยจะต้องแจ้งรายชื่อผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศล่วงหน้ามายังมหาวิทยาลัย/คณะ/หน่วยงานดังกล่าวก่อนการดำเนินงานในกรณีที่มีการเปลี่ยนแปลงรายชื่อหน่วยงานภายนอกจะต้องแจ้งล่วงหน้าก่อนทุกครั้ง

3.4 ในการเข้าปฏิบัติงานภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หน่วยงานภายนอกจะต้องบันทึกรายละเอียดตามเอกสารแบบฟอร์มที่มหาวิทยาลัยจัดไว้ให้โดยต้องระบุเหตุผลความจำเป็นที่ต้องเข้าใช้งานระบบเทคโนโลยีสารสนเทศ ซึ่งต้องมีรายละเอียดอย่างน้อย ดังนี้

3.4.1 เหตุผลในการขอใช้

3.4.2 ระยะเวลาในการใช้

3.4.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

3.4.4 การตรวจสอบ MAC Address ของเครื่องคอมพิวเตอร์ที่เชื่อมต่อ

3.4.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

3.5 หน่วยงานภายนอกที่ทำงานให้กับมหาวิทยาลัย/คณะ/หน่วยงานของมหาวิทยาลัยไม่ว่าจะทำงานอยู่ภายในหรือนอกสถานที่จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัย โดยสัญญาต้องจัดทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบเทคโนโลยีสารสนเทศ

3.6 เจ้าของโครงการ ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอกต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านี้นและให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล

3.7 สำหรับโครงการขนาดใหญ่ หน่วยงานภายนอกที่สามารถเข้าถึงข้อมูลที่มีความสำคัญของมหาวิทยาลัย ผู้บริหาร/ผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความมั่นคงปลอดภัย ทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentially) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

3.8 มหาวิทยาลัยมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น

3.9 หน่วยงานภายนอกต้องจัดทำแผนการดำเนินงาน คู่มือการปฏิบัติงานและเอกสารที่เกี่ยวข้อง รวมทั้งมีการปรับปรุงให้ทันสมัยอยู่เสมอเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการได้อย่างเข้มงวด เพื่อให้มั่นใจได้ว่าเป็นไปตามขอบเขตที่ได้กำหนดไว้

3.10 ทุกครั้งที่จะทำการแก้ไขค่า Config ของอุปกรณ์ทุกชนิดภายในห้องปฏิบัติการเครือข่าย คอมพิวเตอร์ของมหาวิทยาลัย หน่วยงานภายนอกจะต้องทำการสำรองค่า Config เดิมไว้ก่อน รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้น ไม่สามารถใช้งานได้ตามต้องการจะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมาให้สามารถใช้งานได้ตามสภาพเดิม

3.11 ทุกครั้งที่มีการแก้ไขหรือเปลี่ยนแปลงค่า Config ระบบงานสารสนเทศหรือเปลี่ยนแปลงโครงสร้างฐานข้อมูล หน่วยงานภายนอกจะต้องทำการสำรองโปรแกรม/โมดูลหรือฐานข้อมูลเดิมที่มีการแก้ไข รวมทั้งจัดทำบันทึกรายละเอียดการแก้ไขทุกครั้ง หากการแก้ไขมีปัญหาเกิดขึ้นไม่สามารถใช้งานได้ตามต้องการจะต้องทำการเรียกข้อมูลที่ได้ทำการสำรองไว้กลับมาให้ใช้งานได้

3.12 ในกรณีที่หน่วยงานภายนอกจะเข้ามาปฏิบัติงานที่ห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยในวันหยุดหรือนอกเวลาราชการ จะต้องขอความเห็นชอบจากผู้รับผิดชอบหรือ ผู้ดูแลระบบของมหาวิทยาลัยล่วงหน้าก่อนทุกครั้งและการดำเนินงานทุกครั้งจะต้องอยู่ในความดูแลของผู้รับผิดชอบหรือผู้ดูแลระบบของมหาวิทยาลัย

1.13 หากหน่วยงานภายนอกจะทำการเชื่อมต่อจากภายนอกเข้ามายังระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยจะต้องแจ้งให้ผู้รับผิดชอบหรือผู้ดูแลระบบของมหาวิทยาลัยทราบล่วงหน้าก่อนทุกครั้ง ซึ่งจะต้องระบุวัน เวลา ระยะเวลาในการทำงานให้ชัดเจน

3.14 ในกรณีที่เจ้าหน้าที่ของหน่วยงานภายนอกประมาท ทำให้อุปกรณ์และระบบสารสนเทศของมหาวิทยาลัยได้รับความเสียหายหรือสูญหาย หน่วยงานภายนอกนั้นจะต้องรับผิดชอบในการซ่อมแซมแก้ไขหรือเปลี่ยนใหม่ให้อยู่ในสภาพที่สามารถใช้งานได้ดังเดิม

ส่วนที่ 5
นโยบายการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย
(Network Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเครือข่ายและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบสารสนเทศของมหาวิทยาลัย โดยมีการกำหนดนโยบายและแนวปฏิบัติควบคุมการเข้าใช้งานเครือข่ายที่แตกต่างกันของกลุ่มเครือข่ายต่าง ๆ ตามการแบ่งแยกเครือข่ายเป็น VLAN

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ /เจ้าหน้าที่ที่ได้รับมอบหมาย

3. แนวปฏิบัติการควบคุมการเข้าถึงและใช้บริการระบบเครือข่าย

3.1 การใช้งานบริการเครือข่าย

3.1.1 ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือ ศีลธรรมอันดีแห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของมหาวิทยาลัย

3.1.2 มหาวิทยาลัยไม่อนุญาตให้ผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย เช่น การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้าหรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไป เพื่อแสวงหากำไร

3.1.3 ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลง หรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหายถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว มหาวิทยาลัยไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

3.1.4 ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุก เข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

3.1.5 มหาวิทยาลัยให้บัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอนหรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

3.1.6 บัญชีผู้ใช้งาน (User Account) ที่มหาวิทยาลัยให้คับผู้ใช้งานนั้น ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3.1.7 ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

3.1.8 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา/สำนักวิทยบริการฯ

3.1.9 ห้ามเปิดหรือใช้งานโปรแกรมออนไลน์ทุกประเภท เพื่อความบันเทิงในระหว่างปฏิบัติงาน

3.2 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่ายและเจ้าหน้าที่ผู้รับผิดชอบมีแนวทางปฏิบัติ ดังนี้

3.2.1 ผู้ดูแลระบบห้องปฏิบัติการระบบเครือข่ายต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องปฏิบัติการระบบเครือข่ายโดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ และเจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

3.2.2 สิทธิ์ในการเข้า-ออกห้องต่าง ๆ ภายในห้องปฏิบัติการระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับการอนุมัติจากผู้บริหารเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายห้องปฏิบัติการระบบเครือข่าย

3.2.3 ต้องจัดทำระบบเก็บบันทึกการเข้า-ออก ตามกระบวนการที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.2.4 กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำมีความจำเป็นต้องเข้า-ออกห้องปฏิบัติการระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

3.2.5 การเข้าถึงห้องปฏิบัติการระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.3 ผู้ติดต่อจากหน่วยงานภายนอกมีแนวทางปฏิบัติดังนี้

3.3.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคนต้องทำการลงบันทึกข้อมูลลงในสมุดบันทึกตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่”

3.3.2 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานภายในคณะ/หน่วยงาน/มหาวิทยาลัย มาปฏิบัติงานที่ห้องปฏิบัติการระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า-ออก ตามที่ระบุไว้ในเอกสาร “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องชัดเจน

3.3.3 เจ้าหน้าที่ควรตรวจสอบความถูกต้องของข้อมูลในสมุดบันทึกเป็นประจำ

3.4 การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks)

3.4.1 ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

3.4.2 กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอก ต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

3.4.3 อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

3.4.4 ผู้ขอใช้บริการต้องทำหนังสือเป็นลายลักษณ์อักษรถึงผู้อำนวยการสำนักวิทยบริการฯ เรื่อง “การขอเชื่อมต่อเครือข่าย” และต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับขั้น

3.5 การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection)

3.5.1 บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใด ๆ ในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์จะต้องลงชื่อเข้า-ออกใน “แบบฟอร์มการเข้า-ออกพื้นที่” ให้ถูกต้องและได้รับการอนุมัติจากผู้บริหารก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

3.5.2 บุคคลภายนอกเข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่าย หรือบริหารจัดการผ่านระบบเครือข่ายต้องได้รับการอนุมัติจากผู้บังคับบัญชาตามลำดับขั้น

3.5.3 ผู้ดูแลระบบต้องกำหนดการเปิด-ปิด พอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่าง ๆ โดยจะปิดพอร์ตที่เสี่ยงที่จะก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์

3.5.4 ต้องยกเลิกหรือปิดพอร์ตและบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

3.5.5 ทำการควบคุมการเข้าถึงพอร์ตที่ใช้ลำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบทั้งทางกายภาพ และโดยการล็อกอินเข้ามาใช้งาน

3.5.6 ทำการล็อคอุปกรณ์เครือข่ายที่ใช้ลำหรับการปรับแต่งค่าคอนฟิกกูเรชันด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

3.5.7 ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ 2 ครั้ง

3.6 การแบ่งแยกเครือข่าย (segregation in networks)

3.6.1 มหาวิทยาลัยแบ่งแยกเครือข่ายเป็นเครือข่ายย่อย ๆ ตามอาคารต่าง ๆ เพื่อควบคุมการเข้าถึงเครือข่าย โดยไม่ได้รับอนุญาต

3.6.2 มหาวิทยาลัยจัดแบ่งเครือข่ายภายในและเครือข่ายภายนอก เพื่อความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารโดยคณะ/หน่วยงาน ของมหาวิทยาลัยสามารถใช้งานระบบผ่านระบบเครือข่ายภายในได้ แต่ไม่สามารถใช้งานระบบผ่านเครือข่ายภายนอกได้ เพื่อความปลอดภัยของฐานข้อมูล

3.6.3 มหาวิทยาลัยทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการผู้ใช้งานและระบบงานต่าง ๆ ของมหาวิทยาลัย

3.6.4 ผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่งจะไม่สามารถเข้าถึงข้อมูลที่อยู่ในอีกวง เครือข่ายหนึ่งได้โดยตรง

3.6.5 มีการควบคุมการเข้าถึงทางกายภาพสำหรับเครือข่ายย่อย เพื่อป้องกันการเข้าถึงทางกายภาพต่อเครือข่ายย่อยและป้องกันการเปลี่ยนแปลงแก้ไขสายสัญญาณ ดักแอบดูข้อมูลบน เครือข่าย หรืออื่น ๆ โดยไม่ได้รับอนุญาต

3.6.6 มีการใช้ไฟร์วอลล์กั้นหรือแบ่งเครือข่ายภายในออกเป็นเครือข่ายย่อย ๆ

3.6.7 มีการกรองและจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อย

3.6.8 มีการใช้เกตเวย์ เพื่อควบคุมการเข้าถึงเครือข่าย ทั้งจากภายในและภายนอกมหาวิทยาลัย ซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของ มหาวิทยาลัย

3.6.9 มีการแยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่น ๆ ของมหาวิทยาลัย

3.6.10 มีการแยกกลุ่มเครือข่ายเป็น 4 ประเภทใหญ่ ๆ คือ

(1) ระบบเครือข่ายภายใน

(2) ระบบเครือข่ายภายนอก

(3) ส่วนที่มีความสำคัญสูง (DMZ Zone (Demilitarized Zone)) ที่เชื่อมต่อทั้งเครือข่ายภายในและเครือข่ายภายนอก

(4) เครือข่ายสำหรับติดตั้งระบบงานสารสนเทศต่าง ๆ ของมหาวิทยาลัย

3.6.11 มีการจัดทำผังเครือข่ายที่แสดงถึงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก โดยมีการปรับปรุงให้เป็นปัจจุบันหรืออย่างน้อยปีละครั้ง

3.7 การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

3.7.1 มีการตรวจสอบการเชื่อมต่อเครือข่าย

3.7.2 จำกัดสิทธิ ความสามารถของผู้ใช้ในการเชื่อมต่อเข้าสู่เครือข่าย

3.7.3 ระบุอุปกรณ์ เครื่องมือที่ใช้ควบคุมการเชื่อมต่อเครือข่าย

3.7.4 มีระบบการตรวจจับผู้บุกรุกทั้งระดับเครือข่ายและระดับเครื่องคอมพิวเตอร์แม่ข่าย

3.7.5 ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

3.8 การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่าน หรือไหลเวียนของข้อมูลหรือสารสนเทศ สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการ ประยุกต์ใช้งานตามภารกิจ ดังนี้

3.8.1 ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

3.8.2 กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

3.8.3 กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย สามารถเชื่อมเครือข่าย ปลายทางผ่านทางที่กำหนดไว้หรือจำกัดสิทธิในการใช้บริการเครือข่าย

3.8.4 มีการใช้เกตเวย์หรืออุปกรณ์เครือข่ายเพื่อตรวจสอบ IP Address ของทั้งต้นทางและปลายทางและควบคุมการไหลของข้อมูลผ่านเครือข่ายต่าง ๆ จากเครือข่ายหนึ่ง ไปยังอีกเครือข่ายหนึ่ง

3.8.5 มีการกำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

3.8.6 จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้งานบริการสามารถใช้เส้นทางอื่น ๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

3.8.7 มีการกาหนดมาตรการการบังคับใช้เส้นทางเครือข่ายให้สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้หรือจำกัดสิทธิ์ในการเข้าใช้บริการระบบเครือข่ายของมหาวิทยาลัย

ส่วนที่ 6
นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

(Operating System Access Control)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการรวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. ผู้รับผิดชอบ

2.1 ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย
2.3 ผู้ใช้งาน

3. แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

3.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

3.2 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานบริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

3.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ User และ Password ทุกครั้ง

3.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน

3.5 ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

3.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

3.7 ซอฟต์แวร์ลิขสิทธิ์ของมหาวิทยาลัย ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานงานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

3.8 ซอฟต์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็น ห้ามมิให้ผู้ใช้งานงานทำการติดตั้งถอดถอนเปลี่ยนแปลง แก้ไข หรือทำสำเนา เพื่อนำไปใช้งานที่อื่น

3.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

3.10 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

3.11 ห้ามผู้ใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

4. แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจง ซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสม เพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

4.1 มีการตั้งชื่อบัญชีผู้ใช้งานในระบบงานที่แตกต่างกันระหว่างบัญชีของผู้ใช้งานทั่วไป บัญชีของผู้ดูแลระบบบัญชีของผู้ดูแลฐานข้อมูล บัญชีของผู้พัฒนา ระบบบัญชีของเจ้าหน้าที่ทางเทคนิคอื่น ๆ

4.2 ผู้ใช้งานทุกคนต้องมีชื่อผู้ใช้งานแยกจากกันของแต่ละบุคคล เพื่อใช้ในการพิสูจน์ตัวตนที่แตกต่างกัน

4.3 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยโดยใช้ชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบหากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

4.4 ผู้ใช้งานสำหรับระบบงานที่มีความสำคัญสูงต้องทำการพิสูจน์ตัวตนด้วยวิธีการทางเทคนิคที่มีความมั่นคงปลอดภัยสูงโดยใช้วิธีการเข้ารหัสข้อมูล วิธีการทางชีวภาพโดยใช้การสแกน ลายนิ้วมือ เรตินา ฝ่า มือ เสียง

4.5 ผู้ใช้งานที่สามารถเข้าถึงระบบปฏิบัติการได้ จะต้องได้รับการอนุมัติสิทธิ์การเข้าถึงระบบปฏิบัติการจากผู้บังคับบัญชาของหน่วยงานหรือเจ้าของระบบงานเท่านั้น

4.6 ผู้ใช้งาน ที่เป็นเจ้าของบัญชีผู้ใช้ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

4.7 ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้ (Account) ไว้เป็นความลับ และห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่ายหรือจ่ายแจกให้ผู้อื่น

4.8 ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

5. แนวปฏิบัติการใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of System utilities)

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทยูทิลิตี้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำาหนดไว้หรือที่มีอยู่แล้ว โดยมีแนวทางปฏิบัติ ดังนี้

5.1 มีการจัดทำบัญชีรายชื่อโปรแกรมประเภทยูทิลิตี้ที่อนุญาตให้ใช้งานได้เท่านั้น

5.2 มีการจำกัดผู้ที่สามารถใช้งานโปรแกรมยูทิลิตี้และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้

5.3 ผู้ใช้งานที่ต้องการใช้งานโปรแกรมยูทิลิตี้ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบพร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องมีการลงนามเห็นชอบจาก ผู้บังคับบัญชาของผู้ใช้งานอย่างเป็นลายลักษณ์อักษร

5.4 การใช้งานโปรแกรมยูทิลิตี้จะต้องได้รับอนุญาตให้ใช้งานตามระดับสิทธิ์ในการใช้งานที่มหาวิทยาลัยกำหนดไว้แล้วโดยจะได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้เป็นรายครั้งไป

5.5 จำเป็นต้องทำการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ทุกครั้ง แม้จะเป็นการใช้งานเพียงชั่วคราว

5.6 มีการแยกจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน เช่น แยกไว้ในไดเร็คทอรี่ต่างหา กเพื่อให้ง่ายในการควบคุมและจัดการโปรแกรมเหล่านี้

5.7 มีการบันทึกข้อมูลล็อกแสดงการใช้งานโปรแกรมยูทิลิตี้

5.8 มีการยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้ที่ไม่มีความจำเป็นในการใช้งานแล้ว

5.9 ต้องทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

5.10 มีการกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมยูทิลิตี้ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้ เพื่อจำกัดและควบคุมการใช้งาน

5.11 ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

5.12 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

5.13 ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

6. แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

6.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงาน อุปกรณ์เครือข่าย เป็นต้น มีการตัดและหมดเวลาการใช้งาน รวมถึงปิดการใช้งานด้วยหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 10 นาที

6.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการล้างหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 10 นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

6.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการตัดและหมดเวลาการใช้งานที่สั้นขึ้นสำหรับระบบเทคโนโลยีสารสนเทศที่มีความเสี่ยงสูง ทางด้านระบบงบประมาณการเงิน ระบบงานเงินเดือน เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

6.4 กำหนดให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย สำหรับระบบที่มีความสำคัญสูงจะต้องมีการตัดและหมดเวลาการใช้งาน โดยมีกาหนดให้ไม่เกิน 1 ชั่วโมงต่อการพิสูจน์ตัวตนเข้าใช้งาน

6.5 ต้องมีการระบุและพิสูจน์ตัวตน เพื่อเข้าใช้งานระบบเทคโนโลยีสารสนเทศอีกครั้งหลังจากที่ระบบได้หมดเวลาการใช้งานไปแล้ว

ส่วนที่ 7
นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(Application Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้อนุญาตเข้าถึงระบบสารสนเทศของมหาวิทยาลัย และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ที่จะสร้าง ความเสียหายแก่ข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

2.3 ผู้ใช้งาน

3. แนวปฏิบัติการจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

3.1 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนเจ้าหน้าที่ใหม่ของมหาวิทยาลัย ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงาน ภายในหน่วยงาน เป็นต้น

3.2 ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-mail) ระบบอินเทอร์เน็ต (Internet) ระบบเครือข่ายไร้สาย (Wireless LAN) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

3.3 ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

3.1.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

3.3.2 ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัยควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

3.3.3 กำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

3.3.4 กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

3.3.5 กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

3.3.6 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที

เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

3.4 เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ มหาวิทยาลัยควรกำหนดช่องทางการเข้าถึงระบบเทคโนโลยีสารสนเทศที่สำคัญที่มหาวิทยาลัยพัฒนาในรูปแบบของ Web base Application โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน ซึ่งสามารถใช้งานได้เฉพาะสำนักงานที่เป็นจุดเชื่อมโยงเครือข่ายดังกล่าว

3.5 เพื่อรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงานเพื่อส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน

3.6 ผู้ดูแลระบบต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยมีวิธีการปฏิบัติดังนี้

3.6.1 ผู้ดูแลระบบต้องป้องกันการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วงโดยไม่ได้รับอนุญาต

3.6.2 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบ โดยกำหนดขั้นตอนและแบบฟอร์มการใช้งานระบบคอมพิวเตอร์ประกอบด้วยรายละเอียดอย่างน้อย ดังนี้ ชื่อผู้ใช้บริการ เหตุผลในการขอใช้ระยะเวลาในการใช้บริการ

3.6.3 ผู้ดูแลระบบต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

3.6.4 เจ้าของข้อมูลหรือเจ้าของระบบต้องกำหนดรายการข้อมูลสำหรับการให้บริการประกอบ ด้วยรายละเอียดอย่างน้อย ดังนี้ ประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึงเวลาที่ได้เข้าถึงและช่องทางการเข้าถึง เป็นต้น

3.6.5 เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับลำหรับข้อมูลสำคัญในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้บริการและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ควรกำหนดระยะเวลาการใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การรับล่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(5) ควรเปลี่ยนรหัสผ่านของข้อมูลหรือระบบที่มีลำดับความสำคัญตามระยะเวลาที่กำหนด

3.7 มีการใช้เมนู เพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

3.8 มีการลงทะเบียนผู้ใช้งาน เพื่อควบคุม จำกัดหรือให้สิทธิ์การเข้าถึงข้อมูลและฟังก์ชันต่าง ๆ ของระบบงาน โดยให้สอดคล้องกับนโยบายควบคุมการเข้าถึงที่ได้กำหนดไว้

3.9 มีการควบคุมหรือจำกัดสิทธิ์การเข้าถึงระบบงานซึ่งถูกเข้าถึงจากอีกระบบงานหนึ่ง โดยควบคุมให้สามารถเข้าถึงได้เฉพาะข้อมูลและฟังก์ชันต่าง ๆ ที่จำเป็นต้องใช้งานเท่านั้น

3.10 มีการควบคุมหรือจำกัดการนำข้อมูลออกจากระบบงาน เพื่อให้สามารถเข้าถึงได้เฉพาะข้อมูลที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานเท่านั้น

3.11 มีการแสดงเฉพาะข้อมูลพื้นฐาน เพื่อให้ผู้ใช้งานได้รับทราบข้อมูลที่จำเป็นเท่านั้น

3.12 มีการแสดงรายละเอียดเท่าที่จำเป็นของระบบงาน หลังจากที่ล็อกอินเสร็จแล้ว

3.13 มีข้อความแสดงเตือน ห้ามผู้ไม่มีสิทธิ์เข้าถึงระบบงาน

3.14 มีข้อจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ

3.15 มีการตรวจสอบข้อมูลการล็อกอิน หลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบล้วนแล้ว

3.16 มีข้อจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งาน ในลักษณะที่เปิดเผยข้อมูลภายในของระบบงาน

3.17 มีการจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด

3.18 มีการกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบงานได้ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

3.19 มีการส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง

3.20 มีการบันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

3.21 มีการจำกัดช่วงระยะเวลาที่นานที่สุดที่ผู้ใช้งานจะต้องล็อกอินเข้าใช้งานให้สำเร็จ

3.22 มีการแสดงวันเวลาของการล็อกอินครั้งที่แล้ว (ทั้งที่สำเร็จและไม่สำเร็จ)

4. แนวปฏิบัติการจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of Connection Time)

4.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศมีการจำกัดระยะเวลาการเชื่อมต่อสำหรับการใช้งาน เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยกำหนดให้ใช้งานได้ 1 ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้งกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของสำนักงานตามปกติเท่านั้น

4.2 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่สาธารณะหรือพื้นที่ภายนอกมหาวิทยาลัยที่มีความเสี่ยงมีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

4.3 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่ต้องมีการจำกัดช่วงระยะเวลาการใช้งานมีการระบุและพิสูจน์ตัวตนเพื่อเข้าใช้งานใหม่ตามช่วงระยะเวลาที่กำหนดไว้ทุก ๆ 1 ชั่วโมง

5. แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน (Sensitive System isolation)

ระบบซึ่งไวต่อการรบกวนมีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ได้แก่ ระบบ MIS ระบบบริการการศึกษา ระบบทะเบียน ระบบ GFMIS หรือระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์เป็นระบบที่ใช้ในการปฏิบัติงานด้านการงบประมาณการบัญชี การจัดซื้อจัดจ้าง การเบิกจ่าย และการบริหารทรัพยากรดูแลรับผิดชอบโดยกรมบัญชีกลางจะต้องดำเนินการ ดังนี้

5.1 ต้องมีการระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวนหรือมีผลกระทบสูงต่อมหาวิทยาลัย

5.2 ต้องแยกระบบ ซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบงานอื่น ๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัยหรือแยกเครือข่ายโดยใช้วิธีการทางเทคนิค VLAN

5.3 ทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์แม่ข่ายเครื่องหนึ่งต่างหาก

5.4 มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกันระหว่างระบบงานที่มีความสำคัญสูงกับระบบงานอื่น ๆ ที่มีความสำคัญน้อยกว่า

5.5 มีการควบคุมสภาพแวดล้อมของระบบดังกล่าวโดยเฉพาะ

5.6 ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile Computing and Teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

5.7 ทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอกตามข้อกำหนดที่ตั้งค่าไว้ใน Firewall

6. แนวปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ผู้ดูแลระบบต้องกำหนดมาตรการควบคุมการปฏิบัติงานของผู้ปฏิบัติงานจากระยะไกล รวมถึงการเตรียมการระบบเทคโนโลยีสารสนเทศที่เกี่ยวข้อง เพื่อให้มีความมั่นคงปลอดภัยเพียงพอ โดยมีแนวทางปฏิบัติดังนี้

6.1 มีแผนและขั้นตอนการปฏิบัติงานสำหรับเจ้าหน้าที่ของมหาวิทยาลัยที่จำเป็นต้องปฏิบัติงานของมหาวิทยาลัยจากภายนอกหรือจากระยะไกล

6.2 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิ์การเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการ ปฏิบัติงาน

6.3 ผู้ใช้งานระบบจากระยะไกล ต้องได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของระบบงานอย่างเป็นทางการและต้องใช้งานตามระยะเวลาการเข้าถึงที่กำหนดไว้

6.4 ผู้ใช้งานระบบจากระยะไกล ต้องทำการพิสูจน์ตัวตนก่อนเข้าใช้งาน

6.5 มีข้อกำหนดเฉพาะสำหรับการปฏิบัติงานจากระยะไกล ดังนี้

- ชนิดของงานที่อนุญาตและไม่อนุญาตสำหรับการปฏิบัติงานจากระยะไกล
- ระบบงานหรือบริการต่าง ๆ ที่อนุญาตให้เข้าถึงได้จากระยะไกล
- ชั่วโมงหรือช่วงระยะเวลาการปฏิบัติงาน
- ขั้นความลับของข้อมูลที่อนุญาตให้เข้าถึงได้

6.6 มีการควบคุมทางกายภาพที่จำเป็นสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

6.7 มีการป้องกันข้อมูลสำหรับการสื่อสารระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลกับระบบงานต่าง ๆ ภายในมหาวิทยาลัย

6.8 มีการกำหนดระดับความสำคัญของข้อมูลที่จะมีการรับส่งหรือสื่อสารกันระหว่างมหาวิทยาลัยกับสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

6.9 ไม่อนุญาตให้ครอบครัวหรือเพื่อนของผู้ปฏิบัติงานจากระยะไกลเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลของมหาวิทยาลัย

6.10 มีการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล รวมทั้งมาตรการควบคุมการใช้บริการเครือข่ายไร้สายจากที่บ้าน ทั้งนี้เพื่อป้องกันการเข้าถึงระบบหรือข้อมูลของมหาวิทยาลัยโดยไม่ได้รับอนุญาต

6.11 มีการป้องกันทรัพย์สินทางปัญญาที่เกิดขึ้นจากการปฏิบัติงานจากระยะไกล เพื่อป้องกันการโต้แย้งกันว่าใครเป็นเจ้าของทรัพย์สินทางปัญญานั้น

6.12 มีการสงวนสิทธิ์ในการเข้าถึงอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล

6.13 มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

6.14 มีการติดตั้งซอฟต์แวร์พื้นฐานที่จำเป็นในอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล

6.15 มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับการจัดเก็บข้อมูล และอุปกรณ์สื่อสาร

6.16 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล ถ้าอุปกรณ์ตังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยมหาวิทยาลัย

6.17 มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่าง ๆ ที่ใช้งานจากระยะไกล

6.18 มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

6.19 มีการตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

7. การป้องกันอุปกรณ์สื่อสารประเภทพกพา (Mobile computing and communication)

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน แท็ปเล็ต รวมทั้งกำหนดมาตรการการใช้งานอย่างปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

7.1 มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ ประเภทพกพา

7.2 สร้างความตระหนัก เพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพาในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกมหาวิทยาลัย

7.3 ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ ๆ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

7.4 ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือลับในอุปกรณ์ ๆ

7.5 สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์อย่างสม่ำเสมอ

7.6 มีการควบคุมการเข้าถึงระบบงานของมหาวิทยาลัยจากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ ประเภทพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ

7.7 มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของมหาวิทยาลัย จากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา สมาร์ทโฟน แท็ปเล็ต

7.8 มีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของมหาวิทยาลัย

7.9 ผู้ติดต่อจากหน่วยงานภายนอกที่น่าอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาตเข้า - ออกพื้นที่ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

7.10 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกันว่าเป็นพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless Area)

ส่วนที่ 8
นโยบายการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล
(Use of Personal Computer Policy)

1. วัตถุประสงค์

ข้อกำหนดมาตรฐานการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลนี้ได้ถูกจัดทำขึ้น เพื่อช่วยให้ผู้ใช้ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและผู้ใช้ควรทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด เพื่อป้องกันทรัพยากรและข้อมูลที่มีค่าของมหาวิทยาลัยให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 คณะ/หน่วยงาน
2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย
2.4 ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

3.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัยต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อสิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือน่าไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

3.3 ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัย

3.4 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) ส่วนบุคคลจะต้องกำหนดโดยเจ้าหน้าที่ของมหาวิทยาลัยเท่านั้น

3.5 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของคณะ/หน่วยงาน/มหาวิทยาลัยเท่านั้น

3.6 ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ควรมีการตรวจสอบ เพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

3.7 ไม่ควรเก็บข้อมูลสำคัญของมหาวิทยาลัยไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

3.8 ไม่ควรสร้าง Short-cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของมหาวิทยาลัย

3.9 ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์ โดยควรปฏิบัติดังนี้

3.9.1 ไม่ควรนำอาหารหรือเครื่องดื่มอยู่ใกล้บริเวณเครื่องคอมพิวเตอร์

3.9.2 ไม่ควรวางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ Disk Drive

4. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

4.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

4.2 ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

4.3 ในระหว่างเวลาพักกลางวันและหลังเลิกงานผู้ใช้งานควร Logout ออกจากเครื่องคอมพิวเตอร์หรือล็อคหน้าจอด้วยโปรแกรม Screen Saver เมื่อไม่มีการใช้งานโดยตั้งเวลาประมาณ 10 นาที

4.4 มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

5. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานควรปฏิบัติตามแนวทางการใช้รหัสผ่านตามส่วนที่ 3 ข้อ 6.6 การใช้งานรหัสผ่าน (Password User)

6. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

6.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการเว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ

6.2 ผู้ใช้งานมีหน้าที่รับผิดชอบในการติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

6.3 ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Floppy Disk Thumb Drive และ Data Storage อื่น ๆ ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

6.4 ผู้ใช้งานควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

6.5 ผู้ใช้งานควรตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลงหรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

7. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

7.1 ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Hard Disk เป็นต้น

7.2 ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

7.3 ผู้ใช้งานควรประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงานเพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของมหาวิทยาลัย

ส่วนที่ 9
นโยบายการใช้งานเครื่องคอมพิวเตอร์แบบพกพา
(Use of Notebook Computer Policy)

1. วัตถุประสงค์

เพื่อสร้างความมั่นคงปลอดภัยสำหรับอุปกรณ์เครื่องคอมพิวเตอร์แบบพกพาและการนำไปปฏิบัติงานภายนอกมหาวิทยาลัย เพื่อเป็นการป้องกันข้อมูลและอุปกรณ์ของมหาวิทยาลัยให้เกิดความปลอดภัยผู้ใช้จึงควรรับทราบถึงข้อกำหนดและมาตรฐานในการใช้งานการบำรุงรักษาและสิ่งที่ควรหลีกเลี่ยงในการใช้เครื่องคอมพิวเตอร์แบบพกพาให้มีประสิทธิภาพสูงสุด

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 คณะ/หน่วยงาน
2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย
2.4 ผู้ใช้งาน

3. แนวปฏิบัติทั่วไป

3.1 เครื่องคอมพิวเตอร์แบบพกพาที่มหาวิทยาลัยอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้จึงควรใช้งานเครื่องคอมพิวเตอร์แบบพกพาอย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

3.2 โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของมหาวิทยาลัยต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อสิขสิทธิ์ถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ที่ไม่ใช่ของมหาวิทยาลัย หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งาน โดยผิดกฎหมาย

3.3 การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer name) แบบพกพาจะต้องกำหนดโดยเจ้าหน้าที่ของมหาวิทยาลัยเท่านั้น

3.4 การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบพกพาตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ได้รับมอบหมายจากคณะ/หน่วยงานเท่านั้น

3.5 ผู้ใช้ควรศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียด เพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

3.6 ไม่ดัดแปลงแก้ไขส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ และรักษาสภาพของคอมพิวเตอร์ให้มีสภาพเดิม

3.7 ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

3.8 ไม่ควรใส่เครื่องคอมพิวเตอร์แบบพกพาไปในกระเป๋าเดินทางที่เสียงต่อการถูกกดทับโดยไม่ได้ตั้งใจจากการมีของหนักทับบนเครื่องหรืออาจถูกจับโยนได้

3.9 การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

3.10 หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกา กดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

3.11 ไม่ควรวางของทับบนหน้าจอและแป้นพิมพ์

3.12 การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

3.13 ไม่ควรเคลื่อนย้ายเครื่องในขณะที่ Hard Disk กำลังทำงาน

3.14 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ เครื่องดื่มต่าง ๆ เป็นต้น

3.15 ไม่ควรใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพา ควรอยู่ในสภาพแวดล้อมที่มีอุณหภูมิสูงกว่า 34 องศาเซลเซียส

3.16 ไม่ควรวางเครื่องคอมพิวเตอร์แบบพกพาไว้ใกล้อุปกรณ์ที่มีสนามแม่เหล็กไฟฟ้าแรงสูงในระยะใกล้ เช่น แม่เหล็ก โทรทัศน์ ไมโครเวฟ ตู้เย็น เป็นต้น

3.17 ไม่ควรติดตั้งหรือวางคอมพิวเตอร์แบบพกพาในที่มีการสั่นสะเทือน เช่น ในยานพาหนะที่กำลังเคลื่อนที่ เป็นต้น

3.18 การเช็ดทำความสะอาดหน้าจอภาพควรเช็ดอย่างเบามือที่สุดและควรเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวน เพราะจำทำให้หน้าจอมีรอยขีดข่วนได้

4. แนวปฏิบัติการป้องกันความปลอดภัยทางด้านกายภาพ

4.1 ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

4.2 ผู้ใช้งานไม่ควรเก็บหรือใช้งานคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูงและต้องระวังป้องกันการตกกระทบ

4.3 ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

5. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

5.1 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

5.2 ผู้ใช้งานควรกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ใน “การใช้งานรหัสผ่าน” ในนโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

5.3 ผู้ใช้ควรตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ 10 นาที ให้ทำการล็อคหน้าจอเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่าน

5.4 ผู้ใช้ต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

6. แนวปฏิบัติในการใช้รหัสผ่าน

ให้ผู้ใช้งานควรปฏิบัติตามแนวทางการใช้รหัสผ่านตามส่วนที่ 3 ข้อ 6.6 การใช้งานรหัสผ่าน (Password User)

7. แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

7.1 ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการเว็บบราวเซอร์ และโปรแกรมการใช้งานต่าง ๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์เป็นการป้องกันการโจมดี จากภัยคุกคามต่าง ๆ

7.2 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกระบบการป้องกันไวรัสที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์แบบพกพา

7.3 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์แบบพกพาติดชุดคำสั่งไม่พึงประสงค์ (Malware) ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องเข้ากับระบบเครือข่าย เพื่อป้องกันการแพร่กระจายของชุดคำสั่งที่ไม่พึงประสงค์ไปยังเครื่องอื่น ๆ ได้

8. แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

8.1 ผู้ใช้งานควรทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพา โดยวิธีการและสื่อต่าง ๆ เพื่อป้องกันการสูญหายของข้อมูล

8.2 ผู้ใช้งานควรจะเก็บรักษาสื่อสำรองข้อมูล (Backup Media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

8.3 แผ่นสื่อสำรองข้อมูลต่าง ๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

8.4 แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วควรทำลายไม่ให้สามารถนำไปใช้งานได้อีก

ส่วนที่ 10
นโยบายการใช้งานอินเทอร์เน็ต
(Internet Security Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้งานรับทราบกฎเกณฑ์แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัยและเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่งหรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุขทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัยถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 คณะ/หน่วยงาน
2.3 ผู้ดูแลระบบ /เจ้าหน้าที่ที่ได้รับมอบหมาย
2.4 ผู้ใช้งาน

3. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

3.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น เช่น Proxy Firewall IPS/IDS เป็นต้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการสำนักวิทยบริการฯ เป็นลายลักษณ์อักษรแล้ว

3.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์พกพาก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการที่เว็บบราวเซอร์ติดตั้งอยู่

3.3 ในการรับ-ส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับ-ส่งข้อมูลทุกครั้ง

3.4 ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

3.5 ผู้ใช้งานจะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย

3.6 ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

3.7 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

3.8 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จอันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรอันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

3.9 ผู้ใช้งานไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัด ต่อ เติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูก ดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย3.10 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บน อินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

3.11 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึง Patch หรือ Fixes ต่าง ๆ จากผู้ชายต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

3.12 ในการเสนอความคิดเห็นผ่านเว็บบอร์ด (Web board) ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัยและต้องไม่ใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยการทำลายความสัมพันธ์กับเจ้าหน้าที่ของคณะ/หน่วยงานอื่น ๆ

3.13 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้วให้ทำการปิดเว็บบราวเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

ส่วนที่ 11
นโยบายการใช้งานจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

1. วัตถุประสงค์

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ตผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิ์หรือกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัดจะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 ผู้ดูแลระบบ

2.3 ผู้ใช้งาน

3. แนวปฏิบัติในการส่งจดหมายอิเล็กทรอนิกส์

3.1 ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

3.2 ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

3.3 สำหรับผู้ใช้งานงานรายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) ในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นระบบจะต้องมีการบังคับให้เปลี่ยนรหัสผ่านโดยทันที

3.4 รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้นเช่น ‘*’ หรือ ‘o’ ในการพิมพ์แต่ละตัวอักษร

3.5 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

3.6 ผู้ดูแลระบบควรกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ควรมีการล็อกเอาท์ออกจากหน้าจอตัดการใช้งานผู้ใช้เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น 15 นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้งานและรหัสผ่านอีกครั้ง

3.7 ผู้ใช้งานไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

3.8 ผู้ใช้งานงานควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน

3.9 ผู้ใช้งานงานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัย หรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย

3.10 ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่น เพื่ออ่านรับ-ส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

3.11 ผู้ใช้งานงานควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อการทำงานของมหาวิทยาลัยเท่านั้น

3.12 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นควรทำการล็อกเอาท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

3.13 ผู้ใช้งานงานควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น

3.14 ผู้ใช้งานไม่ควรเปิด หรือส่งต่อจดหมายอิเล็กทรอนิกส์ หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

3.15 ผู้ใช้งานไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์

3.16 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

3.17 ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

3.18 ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

3.19 ข้อควรระวังผู้ใช้งานไม่ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ส่วนที่ 12
ข้อตกลงการใช้บริการจดหมายอิเล็กทรอนิกส์
(Terms of Use and Disclaimer)

1. วัตถุประสงค์

1.1 เพื่อให้การรับส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยสามารถสนับสนุนการปฏิบัติงานของมหาวิทยาลัยเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ

1.2 เพื่อให้การติดต่อสื่อสารโดยการรับ-ส่งข้อมูลข่าวสารด้วยระบบจดหมายอิเล็กทรอนิกส์สำหรับเจ้าหน้าที่ของมหาวิทยาลัย คณะ/หน่วยงาน เป็นมาตรฐานอยู่ในกรอบของกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ และมาตรการรักษาความปลอดภัยข้อมูลข่าวสารของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

2. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

2.1 ผู้ใช้บริการระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยจะต้องไม่กระทำการอันละเมิดต่อกฎหมาย ระเบียบ คำสั่ง ข้อบังคับ คำแนะนำ อย่างน้อยดังต่อไปนี้

2.1.1 พระราชบัญญัติกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

2.1.2 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560

2.1.3 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

2.1.4 พระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ. 2540

2.1.5 ระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

2.1.6 ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติ พ.ศ. 2417

2.1.7 ระเบียบว่าด้วยการรักษาความปลอดภัยแห่งชาติเกี่ยวกับการสื่อสาร พ.ศ. 2424

2.1.8 ข้อตกลงเงื่อนไขการใช้บริการที่มหาวิทยาลัยกำหนด

3. ข้อตกลงและเงื่อนไขการใช้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

3.1 คณะ/หน่วยงาน/เจ้าหน้าที่/ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยจะต้องใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อผลประโยชน์ของทางราชการ

3.2 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อการประกอบธุรกิจหรือแสวงหาผลประโยชน์ส่วนตน

3.3 ห้ามใช้บริการนี้ไปในการเผยแพร่ อ้างอิง พาดพิง ดูหมิ่น หรือการกระทำใด ๆ ที่ก่อให้เกิดความเสียหายต่อสถาบัน ชาติ ศาสนา และพระมหากษัตริย์

3.4 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยในการประกอบอาชญากรรมทางคอมพิวเตอร์ หรือการกระทำการใด ๆ ซึ่งผิดกฎหมาย คำสั่ง ระเบียบ ข้อบังคับ และมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารลับของทางราชการ

3.5 ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อการเผยแพร่ข้อมูลข่าวสารหรือภาพเสียง ข้อความ ที่ไม่เหมาะสมหรือสร้างความเสื่อมเสียให้กับผู้อื่น

3.6 ห้ามใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ไปแสดงข้อคิดเห็นส่วนตัวที่ส่งผลกระทบในทางลบหรือสร้างความเสื่อมเสียหรือเสียหายต่อบุคคลหรือมหาวิทยาลัย

3.7 ห้ามกระทำการปลอมแปลงที่อยู่เป็นบุคคลอื่น (Impersonation)

3.8 ห้ามกระทำการที่สร้างปัญหาการใช้ทรัพยากรของระบบ เช่น

(1) การสร้างจดหมายลูกโซ่ (Chain Mail)

(2) การส่งจดหมายจำนวนมาก (Spam Mail)

(3) การส่งจดหมายต่อเนื่อง (Letter Bomb)

(4) การส่งจดหมายเพื่อการแพร่กระจายไวรัสคอมพิวเตอร์

3.9 ห้ามผู้ใช้บริการกระทำการใด ๆ ที่อาจจะนำมาซึ่งความเสื่อมเสียหรือก่อให้เกิดความเสียหายแก่ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

3.10 ผู้ใช้ต้องรักษารหัสผ่าน (Password) ส่วนบุคคล หรือหน่วยงานของจดหมายอิเล็กทรอนิกส์เป็นไว้เป็นความลับ

3.11 ห้ามส่งข้อมูลข่าวสารอันเป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานที่ไม่เกี่ยวข้องกับราชการของมหาวิทยาลัย

3.12 การส่งข้อมูลข่าวสารที่เป็นความลับของทางราชการให้กับบุคคลหรือหน่วยงานนอกมหาวิทยาลัยจะต้องเข้ารหัสข้อมูลข่าวสารนั้นตามวิธีปฏิบัติและมาตรการรักษาความปลอดภัยข้อมูล ข่าวสารตามที่มหาวิทยาลัยกำหนด

3.13 ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail address) และรหัสผ่าน (Password) ของหน่วยหรือบุคคลจะต้องเก็บรักษาไว้เป็นความลับหากสงสัยว่ารั่วไหลจะต้องดำเนินการเปลี่ยนรหัสผ่านทันที โดยรหัสผ่านจะต้องกำหนดให้ยากแก่การคาดเดา (Strong Password)

3.14 ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ มหาวิทยาลัยหรือผู้รับผิดชอบที่อยู่จดหมายอิเล็กทรอนิกส์จะต้องศึกษาคู่มือการใช้งาน ระเบียบปฏิบัติ คำแนะนำ และข้อตกลงเงื่อนไขให้เข้าใจ เพื่อใช้งานจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยได้อย่างถูกต้อง

3.15 กรณีได้รับการร้องเรียน ร้องขอ หรือพบเหตุอันไม่ชอบด้วยกฎหมายขอสงวนสิทธิ์ที่จะทำการยกเลิกหรือระงับบริการแก่ผู้ใช้บริการนั้น ๆ เป็นการชั่วคราวเพื่อทำการสอบสวนและตรวจสอบหาสาเหตุของมูลเหตุนั้น ๆ โดยไม่จำเป็นต้องแจ้งล่วงหน้า

3.16 การกระทำใด ๆ ที่เกี่ยวกับการเผยแพร่ทั้งในรูปแบบของอีเมล์ และ/หรือโฮมเพจของผู้ใช้บริการให้ถือเป็นการกระทำที่อยู่ภายใต้ความรับผิดชอบของผู้ใช้งานมหาวิทยาลัยไม่มีส่วนเกี่ยวข้องใด ๆ

ส่วนที่ 13
นโยบายการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของมหาวิทยาลัย โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงานรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

3. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

3.1 ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่ายของมหาวิทยาลัยจึงจะสามารถใช้งานระบบเครือข่ายไร้สายนี้ได้กรณีที่มหาวิทยาลัยมีนโยบายในการใช้ชื่อผู้ใช้กลางให้ผู้ใช้งานติดต่อเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ เพื่อรับค่า SSID (Service Set Identifier) และ Network Key ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่ายไร้สาย

3.2 ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับ-ส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

3.3 ผู้ดูแลระบบต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณให้ดีขึ้น

3.4 ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจากผู้ผลิตทันทีที่นำ AP มาใช้งาน

3.5 ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อ Login และรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและผู้ดูแลระบบต้องเลือกใช้ชื่อ Login และรหัสผ่านที่มีการคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

3.6 ผู้ดูแลระบบต้องกำหนดค่าใช้ WPA หรือ WPA2 ในการเข้ารหัสหรือข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากขึ้น

3.7 ผู้ดูแลระบบต้องจะมีการติดตั้ง Firewall ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

3.8 ผู้ดูแลระบบต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

3.9 ในการใช้งานเครือข่ายไร้สายผู้ใช้งานต้องปฏิบัติตามนโยบายความปลอดภัยระบบเทคโนโลยีสารสนเทศอย่างเคร่งครัดทางมหาวิทยาลัยสงวนสิทธิ์ในการยกเลิกสิทธิ์ในการเข้าใช้เครือข่ายไร้สาย โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

ส่วนที่ 14
นโยบายการป้องกันไวรัส และซอฟต์แวร์ไม่พึงประสงค์
(Virus and Malicious Software Protection Policy)

1. วัตถุประสงค์

เพื่อควบคุมและป้องกันซอฟต์แวร์และข้อมูลของมหาวิทยาลัยจากซอฟต์แวร์อันตรายหรือไวรัสคอมพิวเตอร์

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ /เจ้าหน้าที่ที่ได้รับมอบหมาย

2.4 ผู้ใช้งาน

3. แนวปฏิบัติในการป้องกันไวรัสและซอฟต์แวร์ที่ไม่ประสงค์ดี

3.1 ก่อนนำซอฟต์แวร์จากภายนอกมาใช้งานภายในมหาวิทยาลัยผู้ใช้งานต้องทำการตรวจสอบซอฟแวร์ดังกล่าวให้แน่ใจว่าซอฟต์แวร์นั้น ๆ ไม่มีไวรัสคอมพิวเตอร์หรือซอฟต์แวร์อันตรายแฝงอยู่

3.2 ผู้ดูแลระบบต้องจัดให้มีการติดตั้งโปรแกรมป้องกันไวรัสเวอร์ชั่นล่าสุดในระดับระบบปฏิบัติการบนเครื่องคอมพิวเตอร์และเครื่องเซิร์ฟเวอร์

3.3 ผู้ดูแลระบบต้องกำหนดให้โปรแกรมต้นหาไวรัสทำงานพร้อมกันกับการเริ่มทำงานของระบบประมวลผล และโปรแกรมดังกล่าวต้องทำงานในขณะที่มีการใช้ระบบด้วย นอกจากนี้ผู้ดูแลระบบต้องมีการปรับปรุงโปรแกรมป้องกันไวรัสให้ทันสมัยอยู่เสมอ

3.4 ผู้ดูแลระบบต้องทำการตรวจทานระบบข้อมูล เพื่อตรวจหาไวรัสและซอฟต์แวร์อันตรายอยู่เป็นประจำ

3.5 ผู้ใช้งานต้องตรวจหาไวรัสของไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตก่อนนำไปใช้งาน

3.6 ห้ามมิให้เจ้าหน้าที่ดำเนินการใด ๆ ที่เกี่ยวกับการพัฒนาไวรัสหรือซอฟต์แวร์อันตรายหรือเก็บไว้เป็นเจ้าของ

3.7 ในกรณีที่มีการนำสื่อบันทึกข้อมูลจากหน่วยงานภายนอกมหาวิทยาลัยมาใช้ผู้ใช้งานสื่อข้อมูลนั้น ต้องตรวจสอบไวรัสคอมพิวเตอร์ก่อนใช้งานทุกครั้ง

ส่วนที่ 15
นโยบายการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก
(Firewall & IPS Policy)

1. วัตถุประสงค์

เพื่อควบคุมการใช้งานเครือข่าย และกรองแพ็คเก็จที่ผ่านเข้ามาในระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ

3. แนวปฏิบัติในการป้องกันระบบเครือข่ายและตรวจจับการบุกรุก

3.1 อนุญาตเฉพาะบริการเครือข่ายที่จำเป็นต่อการใช้งานบริการเครือข่ายอื่น ๆ ที่เหลือปิดให้หมด

3.2 ไม่อนุญาตให้สแกน เพื่อตรวจสอบเครือข่ายด้วยโปรแกรมประเภท Network Scanning Tools เช่น NMAP เป็นต้น

3.3 ปิดบริการรวมทั้งซอฟต์แวร์ที่ไม่จำเป็นบนไฟร์วอลล์

3.4 จำกัดบริการเครือข่ายที่ทำงานบนไฟร์วอลล์ให้มีน้อยที่สุด โดยให้แยกบริการอื่น ๆ เหล่านั้นไปทำงานบนเครื่องอื่น

3.5 จำกัดชื่อบัญชีผู้ใช้งานบนเครื่องไฟร์วอลล์ให้มีน้อยที่สุดและไม่รันไฟร์วอลล์ โดยใช้ชื่อบัญชีผู้ใช้งานที่เป็น Root หรือ Administrator

3.6 เปลี่ยนรหัสผ่านสำหรับ Root หรือ Administrator ที่ผู้ขายกำหนดมาให้เป็นรหัสอื่นที่ยากต่อการเดา

3.7 ควรใช้ไฟร์วอลล์หลายชนิดรวมกัน เช่น ไฟร์วอลล์แบบกรองแพ็คเก็จ ไฟร์วอลล์แบบพร็อกซี่ เพื่อเป็นการเสริมความมั่นคงปลอดภัยในแง่มุมที่ต่างกัน

3.8 ควรใช้ระบบอื่นทำงานรวมกับไฟร์วอลล์ ได้แก่ ระบบป้องกันการบุกรุก (IPS) ไฟร์วอลล์ส่วนตัว (Personal Firewall) โปรแกรมป้องกันไวรัส (Antivirus) โปรแกรมกรองอีเมลและกรองเว็บ (Anti-Spam) ซึ่งเป็นการเสริมการรักษาความมั่นคงปลอดภัยภาพรวมได้สูงขึ้น

3.9 กำหนดกฎในไพร์วอลล์ให้กรองทิ้งแพ็คเก็จที่ไม่ประสงค์ดีตามรายการช่องโหว่ที่แพร่ระบาดอยู่ในปัจจุบันเสมอ

3.10 ป้องกันการเข้าถึงทางกายภาพต่อไฟร์วอลล์ให้มีความแข็งแกร่ง เช่น จัดทำเป็นห้องที่มีการควบคุมการเข้า-ออกอย่างเข้มงวด เป็นต้น

3.11 หมั่นตรวจสอบกฎของไฟร์วอลล์ เพื่อการจัดกฎที่ไม่มีความจำเป็นทิ้งไป เพื่อเพิ่มประสิทธิภาพของการประมวลผลกฎที่กำหนดไว้ของไฟร์วอลล์

3.12 เมื่อเพิ่มกฎข้อใหม่เข้าไปในไฟร์วอลล์ตรวจสอบว่ากฎที่ใส่เข้าไปนั้นไม่ขัดแย้งกับกฎที่มีอยู่แล้วเดิม รวมทั้งทดสอบด้วยว่าไฟร์วอลล์สามารถป้องกันได้จริงตามกฎข้อใหม่นั้น

3.13 ตรวจสอบว่ากฎที่กำหนดไว้บนไฟร์วอลล์ไม่มีข้อใดขัดแย้งกับนโยบายความมั่นคงปลอดภัยของมหาวิทยาลัยอย่างน้อยควรทำปีละครั้ง

3.14 ไม่อนุญาตให้เขาถึงไฟร์วอลล์จากทางไกลโดยโปรแกรมประเภท Telnet หรือแม้แต่ SSH โดยการเข้าถึงให้ทำได้จากตัวเครื่องไฟร์วอลล์โดยตรง

3.15 สร้างความแข็งแกร่งให้กับระบบปฏิบัติการของไฟร์วอลล์ โดยการ Update Patch อยู่เสมอ

3.16 ตรวจสอบและติดตั้งโปรแกรมอุดช่องโหว่สำหรับระบบปฏิบัติการของไฟร์วอลล์อย่างสม่ำเสมอ

3.17 ก่อนการอัพเกรด หรือแก้ไขช่องโหว่ของไฟร์วอลล์ให้ทำสำรองข้อมูลแบบ Full Backup ของเครื่องไฟร์วอลล์นั้นเก็บไว้ก่อน หากมีปัญหาจะได้นำกลับมาติดตั้งและใช้งานได้อย่างรวดเร็ว

3.18 ใช้ไฟร์วอลล์รวมกับเราท์เตอร์ เพื่อป้องกันปัญหา DoS (Denial of Service) และปัญหาการเจาะระบบเข้าสู่ไฟร์วอลล์ได้โดยตรง

3.19 ใช้ไฟร์วอลล์ เพื่อกั้นเครือข่ายภายในในกรณีที่มีความจำเป็น เช่น เครือข่ายส่วนนั้น อนุญาตให้เฉพาะผู้ใช้ที่มีสิทธิเท่านั้นในการเข้าถึง เป็นต้น

3.20 บันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์เก็บไว้รวมทั้งหากไฟร์วอลล์มีขีดความสามารถในการแจ้งเตือนให้เปิดใช้ขีดความสามารถนี้ด้วย

3.21 ใช้เซิร์ฟเวอร์ เช่น Syslog แยกต่างหากอีกเครื่องหนึ่งจากเครื่องของไฟร์วอลล์ เพื่อเก็บบันทึกข้อมูล Log ของการเข้าถึงไฟร์วอลล์ไว้บนเซิร์ฟเวอร์นั้น ซึ่งจะทำให้การเปลี่ยนแปลงแก้ไขข้อมูล Log โดยผู้บุกรุกทำได้ยากขึ้น

3.22 หากหน่วยงานอื่นต้องการนำระบบขึ้นจะต้องทำเป็นหนังสือผ่านผู้อำนวยการสำนักวิทยบริการฯ เพื่อแจ้งเจ้าหน้าที่ให้ดำเนินการเป็นกรณีไป

ส่วนที่ 16
นโยบายการสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

1. วัตถุประสงค์

เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลเสียหายหรือถูกทำลายจากไวรัสคอมพิวเตอร์ ผู้บุกรุกทำลายหรือเปลี่ยนแปลงข้อมูล โดยสามารถนำข้อมูลที่มีปัญหากลับมาใช้งานได้

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

2.4 ผู้ใช้งาน

3. การสำรองข้อมูลและระบบคอมพิวเตอร์

ผู้ดูแลระบบหรือคณะทำงานที่เกี่ยวข้องจะต้องระบุแนวปฏิบัติสำหรับการจัดทำระบบสำรองข้อมูลที่ชัดเจน เพื่อให้ระบบสารสนเทศอยู่ในสภาพพร้อมใช้อยู่เสมอ โดยมีวิธีการปฏิบัติดังนี้

3.1 กำหนดหน้าที่และความรับผิดชอบของเจ้าหน้าที่ ซึ่งดูแลรับผิดชอบระบบสารสนเทศและระบบสำรองข้อมูลของมหาวิทยาลัย

3.2 ผู้ดูแลระบบต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการจัดทำระบบสำรองข้อมูลและสารสนเทศของมหาวิทยาลัย

3.3 ทำการพิจารณาคัดเลือกระบบสารสนเทศที่จำเป็นต้องจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้ตามลำดับความสำคัญ

3.4 ระบบที่จะทำการสำรองข้อมูลต้องเป็นระบบที่มีความสำคัญต่อภารกิจของมหาวิทยาลัย

3.5 มีการกำหนดประเภทของข้อมูลที่ต้องทำสำรองเก็บไว้ และความถี่ในการสำรอง

3.6 จัดทำแผนการสำรองที่เหมาะสมกับความสำคัญของแต่ละระบบสารสนเทศ

3.7 ดำเนินการตามกระบวนการสำรองข้อมูลสำหรับแต่ละระบบสารสนเทศโดยเคร่งครัด

3.8 มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูล

3.9 การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก ฯลฯ

3.10 มีขั้นตอนปฏิบัติในการสำรองข้อมูลและคู้คืนข้อมูลแยกตามระบบสารสนเทศแต่ละระบบอย่างถูกต้องทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ

3.11 การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้นรวมทั้งวิธีการที่ใช้แก้ไขด้วย

3.12 ให้มีการมอบหมายเจ้าหน้าที่สำรอง เพื่อทำหน้าที่สำรองข้อมูลในกรณีที่ผู้ดูแลระบบไม่สามารถปฏิบัติงานได้

3.13 ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุให้ไม่สามารถดำเนินการได้อย่างสมบูรณ์ ให้ดำเนินการแก้ไขปัญหา สรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชาทราบ

3.14 ให้ผู้ดูแลระบบกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Back up) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

3.15 ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูล (Encrypted backup) ในการสำรองข้อมูลที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

3.16 ผู้ดูแลระบบต้องปฏิบัติตามขั้นตอนปฏิบัติ (Backup Procedure) ตามนโยบายที่เกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) โดยเคร่งครัด

4. การปฏิบัติเกี่ยวกับการสำรองข้อมูล มีวิธีการปฏิบัติดังนี้

4.1 ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติหรือทำการสำรองข้อมูลของระบบ ซึ่งอยู่ในความรับผิดชอบของตนเองตาม โดยจะใช้วิธีสำรองข้อมูลแบบ Full Backup ตามความถี่ดังนี้

(1) Web Servers: สำรองข้อมูลเผยแพร่บนเว็บไซต์ 1 ครั้งต่อเดือน

(2) Database Servers: สำรองข้อมูลในฐานข้อมูลของระบบที่สำคัญ 1 ครั้งต่อสัปดาห์

(3) Firewall Server: สำรองข้อมูล Rule ของ Firewall 1 ครั้งต่อเดือน

(4) Server อื่น ๆ : สำรองข้อมูลบนเซิร์ฟเวอร์อื่น ๆ เช่น ระบบงานต่าง ๆ 1 ครั้งต่อเดือน

4.2 ผู้ดูแลระบบต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการสำรองข้อมูลตามรายละเอียดข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

4.3 หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใดเป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

4.4 ผู้ดูแลระบบต้องทำการทดสอบคู่ข้อมูลสำรองในทุกระบบ โดยต้องมีการทดสอบอย่างน้อยปีละ 1 ครั้ง ซึ่งการทดสอบกังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริงแต่ทดสอบบนระบบทดสอบ

4.4 ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ของมหาวิทยาลัยและเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลของมหาวิทยาลัย โดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

5.การทดสอบและการกู้คืนระบบ

มหาวิทยาลัยต้องกำหนดแผนการทดสอบกู้คืนข้อมูลตามชนิดของการสำรองข้อมูลที่กำหนดไว้แล้ว เพื่อให้ระบบสารสนเทศมีสภาพพร้อมใช้งานอยู่เสมอ โดยมีวิธีการปฏิบัติดังนี้

5.1 ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทาให้ต้องกู้คืนระบบ ผู้ดูแลระบบจะต้องดำเนินการแก้ไข พร้อมทั้งรายงานผลการแก้ไข บันทึก และสรุปผลการปฏิบัติงานต่อผู้บังคับบัญชาหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาทราบ

5.2 การกู้คืนระบบ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม

5.3 หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้ระบบทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

5.4 กำหนดให้มีการทดสอบและปรับปรุงแผนการกู้คืนระบบ อย่างน้อยปีละ 1 ครั้ง

6. การกู้คืนข้อมูล

เพื่อให้การพินฟูระบบ/ข้อมูลจากความเสียหายที่อาจเกิดขึ้นจากการหยุดทำงานของการประมวลโปรแกรม (Hang) หรือไฟฟ้าดับ ตลอดจนเหตุการณ์อื่นใดซึ่งส่งผลต่อเครื่องคอมพิวเตอร์หรือการประมวลผลของคอมพิวเตอร์หยุดทำงานอย่างกะทันหัน หรือเปลี่ยนการทำงานไปจากเดิมทำให้ไม่สามารถบันทึกข้อมูลได้ทันเวลาหรือไม่สามารถใช้งานคอมพิวเตอร์ได้ตามปกติมีมาตรการในการกู้คืนข้อมูล ดังนี้

6.1 ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

6.2 ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์/อุปกรณ์และการติดตั้งซอฟต์แวร์ใหม่ เพื่อทดแทนของเดิมที่เสียหาย

6.3 ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุน เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

7. แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการ ด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งาน ตามภารกิจ ตามแนวทางต่อไปนี้

7.1 มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อยดังนี้

7.1.1 มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

7.1.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประห้วงทำให้ไม่ สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

7.1.3 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

7.1.4 มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

7.1.5 มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เป็นต้น เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

7.1.6 การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

7.1.7 มีการทบทวน เพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ 1 ครั้ง

ส่วนที่ 17
นโยบายด้านการปฏิบัติตามข้อบังคับ
(Compliance Policy)

1. วัตถุประสงค์

การปฏิบัติตามข้อบังคับด้านกฎหมาย เพื่อลดความเสี่ยงที่เกิดจากการละเมิดข้อบังคับทางกฎหมายที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย การที่มหาวิทยาลัยทราบถึงข้อกำหนดต่าง ๆ ที่เกี่ยวข้องจะสามารถทำให้เจ้าหน้าที่ความตระหนักถึงความเสี่ยงที่เกิดขึ้นรวมทั้งวางมาตรการควบคุมที่เหมาะสมได้ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นจากการละเมิดดังกล่าว

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
2.2 กลุ่มงานนิติการ กองการเจ้าหน้าที่
2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย
2.4 ผู้ใช้งาน

3. แนวปฏิบัติในการปฏิบัติตามข้อบังคับ

3.1 การปฏิบัติตามข้อบังคับด้านกฎหมาย บรรดากฎหมายใด ๆ ที่ได้ประกาศใช้ในประเทศไทยถือเป็นสิ่งสำคัญที่ผู้ใช้งานคอมพิวเตอร์จะต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้นหากผู้ใช้งานคอมพิวเตอร์กระทำผิดตามกฎหมายดังกล่าว มหาวิทยาลัยถือว่าความผิดนั้นเป็นความผิดส่วนบุคคล

3.2 การปกป้องข้อมูลส่วนบุคคล

3.2.1 ข้อมูลรายละเอียดที่เกี่ยวกับการดำเนินงานของมหาวิทยาลัยถือว่าเป็นข้อมูลที่มีความสำคัญ เฉพาะเจ้าหน้าที่ที่ได้รับมอบหมายตามหน้าที่งานหรือได้รับอนุญาตจากผู้บริหารเท่านั้น ที่สามารถเปลี่ยนแปลงแก้ไขข้อมูลดังกล่าวได้

3.2.2 ข้อมูลส่วนตัวของเจ้าหน้าที่ถือว่าเป็นข้อมูลลับและสามารถเปิดเผยได้เฉพาะผู้ที่มีสิทธิ์ เช่น เจ้าหน้าที่เองหรือผู้ทำงานที่มีความเกี่ยวข้องเท่านั้น อย่างไรก็ดีมหาวิทยาลัยสงวนสิทธิ์ในการเข้าถึงข้อมูลทั้งหมดที่สร้างและเก็บอยู่ในระบบสารสนเทศของมหาวิทยาลัย เป็นต้น

3.3 ลิขสิทธิ์ซอฟต์แวร์

3.3.1 ห้ามมิให้เจ้าหน้าที่นำซอฟต์แวร์ภายนอกมาใช้ในระบบประมวลผลของมหาวิทยาลัย โดยมิได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในคณะ/หน่วยงาน ทั้งนี้ผู้บังคับบัญชาต้องสอบทานกับสำนักวิทยบริการฯ ในเรื่องลิขสิทธิ์ของมหาวิทยาลัยและความเสี่ยง ด้านความปลอดภัยสารสนเทศในการนำซอฟต์แวร์ดังกล่าวมาใช้ตามลำดับ

3.3.2 เจ้าหน้าที่ต้องไม่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่มหาวิทยาลัยได้จัดซื้อลิขสิทธิ์ เพื่อการใช้งาน ยกเว้นการทำสำเนานั้นเพียงแต่เพื่อไว้ใช้สำหรับเหตุฉุกเฉินหรือเพื่อเป็นสำเนาไว้ใช้แทนซอฟต์แวร์ต้นฉบับเท่านั้น

3.3.3 ซอฟต์แวร์ที่พัฒนาภายในมหาวิทยาลัย ทั้งโดยบุคคลอื่นหรือเจ้าหน้าที่ของมหาวิทยาลัยถือว่าเป็นทรัพย์สินของมหาวิทยาลัย ไม่อนุญาตให้เจ้าหน้าที่ทำสำเนาหรือเผยแพร่ซอฟต์แวร์ที่เป็นทรัพย์สินของมหาวิทยาลัยโดยไม่ได้รับการอนุญาตจากผู้บริหารเป็นลายลักษณ์อักษร

3.3.4 ผู้ที่ใช้งานซอฟต์แวร์บนระบบสารสนเทศของมหาวิทยาลัยทั้งหมดต้องยึดถือและปฏิบัติตามกฎหมายสิขสิทธิ์และข้อกำหนดของผู้ผลิตซอฟต์แวร์อย่างเคร่งครัด

3.3.5 ซอฟต์แวร์ที่ได้จัดซื้อจากภายนอกอาจมีเงื่อนไขในเรื่องสิขสิทธิ์ด้านการใช้งานที่แตกต่างกัน หน่วยงานที่รับผิดชอบด้านการจัดซื้อต้องรับผิดชอบในการศึกษาถึงเงื่อนไขดังกล่าว และต้องสร้างความตระหนักถึงผู้ใช้งานงานซอฟต์แวร์ดังกล่าวได้ทราบถึงเงื่อนไขต่าง ๆ และข้อห้ามที่เกี่ยวข้อง

3.3.6 การจัดซื้อหรือใช้ซอฟต์แวร์ของบุคคลอื่นต้องปฏิบัติให้สอดคล้องกับข้อตกลงด้านสิขสิทธิ์ ห้ามนำซอฟต์แวร์ที่ซื้อไปติดตั้งที่คอมพิวเตอร์เครื่องอื่นนอกเหนือจากเครื่องที่ได้มีการติดตั้งแล้วตามข้อตกลงเรื่องลิขสิทธิ์ซอฟต์แวร์

3.3.7 ทำการตรวจสอบการใช้งานคอมพิวเตอร์ของมหาวิทยาลัยอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าการใช้งานอุปกรณ์คอมพิวเตอร์ทุกชนิดเป็นไปตามข้อตกลงด้านสิขสิทธิ์ซอฟต์แวร์

3.3.8 เจ้าหน้าที่ที่ฝ่าฝืน ละเมิดข้อตกลงด้านสิขสิทธิ์ของเจ้าของซอฟต์แวร์ถือว่าเป็นการละเมิดนโยบายความปลอดภัยสารสนเทศของมหาวิทยาลัยถึงแม้การละเมิดนั้นจะเป็นไปเพื่อการปฏิบัติงานของมหาวิทยาลัยก็ตามเจ้าหน้าที่ต้องรับผิดชอบผลเสียหายทั้งหมด

ส่วนที่ 18
นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Information Security Risk Assessment Policy)

1. วัตถุประสงค์

การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศนั้นมีวัตถุประสงค์ เพื่อให้มั่นใจว่ามาตรฐานต่าง ๆ ด้านความปลอดภัยสารสนเทศมีการปฏิบัติตามอย่างมีประสิทธิผลในทางปฏิบัติมหาวิทยาลัยจำเป็นต้องมีการตรวจสอบอย่างสม่ำเสมอ ทั้งทางด้านกระบวนการทำงานรวมถึงด้านเทคนิค ทั้งนี้การตรวจสอบมิได้จำกัดเฉพาะหน่วยงานตรวจสอบหรือคณะทำงานสอบทาน แต่ยังรวมถึงการตรวจสอบภายในโดยคณะ/หน่วยงานของตนเอง

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 ผู้ตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

2.3 ผู้ดูแลระบบ/เจ้าหน้าที่ที่ได้รับมอบหมาย

3. แนวทางปฏิบัติในการสอบทาน

3.1 มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and assessment) อย่างน้อยปีละ 1 ครั้ง โดยมีวิธีการปฏิบัติดังนี้

(1) มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

(2) มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(3) มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

(4) มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย 1 ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพ และผลการตรวจสอบเป็นที่น่าเชื่อถือ

3.2 การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (Internal IT Auditor) เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของมหาวิทยาลัย โดยมีวิธีการปฏิบัติดังนี้

3.2.1 กำหนดให้หน่วยตรวจสอบภายในของมหาวิทยาลัยเป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศและให้ตรวจสอบและประเมินความเสี่ยง อย่างน้อย 1 ครั้งต่อปี

3.2.2 มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

3.2.3 มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ในลักษณะที่อ่านได้เพียงอย่างเดียว

3.2.4 มีวิธีการที่ปลอดภัยสาหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูลชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

3.2.5 มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

3.2.6 มีการทำลายหรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

3.2.7 มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจ

3.2.8 มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

3.2.9 มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแลหรือรับผิดชอบ)

3.3 มีแนวทางในตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง อย่างน้อยดังนี้

3.3.1 มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ 1 ครั้ง

3.3.2 มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ 1 ครั้ง

3.3.3 มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อม ข้อเสนอแนะให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

3.4 มีมาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อยดังนี้

3.4.1 ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

3.4.2 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

3.4.3 ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

3.4.4 ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงรันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

3.4.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

3.5 รายการที่สอบทาน

3.5.1 การป้องกันการบุกรุกระบบ

3.5.2 การสำรองข้อมูล

3.5.3 การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

3.5.4 การควบคุมผู้เข้า-ออกอาคาร

3.5.5 การซ้อมรับสถานการณ์ฉุกเฉิน

3.5.6 สอบทานการเข้าถึงระบบสารสนเทศ

3.5.7 สอบทานการกำหนดการใช้งานตามภารกิจ

3.6 การกำกับดูแลการปฏิบัติตามด้านเทคนิค

3.6.1 ผู้บริหารต้องกำกับดูแล เพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่จากการปฏิบัติตามมาตรฐานความปลอดภัยของสารสนเทศ

3.6.2 มหาวิทยาลัยต้องสอบทานต้องตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น

3.6.3 ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูงต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เช่น การทดสอบการเจาะระบบ เป็นต้น เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัย

3.6.4 เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ระบบงาน และเอกสารที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ต้องได้รับการปกป้องจากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

ส่วนที่ 19
นโยบายการและแนวปฏิบัติในการใช้สื่อสังคมออนไลน์
(Social Network Policy)

1. วัตถุประสงค์

เนื่องจากสื่อสังคมออนไลน์ (Social Network) เป็นเครื่องมือที่มีทั้งประโยชน์และโทษที่ควรระวัง โดยเฉพาะข้อมูลข่าวสารบางอย่างที่เผยแพร่ออกสู่สาธารณะไปแล้วอาจไม่สามารถเรียกกลับคืนได้และอาจก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อมหาวิทยาลัย ดังนั้นเพื่อเป็นแนวทางในการกำกับดูแล การเผยแพร่ข้อมูล และการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของมหาวิทยาลัย รวมถึงบริการอิเล็กทรอนิกส์ ตลอดจนการแสดงความคิดเห็นของผู้ใช้งานในมหาวิทยาลัยผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อย มีประสิทธิภาพ และเกิดประโยชน์สูงสุด

ดังนั้นมหาวิทยาลัยจึงมีนโยบายและแนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อสังคมออนไลน์ (Social Network) และแสดงตนในฐานะผู้ใช้งานในสังกัดมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ดังนี้

1.1 เพื่อให้มหาวิทยาลัยมีการกำหนดขอบเขตของการใช้สื่อสังคมออนไลน์ทั้งในระดับตัวบุคคลและระดับคณะ หน่วยงาน และมหาวิทยาลัย

1.2 เพื่อสร้างและรักษาภาพลักษณ์ของเจ้าหน้าที่และการดำเนินงานของมหาวิทยาลัย

1.3 เพื่อลดความเสี่ยงหรือหลีกเลี่ยงปัญหาอันอาจจะเกิดขึ้นจากการใช้สื่อสังคมออนไลน์

1.4 เพื่อป้องกันการเปิดเผยข้อมูลความลับในทุกระดับทั้งมหาวิทยาลัย หน่วยงานภายนอก บริการอิเล็กทรอนิกส์ ผู้ใช้งาน และเจ้าหน้าที่ภายในองค์กร

1.5 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติให้ผู้ใช้งาน เจ้าหน้าที่ของมหาวิทยาลัยให้ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ประโยชน์จากสื่อสังคมออนไลน์และปฏิบัติตามอย่างเคร่งครัด

1.6 นโยบายนี้ต้องมีการดำเนินการตรวจสอบ ประเมิน รวมทั้งปรับปรุงนโยบายและข้อปฏิบัติตามระยะเวลา 1 ครั้งต่อปี

2. ขอบเขตของนโยบาย

ภายใต้นโยบายนี้การเข้าถึงสื่อเครือข่ายสังคมออนไลน์และการเผยแพร่ข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เสียง ข้อมูลใด ๆ หรือแสดงความคิดเห็นส่วนตัวผ่านสื่อสังคมออนไลน์ มีผลบังคับเหมือนกับการเผยแพร่ข้อมูล หรือแสดงความคิดเห็นผ่านทางช่องทางอื่น ๆ โดยการใช้งานสื่อสังคมออนไลน์ ทุกประเภทจะต้องปฏิบัติและสอดคล้องตามแนวนโยบายของมหาวิทยาลัย ได้แก่ พระราชบัญญัติข้อมูล ข่าวสารของทางราชการ พ.ศ. 2540 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2540 พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 และนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยอย่างเคร่งครัด

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้ ประกอบด้วย

สื่อสังคมออนไลน์ (Social Network) หมายถึง สื่อหรือช่องทางในการติดต่อในลักษณะของการสื่อสารแบบสองทางผ่านระบบเครือข่ายอินเทอร์เน็ตเป็นสื่อรูปแบบใหม่ที่บุคคลทั่วไปสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะ โดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประเภทต่าง ๆ ในปัจจุบันมีแหล่งให้บริการสื่อสังคมออนไลน์เกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจำนวนมาก ตัวอย่างเช่น Facebook, Twitter, Linkedln, Google Plus, Myspace, YouTube, Blog, Wiki รวมทั้ง เว็บไซต์ต่าง ๆ ทั่งในประเทศ และต่างประเทศที่เปิดให้บริการในลักษณะเดียวกันและรวมถึงสื่อสังคมออนไลน์อื่น ๆ ที่จะเกิดขึ้นในอนาคต

โพสต์ (Post) หมายถึง การส่งข้อความตัวอักษร ภาพ หรือวีดิโอคลิป เข้าสู่สื่อออนไลน์ เพื่อแสดงความคิดเห็นหรือเผยแพร่ข้อมูลข่าวสาร

3. แนวนโยบายและแนวปฏิบัติในการใช้สื่อสังคมออนไลน์ (Social Network) ทั่วไป

3.1 หลักการและแนวปฏิบัติทั่วไป

3.1.1 มหาวิทยาลัยอนุญาตให้ใช้ระบบเครือข่ายสำหรับเข้าถึงสื่อสังคมออนไลน์ (Social Network) ประเภทเว็บไซต์ที่ไม่มีเนื้อหาขัดต่อกฎหมาย ศีลธรรม และหลักจรรยาบรรณ ระเบียบ ข้อบังคับ ของมหาวิทยาลัย

3.1.2 คณะ/หน่วยงานภายในมหาวิทยาลัย ผู้ใช้งาน เจ้าหน้าที่ นิสิต นักศึกษา สามารถแสดงชื่อผู้ใช้งานในโลกออนไลน์ เพื่อประโยชน์ในการเผยแพร่ ประชาสัมพันธ์ที่เกี่ยวข้องกับมหาวิทยาลัยติดต่อสื่อสารระหว่างกัน แต่ต้องแยกแยะให้ขัดเจนว่าข้อความใดเป็น “ข่าวประชาสัมพันธ์” ข้อความใดเป็น “ความคิดเห็น” “ความคิดเห็นส่วนบุคคล” “การแลกเปลี่ยนข่าวสารส่วนตัว” “การเผยแพร่ข่าวสารเรื่องงาน” หรืออื่น ๆ และความคิดเห็นดังกล่าวควรคำนึงถึงประโยชน์สาธารณะด้วย

3.1.3 การเผยแพร่ประชาสัมพันธ์ที่ประชาสัมพันธ์ในนามของมหาวิทยาลัย คณะ/หน่วยงาน ผู้เผยแพร่ต้องแสดงตำแหน่ง หน้าที่ สังกัด ให้ขัดเจน เพื่อความน่าเชื่อถือ และเพื่อให้ผู้ที่ติดตามสามารถใช้ดุลพินิจในการติดตามได้

3.1.4 พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น หรือหมิ่นประมาทบุคคลอื่น และควรใช้ภาษาให้ถูกต้อง สุภาพ สร้างสรรค์

3.1.5 พึงงดเว้นการโต้ตอบ ด้วยความรุนแรง กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง การละเว้นไม่โต้ตอบจะทำให้ความขัดแย้งไม่บานปลายจนหาที่สิ้นสุดไม่ได้

3.1.6 พึงงดเว้นการใช้สื่อสังคมออนไลน์วิพากษ์วิจารณ์ ตลอดจนแสดงความเห็ ในเรื่องที่เป็นข้อมูลภายในมหาวิทยาลัยหรืออาจส่งผลกระทบต่อมหาวิทยาลัยได้

3.1.7 พึงใช้รูปแสดงตัวตนที่แท้จริง และพึงงดเว้นการนำรูปบุคคลอื่น รูปบุคคลสาธารณะมาแสดงว่าเป็นรูปของตนเอง

3.1.8 มหาวิทยาลัย คณะ/หน่วยงาน อาจใช้รูปสัญลักษณ์ เครื่องหมายแสดงสังกัดได้แต่ต้องคำนึงถึงความเหมาะสมในการใช้งาน

3.1.9 พึงระมัดระวังข้อความที่ส่งผลกระทบต่อเด็ก สตรี หรือละเมิดสิทธิมนุษยชน

3.1.10 การใช้สื่อสังคมออนไลน์ (Social Network) ที่แสดงสังกัดคณะ/หน่วยงาน ภายในมหาวิทยาลัย ควรแจ้งให้ผู้บังคับบัญชาทราบก่อนทุกครั้ง

3.2 หลักการส่งต่อข้อมูล

3.2.1 ควรส่งข้อมูลข่าวสารเฉพาะบุคคลที่รู้จักแสดงตัวตน ตำแหน่ง หน้าที่การงาน สถานะที่ชัดเจนเท่านั้น

3.2.2 ละเว้นการส่งข้อมูลที่เป็นข่าวลือ ข่าวไม่ปรากฏที่มาหรือเป็นเพียงการคาดเดา

3.2.3 งดเว้นการส่งต่อข้อความเกี่ยวข้องกับองค์กรทุกกรณี ยกเว้น ข้อความนั้น ๆ เป็นที่เผยแพร่ต่อสาธารณะแล้ว

3.2.4 พึงระลึกเสมอว่าการส่งต่อข้อความที่เป็นเท็จหรือข้อความที่เจ้าของประสงค์กระจายข่าวสร้างความสับสนวุ่นวายในบ้านเมืองเท่ากับตกเป็นเครื่องมือของบุคคลเหล่านั้น

3.2.5 ควรงดเว้นการส่งต่อข้อความเรื่องบุคคลเสียชีวิต เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้ว

3.2.6 การส่งต่อข้อความเชิญชวนไปร่วมชุมนุมหรือกระทำกิจกรรมทางสังคมใด ๆ ต้องตรวจสอบข้อเท็จจริงให้แน่ชัดเสียก่อน

3.3 หลักความรับผิดชอบ

3.3.1 ควรแสดงความรับผิดชอบด้วยการขอโทษ แสดงความเสียใจทันที เมื่อรู้ว่ามีการเผยแพร่ข้อมูลที่ผิดพลาดหรือกระทบต่อบุคคลอื่น

3.3.2 กรณีการส่งต่อข้อความข่าวลือหรือข่าวเท็จต้องแก้ไขข้อความนั้นโดยทันทีหากสามารถตรวจสอบข้อเท็จจริงได้พึงแสดงข้อเท็จจริงให้เป็นที่ประจักษ์

3.3.3 หากพบข้อมูลที่ไม่ถูกต้อง ควรดำเนินการแก้ไขอย่างรวดเร็ว และแสดงให้เห็นอย่างชัดเจนว่าเป็นผู้ดำเนินการดังกล่าว

3.3.4 หากพบข้อมูลใด ๆ ที่ไม่เหมาะสม (เช่น สิ่งที่เป็นสิขสิทธิ์ของผู้อื่นหรือการแสดงความคิดเห็นที่เป็นการหมิ่นประมาท) ควรดำเนินการอย่างรวดเร็ว โดยลบข้อความดังกล่าวออกทันที เพื่อลดโอกาสที่จะเกิดข้อขัดแย้งทางกฎหมาย และผลกระทบด้านลบต่อมหาวิทยาลัย

3.4 การพบข้อร้องเรียนและประเด็นขัดแย้ง

3.4.1 หากพบเห็นข้อร้องเรียนเกี่ยวกับบริการอิเล็กทรอนิกส์ของมหาวิทยาลัย หรือพบเห็นข้อร้องเรียนอื่น ๆ ที่เกี่ยวข้องกับมหาวิทยาลัยสามารถแจ้งมายังหน่วยงานที่ได้รับมอบหมาย/หรือสำนักวิทยบริการฯ ทราบโดยเร็วที่สุด โดยหลีกเลี่ยงการถกเถียงหรือโต้ตอบ ซึ่งนำไปสู่การกระตุ้น ให้เกิดอารมณ์รุนแรงและพาดพิงไปยังผู้อื่น

3.4.2 หากพบเห็นการบิดเบือนข้อเท็จจริงที่เกี่ยวข้องกับบริการอิเล็กทรอนิกส์ของมหาวิทยาลัยหรือพบเห็นประเด็นขัดแย้งอื่น ๆ ที่เกี่ยวข้องกับมหาวิทยาลัยสามารถแจ้งมายังหน่วยงานที่ได้รับมอบหมาย/หรือ สำนักวิทยบริการฯ ทราบโดยเร็วที่สุด โดยหลีกเลี่ยงการถกเถียงหรือโต้ตอบ ซึ่งนำไปสู่การกระตุ้นให้เกิดอารมณ์รุนแรงและพาดพิงไปยังผู้อื่น

3.5 การไม่เปิดเผยข้อมูลที่เป็นความลับ

การพูดคุยแลกเปลี่ยนกับชุมชนออนไลน์ รวมถึงการโพสต์ข้อความที่เกี่ยวข้องกับงานประจำเป็นสิ่งที่บุคคลสามารถกระทำได้ ถ้าไม่ขัดต่อระเบียบ/ข้อบังคับของมหาวิทยาลัยหรือหลักจรรยาบรรณของวิชาชีพ เว้นแต่ข้อมูลนั้นเป็นข้อมูลที่มีความสำคัญหรือเป็นความลับของมหาวิทยาลัย ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการการลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น

3.6 ความน่าเชื่อถือของข้อมูล

ไม่โพสต์ข้อความที่เป็นเท็จหรือก่อให้เกิดความเข้าใจผิด และระบุที่มาของข้อมูลนั้นอย่างชัดเจน การโพสต์ข้อความใด ๆ ควรพิจารณาเนื้อหาอย่างรอบคอบและระมัดระวัง โดยเฉพาะการเปิดเผยข้อมูลส่วน บุคคล

3.7 ไม่ละเมิดกฎหมายสิขสิทธิ์และทรัพย์สินทางปัญญา

ไม่ละเมิดกฎหมายลิขสิทธิ์การใช้งานใด ๆ ที่เป็นสิขสิทธิ์ของผู้อื่นรวมทั้งของมหาวิทยาลัย ทั้งนี้ การอ้างอิงคำพูดหรือข้อมูลของผู้อื่น ควรใช้ข้อความที่คัดลอกมาสั้น ๆ เท่านั้น และควรระบุถึงที่มาของแหล่งข้อมูล หรือเจ้าของผลงานเสมอ การเชื่อมลิงก์ไปยังงานของเจ้าของข้อมูลถือเป็นการปฏิบัติที่เหมาะสมกว่าการคัดลอก ข้อมูลมาใช้งาน

3.8 คำนึงถึงผู้เข้าชมและผู้เกี่ยวข้อง

เจ้าหน้าที่/นิสิตของมหาวิทยาลัยไม่ควรโพสต์ข้อมูลใด ๆ ที่ขัดแย้งกับข้อระเบียบ/ข้อบังคับ/ ข้อกำหนดของมหาวิทยาลัย รวมถึงละเว้นการแสดงออกถึงความคิดเห็นที่ก้าวร้าว หมิ่นประมาท ดูถูกเป็นการ ส่วนตัว ลามกอนาจาร และอื่น ๆ ที่ไม่เหมาะสม ตลอดจนหัวข้อที่เป็นความคิดเห็นส่วนตัวที่อาจเป็นการยั่วยุหรือ ขัดต่อจริยธรรม เช่น การเมือง ศาสนา ชนชาติ เป็นต้น การแสดงความคิดเห็นต่าง ๆ ที่โพสต์โดยบุคลากรของ มหาวิทยาลัย โดยที่ไม่ได้รับมอบหมายอย่างเป็นทางการถือเป็นการแสดงความเห็นส่วนบุคคลเท่านั้นไม่ได้เป็น ความคิดเห็นอย่างเป็นทางการของมหาวิทยาลัย

3.9 การปกป้องผู้มีส่วนได้ส่วนเสียภายในและภายนอกมหาวิทยาลัย และผู้มีส่วนเกี่ยวข้อง

ไม่ควรอ้างอิง หรือเปิดเผยถึงข้อมูลผู้มีส่วนได้ส่วนเลีย และคณะ/หน่วยงานภายในมหาวิทยาลัย และหน่วยงานภายนอกมหาวิทยาลัย ตลอดจนผู้มีส่วนเกี่ยวข้องอย่างเปิดเผยก่อนได้รับอนุญาต ตลอดจนไม่ พาดพิงถึงรายละเอียดที่เป็นความลับเกี่ยวกับข้อผูกพันกับผู้มีส่วนได้ส่วนเลียทั้งนี้ ควรพิงระวังการใช้งานเครือข่าย สังคมออนไลน์เป็นเครื่องมือในการทำธุรกรรมทางการค้ากับผู้มีส่วนได้ส่วนเสียหน่วยงานภายนอกรวมถึงผู้มีส่วน เกี่ยวข้องกับมหาวิทยาลัย

3.10 การคำนึงถึงผลกระทบจากการใช้งาน

คำนึงถึงผลกระทบของการโพสต์ข้อความในเว็บบล็อกส่วนตัว โดยเฉพาะข้อความที่อาจจะ ก่อให้เกิดความขัดแย้งกับมหาวิทยาลัย ดังนั้นจึงควรระมัดระวังในการถูกนำข้อความในเว็บบล็อกส่วนตัวมาเป็น ข้อมูลอ้างอิง

3.11 การคำนึงถึงผลกระทบต่อการปฏิบัติงาน

การใช้สื่อเครือข่ายสังคมออนไลน์จะต้องไม่รบกวนการปฏิบัติงานหรือหน้าที่ความรับผิดชอบที่ ได้รับมอบหมาย

3.12 การฝ่าฝืนและบทลงโทษ

3.12.1 มหาวิทยาลัยไม่รับผิดชอบต่อผลของการกระทำที่เกิดจากผู้ใช้งาน และ/หรือบัญชี ผู้ใช้งานที่ฝ่าฝืนต่อนโยบายนี้

3.12.2 หากมหาวิทยาลัยตรวจสอบแล้วพบว่าบัญชีผู้ใช้งานใดละเมิดต่อนโยบายนี้ มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับ และ/หรือยกเลิกบัญชีผู้ใช้งานอินเทอร์เน็ต และ/หรือหยุดให้บริการแก่ ผู้ใช้งานนั้น

3.12.3 หากการกระทำอันฝ่าฝืนต่อนโยบายนี้เป็นความผิดตามกฎหมายให้มหาวิทยาลัยดำเนินคดีตามกฎหมายโดยลำดับต่อไป

4. แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับบุคคล

การนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของนิสิต/นักศึกษา/เจ้าหน้าที่ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก มีแนวนโยบายและแนวปฏิบัติดังนี้

4.1 กรณีใช้ชื่อบัญชีผู้ใช้งาน (User Account) ที่ระบุถึงต้นสังกัดผู้ใช้งานพึงใช้ความระมัดระวังในการปฏิบัติตามระเบียบข้อบังคับ จรรยาบรรณ จริยธรรม หลักเกณฑ์และแนวปฏิบัติของมหาวิทยาลัยที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย โดยเฉพาะความถูกต้องและการใช้ภาษาที่เหมาะสม

4.2 กรณีใช้ชื่อบัญชีผู้ใช้งานที่ระบุถึงตัวตนอันอาจทำให้ผู้ติดตาม (Followers) หรือเพื่อนในเครือข่าย (Friends) เข้าใจได้ว่าเป็นบุคลากรในมหาวิทยาลัย ผู้ใช้งานพึงระมัดระวังการนำเสนอข้อมูล ข่าวและการแสดงความคิดเห็นที่อาจนำไปสู่การละเมิดจริยธรรมของผู้อื่น

4.3 ในการรวบรวมข้อมูลข่าวสาร การนำเสนอ และการแสดงความคิดเห็นผู้ใช้งานพึงระวังการละเมิดสิทธิส่วนบุคคล ศักดิ์ศรีความเป็นมนุษย์ สิทธิเด็กและสตรี ภาพอุจาด ลามก อนาจาร

4.4 หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ของเจ้าหน้าที่/ผู้ใช้งานของมหาวิทยาลัยเกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรอื่น ผู้ใช้งานต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือองค์กรที่ได้รับความเสียหาย ทั้งนี้ต้องให้ผู้ที่ได้รับความเสียหายได้มีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

5. แนวนโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์ในระดับคณะ/หน่วยงาน/มหาวิทยาลัย

5.1 การจัดทำสื่อสังคมออนไลน์ในระดับคณะ/หน่วยงาน/มหาวิทยาลัย ควรที่จะคำนึงถึงหลักการพื้นฐานดังต่อไปนี้

5.1.1 วัตถุประสงค์ของการจัดทำ

5.1.2 แนวทางการใช้งานสื่อสังคมออนไลน์ เพื่อช่วยพัฒนาและดำเนินงานของคณะ/หน่วยงาน/มหาวิทยาลัย

5.2 การตั้งคำบนสื่อสังคมออนไลน์ของคณะ/หน่วยงาน/มหาวิทยาลัย การใช้ชื่อหรือตราสัญลักษณ์ของคณะ/หน่วยงาน/มหาวิทยาลัย เพื่อเปิดบัญชีผู้ใช้งานสื่อสังคมออนไลน์ โดยมีวัตถุประสงค์เพื่อการประชาสัมพันธ์เผยแพร่ข้อมูลข่าวสาร หรือการสื่อสารภายในคณะ/หน่วยงาน/มหาวิทยาลัยจะต้องผ่านการรับทราบและเห็นชอบจาก CIO / ผู้อำนวยการสำนักวิทยบริการฯ ก่อน รวมทั้งจะต้องมีการตระหนักถึงหลักการพื้นฐาน ดังที่กล่าวมาข้างต้น

5.3 การนำเสนอข่าวโดยการใช้สื่อสังคมออนไลน์ของคณะ/หน่วยงาน/มหาวิทยาลัย ควรมีหลักในการอ้างอิงดังต่อไปนี้

5.3.1 ชื่อคณะ/หน่วยงาน/มหาวิทยาลัย ที่เผยแพร่ข้อมูลข่าวสาร

5.3.2 รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงคณะ/หน่วยงาน/มหาวิทยาลัย

5.3.3 มาตรการทางเทคนิคที่ยืนยันถึงสถานะและความมีตัวตนของคณะ/หน่วยงาน/มหาวิทยาลัย (ถ้ามี)

5.3.4 ชื่อตัวแทนเจ้าหน้าที่ที่ได้รับมอบหมายให้นำเสนอข่าวสาร (ถ้ามี)

5.4 การปกป้องข้อมูลที่เป็นความลับของมหาวิทยาลัย

ในกรณีที่มีบัญชีผู้ใช้งานของมหาวิทยาลัย ควรมีการตั้งค่าความเป็นส่วนตัว (Privacy) เพื่อป้องกันไม่ให้บุคคลอื่นโพสต์ข้อความหรือเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับของมหาวิทยาลัย ซึ่งห้ามเปิดเผยโดยเด็ดขาด เช่น รายละเอียดของโครงการการลงทุน ข้อมูลสำคัญทางการเงิน งานวิจัย เป็นต้น โดยมีการกำหนดให้อยู่ในวงจำกัดเท่านั้น และควรให้ความระมัดระวังในการโพสต์ข้อความเฉพาะกลุ่มหรือส่วนบุคคลที่ไม่ต้องการเผยแพร่ให้สาธารณะชนรับรู้

5.5 การนำเสนอข้อมูลข่าวสารของคณะ/หน่วยงาน/มหาวิทยาลัยผ่านสื่อสังคมออนไลน์ควรเป็นไปตามระเบียบ/ข้อบังคับ/จริยธรรม/จรรยาบรรณในวิชาชีพ รวมทั้งหลักเกณฑ์และแนวปฏิบัติของมหาวิทยาลัยที่กำกับดูแลตามที่ระบุไว้ในขอบเขตของนโยบาย และต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในชาติจนอาจนำไปสู่ความขัดแย้งและเลียหายรุนแรงขึ้นในสังคม

5.6 มหาวิทยาลัยต้องให้ความเคารพและยอมรับข้อมูลข่าวสารหรือภาพข่าวที่ผลิตโดยบุคคลอื่นผ่านสื่อสังคมออนไลน์ การคัดลอก เลียน ข้อความใด ๆ จากสื่อสังคมออนไลน์ พึงได้รับการอนุญาตจากเจ้าของข้อความนั้น ๆ ตามแต่กรณีจำเป็นเพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสารต้องอ้างอิงถึงแหล่งที่มาของข้อความและข่าวสารนั้นโดยรับรู้ถึงสิทธิหรือลิขสิทธิ์ขององค์กรหรือบุคคลผู้เป็นเจ้าของข้อมูลดังกล่าว

5.7 หลีกเลี่ยงการสื่อสารข้อความ ภาพนิ่ง ภาพเคลื่อนไหว เลียง และข้อมูลใด ๆ ของมหาวิทยาลัยหรือที่เกี่ยวข้องกับมหาวิทยาลัยที่ก่อให้เกิดความขัดแย้ง หรือโต้แย้งในสังคมขัดต่อหลักกฎหมายทั้งในประเทศ และในระดับสากล

5.8 ไม่นำข้อมูลที่เป็นความลับทุกระดับชั้นของมหาวิทยาลัยมาเผยแพร่ผ่านสื่อสังคมออนไลน์ทุกประเภท

ส่วนที่ 20
นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Awareness Policy)

1. วัตถุประสงค์

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับผู้บริหาร และเจ้าหน้าที่ของมหาวิทยาลัยได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. ผู้รับผิดชอบ

2.1 สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

2.2 คณะ/หน่วยงาน

2.3 เจ้าหน้าที่ได้รับมอบหมาย

3. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3.1 จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงาน อย่างน้อยปีละ 1 ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานของระบบสารสนเทศ

3.2 จัดทำคู่มือการใช้งานระบบสารสนเทศอย่างปลอดภัย และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย/คณะ/หน่วยงาน หรือในระบบ E-Document ของมหาวิทยาลัย

3.3 จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของหน่วยงาน

3.4 จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยการจัดสัมมนาควรจัดปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจ และนำไปปฏิบัติได้ง่าย ซึ่งมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ โดยการติดประกาศ ประชาสัมพันธ์ แผ่นพับ เผยแพร่ผ่านเว็บไซต์

3.5 ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

3.6 ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้งาน

ภาคผนวก ก

การประเมินสถานการณ์ความเสี่ยง

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก พบว่า ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สามารถแยกเป็นภัยต่าง ๆ ได้ ดังนี้

1. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human error)
2. ภัยที่เกิดจาก Software
3. ภัยจากไฟไหม้ หรือระบบไฟฟ้า
4. ภัยจากอุทกภัย

1. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้ เกิดการชะงักงัน หรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากเจ้าหน้าที่หรือบุคลากร (Human Error)

สำนักวิทยบริการฯ ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

1. จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เป็นการลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด เพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศ ทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้น อีกทั้งยังเป็นการทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง
2. ออกคำสั่งมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกเรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคง ปลอดภัยด้านสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก พ.ศ. 2565 เพื่อแจ้งเวียนนโยบายและแนวปฏิบัติดังกล่าวให้ทุกคณะ/หน่วยงานทราบและถือปฏิบัติ รวมทั้งประกาศในระบบ E-Doc ของมหาวิทยาลัยฯ
3. จัดทำหนังสือแจ้งเวียนคณะ/หน่วยงาน เรื่อง การใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์ เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง
4. พัฒนาเจ้าหน้าที่ผู้รับผิดชอบให้มีความรู้ความชำนาญในการทำหน้าที่ดูแลแก้ไขปัญหาให้คำปรึกษา ตรวจสอบ และบำรุงรักษาระบบเครือข่ายคอมพิวเตอร์หลัก

2. ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้า โทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) เป็นต้น โดย Software เหล่านี้อาจรบกวนการทำงาน และก่อให้เกิดความ

เสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกใช้งานไม่ได้

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกได้ตระหนักถึงปัญหาดังกล่าว จึงได้ดำเนินการดังนี้

1. ติดตั้งอุปกรณ์รักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ (Firewall) เพื่อรักษาความปลอดภัยให้กับระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ป้องกันการบุกรุกจากภายนอก

2. แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านเว็บไซต์สำนักวิทยบริการฯ อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัย ที่จะเกิดจาก Software ดังกล่าว ให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

3. ติดตั้งโปรแกรมป้องกันและตรวจจับไวรัส (Anti-Virus) ครอบคลุมทุกเครื่องแม่ข่ายและลูกข่ายเพื่อป้องกันความเสียหายของข้อมูล

3. ภัยจากไฟไหม้ หรือ ระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่สร้างความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการดังนี้

1. ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) ยี่ห้อ Victron UPS ขนาด 120 KVA เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง ซึ่งระบบสำรองไฟฟ้าที่ใช้ควบคุมห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลักของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สามารถสำรองไฟฟ้า แบบ Full Load เพื่อใช้งานได้นาน 15 นาที ในกรณีที่เกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถสั่งการให้ระบบทำการ Shutdown โดยที่ไม่เกิดความเสียหายต่ออุปกรณ์หรือข้อมูล

2. ติดตั้งระบบเตือนภัยและดับเพลิงความไวสูงห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลัก โดยมีอุปกรณ์ตรวจจับควันความไวสูง กรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์อุปกรณ์ดังกล่าวจะส่งสัญญาณกริ่ง เพื่อแจ้งเตือนและส่งข้อความไปยังโทรศัพท์ติดตามตัวของผู้รับผิดชอบเพื่อให้ผู้รับผิดชอบทราบถึงเหตุฉุกเฉินดังกล่าว ในกรณีที่เกิดไฟไหม้ ชภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลักระบบจะมีการตัด การจ่าย กระแสไฟฟ้าอัตโนมัติ และในการดับเพลิงระบบจะฉีดสารดับเพลิงชนิด Novec 1230 เพื่อทำการดับเพลิงโดยทำได้ทั้งระบบอัตโนมัติและด้วยมือตามโปรแกรมที่กำหนดไว้ ทั้งนี้ระบบดังกล่าวมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สำนักวิทยบริการฯ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์

ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้มีการจัดเตรียมอุปกรณ์และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

1. แผ่น Boot Disk
2. แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
3. แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
4. แผ่นโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์
5. แผ่น Driver อุปกรณ์ต่าง ๆ
6. ระบบสำรองไฟฉุกเฉิน
7. Hard Disk สำรอง
8. สำเนารายละเอียดการบันทึกค่า Configuration ต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

4. ภัยจากอุทกภัยหรือจากน้ำและความชื้น จัดเป็นภัยที่สร้างความเสียหายด้านกายภาพ เช่น เครื่องแม่ข่าย อุปกรณ์กระจายสัญญาณหลักคอมพิวเตอร์หรือสร้างความเสียหายแก่อุปกรณ์ต่อพ่วงกับคอมพิวเตอร์ เช่น เครื่องพิมพ์ เป็นต้น

แนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากอุทกภัย

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้ตระหนักถึงปัญหาดังกล่าวที่อาจจะเกิดขึ้น จึงได้ดำเนินการดังนี้

1. เฝ้าระวังภัยอันเกิดจากน้ำท่วม โดยติดตามการพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา
2. เมื่อเกิดน้ำขังสูงกว่าปกติ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อย ๆ และท่วมขังมาถึงบริเวณห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ให้ดำเนินการปิดเครื่องคอมพิวเตอร์/อุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ทั้งหมดและนำไปเก็บไว้ในที่ปลอดภัย
3. ดำเนินการตัดระบบไฟฟ้าห้องควบคุม โดยปิดเบรกเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหาย และป้องกันภัยจากไฟฟ้า
4. เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์ และอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ไว้ในที่สูง
5. กรณีน้ำลดเรียบร้อยแล้ว ให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมว่าใช้งานได้ตามปกติหรือไม่และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์
6. เมื่อระบบไฟฟ้าใช้งานได้ตามปกติ ผู้ดูแลระบบ/เจ้าหน้าที่ผู้รับผิดชอบช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์และอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์มาติดตั้ง และทดสอบการใช้งานได้ตามปกติหรือไม่และสามารถเชื่อมต่อกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยได้หรือไม่
7. เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์สามารถใช้งานได้ตามปกติ และสามารถเชื่อมต่อเข้ากับระบบเครือข่ายของมหาวิทยาลัยได้แล้วให้แจ้งผู้บังคับบัญชาหน่วยงานที่เกี่ยวข้อง และผู้ใช้งานทราบ เพื่อเข้ามาใช้บริการได้ตามปกติ

การจัดเตรียมอุปกรณ์ที่จำเป็น

ในการเตรียมพร้อมรับภัยพิบัติที่จะเกิดขึ้นต่อระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สำนักวิทยบริการฯ ซึ่งเป็นหน่วยงานหลักที่ดูแลด้านระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้มีการจัดเตรียมอุปกรณ์ และเครื่องมือที่จำเป็นในกรณีคอมพิวเตอร์เกิดขัดข้องใช้งานไม่ได้ โดยมีการเตรียมอุปกรณ์ดังนี้

1. แผ่น Boot Disk
2. แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ
3. แผ่นสำรองข้อมูลและระบบงานที่สำคัญ
4. แผ่นโปรแกรมป้องกันและกำจัดไวรัสคอมพิวเตอร์
5. แผ่น Driver อุปกรณ์ต่าง ๆ
6. ระบบสำรองไฟฉุกเฉิน
7. Hard Disk สำรอง
8. สำเนารายละเอียดการบันทึกค่า Configuration ต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

ภาคผนวก ข
แผนเตรียมความพร้อมกรณีฉุกเฉิน
แผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ
มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก
(IT Contingency Plan)

หลักการและเหตุผล

มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกเป็นสถาบันการศึกษา ที่มีพันธกิจสำคัญ 4 ประการ ได้แก่

1) จัดการศึกษา และวิชาชีพชั้นสูงโดยมุ่งเน้นพัฒนาคุณภาพการศึกษาการผลิตบัณฑิตที่มีคุณภาพ ตามมาตรฐานและมีคุณลักษณะที่พึงประสงค์

2) สร้างผลิตผลจากงานวิจัยที่เป็นองค์ความรู้ใหม่และมีคุณภาพในทุกสาขาวิชา เพื่อสนับสนุนการเรียนการสอน การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม และนำไปใช้ประโยชน์ตามความเหมาะสม

3) ให้บริการวิชาการแก่ชุมชนและสังคม เพื่อให้ชุมชนและสังคมสามารถพึ่งพาตนเองได้อย่างยั่งยืน

4) อนุรักษ์ ฟื้นฟู ปกป้อง เผยแพร่ และพัฒนาศิลปวัฒนธรรมและขนบธรรมเนียมประเพณีการขับเคลื่อนพันธกิจต่าง ๆ เป็นไปอย่างมีประสิทธิภาพ และประสิทธิผล มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกจึงได้มีการนำระบบเทคโนโลยีสารสนเทศมาใช้ในการดำเนินงาน เพื่อเพิ่มประสิทธิภาพในการบริหารจัดการงานและการให้บริการด้านต่าง ๆ เพื่อให้นิสิตนักศึกษาได้รับความสะดวกมากขึ้น ขณะเดียวกันระบบสารสนเทศของมหาวิทยาลัย อาจได้รับความเสียหายจากภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศ อาทิ ไฟฟ้าดับ ไวรัสคอมพิวเตอร์ การบุกรุก (Hacker) หรือความเสียหายจากการปฏิบัติงานของเจ้าหน้าที่ที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศ สถานการณ์ หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนา อันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลาย ปฏิเสธการทำงาน หรือการกระทำอื่น ๆ และ/หรือปัจจัยอื่น ๆ ที่เกี่ยวข้อง เพื่อเป็นการป้องกัน แก้ไขปัญหา และรองรับสถานการณ์ที่อาจเกิดขึ้น แผนนี้จึงจัดแบ่งออกเป็น 3 ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan) แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operation plan) และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Plan)

วัตถุประสงค์

1. เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพสามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

2. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงานเป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

3. เพื่อลดความเสียหายที่อาจเกิดขึ้นแก่ระบบสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

4. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก

1. แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก (Contingency Plan)

ข้อควรปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติหรือการใช้งานระบบเครือข่ายขัดข้อง กรณีเครื่องลูกข่าย

1. ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้นแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบของ คณะ/หน่วยงานทราบ หรือกรณีมีเหตุอันทำให้ไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ สำนักวิทยบริการฯ จะต้องประกาศให้ทุก คณะ/หน่วยงานในมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกทราบ

2. กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการ

3. ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่องาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

4. ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด

5. ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

6. ให้เจ้าหน้าที่สำนักวิทยบริการฯ แจ้งเหตุขัดข้องนั้นให้ผู้อำนวยการสำนักวิทยบริการฯ ทราบโดยเร็วที่สุด

กรณีเครื่องบริการ (Server) และอุปกรณ์เครือข่าย

1. ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายคอมพิวเตอร์และเครื่องคอมพิวเตอร์แม่ข่ายตามลำดับความสำคัญของการให้บริการ

2. ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ โดยพิจารณาตามลำดับความสำคัญของการให้บริการ ระยะเวลาที่ไฟฟ้าดับ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

3. ตัดระบบจ่ายไฟ ในกรณีไฟไหม้ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

4. รีบขนย้ายเครื่องไปไว้ในที่ปลอดภัย

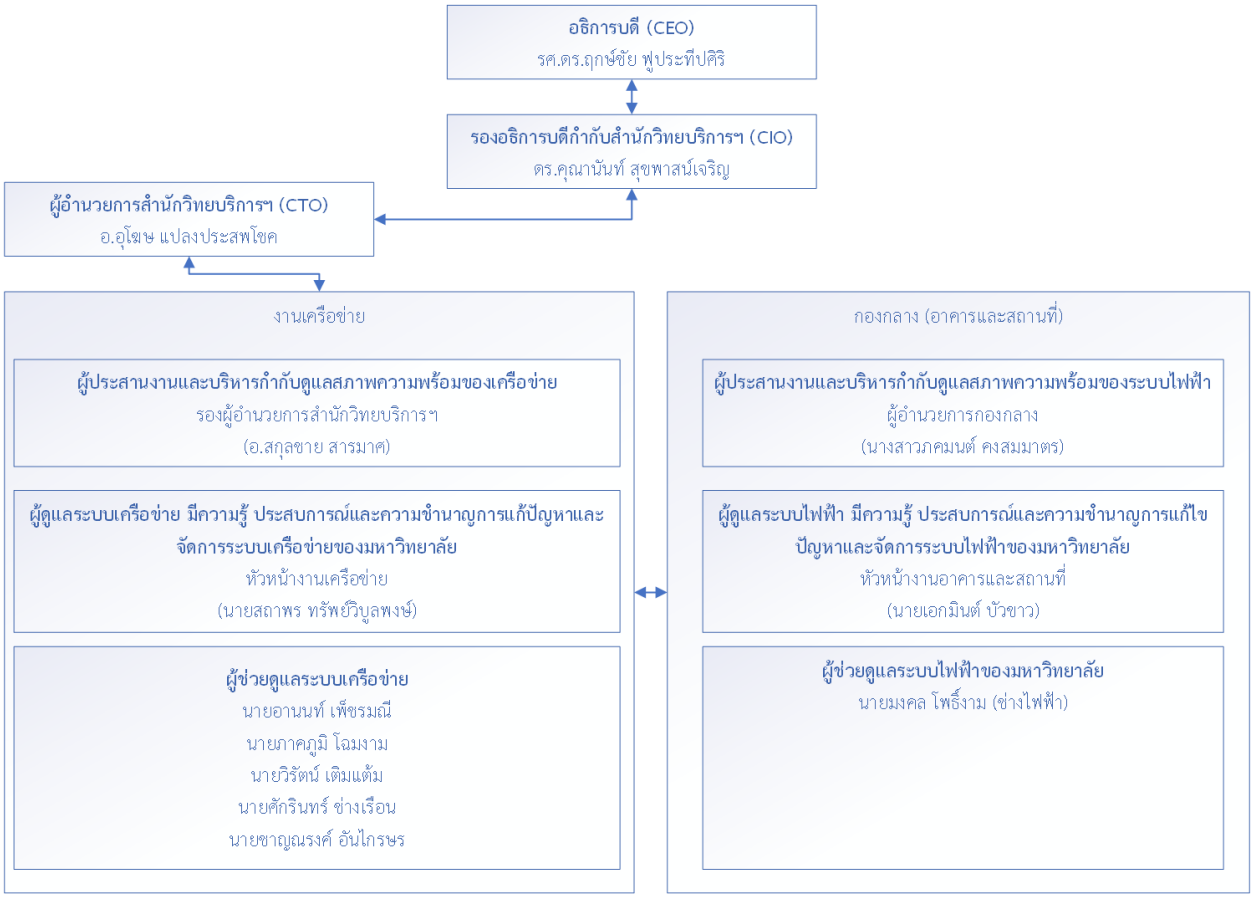
5. ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลระบบคอมพิวเตอร์แม่ข่าย และ/หรือผู้เชี่ยวชาญระบบเครือข่ายที่เกี่ยวข้องโดยเร็วที่สุด

6. ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

7. ผู้ดูแลระบบ ต้องรีบแจ้งให้ผู้อำนวยการสำนักวิทยบริการฯ ทราบโดยเร็ว

2. ผู้รับผิดชอบตามแผนดำเนินการเพื่อให้ระบบใช้งานได้อย่างต่อเนื่อง (Continuity of Operation Plan)

เพื่อแก้ไขระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ที่เกิดจากภัยพิบัติให้ใช้งานได้อย่างรวดเร็วและต่อเนื่องอย่างมีประสิทธิภาพ มหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ได้กำหนดโครงสร้าง หน่วยงานและผู้รับผิดชอบดำเนินงานดังนี้



การจัดองค์กรปฏิบัติการฉุกเฉินในระบบสารสนเทศมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออกเมื่อเกิดเหตุฉุกเฉิน

การจัดองค์กรปฏิบัติการฉุกเฉินหรือผู้รับผิดชอบตามสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

1.1 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO)

1.1.1 กำหนดนโยบายให้สำนักวิทยบริการฯ เป็นผู้รับผิดชอบ

1.1.2 ให้คำปรึกษาแก่ผู้อำนวยการสำนักวิทยบริการฯ ในฐานะประธานศูนย์ฯ

1.2 ผู้อำนวยการสำนักวิทยบริการฯ (Chief Technology Officer: CTO)

1.2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

1.2.2 มีอำนาจสั่งการให้ทุกคณะ/หน่วยงานหยุด หรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

1.2.3 มีอำนาจสั่งทำลายกุญแจอาคารเก็บวัตถุอันตราย เพื่อการระงับเหตุฉุกเฉิน

1.2.4 ประชุมหารือกับคณะกรรมการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์และคณะกรรมการอื่นที่เกี่ยวข้อง

1.2.5 ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผน ๆ ตามความเหมาะสม

1.2.6 รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

1.3 ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย (หัวหน้างานพัฒนาเครือข่ายคอมพิวเตอร์)

1.3.1 วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อผู้อำนวยการสำนักวิทยบริการฯ

1.3.2 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินชั้นต้นจนกว่าผู้อำนวยการระงับเหตุ ฉุกเฉินจะมาถึงที่เกิดเหตุ

1.3.3 สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผน

1.3.4 ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

1.3.5 ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะ และหน่วยดับเพลิง เป็นต้น

1.3.6 รายงานให้ผู้อำนวยการระงับเหตุฉุกเฉินทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

1.3.7 กำหนดอัตรากำลังพล วัสดุอุปกรณ์ และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

1.3.8 ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

1.4 ผู้ดูแลระบบเครือข่ายคอมพิวเตอร์ (Network Administer)

1.4.1 กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

1.4.2 พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย

1.4.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

1.4.4 ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

1.4.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ ที่ชำรุด เสียหาย แล้วรายงานให้ประธานศูนย์ประสานงานรักษาความปลอดภัยสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, Worm, Spy Ware
- ทำการตรวจสอบอุปกรณ์ระบบสำรองกระแสไฟฟ้า (UPS)
- ทำการตรวจสอบ Transaction Log Files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

- ทำการตรวจสอบค่า Configuration ของระบบ

1.4.6 เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ ที่เกี่ยวข้องเพื่อดำเนินการคู้ระบบโดยเร็ว

1.4.7 ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกและบริษัทที่ปรึกษาในการกู้ระบบ

1.4.8 ทำการสำรองข้อมูลทุกรัน วันจันทร์ถึงวันพฤหัสบดี ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) วันศุกร์ทำการสำรองข้อมูลทั้งระบบ

1.4.9 ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรมและแฟ้มข้อมูล, Tape /อุปกรณ์ Backup, รายชื่อโปรแกรมเอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรมรายการฮาร์ดแวร์สำรอง สำเนาคู่มือ

1.4.10 น่าระบบสำรองข้อมูลออกมาใช้ เพื่อให้ระบบสามารถดำเนินการต่อไปได้

1.5 ที่ปรึกษาด้านเทคนิค (วิศวกรที่ปรึกษาและเจ้าหน้าที่บริษัทที่ปรึกษา)

1.5.1 ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

1.5.2 ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญ หรือหน่วยราชการที่เกี่ยวข้อง

1.5.3 ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็วหลังจากเหตุฉุกเฉินสงบแล้ว

1.6 หัวหน้าหน่วยงานที่เกิดเหตุ (On-site Manager)

1.6.1 แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

1.6.2 ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบสารสนเทศ

1.6.3 นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

3. แผนการสำรองและกู้คืนข้อมูล (Backup and Recovery Plan)

เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก อยู่ในสภาพพร้อมรองรับการให้บริการได้ตลอด 24 ชั่วโมง ให้ผู้ดูแลระบบปฏิบัติตามแผนการ Backup and Recovery Plan ดังนี้

3.1 Backup Plan

1. ระบบงานที่ต้องการลำรองมีรายการ ดังนี้

1.1 ระบบสารสนเทศเพื่อการบริหารจัดการ

1.2 ระบบบริการการศึกษาและระบบทะเบียน

2. บุคลากรผู้รับผิดชอบ

2.1 ระบบสารสนเทศเพื่อการบริหารจัดการ

3. จัดเตรียม Storage ที่ใช้ในการเก็บข้อมูลที่ต้องการสำรอง รวมถึงระบบ/Software ที่ใช้ในการสำรองและกู้คืน

4. ทำการทดสอบความพร้อมของระบบ และดำเนินการสำรองระบบงานที่ได้คัดเลือกไว้

5. ตรวจสอบความถูกต้องของระบบงาน หลังจากที่ทำการสำรอง

6. บันทึกข้อมูลลงใน แบบฟอร์มบันทึกการสำรองข้อมูล/แบบฟอร์มรายงานข้อผิดพลาดในการสำรองข้อมล

7. หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถสำรองข้อมูลได้สำเร็จให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการสำรองข้อมูลอีกครั้ง

3.2 Recovery Plan

1. รายงานปัญหา/สาเหตุที่ต้องทำการกู้คืนข้อมูลต่อผู้อำนวยการสำนักวิทยบริการฯ หรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการสำนักวิทยบริการฯ ทราบ

2. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์หรือระบบเครือข่ายกระทบต่อการให้บริการหรือการใช้งานของผู้ใช้ระบบให้แจ้งผู้ใช้งานทราบทันที

3. ใช้ข้อมูลล่าสุด/ทันสมัยที่สุด (Latest Update) ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

• กรณีเกิดความเสียหายขึ้นกับระบบงาน (Source Code) จะทำการติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด

• กรณีเกิดความเสียหายขึ้นกับฐานข้อมูล (Database) จะนำฐานข้อมูลที่เก็บไว้ล่าสุดกู้คืนเพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด

• กรณีเกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ Hardware ยังคงทำงานปกติ จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด รวมถึงทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

• กรณีเกิดความเสียหายขึ้นกับ Hardware ให้บริษัทผู้ดูแลทำการแก้ไขเบื้องต้นให้ Hardware สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับ OS และระบบงานจะทำการติดตั้ง OS และระบบงานนั้นใหม่จาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

4. ดำเนินการกู้คืนข้อมูลระบบงานที่มีปัญหา

5. ตรวจสอบความถูกต้องของระบบงาน หลังจากทำการกู้คืนระบบเสร็จเรียบร้อยแล้ว

6. หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการกู้คืนข้อมูลจนเป็นเหตุให้ไม่สามารถกู้คืนข้อมูลได้สำเร็จให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการกู้คืนข้อมูลอีกครั้ง

7. แจ้งผลการกู้คืนข้อมูลให้ผู้ใช้งานทราบ

4. การเตรียมการป้องกันและการแก้ไข

4.1 การสำรองข้อมูลและระบบงาน (Back Up) เพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้นเมื่อข้อมูลถูกทำลายหรือถูกบุกรุกหรือไม่สามารถให้บริการได้

4.2 การป้องกันไวรัสคอมพิวเตอร์

4.2.1 ติดตั้งโปรแกรมป้องกันและตรวจจับไวรัส (Anti-Virus) ครอบคลุมทุกเครื่องแม่ข่ายและลูกข่าย เพื่อป้องกันความเสียหายของข้อมูล

4.2.2 Update ข้อมูลไวรัสอย่างสม่ำเสมอ อย่างน้อยสัปดาห์ละ 1 ครั้ง โดยเจ้าหน้าที่สามารถทำการ Update ไวรัสได้จากเครื่องคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก ซึ่งจะมีการแนะนำถึงขั้นตอนและวิธีการ Update ให้เจ้าหน้าที่สามารถดำเนินการได้ด้วยตนเอง

4.2.3 ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นดิสก์หรือสื่อบันทึกข้อมูลต่าง ๆ

4.2.4 มีการแนะนำผู้ใช้คอมพิวเตอร์ให้ระวังภัยจากการเปิด File และ E-mail โดย Scan สื่อสำหรับจัดเก็บข้อมูลก่อนการใช้งานไม่เปิดอ่าน E-mail โดยไม่รู้ที่มาและให้ลบเมล์นั้นทิ้งทันทีอย่าเปิดอ่าน

4.3 การป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ

4.3.1 ติดตั้งอุปกรณ์สำรองไฟฟ้า (Uninterruptible Power Supply, UPS) ที่เครื่องของเจ้าหน้าที่ในคณะ/หน่วยงานของมหาวิทยาลัยเทคโนโลยีราชมงคลตะวันออก สำหรับในกรณีที่ไฟฟ้าดับ ซึ่งสามารถจะสำรองไฟฟ้าไว้ได้ภายในระยะเวลา 14 นาที ซึ่งเพียงพอที่จะสั่งการให้ระบบทำการ Shutdown โดยที่ไม่เกิดความเสียหายต่ออุปกรณ์หรือข้อมูล

4.3.2 ดำเนินการเชื่อมโยงระบบไฟฟ้าสำรองของฝ่ายอาคาร

4.4 การป้องกันความเสียงจากไฟไหม้

4.4.1 ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลัก เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) เพื่อการควบคุมเพลิงเบื้องต้นได้

4.4.2 ในกรณีที่เกิดไฟไหม้ภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลักจะมีการตัดการจ่ายกระแสไฟฟ้าภายในบริเวณใกล้เคียง

4.5 การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker)

4.5.1 ติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยให้กับระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ป้องกันการบุกรุกจากภายนอก

4.6 การป้องกันอุปกรณ์ระบบคอมพิวเตอร์แม่ข่ายชำรุด

4.6.1 มีการใช้ Hard disk แบบ RAID- 5 เพื่อป้องกันข้อมูลเสียหายให้กับระบบงานต่าง ๆ

4.7 การป้องกันความเสียงในการปฏิบัติงานของเจ้าหน้าที่

4.7.1 จัดอบรมเสริมสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศเบื้องต้นในด้าน Hardware และ Software เพื่อลดความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ให้น้อยที่สุด

4.8 การป้องกันความเสียงในกรณีที่ระบบเครือข่ายคอมพิวเตอร์มีปัญหา

4.8.1 ดำเนินการติดตั้งเส้นทางสำรองสำหรับระบบงานบริการให้สามารถบริการได้อย่างต่อเนื่อง

4.8.2 ดำเนินการบำรุงรักษาอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์หลักอย่างสม่ำเสมอ

5. การกำหนดผู้รับผิดชอบ

หน้าที่ความรับผิดชอบของผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ มีดังนี้

5.1 เจ้าหน้าที่ดูแลระบบงานและฐานข้อมูลรับผิดชอบดูแล บำรุงรักษาระบบงานและฐานข้อมูล โดยมีหน้าที่ ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่าง ๆ ของระบบงานคอมพิวเตอร์ และการสำรองระบบงาน/ฐานข้อมูล

5.2 เจ้าหน้าที่ดูแลระบบรับผิดชอบ ดูแล บำรุงรักษา ระบบเครือข่ายคอมพิวเตอร์ และความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุง รักษา แก้ไขข้อบกพร่องต่าง ๆ ของระบบเครือข่าย

6. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

6.1 กรณีระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์

6.1.1 ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ โดยพิจารณาตามลำดับความสำคัญของการให้บริการ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

6.1.2 ในกรณีไฟไหม้ ให้ตัดระบบจ่ายไฟ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว 6.1.3 ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลบำรุงรักษาระบบคอมพิวเตอร์แม่ข่าย และ/หรือผู้เชี่ยวชาญระบบเครือข่ายคอมพิวเตอร์โดยเร็วที่สุด

6.1.3 ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสียให้รีบหาอุปกรณ์สำรองหรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษานำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

6.2 กรณีเครื่องลูกข่าย

6.2.1 ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติให้เจ้าหน้าที่ผู้นั้นแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบ อาทิ นักวิชาการคอมพิวเตอร์ของคณะ/หน่วยงาน/สำนักวิทยบริการฯ ทราบ หรือกรณีมีเหตุอันทำให้ฝ่ายการให้บริการระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ไม่สามารถให้บริการได้ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบ เพื่อดำเนินการแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษารีบดำเนินการให้โดยด่วน

6.2.2 กรณีเกิดการชัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้เจ้าหน้าที่ผู้รับผิดชอบดำเนินการ

7. แผนการนำระบบเทคโนโลยีสารสนเทศกลับสู่สภาพปกติ

การกู้คืนระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ โดยปกติจะต้องอยู่ในสภาพพร้อมให้บริการได้ตลอด 24 ชั่วโมง หากไม่สามารถให้บริการจะต้องดำเนินการกู้คืนระบบให้เร็วที่สุดเท่าที่จะทำได้ เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะปกติ เมื่อระบบเสียหายหรือหยุดทำงาน ดังนี้

7.1 ซ่อมอุปกรณ์ที่เสียหายให้เสร็จ ภายใน 48 ชั่วโมง

7.2 สำรองอุปกรณ์ทดแทนหรือยืมอุปกรณ์จากหน่วยงานอื่นมาใช้ทดแทน

7.3 นำข้อมูลที่ได้ทำการสำรองไว้ (Backup) กลับมาใช้ (Restore) เพื่อกู้ระบบให้กลับมาภายใน 48 ชั่วโมง

7.4 ตรวจสอบระบบปฏิบัติการระบบงานและฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลอื่น ๆ ที่เกี่ยวข้อง