เรื่อง นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ พ.ศ. ๒๕๕๙

คำนำ

ตามมาตรา ๕ และมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และ ฉบับที่ ๒ พ.ศ. ๒๕๕๖ กำหนดให้ “หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร”

ทั้งนี้ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ถือว่าเป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่อง และจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่าย นอกจากนั้นยังต้องมีการตรวจสอบอย่างสม่ำเสมอ เพื่อปรับปรุงให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็ว เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยแม่โจ้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้มีการถูกคุกคามจากภัยต่างๆ ขึ้น

ดังนั้น มหาวิทยาลัยแม่โจ้ จึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ พ.ศ. ๒๕๕๙ ขึ้น และให้มีการปรับปรุงปีละ ๑ ครั้ง เพื่อเผยแพร่ให้ผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอกได้รับทราบ และขอความร่วมมือให้ปฏิบัติตามอย่างเคร่งครัดต่อไป

มหาวิทยาลัยแม่โจ้
พฤศจิกายน ๒๕๕๙

สารบัญ

นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้

๑. หลักการและเหตุผล

เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ มหาวิทยาลัยแม่โจ้ จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามมาตรา ๕ และมาตรา ๗ ภายใต้พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้ “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และฉบับที่ ๒ พ.ศ. ๒๕๕๖ กำหนดให้ “หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร”

๒. วัตถุประสงค์และขอบเขต

กำหนดวัตถุประสงค์ในการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นปลอดภัยฯ ไว้ดังนี้

๑) เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของมหาวิทยาลัยแม่โจ้ ให้สามารถดำเนินไปได้อย่างมีประสิทธิภาพ

๒) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ อ้างอิงตามมาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕) และมีการปรับปรุงอย่างต่อเนื่อง

๓) เพื่อเผยแพร่และส่งเสริมให้เจ้าหน้าที่ผู้ดูแลระบบ ผู้ใช้งานระบบ และผู้ที่เกี่ยวข้อง มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และถือปฏิบัติตามอย่างเคร่งครัด ตามหลักจริยธรรมและหลักกฎหมาย

๓. แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้

๑) ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ตอบสนองต่อพันธกิจและนโยบายของมหาวิทยาลัยแม่โจ้

๒) มุ่งกำหนดแนวปฏิบัติ แนวทางการป้องกันและแก้ไข ที่เหมาะสม รวมทั้งการติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายที่เกี่ยวข้อง

๓) เน้นกำกับดูแลการดำเนินงาน เพื่อบริหารจัดการระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ ให้เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง ที่อาจส่งผลให้มีการถูกคุกคามจากภัยต่างๆ ขึ้น

๔) เผยแพร่และส่งเสริมให้เจ้าหน้าที่ผู้ดูแลระบบ ผู้ใช้งานระบบ และผู้ที่เกี่ยวข้อง มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย และถือปฏิบัติตามอย่างเคร่งครัด

๕) ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่งคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับการพัฒนาของระบบเทคโนโลยีและการสื่อสาร

๔. องค์ประกอบของนโยบายและแนวปฏิบัติ

ส่วนที่ ๑ คำนิยาม

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยแม่โจ้

๑) นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

กำหนดมาตรการควบคุมและป้องกัน เพื่อการรักษาความมั่นคงปลอดภัย ที่เกี่ยวข้องกับการเข้าใช้งาน หรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศ ข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่า และอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้

๒) นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

กำหนดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓) นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

๔) นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ กำหนดให้มีการสร้างความรู้ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนดในการรักษาความมั่นคงปลอดภัยสารสนเทศ

๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๑) แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

(๒) แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

(๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ

(๑) แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

(๒) แนวปฏิบัติการกู้คืนระบบ

๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑) แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)

๔) การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

(๑) แนวปฏิบัติการการสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

ส่วนที่ ๑ คำนิยาม

๑) มหาวิทยาลัย	หมายถึง	มหาวิทยาลัยแม่โจ้
๒) วิทยาเขต	หมายถึง	เขตการศึกษาซึ่งประกอบด้วยส่วนงานของมหาวิทยาลัยที่ตั้งอยู่ในเขตท้องที่ตามที่สภามหาวิทยาลัยกำหนด ดังนี้ - มหาวิทยาลัยแม่โจ้แพร่เฉลิมพระเกียรติ - มหาวิทยาลัยแม่โจ้–ชุมพร
๓) หน่วยงาน	หมายถึง	คณะ/สำนัก/วิทยาลัย/ศูนย์/สถาบัน
๔) หน่วยงานภายนอก	หมายถึง	องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของมหาวิทยาลัย โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล
๕) ผู้บริหารระดับสูงสุด (Chief Executive Officer : CEO)	หมายถึง	อธิการบดี
๖) ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศและการสื่อสาร (CIO)	หมายถึง	ผู้บริหาร/ผู้บริหารระดับสูง ที่ได้รับมอบหมายจากอธิการบดีให้กำกับดูแลงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย และมีคุณสมบัติตามมติคณะรัฐมนตรี เมื่อวันที่ ๙ มิถุนายน ๒๕๔๑
๗) ผู้บริหารด้านไอที	หมายถึง	อธิการบดีหรือผู้ที่อธิการบดีมอบหมายให้กำกับดูแลศูนย์เทคโนโลยีสารสนเทศ และการพัฒนาระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของมหาวิทยาลัย
๘) ผู้บังคับบัญชา	หมายถึง	ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของมหาวิทยาลัย
๙) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ	หมายถึง	ผู้อำนวยการ รองผู้อำนวยการ ผู้ช่วยผู้อำนวยการ หัวหน้าหน่วยงานที่ได้รับมอบหมายให้ดูแลด้านไอที
๑๐) ศูนย์เทคโนโลยีสารสนเทศ	หมายถึง	หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่งโปรแกรมและเครือข่ายภายในมหาวิทยาลัย

๑๑) ผู้ดูแลระบบ (System Administrator)	หมายถึง	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
๑๒) ผู้พัฒนาระบบ	หมายถึง	ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ
๑๓) เจ้าของข้อมูล	หมายถึง	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย
๑๔) ผู้ใช้งาน	หมายถึง	บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ โดยมีสิทธิ์และหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของมหาวิทยาลัยได้ ได้แก่ **ผู้บริหาร** หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี ผู้อำนวยการสำนักฯ กองฯ ศูนย์ฯ คณบดี หัวหน้างาน **ผู้ดูแลระบบ (System Administrator)** หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหาร ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ/จ้างเหมา **นักศึกษา** หมายถึง นักศึกษามหาวิทยาลัยแม่โจ้ ระดับปริญญาตรี ปริญญาโท ปริญญาเอก **บุคคลภายนอก** หมายถึง เจ้าหน้าที่จากหน่วยงานภายนอกที่ปฏิบัติการร่วมกับ มหาวิทยาลัยแม่โจ้
๑๕) การรักษาความมั่นคงปลอดภัย	หมายถึง	การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสาร
๑๖) มาตรฐาน (Standard)	หมายถึง	บรรทัดฐานที่บังคับใช้ในการปฏิบัติการจริง เพื่อให้ได้ตามวัตถุประสงค์ หรือเป้าหมาย

๑๗) วิธีการปฏิบัติ (Procedure)	หมายถึง	รายละเอียดที่บอกขั้นตอนเป็นข้อ ๆ ที่ต้องนำมาปฏิบัติเพื่อให้ได้มาซึ่งมาตรฐานที่ได้กำหนดไว้ตามวัตถุประสงค์
๑๘) แนวทางปฏิบัติ (Guideline)	หมายถึง	แนวทางที่ไม่ได้บังคับให้ปฏิบัติแต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น
๑๙) สิทธิของผู้ใช้งาน	หมายถึง	สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัย
๒๐) สินทรัพย์	หมายถึง	ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับมหาวิทยาลัย ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อาทิ บุคลากร ฮาร์ดแวร์ ซอฟต์แวร์ คอมพิวเตอร์ เครื่องคอมพิวเตอร์แม่ข่าย ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์ระบบเครือข่าย เลขไอพี โดเมนเนม รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์ หรือสิ่งใดก็ตามที่มีคุณค่าต่อหน่วยงาน
๒๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ	หมายถึง	การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทายกายภาพ ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
๒๒) ความมั่นคงปลอดภัยด้านสารสนเทศ	หมายถึง	ความมั่นคงและความปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ โดยธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)
๒๓) เหตุการณ์ด้านความปลอดภัย	หมายถึง	เหตุการณ์ที่เกิดขึ้นกับระบบคอมพิวเตอร์ และระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หรือเหตุการณ์ที่สงสัยว่าจะเป็นจุดอ่อน หรืออาจสร้างความเสียหายและส่งผลให้ ๑. เกิดการหยุดชะงักต่อกระบวนการหรือขั้นตอนการ

		ปฏิบัติงานสำคัญ เช่น ระบบงานสารสนเทศของหน่วยงานหยุดชะงัก เป็นต้น ๒. เป็นการละเมิดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ๓. เป็นการละเมิดต่อกฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดต่างๆ ที่กำหนดไว้ ๔. เกิดภาพลักษณ์ที่ไม่ดีต่อมหาวิทยาลัย หรือทำให้สูญเสียชื่อเสียง เช่น การโพสต์ข้อความพาดพิงถึงมหาวิทยาลัยในเว็บไซต์ภายนอก ซึ่งทำให้เกิดความเสียหายต่อชื่อเสียงของมหาวิทยาลัย เป็นต้น ๕. เหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุการณ์ ที่เป็นจุดอ่อนจำเป็นต้องได้รับรายงานจากผู้ใช้งาน เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นอย่างเหมาะสม ได้ผลและทันกาล
๒๔) สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด	หมายถึง	สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ที่อาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
๒๕) ข้อมูลคอมพิวเตอร์	หมายถึง	ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์
๒๖) สารสนเทศ	หมายถึง	ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผลการจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิกให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ
๒๗) ระบบคอมพิวเตอร์	หมายถึง	อุปกรณ์ หรือ ชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๒๘) ระบบเทคโนโลยีสารสนเทศ	หมายถึง	ระบบงานของมหาวิทยาลัยที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่มหาวิทยาลัยสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการการพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ
๒๙) ระบบเครือข่าย	หมายถึง	ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศ ระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของมหาวิทยาลัยได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) และระบบอินเทอร์เน็ต (Internet)
๓๐) ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet)	หมายถึง	เครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบคอมพิวเตอร์ต่าง ๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน
๓๑) ระบบอินเทอร์เน็ต (Internet)	หมายถึง	ระบบเครือข่ายอิเล็กทรอนิกส์ ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงาน เข้ากับเครือข่ายอินเทอร์เน็ตสากล
๓๒) จดหมายอิเล็กทรอนิกส์ (e–Mail)	หมายถึง	ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่ง จะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน ผ่านโพรโตคอลมาตรฐานที่ใช้ในการรับ–ส่งข้อมูล ได้แก่ SMTP, POP๓ และ IMAP เป็นต้น โดยชื่อที่ใช้ในการับส่งจดหมายอิเล็กทรอนิกส์จะประกอบด้วย ๒ ส่วน คือ ชื่อผู้ใช้งาน และชื่อโดเมน เช่น User@mju.ac.th, User@phrae.mju.ac.th
๓๓) สื่อบันทึกพกพา (Portable Media)	หมายถึง	สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD, DVD, Flash Drive, External Hard Disk
๓๔) ชื่อผู้ใช้งาน (Username)	หมายถึง	ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้ในระบบคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๓๕) รหัสผ่าน (Password)	หมายถึง	ชุดของตัวอักษร หรืออักขระ หรือตัวเลข ที่ถูกกำหนดขึ้นเพื่อใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล ในการควบคุมการเข้าถึงข้อมูลและระบบเครือข่าย
๓๖) การเข้ารหัสลับ (Encryption)	หมายถึง	การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
๓๗)อุปกรณ์จัดเส้นทาง (Router)	หมายถึง	อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น
๓๘) การพิสูจน์ยืนยันตัวตน (Authentication)	หมายถึง	ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
๓๙) SSID (Service Set Identifier)	หมายถึง	ชื่อระบุเครือข่ายไร้สาย
๔๐) WPA (Wi–Fi Protected Access)	หมายถึง	ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายพัฒนาขึ้นมาใหม่มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP
๔๑) MAC Address (Media Access Control Address)	หมายถึง	หมายเลขเฉพาะที่ใช้อ้างอิงถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอินเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
๔๒) VPN (Virtual Private Network)	หมายถึง	เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ–ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
๔๓) แผนผังระบบเครือข่าย (Network Diagram)	หมายถึง	แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัย

๔๔) ชุดคำสั่งไม่พึงประสงค์	หมายถึง	ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้
๔๕) สถานการณ์ความเสี่ยง	หมายถึง	ความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ได้แก่ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน ภัยที่เกิด Software ภัยจากไฟไหม้หรือระบบไฟฟ้า และภัยจากน้ำท่วม (อุทกภัย)

ส่วนที่ ๒ นโยบายการรักษาความมั่นคงปลอดภัยสารสนเทศ มหาวิทยาลัยแม่โจ้

หมวดที่ ๑ นโยบายการควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศของมหาวิทยาลัย

๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร ผู้ใช้งาน ผู้ดูแลระบบ และบุคคลภายนอก ที่ปฏิบัติงานให้กับมหาวิทยาลัย ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) ศูนย์เทคโนโลยีสารสนเทศ

๒) หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ข่าย

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

๔) ผู้ใช้งาน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

นโยบาย

กำหนดนโยบายควบคุมการเข้าถึงและใช้งานระบบสารสนเทศ เป็นการกำหนดมาตรฐานแนวทางปฏิบัติที่มีความสอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสำหรับผู้ใช้งาน เจ้าหน้าที่ รวมถึงบุคคลภายนอก เพื่อควบคุมให้เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต โดยมีมาตรการควบคุมการเข้าถึงและใช้งานสารสนเทศ ตามแนวปฏิบัติ ดังต่อไปนี้

(๑) แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

(๑.๑) ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

(๑.๑.๑) การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

- การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
- การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย
- การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(๑.๑.๒) การอนุญาต กำหนดสิทธิ หรือการมอบอำนาจ ในการเข้าถึงและใช้งานระบบสารสนเทศ

(๑.๑.๓) การจัดหมวดหมู่และการเข้าถึงระบบสารสนเทศ

- ประเภทของข้อมูล

- ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล
- ระดับชั้นการเข้าถึง
- เวลาที่ได้เข้าถึง
- ช่องทางการเข้าถึง

(๑.๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(๑.๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

(๑.๓.๑) การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

(๑.๓.๒) การลงทะเบียนผู้ใช้งาน (User Registration)

(๑.๓.๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

(๑.๓.๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password management)

(๑.๓.๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

(๑.๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

(๑.๔.๑) การใช้งานรหัสผ่าน (Password Use)

(๑.๔.๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

(๑.๔.๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

(๑.๔.๔) การเข้ารหัสข้อมูลที่เป็นความลับ

(๑.๔.๕) การใช้งานระบบจดหมายอิเล็กทรอนิกส์

(๑.๔.๖) การใช้งานระบบอินเทอร์เน็ต

(๑.๔.๗) การใช้งานเครือข่ายสังคมออนไลน์

(๒) แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

(๒.๑) การใช้บริการเครือข่าย

(๒.๒) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

(๒.๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

(๒.๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๒.๕) การแบ่งแยกเครือข่าย (Segregation in Networks)

(๒.๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

(๒.๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

(๒.๘) การบริหารจัดการการบันทึกและตรวจสอบ

(๒.๙) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

(๒.๑๐) การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

(๒.๑๑) การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

(๓) แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๔) แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

(๔.๑) การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

(๔.๒) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

(๔.๓) การบริหารจัดการรหัสผ่าน (Password Management System)

(๔.๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

(๔.๕) การจำกัดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time-Out)

(๔.๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time)

(๕) แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

(๕.๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

(๕.๒) การควบคุมการเข้าถึงระบบซึ่งไวต่อการรบกวน

(๕.๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารและการปฏิบัติงานจากภายนอกองค์กร (Mobile Compution and Teleworking)

(๕.๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๕.๕) การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

หมวดที่ ๒ นโยบายการจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑) เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและระบบคอมพิวเตอร์

๒) เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับมหาวิทยาลัย

๓) เพื่อป้องกันและขจัดปัญหาข้อมูลสำคัญสูญหาย

ผู้รับผิดชอบ

๑) ศูนย์เทคโนโลยีสารสนเทศ

๒) หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ข่าย

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

นโยบาย

กำหนดให้มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยมีมาตรการ ตามแนวปฏิบัติ ดังต่อไปนี้

(๑) แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

- (๑.๑) การคัดเลือกและจัดทำระบบสำรอง
- (๑.๒) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- (๑.๓) การกำหนดหน้าที่และความรับผิดชอบระบบสารสนเทศ ระบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน
- (๑.๔) การทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉิน

(๒) แนวปฏิบัติการกู้คืนระบบ

หมวดที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

๒) เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศ

ผู้รับผิดชอบ

๑) ศูนย์เทคโนโลยีสารสนเทศ

๒) สำนักงานตรวจสอบภายใน (Internal Auditor) หรือผู้ตรวจสอบจากภายนอก (External Auditor)

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย/เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

นโยบาย

กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยมีมาตรการตามแนวปฏิบัติ ดังต่อไปนี้

(๑) แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)

(๒) การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการ โดยผู้ตรวจสอบภายในหน่วยงานของรัฐ (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

หมวดที่ ๔ นโยบายการสร้างความรู้ ความเข้าใจการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑) เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของมหาวิทยาลัย

๒) เพื่อเป็นการป้องกันการกระทำผลิที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้งาน

๓) เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) ศูนย์เทคโนโลยีสารสนเทศ

๒) กองการเจ้าหน้าที่

๓) ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชั่น ๒.๕)

นโยบาย

กำหนดให้มีการสร้างความรู้ความเข้าใจ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้แก่ผู้ใช้งานทั้งภายในและภายนอก โดยมีมาตรการตามแนวปฏิบัติ ดังต่อไปนี้

(๑) แนวปฏิบัติการการสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและ/หรือระบบคอมพิวเตอร์

ส่วนที่ ๓ แนวปฏิบัติและข้อกำหนด ในการรักษาความมั่นคงปลอดภัยสารสนเทศ

แนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศ

๑. ข้อกำหนดการเข้าถึงและควบคุมการใช้งานสารสนเทศ (Access Control)

เพื่อกำหนดมาตรการควบคุมบุคคลที่ไม่ได้รับอนุญาติเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก จากโปรแกรมชุดคำสั่งไม่พึงประสงค์ ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และทำให้สามารถตรวจสอบ ติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ ได้อย่างถูกต้อง

๑.๑ กระบวนการหลักในการควบคุมการเข้าถึงระบบ

(๑) สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ต้องมีการควบคุมการเข้าออกที่รัดกุมและอนุญาติให้เฉพาะบุคคลที่ได้รับสิทธิและมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

(๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูล และระบบข้อมูล ให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาติจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(๓) ผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูลและระบบข้อมูลได้

(๔) ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูลสำคัญ

(๕) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้าออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาติและไม่ได้รับอนุญาติ เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

๑.๒ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(๑) ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ในการขออนุญาติเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิใน

การเข้าสู่ระบบ และกำหนดให้มีการลงนามอนุมัติเอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

(๒) เจ้าของข้อมูล และ **"เจ้าของระบบงาน"** จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตาม ความจำเป็นขั้นต่ำเท่านั้น

(๓) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูล และระบบงาน ตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

๑.๓ การบริหารจัดการการเข้าถึงของผู้ใช้ (User Account) และรหัสผ่านของเจ้าหน้าที่

(๑) ผู้ดูแลระบบ ที่รับผิดชอบระบบงานนั้นๆ ต้องกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิแยกตามหน้าที่ ที่รับผิดชอบ ซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ใน "การบริหารจัดการการเข้าถึงของผู้ใช้งาน"

(๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามที่กำหนดไว้ใน "การบริหารจัดการการเข้าถึงของผู้ใช้งาน"

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้ หมายถึงผู้ใช้ที่มีสิทธิสูงสุด ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๔) ควรได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบงานนั้น ๆ

(๕) ควรควบคุมการใช้งานอย่างเข้มงวด เช่น กำหนดให้มีการควบคุมการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

(๖) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

(๗) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือนเป็นต้น

๑.๔ การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล

(๑) การควบคุมการติดตั้งซอฟต์แวร์ลงไปยังเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

[๑] ให้ผู้ดูแลระบบที่ได้รับการอบรมแล้ว หรือมีความชำนาญเท่านั้น ที่จะเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย โดยกำหนดบุคคลที่

รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรม ระบบ (System Software) อย่างชัดเจน

[๒] จัดทำคู่มือปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไขรวมทั้งมีการรายงานโดยทันที

[๓] เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น

[๔] ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ

[๕] การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศต้องมีการขออนุมัติให้ติดตั้งก่อนการดำเนินงาน

[๖] ไม่ติดตั้งรหัสต้นฉบับ (Source Code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

[๗] ให้มีการจัดเก็บรหัสต้นฉบับและคลังโปรแกรม (Library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

[๘] ให้มีการระบุความต้องการทางสารสนเทศสำหรับระบบสารสนเทศที่ต้องการปรับปรุงก่อนที่จะเริ่มต้นการพัฒนา และให้ทำการทดสอบซอฟต์แวร์ระบบปฏิบัติการ และระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วนเพียงพอก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

[๙] ให้มีการจัดเก็บซอฟต์แวร์เวอร์ชันเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิม และขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชันเก่าเหล่านั้น

(๒) การทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการของเครื่องแม่ข่ายให้บริการ

[๑] แจ้งให้ผู้ที่เกี่ยวข้องระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

[๒] พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศรวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่มหาวิทยาลัยต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

[๓] มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไป หลังจากการแก้ไข หรือบำรุงรักษาระบบด้วย

๑.๕ การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงและใช้งานระบบสารสนเทศ

การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานแต่ละกลุ่ม มีดังนี้

(๑) การกำหนดสิทธิของผู้ใช้งาน

(๑.๑) สิทธิ์อ่านอย่างเดียว

(๑.๒) สิทธิ์การสร้างข้อมูล

(๑.๓) สิทธิ์การแก้ไขข้อมูล

(๑.๔) สิทธิ์การลบข้อมูล

(๑.๕) สิทธิ์การอนุมัติ/อนุญาต

(๑.๖) ไม่มีสิทธิ์

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของมหาวิทยาลัยจะต้องได้รับการพิจารณาอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย

๑.๖ การแบ่งประเภท ลำดับความสำคัญ ชั้นความลับ และการเข้าถึงข้อมูล

การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสม ในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์

(๑) ประเภทของข้อมูล

จัดแบ่งประเภทของข้อมูล ออกเป็น

(๑.๑) ข้อมูลที่เปิดเผยได้ทั่วไป

(๑.๒) ข้อมูลที่เปิดเผยเฉพาะ ที่มีการจำกัดการเข้าถึง ประกอบด้วย

[๑] ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์และคำรับรอง ข้อมูลบุคลากร ข้อมูลการเงินงบประมาณและบัญชี เป็นต้น

[๒] ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย และข้อมูลด้านบริการวิชาการ เป็นต้น

(๒) ลำดับความสำคัญ

จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๔ ระดับ คือ

(๒.๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด ได้แก่ ข้อมูล ๕ ด้านของมหาวิทยาลัย คือ ฐานข้อมูลนักศึกษาและหลักสูตร บุคลากร วิจัย งบประมาณ และอาคารสถานที่

(๒.๒) ข้อมูลที่มีระดับความสำคัญมาก ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ โครงการ/กิจกรรม

(๒.๓) ข้อมูลที่มีระดับความสำคัญปานกลาง

(๒.๔) ข้อมูลที่มีระดับความสำคัญน้อย

การจัดลำดับความสำคัญของข้อมูล ให้พิจารณาในระดับฐานข้อมูล ด้วยวิธีการประเมินผลกระทบต่อกระบวนการทำงานขององค์กร มีแนวทางการพิจารณา ดังนี้

ระดับความสำคัญ	การประเมินผลกระทบต่อกระบวนการทำงานขององค์กร
ความสำคัญมากที่สุด	ขั้นตอน/กระบวนการทำงานล้มเหลวโดยสิ้นเชิง หรือมีแนวโน้มเกิดความเสี่ยงทางการเงิน หรือการปฏิบัติตามกฎระเบียบต่างๆ
ความสำคัญมาก	ขั้นตอน/กระบวนการทำงานติดขัด และมีผลต่อการดำเนินภารกิจขององค์กร รวมถึงสถานภาพขององค์กร
ความสำคัญปานกลาง	มีผลต่อการดำเนินภารกิจขององค์กรเล็กน้อย
ความสำคัญน้อย	ไม่มีผลกระทบต่อการดำเนินภารกิจขององค์กร

(๓) กำหนดหน่วยงานเจ้าภาพ รับผิดชอบฐานข้อมูล ๕ ด้าน มหาวิทยาลัยแม่โจ้ ดังนี้

ลำดับ	ฐานข้อมูล	หน่วยงานเจ้าภาพ
๑	ข้อมูลด้านนักศึกษาและหลักสูตร	สำนักบริหารและพัฒนาวิชาการ
๒	ข้อมูลด้านบุคลากร	กองการเจ้าหน้าที่ สำนักงานอธิการบดี
๓	ข้อมูลงานวิจัย	สำนักวิจัยและส่งเสริมวิชาการการเกษตร
๔	ข้อมูลงบประมาณ	กองแผนงาน สำนักงานอธิการบดี
๕	ข้อมูลอาคารและพื้นที่ใช้สอย	กองอาคารและสถานที่ สำนักงานอธิการบดี

(๔) ลำดับชั้นความลับ

[๑] ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

[๒] ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

[๓] ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วน

จะก่อให้เกิดความเสียหาย

[๔] ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

การจัดชั้นความลับของข้อมูล ให้พิจารณาจากความสำคัญของเนื้อหา แหล่งข้อมูล วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่สามารถเปิดเผยได้ ผลกระทบหากมีการเปิดเผยข้อมูล และหน่วยงานที่รับผิดชอบ ในฐานะเจ้าของข้อมูล ทั้งนี้ **ให้มีการจัดทำข้อตกลงการรักษาความลับที่เกี่ยวข้องกับข้อมูลส่วนบุคคล ที่เปิดเผยได้เฉพาะบุคคล เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลแล้วเท่านั้น**

(๕) ระดับชั้นการเข้าถึง

โดยการแบ่งสิทธิการเข้าถึงตามประเภทของข้อมูล ดังนี้

(๕.๑) ประเภทของข้อมูลทั่วไป กำหนดสิทธิ์ให้ทุกคนสามารถเข้าถึงข้อมูลได้

(๕.๒) ประเภทของข้อมูลที่ต้องกำหนดสิทธิ์การเข้าถึง มีระดับการเข้าถึง ดังนี้

[๑] ระดับผู้ปฏิบัติงาน

[๒] ระดับผู้ตรวจสอบข้อมูล

[๓] ระดับผู้ลงนามรับรองผล/อนุมัติ

[๔] ระดับการเข้าถึงรายงานสรุป

[๕] ระดับผู้ดูแลระบบ ระดับหน่วยงาน

[๖] ระดับผู้ดูแลระบบย่อย ตามคำสั่งหน่วยงานเจ้าของข้อมูล

[๗] ระดับผู้ดูแลระบบสูงสุด

(๖) เวลาที่ได้เข้าถึง

(๖.๑) ระบบงานบริการ (Front Office) สำหรับผู้ใช้งานทั่วไปสามารถเข้าถึงได้ตลอดเวลา

(๖.๒) ระบบงานภายใน (Back Office) สำหรับผู้ใช้งานภายในมหาวิทยาลัย สามารถเข้าถึงระบบได้ตามช่วงเวลา ดังต่อไปนี้

[๑] ในเวลาราชการ (๐๘.๓๐ น. – ๑๖.๓๐ น.)

[๒] นอกเวลาราชการ (นอกช่วงเวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.)

[๓] ช่วงเวลาวันหยุดราชการ (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

[๔] ช่วงเวลาพิเศษเป็นรายครั้ง โดยระบุเป็นช่วงเวลา ระยะเวลาการเข้าถึง

(๗) ช่องทางการเข้าถึง

(๗.๑) ผู้ใช้งานเข้าใช้บริการผ่านระบบเครือข่ายภายในมหาวิทยาลัย ได้ตลอด ๒๔ ชั่วโมง

(๓/.๒) ผู้ใช้งานเข้าใช้ผ่านระบบเครือข่ายจากภายนอกมหาวิทยาลัย สามารถเข้าใช้บริการผ่านระบบ VPN ได้ตลอด ๒๔ ชั่วโมง

(๓/.๓) การประชุมทางไกล สามารถเข้าถึงได้เฉพาะในเวลาราชการและกำหนดเป็นช่วงเวลาเป็นรายครั้ง

(๓/.๔) การติดต่อด้วยตนเองและการประสานงานผ่านโทรศัพท์ สามารถเข้าถึงได้เฉพาะในเวลาราชการ

๒. ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๒.๑ การควบคุมการเข้าถึงสารสนเทศตามภารกิจ

มหาวิทยาลัยแม่โจ้ จัดให้มีการบริการสารสนเทศ รวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อใช้ประโยชน์ตามภารกิจของมหาวิทยาลัย ได้แก่ การเรียนการสอน การวิจัย การบริการวิชาการ การทำนุบำรุงศิลปวัฒนธรรม และการบริหารจัดการ ทั้งนี้การใช้งานตามภารกิจต้องอยู่บนพื้นฐานของการเคารพสิทธิและความรู้สึกของบุคคลอื่น เคารพและปฏิบัติให้ถูกต้องตามกฎหมาย และต้องไม่เกี่ยวข้องกับการดำเนินธุรกิจการค้าใดๆ โดยกำหนดสิทธิการเข้าถึง จะแบ่งตามลำดับชั้นการบริหารจัดการของผู้บริหาร ดังนี้

(๑) ผู้บริหารระดับสูง ได้แก่ อธิการบดี รองอธิการบดี สามารถเข้าถึงข้อมูลได้ตามภารกิจที่ได้รับมอบหมายให้กำกับดูแล

(๒) ผู้บริหารระดับหน่วยงาน / หลักสูตร ได้แก่ ผู้อำนวยการ คณบดี ประธานหลักสูตร สามารถเข้าถึงข้อมูลภายใต้ความรับผิดชอบดูแล

(๓) ผู้ปฏิบัติงาน สามารถเข้าถึงได้เฉพาะส่วนงานที่ตนเองได้รับมอบหมาย

๒.๒ การอนุญาตและการทบทวนสิทธิการเข้าถึงตามภารกิจ

(๑) ผู้ใช้งานจะต้องได้รับอนุญาตจากหน่วยงานเจ้าของข้อมูลและผู้ดูแลระบบตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

(๒) เจ้าของข้อมูล และเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะส่วนที่จำเป็นตามหน้าที่งานที่ได้รับมอบหมายเท่านั้น

(๓) ผู้ดูแลระบบมีหน้าที่ตรวจสอบการอนุมัติ และกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งาน ซึ่งต้องมีการจัดทำเอกสารขอสิทธิ์ในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ

(๔) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามแนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) ที่กำหนดไว้

๒.๓ ข้อมูลพื้นฐานที่ใช้ประกอบการควบคุมและจำกัดสิทธิ์สำหรับผู้ใช้งาน

(๑) ตำแหน่ง / ตำแหน่งทางการบริหาร

(๒) หน่วยงานต้นสังกัด

(๓) คำสั่งมอบหมายงานและหน้าที่รับผิดชอบ

(๔) สำเนาสัญญาจ้าง (สำหรับบุคลากรจ้างเหมา)

(๕) วันที่เริ่มต้น–สิ้นสุดสัญญา

(๖) ลายเซ็นอนุมัติจากหัวหน้างาน

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบเทคโนโลยีสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบเทคโนโลยีสารสนเทศและเครือข่ายภายใน โดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบเทคโนโลยีสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ ดังนี้

๓.๑ การสร้างความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยสารสนเทศ

(๑) มีการเผยแพร่นโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ใช้งานได้รับทราบ

(๒) มีการจัดฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

๓.๒ การลงทะเบียนผู้ใช้งาน (User Registration)

(๑) การลงทะเบียนเจ้าหน้าที่ใหม่ของมหาวิทยาลัยแม่โจ้ กำหนดให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น และผู้ดูแลระบบ

(๒) จัดทำแบบฟอร์มขอใช้บริการสารสนเทศ ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิ์และดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๓) มีการระบุชื่อบัญชีผู้ใช้งาน (Username) แยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

[๑] การระบุชื่อบัญชีผู้ใช้ สำหรับนักศึกษาจะใช้อักษร mju ตามด้วยรหัสนักศึกษา

[๒] การระบุชื่อบัญชีผู้ใช้ สำหรับบุคลากรสามารถกำหนดเองได้ โดยต้องไม่ซ้ำกับชื่อบัญชีของผู้ใช้รายอื่น

(๔) ใช้ @mju.ac.th สำหรับบุคลากรและนักศึกษามหาวิทยาลัยแม่โจ้ ทุกคน และ @phare.mju.ac.th สำหรับบุคลากรที่ใช้งานระบบสารสนเทศภายในของมหาวิทยาลัยแม่โจ้แพร่เฉลิมพระเกียรติ

(๕) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกัน และอนุญาตให้ใช้เท่าที่จำเป็น

(๖) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการยกเลิก เพิกถอน การอนุญาต ให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งาน เมื่อมีการ ลาออก เปลี่ยนตำแหน่ง โอนย้าย สิ้นสุดการจ้าง โดยต้องทำการยกเลิกสิทธิการใช้งาน เมื่อเจ้าหน้าที่ลาออกจากการเป็นบุคลากรภายใน ๒๔ ชั่วโมง หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องทำภายใน ๗ วัน ทั้งนี้โดยอ้างอิงจากเอกสารราชการของกองการเจ้าหน้าที่เป็นสำคัญ

(๙) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบ ต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

(๑๐) มีการแจ้งให้ผู้ใช้งานเปลี่ยนรหัสผ่าน อย่างน้อยทุก ๖ เดือนสำหรับผู้ใช้งานทั่วไป และอย่างน้อยทุก ๓ เดือน สำหรับผู้บริหารและผู้ดูแลระบบ หรือตามระยะเวลาที่เหมาะสม

๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

(๑) ผู้ดูแลระบบ ต้องกำหนด ชื่อบัญชีผู้ใช้ รหัสผ่าน และสิทธิในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ ตามหน้าที่ความรับผิดชอบ ของแต่ละกลุ่มผู้ใช้งาน เพื่อใช้ในการตรวจสอบยืนยันตัวตนของผู้ใช้งาน

(๒) ผู้ใช้งาน ต้องรับทราบสิทธิและหน้าที่ เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ผู้ใช้งานนั้นต้องได้รับความเห็นชอบ และอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว ทั้งนี้ต้องได้รับหนังสือจากต้นสังกัด โดยให้มีการพิจารณาควบคุมการใช้งาน ดังนี้

[๑] ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบนั้นๆ

[๒] ควบคุมการใช้งานอย่างเข้มงวด กำหนดให้มีการใช้งานเฉพาะกรณีจำเป็นเท่านั้น

[๓] กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าว

[๔] มีการเปลี่ยนรหัสผ่านทุกครั้งหลังหมดความจำเป็นในการใช้งาน หรือหากมีความจำเป็นต้องใช้งานเป็นระยะเวลานาน ต้องเปลี่ยนรหัสผ่านอย่างน้อยทุก ๓ เดือน

๓.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password management)

โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

(๑) กระบวนการจัดสรร หรือแจกจ่ายรหัสผ่านให้แก่ผู้ใช้งาน

[๑] กำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

[๒] การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

[๓] ส่งมอบรหัสผ่านชั่วคราว ให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ ในการจัดส่งรหัสผ่าน

[๔] ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

[๕] มีการแจ้งหน้าที่รับผิดชอบของผู้ใช้งานให้ดูแลรหัสผ่านและดูแลการใช้งาน e-Mail ในทางที่ถูกต้อง โดยไม่ผิดต่อพระราชบัญญัติที่ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๒) ขั้นตอนการเปลี่ยนรหัส

[๑] อนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเอง

[๒] การเปลี่ยนรหัสผ่าน ต้องตรวจสอบบัญชีรายชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

[๓] ผู้ใช้งาน ควรทำการล็อกอินเข้าใช้งานระบบงานครั้งแรกและทำการเปลี่ยนรหัสผ่านทันที หลังจากได้รับรหัสผ่านชั่วคราว

๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

(๑) กองการเจ้าหน้าที่ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศ ทราบทันทีเมื่อ

[๑] มีการว่าจ้างงาน

[๒] มีการเปลี่ยนแปลงสภาพการจ้างงาน

[๓] มีการลาออกจากงาน หรือสิ้นสุดการเป็นผู้บริหาร บุคลากร และลูกจ้าง หรือการถึงแก่กรรม

[๔] มีการโยกย้ายหน่วยงาน

[๕] มีการพักงาน การลงโทษทางวินัย หรือถูกระงับการปฏิบัติหน้าที่

(๒) ผู้ดูแลระบบ ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง ดังนี้

[๑] ผู้ดูแลระบบต้องดำเนินการแก้ไขสิทธิการเข้าถึงของผู้ใช้ ทันทีที่ได้รับ แจ้งการเปลี่ยนแปลงจากกองการเจ้าหน้าที่

[๒] ผู้ดูแลระบบทบทวนสิทธิสำหรับผู้ที่มีสิทธิการเข้าถึงระดับสูง ได้แก่ สิทธิ์ผู้ดูแลระบบระดับหน่วยงาน สิทธิ์ผู้ดูแลระบบย่อย ตามคำสั่งมอบหมายของหน่อยงานเจ้าของระบบ และสิทธิ์ผู้ดูแลระบบสูงสุด ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป

[๓] ผู้ดูแลระบบ ต้องกำหนดให้มีการบันทึกการเปลี่ยนแปลงต่อบัญชีผู้ใช้งานที่มีสิทธิการเข้าถึงในระดับสูง เพื่อใช้ในการทบทวนในภายหลัง

๓.๖ การเพิกถอนสิทธิการเข้าถึงของผู้ใช้งาน

(๑) ผู้ดูแลระบบดำเนินการเพิกถอนสิทธิผู้ใช้งานที่พ้นสภาพการเป็นนักศึกษาและบุคลากรของมหาวิทยาลัยแม่โจ้ ยกเว้นกรณีเกษียณอายุราชการ อย่างน้อยปีละ ๑ ครั้ง โดยผู้ใช้งานที่เป็นข้าราชการเกษียณอายุ นักศึกษาที่จบการศึกษาแล้ว อนุญาตให้ใช้บัญชีรายชื่อผู้ใช้งานได้

(๒) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออก/เปลี่ยนตำแหน่งงาน/โอนย้ายข้ามหน่วยงานราชการ/ถึงแก่กรรม โดยอ้างอิงหนังสือราชการจากกองการเจ้าหน้าที่

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ เป็นการป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต มีข้อปฏิบัติดังนี้

๔.๑ การใช้งานรหัสผ่าน (Password Use)

(๑) การตั้งและการเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๑.๑) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที

(๑.๒) กำหนดรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น โดยมีเทคนิคที่ง่ายต่อการจดจำ

(๑.๓) เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

(๑.๔) กำหนดรอบระยะเวลาการเปลี่ยนรหัสผ่าน ดังนี้

[๑] ผู้ดูแลระบบและผู้บริหาร ทุก ๓ เดือน

[๒] ผู้ใช้งานทั่วไป ทุก ๖ เดือน

(๒) คุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

(๒.๑) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๒.๒) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

(๒.๓) หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน (๑๒๓ , abcd) หรือกลุ่มของตัวอักขระที่เหมือนกัน (๑๑๑ , aaa)

(๓) หน้าที่รับผิดชอบของผู้ดูแลระบบ

(๔.๑) ผู้ดูแลระบบทำหน้าที่เฝ้าระวังติดตามการใช้งานผิดวัตถุประสงค์

(๔.๒) ผู้ดูแลระบบมีหน้าที่รายงานเหตุการณ์ที่ผิดปกติให้กับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

(๔.๓) ผู้ดูแลระบบต้องมีรหัสผ่าน ๒ ชุด เพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

(๔) การใช้งานรหัสผ่าน ของผู้ใช้ ต้องปฏิบัติดังนี้

(๓.๑) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๓.๒) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๓.๓) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๓.๔) ไม่กำหนดให้มีการบันทึกช่วยจำรหัสผ่านส่วนบุคคล

(๓.๕) ไม่อนุญาตให้ผู้อื่นใช้รหัสผ่านของตน หากเกิดปัญหาจากการใช้งานที่ผิดต่อกฎหมาย เจ้าของบัญชีต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

(๓.๖) ไม่ลับลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

(๓.๗) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

(๓.๘) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

(๓.๙) ให้มีการรายงานการล่วงละเมินความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

(๓.๑๐) ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด และปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

๔.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ข้อปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัยในขณะที่ไม่มีผู้ดูแล มีดังนี้

(๑) เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและผู้ดูแลระบบ

(๒) เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบล๊อกหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน ๓๐ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงสามารถเปิดหน้าจอได้

(๓) ให้ทำการล๊อกอุปกรณ์ที่สำคัญเมื่อไม่ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๔.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy)

การควบคุมไม่ให้ทรัพย์สินสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

(๑) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

(๑.๑) การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

[๑] จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ มีจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น โดยกำหนดพื้นที่ ดังนี้

[๑.๑] ห้องควบคุมระบบ แบ่งเป็น ๒ พื้นที่ คือ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area)

[๑.๒] พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึง เป็นห้องที่มีการติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย

(๑.๒) การจัดพื้นที่ห้องควบคุมระบบทางกายภาพ

[๑] แยกอุปกรณ์และระบบที่มีความสำคัญมากออกจากอุปกรณ์และระบบที่ใช้งานทั่วไป โดยกำหนดลำดับความสำคัญของอุปกรณ์และระบบแต่ละชนิดไว้

[๒] มีตู้ Rack สำหรับเก็บอุปกรณ์และระบบต่างๆ ที่เหมาะสม เพื่อสะดวกในการบำรุงรักษา

[๓] ตำแหน่งของการวางอุปกรณ์ต่างๆ ไม่ควรวางไว้ใกล้ประตู หน้าต่าง เพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้นได้ ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรง เพื่อหลีกเลี่ยงความชื้น

(๑.๓) การเดินสายไฟ สายสื่อสาร สายเคเบิ้ลอื่นๆ

[๑] หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของมหาวิทยาลัยในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

[๒] ให้มีการป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ เพื่อทำให้เกิดความเสียหาย

[๓] ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

[๔] ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณผิดเส้น

[๕] จัดทำผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

[๖] ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

(๑.๔) ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilies)

[๑] ต้องมีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยที่เพียงพอต้องความต้องการใช้งาน ได้แก่ ระบบปรับอากาศ ระบบระบายอากาศ ระบบกระแสไฟฟ้า ระดับกระแสไฟฟ้า อุปกรณ์สำรองกระแสไฟฟ้า และต้องมีการตรวจสอบหรือทดสอบระบบสนับสนุนอย่างสม่ำเสมอ เพื่อให้มั่นใจว่าระบบทำงานได้ปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

[๒] ต้องมีระบบสำรองกระแสไฟฟ้า เพื่อป้องกันอุปกรณ์เสียหายจากความไม่สม่ำเสมอของกระแสไฟฟ้า และต้องทดสอบระบบสำรองกระแสไฟฟ้าอย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

[๓] ต้องมีระบบไฟฟ้าส่องสว่างฉุกเฉิน เพื่อรองรับในกรณีที่กระแสไฟฟ้าหลักเกิดขัดข้อง

[๔] ต้องมีระบบแจ้งเตือนกรณีระบบสนับสนุนภายในห้องควบคุมระบบทำงานผิดปกติหรือหยุดทำงาน

[๕] ต้องมีระบบสายสื่อสารสำรอง ซึ่งเชื่อมต่อไปยังผู้ให้บริการอินเทอร์เน็ต และ/หรือ ผู้ให้บริการโทรคมนาคม เป็นเส้นทางสำรอง

[๖] ต้องมีระบบรักษาความปลอดภัย กล้องวงจรปิด และระบบบันทึกการเข้าออกพื้นที่ด้วยระบบ Finger Scan

[๗] ต้องมีระบบสังเกตการณ์อุณหภูมิภายในห้องควบคุมระบบ ระบบแจ้งเตือนและป้องกันอัคคีภัย

(๑.๕) การบำรุงรักษาอุปกรณ์

[๑] ให้มีการกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

[๒] ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

[๓] จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

[๔] จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

[๕] ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในมหาวิทยาลัย

[๖] จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

(๒) การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย (Network System Control Room)

(๒.๑) ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

[๑] หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต

- อนุมัติสิทธิเข้าออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

[๒] ผู้ดูแลห้องควบคุมระบบเครือข่าย

- ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในศูนย์ปฏิบัติการให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

(๒.๒) การควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

ผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่ มีแนวทางปฏิบัติดังนี้

[๑] ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิ์บุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้องและมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่”

[๒] การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลง “บันทึกการเข้าออกพื้นที่” ด้วยอุปกรณ์ Finger Scan

[๓] บุคคลภายนอกเข้ามาติดต่อต้องมีหนังสือขอความอนุเคราะห์เข้าศึกษาดูงาน ถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

[๔] บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต

[๕] ประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาต ให้รับทราบทั่วกัน

[๖] หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในมหาวิทยาลัย จะต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒.๓) การควบคุมการพัฒนาซอฟต์แวร์และส่งมอบระบบโดยบุคลภายนอก

[๑] ต้องตรวจคุณสมบัติของผู้รับจ้างให้บริการพัฒนาระบบ ไม่มีประวัติการบุก แก้ไข ทำลาย หรือโจรกรรมข้อมูลสารสนเทศของหน่วยงานใดมาก่อน

[๒] ต้องจัดให้ลงนามในสัญญาระหว่าง “ผู้รับจ้างพัฒนาระบบ” กับ “หน่วยงาน” ว่าจะไม่เปิดเผยความลับของหน่วยงาน (Non–Disclosure Agreement : NDA) โดยการลงนามนี้จะเป็นส่วนหนึ่งของสัญญาจ้าง ทั้งนี้ต้องมีผลผูกพันต่อเนื่องเป็นเวลาไม่น้อยกว่า ๑ ปี ภายหลังจากสิ้นสุดการจ้างแล้ว

[๓] ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับรหัสต้นฉบับ ในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

[๔] มหาวิทยาลัยต้องสงวนสิทธิ์ในการตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่มีการพัฒนาโดยผู้ให้บริการจากภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

[๕] ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (Malware) ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้งในอุปกรณ์ที่ใช้งานจริง

(๒.๔) การนำทรัพย์สินของมหาวิทยาลัยออกนอกมหาวิทยาลัย

[๑] ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกมหาวิทยาลัย

[๒] กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกมหาวิทยาลัย

[๓] เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

[๔] บันทึกข้อมูลการนำอุปกรณ์ของมหาวิทยาลัยออกไปใช้งานนอกมหาวิทยาลัย เพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

(๒.๕) การจัดการอุปกรณ์ที่ใช้งานอยู่นอกมหาวิทยาลัย

[๑] ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของมหาวิทยาลัยไว้โดยลำพังในที่สาธารณะ

[๒] เจ้าหน้าที่มีความรับผิดชอบอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

(๒.๖) การกำจัดอุปกรณ์ หรือการนำอุปกรณ์กลับมาใช้ใหม่อีกครั้ง (Secure disposal or re-use of Equipment)

[๑] ต้องทำการเคลียร์ข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสต์หรือสื่อบันทึกข้อมูลก่อนการทำลายหรือจำหน่าย

[๒] ต้องทำการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อไป เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

[๓] ต้องการทำการ Format ฮาร์ดดิสต์ เพื่อป้องกันการกู้คืน ข้อมูลในฮาร์ดดิสต์โดยการ

- ใช้วิธีแบบเขียนทับซ้ำจำนวน ๑ ครั้ง ตามมาตรฐาน NIST ๘๐๐-๘๘ สำหรับข้อมูลที่มีความลับระดับต่ำ
- ใช้วิธีแบบเขียนทับซ้ำจำนวน ๓ ครั้ง ตามมาตรฐาน DoD ๕๒๒๐.๒๒-M สำหรับข้อมูลที่มีความลับระดับปานกลาง
- ใช้วิธีแบบเขียนทับซ้ำจำนวน ๗ ครั้ง ตามมาตรฐาน NSA สำหรับข้อมูลที่มีความลับระดับสูง

[๔] ควรลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ ๕ ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสต์ภายนอก (External Harddisk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

[๕] ต้องได้รับความเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและ/หรือผู้บังคับบัญชาของหน่วยงานเจ้าของข้อมูล ในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

[๖]มาตรฐานการทำลายสื่อบันทึกข้อมูลและข้อมูลอิเล็กทรอนิกส์ มีดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
– Harddisk – Memory Device แบบ USB – Flash Drive – SD Card	๑) ทำลายข้อมูลโดยใช้เทคโนโลยีซอฟต์แวร์ Wiping ที่สอดคล้องกับมาตรฐาน DoD ๕๒๒๐.๒๒ M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลหลายรอบ ดังนี้ – ใช้ซอฟต์แวร์ Disk Wiping (http://www.diskwipe.org) ในการทำลายข้อมูลทั้ง Hardisk หรือ Memory Divices สามารถดาว์นโหลดซอฟต์แวร์ได้ที่ http://www.diskwipe.org/download.php – ใช้ซอฟต์แวร์ Erase (http://eraser.heidi.ie) ในการลบแฟ้มข้อมูล/ไฟล์ข้อมูล สามารถดาว์นโหลดซอฟต์แวร์ได้ที่ http://eraser.heidi.ie/download.php ๒) ทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้วิธีการหั่น ตัด เผา ให้สิ้นสภาพการใช้งาน
เทป DDS, DAT, LTO	๑) ใช้วิธีการลบข้อมูลทั้งม้วน (Erase) ผ่าน Tap Device ก่อนการทำลายม้วนเทป ๒) ทุบหรือบดให้เสียหาย หรือเผาให้สิ้นสภาพการใช้งาน

(๒.๗) การรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ

[๑] จัดเก็บเอกสารที่เกี่ยวข้องกับระบบสารสนเทศไว้ในสถานที่ที่มั่นคงปลอดภัย

[๒] กำหนดสิทธิการเข้าถึงเอกสารที่เกี่ยวข้องกับระบบสารสนเทศที่จัดเก็บหรือเผยแพร่อยู่บนระบบเครือข่ายอินเทอร์เน็ต เพื่อป้องกันการเข้าถึงหรือเปลี่ยนแปลงแก้ไขเอกสารนั้น

(๒.๘) มาตรการควบคุมช่องโหว่ทางเทคนิค

[๑] ให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังต่อไปนี้

– ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน

- สถานที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้นๆ

[๒] กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบดำเนินการดังนี้

- มีการเฝ้าระวังติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหน่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของมหาวิทยาลัย
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับการแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

[๓] ปิดการใช้งานหรือควบคุมการเข้าพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็นโดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

(๒.๙) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) ให้มีการบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

[๑] ข้อมูลบัญชีผู้ใช้งาน
[๒] ข้อมูลวันเวลาที่เข้าถึงระบบ
[๓] ข้อมูลวันเวลาที่ออกจากระบบ
[๔] ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
[๕] ข้อมูลการล๊อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
[๖] ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
[๗] ข้อมูลการเปลี่ยนคอนฟิกกูเรชัน (Configuration) ของระบบ
[๘] ข้อมูลแสดงการใช้งานแอพพลิเคชัน
[๙] ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์
[๑๐] ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง
[๑๑] ข้อมูลโพรโทคอลเครือข่ายที่ใช้
[๑๒] ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
[๑๓] ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

(๒.๑๐) หน้าที่รับผิดชอบของผู้ใช้งาน ดังนี้

[๑] ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย

[๒] ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

[๓] จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

[๔] ล๊อคเครื่องคอมพิวเตอร์ เมื่อไม่ใช้งาน

[๕] ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

[๖] ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารไปรษณีย์

[๗] ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร โดยไม่ได้รับอนุญาต

[๘] นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๔.๔ การเข้ารหัสข้อมูลที่เป็นความลับ

ผู้ใช้อาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ ได้แก่

(๑) การสำรองข้อมูลที่เป็นข้อมูลลับต้องเข้ารหัสด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ ๑๒๘ bits (๑๒๘ –bits Encryption) เป็นอย่างน้อยเพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง

(๒) การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ์

(๓) ไม่อนุญาตให้ส่งข้อมูลลับผ่านเครือข่าย หากต้องการส่งต้องขออนุญาตจากผู้บังคับบัญชาทุกครั้ง และในกรณีที่เป็นไฟล์แนบต้องเข้ารหัสด้วยรหัสผ่านทุกครั้ง

(๔) การสำเนาข้อมูลชั้นความลับ ต้องจดบันทึกจำนวนชุดที่ทำสำเนา รายละเอียดผู้ดำเนินการทุกครั้ง

๕. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

วิธีการปฏิบัติ มีดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีการปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) เจ้าของข้อมูล จะต้องมีการทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานเหล่านี้ อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึง โดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับข้อมูล

(๔) การรับส่งข้อมูลข้อมูลสาคัญผ่านเครือข่ายสาธารณะ ต้องได้รับการเข้ารหัสลับ (encryption) ที่เป็นมาตรฐานสากล

(๕) การส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องทำการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อก่อน

(๖) การใช้ข้อมูลภายในร่วมกันต้องอยู่ในกรอบหน้าที่และความรับผิดชอบที่ได้รับมอบหมายเท่านั้น

(๗) **การแสดงชั้นความลับของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์** ให้แสดงชั้นความลับไว้ที่หน้าจอภาพทั้งหมดทุกหน้าของข้อมูลข่าวสารลับ ที่แสดงภาพบนจอนั้น และบนภาชนะสื่ออิเล็กทรอนิกส์ที่จัดเก็บ ให้แสดงชั้นความลับบนภาชนะที่บรรจุ หรือใช้กระบวนการทางคอมพิวเตอร์ให้ปรากฏลายน้ำบนข้อมูลทางระบบอิเล็กทรอนิกส์

(๘) **การป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์** ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ทุกชั้นความลับ ต้องเข้ารหัสด้วยเครื่องเข้ารหัสหรือโปรแกรมเข้ารหัส ซึ่งการใช้กุญแจรหัสประเภทใดและจำนวนครั้งของการเข้ารหัสขึ้นอยู่กับความสำคัญของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ให้อยู่ในดุลพินิจของเจ้าของข้อมูล

(๙) **การป้องกันสื่อบันทึกข้อมูลลับ** ต้องมีระบบสำรองข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ และเครื่องคอมพิวเตอร์แม่ข่ายสำรอง โดยแยกจัดเก็บในสถานที่ปลอดภัย เพื่อให้ข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์ดำเนินการได้อย่างต่อเนื่อง และความคงอยู่ของข้อมูลข่าวสารลับทางระบบอิเล็กทรอนิกส์

(๑๐) **การทำลายสื่อบันทึกข้อมูลลับ และแฟ้มข้อมูลลับ เพื่อป้องกันการกู้คืน** สำหรับสื่อที่สามารถใช้บันทึกซ้ำได้ ให้ใช้ชุดคำสั่งในระบบปฏิบัติการหรือโปรแกรม ซึ่งทำหน้าที่ลบแฟ้มข้อมูลโดยไม่สามารถกู้กลับคืนได้ กรณีที่จัดเก็บอยู่ในสื่อที่ไม่สามารถใช้บันทึกซ้าได้ ให้ใช้การทำลายด้วยวิธีทุบ ทำลายให้สิ้นสภาพการใช้งาน

แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๑. การใช้บริการเครือข่าย

๑.๑ สิทธิ์การใช้งานเครือข่าย

(๑) สิทธิ์การใช้งานเครือข่ายเป็นสิทธิพิเศษ (Pivilege) ที่มหาวิทยาลัยแม่โจ้ มอบให้บุคคลหรือหน่วยงานได้รับสิทธิ์ ไม่สามารถโอนสิทธิ์ให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

(๒) ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมินความเป็นส่วนตัวของผู้ใช้รายอื่น

(๓) ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่มหาวิทยาลัยกำหนดและตามวิถีสากล

(๔) กำหนดให้ผู้ใช้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๕) การใช้งานระบบสารสนเทศที่สำคัญต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ ปีละ ๑ ครั้ง

๑.๒ การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

(๑) การใช้ระบบเครือข่ายคอมพิวเตอร์ เพื่อการกระทำสิ่งที่ผิดกฎหมาย

(๒) การเข้าใช้ระบบคอมพิวเตอร์ด้วยบัญชีรายชื่อของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

(๓) การเข้าถึงข้อมูลของผู้อื่น เพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

(๔) การเผยแพร่ข้อมูลของผู้อื่นหรือของหน่วยงาน โดยไม่ได้รับอนุญาต

(๕) การใช้งานที่เป็นสาเหตุใช้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทำงานของระบบ

(๖) การพยายามทำลายหรือทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

(๗) การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

(๘) การลักลอบดักจับขอมูลในระบบเครือขายคอมพิวเตอร

(๙) การปลอมแปลงเปนบุคคลอื่น เพื่อสรางความเขาใจผิดใหแกระบบคอมพิวเตอรและผูใชอื่น

(๑๐) การใชทรัพยากรและระบบเครือขายคอมพิวเตอรเพื่อสรางความเสียหายแกระบบคอมพิวเตอรหรือ เครือขายอื่น

(๑๑) การเผยแพรและ/หรือการเขาถึงสื่อลามกอนาจาร

(๑๒) การใชทรัพยากรและระบบเครือขายคอมพิวเตอรเพื่อเปดใหบริการใด ๆ โดยไมไดรับอนุญาต

(๑๓) การใชทรัพยากรและระบบเครือขายคอมพิวเตอรเพื่อประกอบธุรกิจ หรือเข้าข่ายลักษณะเพื่อการค้าหรือเพื่อแสวงหากำไร ผ่านเครื่องคอมพิวเตอร์ และเครื่องแม่ข่าย ได้แก่ การประกาศแจ้งความการซื้อหรือการจำหน่ายสินค้า การนำข้อมูลไปขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การบริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

(๑๔) การนำไอพีแอดเดรสของมหาวิทยาลัยแม่โจ้ไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อ โดเมน mju.ac.th โดยไมไดรับอนุญาต

(๑๕) การใชระบบเครือขายคอมพิวเตอรอื่นใดที่ขัดตอนโยบายและระเบียบของมหาวิทยาลัยแม่โจ้

๑.๓ การฝ่าฝืนระเบียบและการพิจารณาลงโทษ

(๑) มหาวิทยาลัยแม่โจ้ จะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้และ/หรือบัญชีผู้ใช้

(๒) ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับ และ/หรือ ยกเลิกบัญชีผู้ใช้

(๓) ศูนย์เทคโนโลยีสารสนเทศ จะแจ้งหน่วยงานต้นสังกัดเพื่อพิจารณาโทษผู้ใช้ที่ฝ่าฝืนระเบียบ

๒. การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร (User Authentication for External Connections)

สำหรับผู้ใช้ที่อยู่ภายนอกมหาวิทยาลัยแม่โจ้ ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตเข้าใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

(๑) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

(๒) ผู้ใช้งานที่จะเข้าใช้งานระบบ ต้องยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน (Password)

(๓) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัย จะต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนผู้ใช้งานอีกครั้ง จึงอนุญาตให้เข้าถึงระบบข้อมูลได้

๓. การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks)

(๑) ให้ศูนย์เทคโนโลยีสารสนเทศ ทำหน้าที่จัดสรร หมายเลข IP Address อย่างเพียงพอและมีประสิทธิภาพ โดยศูนย์เทคโนโลยีสารสนเทศสามารถปรับเปลี่ยน หมายเลข IP Address ที่

จัดสรรให้กับอุปกรณ์จากหมายเลขเดิมเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้สามารถบริหารจัดการได้อย่างมีประสิทธิภาพ

(๒) อุปกรณ์เครือข่าย ต้องสามารถตรวจสอบหมายเลข IP Address ของทั้งต้นทางและปลายทางได้

(๓) ต้องมีกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของมหาวิทยาลัยกับเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตหรือไม่

(๔) การขอหมายเลขไอพี (IP Address) และชื่อโดเมน (Domain Name) ของหน่วยงานใดๆ หน่วยงานนั้นจะต้องทำหนังสือขออนุญาติส่งผ่านหน่วยงานต้นสังกัดมายังศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาดำเนินการ และระบุชื่อผู้ดูแลเว็บไซต์ด้วย

๔. การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection)

(๑) บุคคลภายนอกเข้ามาติดต่อหรือเข้ามาดำเนินการใดๆ ในห้องควบคุมระบบเครือข่ายจะต้องลงชื่อ เข้า–ออก พื้นที่ ให้ถูกต้องและได้รับการอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน ซึ่งต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

(๒) บุคคลภายนอกที่เข้ามาดำเนินการบำรุงรักษา บริหารจัดการพอร์ตของอุปกรณ์เครือข่ายหรือบริหารจัดการผ่านระบบเครือข่าย ต้องได้รับอนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน

(๓) ผู้ดูแลระบบต้องกำหนดการเปิด–ปิดพอร์ตของอุปกรณ์เครือข่าย เพื่อควบคุมการเข้าถึงต่อพอร์ตของอุปกรณ์เครือข่ายต่างๆ โดยจะปิดพอร์ตที่เสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบเครือข่ายคอมพิวเตอร์

(๔) ต้องยกเลิกหรือปิดพอร์ต และบริการบนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕) ทำการควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและตั้งค่าระบบ ทั้งกายภาพ และโดยการล๊อกอินเข้ามาใช้งาน

(๖) ทำการล๊อกอุปกรณ์เครือข่ายที่ใช้สำหรับปรับแต่งค่าคอนฟิกกูเรชั่นด้วยกุญแจ เพื่อป้องกันการเข้าถึงทางกายภาพต่ออุปกรณ์ และทำการเปลี่ยนแปลงแก้ไขโดยไม่ได้รับอนุญาต

(๗) ตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๒ ครั้ง

๕. การแบ่งแยกเครือข่าย (Segregation in Networks)

(๑) การแบ่งเครือข่ายภายในมหาวิทยาลัยออกเป็น ๒ ส่วน คือ เครือข่ายภายใน และเครือข่ายภายนอก

(๒) มีการจัดแบ่งเครือข่ายสำหรับผู้ใช้งานภายใน ออกเป็นเครือข่ายย่อยๆ ตามอาคารต่างๆ

(๓) ทำ IP Switching เพื่อแบ่งแยกเครือข่ายออกเป็นส่วนๆ รวมทั้งควบคุมการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น

(๔) มีการแยกวงเครือข่ายไร้สายออกจากเครือข่ายส่วนอื่นๆ ของมหาวิทยาลัย

(๕) ผู้ใช้จะสามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาติเท่านั้น และผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่อีกวงเครือข่ายหนึ่งได้โดยตรง

(๖) ให้มีการจัดแบ่งเครือข่ายภายในมหาวิทยาลัยให้สอดคล้องกับนโยบายควบคุมการเข้าถึง ความต้องการในการเข้าถึงเครือข่ายหรือระบบงาน รวมถึงความสำคัญและชั้นความลับของข้อมูลที่ใช้งานอยู่ภายในเครือข่ายของมหาวิทยาลัย

(๗) มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่แสดงขอบเขตที่ครอบคลุมแต่ละส่วนที่แบ่งแยก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๖. การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)

ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

(๑) ใช้ Monitor Tool (Fortinet) ในการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัย ในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

(๓) ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยแม่โจ้ ที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัย ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก (Firewall) เพื่อป้องกันเครือข่ายย่อยจากการถูกบุกรุก หรือเข้าถึงโดยไม่ได้รับอนุญาต และทำการกรองหรือจำกัดการไหลของข้อมูลระหว่างเครือข่ายย่อยเหล่านั้น

(๔) การเข้าสู่ระบบงานเครือข่ายภายในมหาวิทยาลัยแม่โจ้ โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการล๊อกอินและต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(๕) ห้ามบุคคลใดกระทำการเคลื่อนย้าย หรือทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความเสียหายแก่ระบบเครือข่ายหลักของมหาวิทยาลัยแม่โจ้ได้

(๖) ในกรณีที่ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติต่อระบบเครือข่ายหลักของมหาวิทยาลัยแม่โจ้ ศูนย์เทคโนโลยีสารสนเทศ จะทำการหยุดให้บริการจากระบบเครือข่ายกลาง โดยไม่มีการแจ้งให้ทราบล่วงหน้า จนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

๗. การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control)

ต้องควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) กำหนดตารางการใช้เส้นทางบนระบบเครือข่าย บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานใช้เฉพาะเส้นทางที่ได้รับอนุญาตเท่านั้น

(๒) IP Address ภายในของระบบงานเครือข่ายภายในของมหาวิทยาลัยแม่โจ้ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่าย และส่วนประกอบของระบบเทคโนโลยีสารสนเทศและการสื่อสารได้โดยง่าย

(๓) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๔) กำหนดบุคคลที่รับผิดชอบในการ ตั้งค่า แก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และต้องมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง

(๕) ห้ามทำการวางสายเครือข่ายเพิ่มเติมเองโดยไม่ได้รับอนุญาติ ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สายด้วย (Wireless Network) โดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

๘. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของมหาวิทยาลัยแม่โจ้ โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบเพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย เพื่อสร้างความมั่นคงปลอดภัยขอการใช้งานระบบเครือข่ายไร้สาย

แนวทางปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

(๑) ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยแม่โจ้ จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการศูนย์หรือผู้ที่ได้รับมอบหมายอย่างเป็นลายลักษณ์อักษร

(๒) ผู้ดูแลระบบ ต้องดำเนินการดังนี้

[๑] ทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สาย ให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้

สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

[๒] ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

[๓] ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

[๔] เลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และต้องสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณ อาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

[๕] ทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

[๖] ต้องเปลี่ยน “ชื่อล๊อกอินและรหัสผ่าน” สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และกำหนดชื่อล๊อกอินและรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

[๗] ต้องกำหนดค่าใช้ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

[๘] เลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้ที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้รหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้อย่างถูกต้อง

[๙] มีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัยแม่โจ้

[๑๐] ผู้ใช้ในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการโจมตี

[๑๑] ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้อำนวยการศูนย์ทราบโดยทันที

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

เพื่อให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ ดังนี้

๑. การกำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

(๑) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ในห้องให้บริการสารสนเทศส่วนกลางของมหาวิทยาลัย และกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๓) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบจะเสร็จสมบูรณ์

(๔) จำกัดระยะเวลา และ/หรือ จำนวนครั้งในการพิมพ์ผิด สำหรับใช้ในการป้องกันการคาดเดารหัสผ่าน

(๕) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

(๖) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล ที่ใช้ในการปฏิบัติงาน ผู้ใช้ต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนรับผิดชอบ และตั้งให้มีการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เมื่อว่างเว้นจากการใช้งาน และต้องให้มีการใส่รหัสผ่านก่อนจึงจะเข้าใช้งานได้

(๗) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง และให้ทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่หน้าจอเป็นเวลานาน

๒. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง ดังนี้

(๑) กำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดขอบของแต่ละคนได้

(๒) ถ้าผู้ใช้จำเป็นต้องเข้าถึงข้อมูลหรือบริการจากหลายระบบ และจำเป็นต้องดูแลจดจำรหัสผ่านหลายตัว สามารถใช้รหัสผ่านเดียวที่มีคุณภาพ สำหรับการเข้าถึงทุกระบบได้ ซึ่งระบบเหล่านั้นควรมีการรักษาความมั่นคงปลอดภัยในระดับที่เชื่อถือได้

(๓) วิธีการทางเทคนิค สำหรับการยืนยันตัวบุคคล ของมหาวิทยาลัยแม่โจ้ เป็นแบบ หนึ่งผู้ใช้หนึ่งรหัสผ่าน One Username One Password โดยการตรวจสอบตัวบุคคลด้วย Username ยืนยันตัวตนด้วย Password ที่มีการรักษาความมั่นคงปลอดภัย โดยการอ้างอิงด้วยหมายเลขบัตรประชาชน เพื่อเป็นยืนยันสถานะตามที่ลงทะเบียนไว้ในระบบบัญชีรายชื่อของมหาวิทยาลัยแม่โจ้

(๔) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้ง ก่อนใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยใช้ Username และ Password เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งาน หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไข

๓. การบริหารจัดการรหัสผ่าน (Password Management System)

มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ เมื่อได้ดำเนินการติดตั้งระบบแล้วให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้งานที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๔. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

(๑) โปรแกรมอรรถประโยชน์ สำหรับระบบปฏิบัติการ (OS Utilities Programs) ได้แก่ โปรแกรมที่ติดตั้งมาพร้อมระบบปฏิบัติการอยู่แล้ว อำนวยวามสะดวกในการทำงานร่วมกับฮาร์ดแวร์ ประกอบด้วย โปรแกรมจัดการไฟล์ (File Manager) โปรแกรมยกเลิกการติดตั้งโปรแกรม (Uninstaller) โปรแกรมสแกนดิสก์ (Disk Scanner) โปรแกราจัดเรียงพื้นที่จัดเก็บข้อมูลของฮาร์ดดิสต์ (Disk Defragment) โปรแกรมรักษาหน้าจอ (Screen Saver) โปรแกรมเหล่านี้ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งาน โดยใช้ระบบปฏิบัติการที่ถูกต้องตามลิขสิทธิ์มหาวิทยาลัยแม่โจ้ และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้ หากผู้ใช้งานต้องการใช้โปรแกรมอรรถประโยชน์ เหล่านี้ ต้องแจ้งความจำเป็นในการใช้งาน

(๒) โปรแกรมอรรถประโยชน์อื่นๆ (Standalone Utility Programs) เป็นโปรแกรมที่ช่วยให้เครื่องคอมพิวเตอร์ทำงานได้อย่างมีประสิทธิภาพ ได้แก่ โปรแกรมบีบอัดไฟล์ (File Compression Utility) โปรแกรมไฟร์วอลล์ (Firewall) โปรแกรมป้องกันไวรัส (Anti Virus Program) โปรแกรมติดตั้งเพื่อความบันเทิง โปรแกรมด้านการพิมพ์และจัดการเอกสาร โปรแกรมเกี่ยวกับภาพ โปรแกรมเพื่อการแบ่งปันและทำสำเนา โปรแกรมเพื่อการศึกษาและนำเสนอ

โปรแกรมอรรถประโยชน์ เหล่านี้ ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งาน เพื่อป้องกันการละเมิดลิขสิทธิ์ โดยต้องมีการปฏิบัติดังนี้

[๑] มีการจัดทำบัญชีรายชื่อโปรแกรมประเภทอรรถประโยชน์ที่อนุญาตให้ใช้งานได้

[๒] มีการจำกัดผู้ที่สามารถใช้งานโปรแกรมอรรถประโยชน์ และไม่อนุญาตให้ผู้ใช้งานทั่วไปสามารถใช้งานได้

[๓] ผู้ใช้งานที่ต้องการใช้โปรแกรมอรรถประโยชน์ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความจำเป็น โดยต้องมีลงนามเห็นชอบจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

[๔] การใช้งานโปรแกรมอรรถประโยชน์ จะต้องได้รับอนุญาตให้ใช้งาน เป็นรายครั้งไป

[๕] มีการแยกไดเรกทอรีสำหรับจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน เพื่อให้ง่ายต่อการควบคุมและจัดการโปรแกรม

[๖] จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

[๗] ต้องมีการตรวจสอบบันทึกการเรียกใช้งานโปรแกรมอรรถประโยชน์อย่างสม่ำเสมอ

[๘] ต้องมีการยกเลิก หรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ระบบงานที่ไม่มีความจำเป็นในการใช้งาน รวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้ ก่อนได้รับอนุญาต

๕. การจำกัดระยะเวลาการใช้งานระบบสารสนเทศ (Session Time-Out)

เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-Out) มีวิธีการปฏิบัติ ดังนี้

(๑) ให้มีการยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๒) ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น

(๓) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๔) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๖. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time)

จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชันที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลา ๑ ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หากต้องการเชื่อมต่อใหม่ ให้ทำการเข้ารหัสผ่านเพื่อยืนยันตัวตนอีกครั้ง

แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

๑.๑ การจำกัดการเข้าถึงของผู้ใช้

(๑) เข้าได้ตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

(๒) กำหนดสิทธิ์การเข้าถึงข้อมูลส่วนบุคคล

(๓) ต้องบันทึกการออกจากระบบงานโดยทันทีที่ใช้งานเสร็จ

(๔) แบ่งกลุ่มบุคลากรที่ปฏิบัติงานด้านสารสนเทศ ออกเป็น ๗ กลุ่ม คือ

[๑] ระดับผู้ปฏิบัติงาน

[๒] ระดับผู้ตรวจสอบข้อมูล

[๓] ระดับผู้ลงนามรับรองผล/อนุมัติ

[๔] ระดับการเข้าถึงรายงานสรุป

[๕] ระดับผู้ดูแลระบบ ระดับหน่วยงาน

[๖] ระดับผู้ดูแลระบบย่อย ตามคำสั่งหน่วยงานเจ้าของข้อมูล

[๗] ระดับผู้ดูแลระบบสูงสุด

(๕) การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ ต้องบันทึกข้อมูลพฤติกรรมการใช้งาน การเข้าถึงระบบสารสนเทศที่สำคัญ ดังนี้

[๑] ชื่อบัญชีผู้ใช้

[๒] วันเวลาที่เข้าถึงระบบ

[๓] วันเวลาที่ออกจากระบบ

[๔] เหตุการณ์สำคัญที่เกิดขึ้น

[๕] บันทึกการเข้าใช้ทั้งที่สำเร็จและไม่สำเร็จ

[๖] ความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

[๗] แสดงการใช้สิทธิการเข้าถึงของผู้ใช้

[๘] แสดงการเข้าถึงไฟล์และการกระทำกับไฟล์

[๙] หมายเลขไอพีแอดเดรสที่เข้าถึง

[๑๐] แสดงการหยุดการทำงานของระบบป้องกันการบุกรุก

[๑๑] แสดงการหยุดการทำงานของระบบงานที่สำคัญๆ

(๖) การรับ–ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ตามหน้าที่รับผิดชอบของผู้ใช้งาน

(๗) ต้องมีวิธีการพิสูจน์ตัวตนสำหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศของมหาวิทยาลัย

(๘) ผู้ดูแลระบบสารสนเทศ ต้องตัดการเชื่อมต่อระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม ยกเว้นในระบบที่มีความจำเป็นให้มีระยะเวลาที่นานขึ้น ให้พิจารณาเป็นรายระบบตามความเหมาะสมจำเป็น

๑.๒ การควบคุมผู้รับเหมา (Outsource) เข้าถึงสารสนเทศ

การควบคุมผู้รับเหมา (Outsource) กรณีมีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ มีวิธีการปฏิบัติดังนี้

(๑) มีกระบวนการคัดเลือกผู้รับเหมาโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาที่ชัดเจน เพื่อให้ได้ผู้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ ดังนี้

[๑] ต้องมีประสบการณ์

[๒] มีลูกค้าอ้างอิงน่าเชื่อถือ

[๓] มีใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล

[๔] มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของฮาร์ดแวร์และซอฟท์แวร์รวมถึงระบบสนับสนุนอื่นๆ

(๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาและ ต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาต้องนำเสนอ รายละเอียดขอบเขตงานอย่างครบถ้วน

(๓) มหาวิทยาลัยแม่โจ้ มีสิทธิในการตรวจสอบตามสัญญาการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อให้มั่นใจได้ว่ามหาวิทยาลัยแม่โจ้ สามารถควบคุมการใช้งานได้อย่างทั่วถึงตามสัญญานั้น ดังนี้

[๑] รายละเอียดเกี่ยวกับวิธีการทำงาน

[๒] การกำหนดระยะเวลาตรวจ ติดตามคุณภาพของผู้รับเหมาเป็นระยะๆ หรือแบบสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วง

ใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาในการกระทำตามข้อกำหนดของหน่วยงาน

(๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลอง แทนข้อมูลจริง และต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

[๑] เหตุผลในการขอใช้งาน

[๒] ระยะเวลาในการใช้งาน

[๓] การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

[๔] การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

(๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

(๖) ผู้รับเหมาที่ทำงานให้กับมหาวิทยาลัยทุกหน่วยงาน ไม่ว่าจะทำงานอยู่ภายในมหาวิทยาลัยหรือนอกสถานที่ จำเป็นต้องลงนามใน **“สัญญาการไม่เปิดเผยข้อมูลของมหาวิทยาลัย”** โดยสัญญาต้องทำให้แล้วเสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้นๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability) และให้กำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น

(๗) ผู้รับเหมาต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้องรวมทั้ง มีการปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๒. การควบคุมการเข้าถึงระบบซึ่งไวต่อการรบกวน

ต้องมีการระบุระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อมหาวิทยาลัย ดังนี้

(๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย

ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ได้แก่

(๑) ระบบ e-Manage ซึ่งเป็นระบบสารสนเทศกลางของมหาวิทยาลัย พัฒนาโดยศูนย์เทคโนโลยีสารสนเทศ

(๒) ระบบฐานข้อมูล ๕ ด้านของมหาวิทยาลัย

[๑] ข้อมูลด้านนักศึกษาและหลักสูตร	สำนักบริหารและพัฒนาวิชาการ
[๒] ข้อมูลด้านบุคลากร	กองการเจ้าหน้าที่ สำนักงานอธิการบดี
[๓] ข้อมูลงานวิจัย	สำนักวิจัยและส่งเสริมวิชาการการเกษตร
[๔] ข้อมูลงบประมาณ	กองแผนงาน สำนักงานอธิการบดี
[๕] ข้อมูลอาคารและพื้นที่ใช้สอย	กองอาคารและสถานที่ สำนักงานอธิการบดี

(๒) แนวปฏิบัติในการควบคุมสภาพแวดล้อมของระบบซึ่งไวต่อการรบกวน

(๑) ต้องแยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบงานอื่นๆ และแสดงให้เห็นถึงผลกระทบและระดับความสำคัญต่อมหาวิทยาลัย

(๒) มีห้องปฏิบัติงานแยกเป็นสัดส่วน และต้องกำหนดสิทธิ์ให้เฉพาะผู้ที่มีหน้าที่ที่ได้รับมอบหมายเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

(๓) ทำการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์แม่ข่ายเครื่องหนึ่งต่างหาก

(๔) ทำการป้องกันการมีทรัพยากรไม่เพียงพอ

(๕) มีการประเมินความเสี่ยงสำหรับการใช้งานทรัพยากรร่วมกัน ระหว่างระบบงานที่มีความสำคัญสูง กับระบบงานอื่นๆ ที่มีความสำคัญน้อยกว่า

(๖) ทำการตั้งค่าไฟร์วอลล์ ควบคุมการเข้าใช้งานจากเครือข่ายภายในและภายนอกมหาวิทยาลัย

(๗) มีระบบเฝ้าระวังการเข้าถึงข้อมูลสำคัญโดยผู้ไม่ได้รับอนุญาต

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารและการปฏิบัติงานจากภายนอกองค์กร (Mobile Compution and Teleworking) ที่เกี่ยวข้องกับระบบซึ่งไวต่อการรบกวน

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการ สำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ ประเภทพกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก สมาร์ทโฟน แท็ปเล็ต รวมทั้งกำหนดมาตรการการใช้งานอย่าง ปลอดภัยและเหมาะสม โดยมีแนวทางปฏิบัติ ดังนี้

(๑) มีการวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทพกพา

(๒) สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภท พกพาในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอก มหาวิทยาลัย

(๓) ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัส ข้อมูล

(๔) ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสาคัญหรือลับในอุปกรณ์ฯ

(๕) สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

(๖) มีการควบคุมการเชื่อมถึงระบบงานของมหาวิทยาลัยจากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ ประเภทพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ ด้วยการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของมหาวิทยาลัย จากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา สมาร์ทโฟน แท็ปเล็ต

(๗) มีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของมหาวิทยาลัย

(๘) ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้า มาปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย ต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขอ อนุญาต เข้า – ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

(๙) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกันว่าเป็นพื้นที่ ใช้งานเครือข่ายไร้สาย (Wireless area)

๓. การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ต้องปฏิบัติดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของคอมพิวเตอร์ และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่ และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) การยืมใช้อุปกรณ์ ต้องมีการบันทึกรายละเอียดการยืมใช้งานอย่างเป็นลายลักษณ์อักษร

(๓) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากคอมพิวเตอร์ที่นำไปใช้ได้ เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๔) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้ว ให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๕) เจ้าหน้าที่รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๖) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้น เกิดจากความประมาณอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๔. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ภายในมหาวิทยาลัย เพื่อดูแลรักษา ความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องได้รับการอนุมัติจาก ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน

(๒) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามา นั้น ต้องดูแลและจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสม

(๓) การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น

(๔) การเปิดพอร์ต ต้องไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และให้ทำการตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วทันที โดยการเปิดพอร์ตนั้น จะอนุญาตให้เปิด ให้ใช้ได้ ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

(๕) ไม่อนุญาตให้ครอบครัวหรือเพื่อนเข้าถึงระบบเทคโนโลยีสารสนเทศและข้อมูลสำหรับการปฏิบัติงาน จากภายนอกมหาวิทยาลัย

(๖) มีการตรวจสอบว่าซอฟต์แวร์ที่ใช้งานบนอุปกรณ์ที่เป็นของส่วนตัว ซึ่งใช้ในการเชื่อมต่อเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยจากระยะไกล มีใบอนุญาตการใช้งานที่ถูกต้องและครบถ้วน

(๗) มีการจัดเตรียมอุปกรณ์ที่จำเป็นสำหรับการปฏิบัติงานจากระยะไกล ซึ่งรวมถึงอุปกรณ์สำหรับ การจัดเก็บข้อมูล และอุปกรณ์สื่อสาร

(๘) ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยสารสนเทศของมหาวิทยาลัยจากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลโดยมหาวิทยาลัย

(๙) มีการบำรุงรักษาและให้บริการสนับสนุนสำหรับซอฟต์แวร์และฮาร์ดแวร์ต่างๆ ที่ใช้งานจากระยะไกล

(๑๐) มีการสำรองข้อมูลสำหรับการปฏิบัติงานจากระยะไกล

(๑๑) มีการตรวจสอบความมั่นคงปลอดภัยของสถานที่ที่จะมีการปฏิบัติงานจากระยะไกล

แนวปฏิบัติการจัดระบบสารสนเทศและระบบสำรองของสารสนเทศ

๑. แนวปฏิบัติการสำรองข้อมูลและระบบคอมพิวเตอร์

๑.๑ การคัดเลือกและจัดทำระบบสำรอง

(๑) แนวทางการพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญ ระบบนั้นต้องเป็นระบบข้อมูลและสารสนเทศที่มีความสำคัญ สอดคล้องเชื่อมโยงกับภารกิจของมหาวิทยาลัย แผนปฏิบัติราชการ คำรับรองการปฏิบัติราชการ และนโยบายของมหาวิทยาลัย ได้แก่ ฐานข้อมูล ๕ ด้านของมหาวิทยาลัย (นักศึกษาและหลักสูตร, บุคลากร, การเงินและบัญชี, งานวิจัย, อาคารสถานที่) และระบบสารสนเทศกลาง (e-manage)

(๒) กำหนดให้มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย

(๓) กำหนดให้มีการจัดทำระบบสำรองข้อมูลของแต่ละระบบสารสนเทศ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

[๑] กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

[๒] กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

[๓] มีขั้นตอนการปฏิบัติการจัดทำการสำรองข้อมูลและกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

[๔] กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล

[๕] การจัดทำบันทึกการสำรองข้อมูล (Operator Logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ วัน/เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรองข้อมูล ชนิดของข้อมูลที่บันทึก สำเร็จ/ไม่สำเร็จ

[๖] ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุ ไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหา และสรุปผลการแก้ไขปัญหา และรายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

[๗] ตรวจสอบข้อมูลทั้งหมดระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ทั้งในส่วนของซอฟต์แวร์ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (Configuration) ข้อมูลในฐานข้อมูล

[๘] จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บสำรองกับมหาวิทยาลัยควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลจัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับมหาวิทยาลัย

[๙] ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

[๑๐] ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

[๑๑] จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

[๑๒] ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

[๑๓] ให้ผู้ดูแลระบบคอมพิวเตอร์ มอบหมายหน้าที่การสำรองข้อมูลให้กับเจ้าหน้าที่คนอื่นเพื่อช่วยสำรองข้อมูล ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

[๑๔] การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

(๔) ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรองข้อมูลแต่ละรายการตามความถี่ ด้วยวิธีแบคอัพแบบ Full Backup ดังนี้

รายการ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรองข้อมูล
๑ Mail Server	– ค่า Configure – ข้อมูลในเมล์บ๊อกซ์	– ก่อนและหลังการเปลี่ยนแปลง – ๑ ครั้งต่อเดือน
๒ Web Server	– ค่า Configure – ข้อมูลเผยแพร่บนเว็บไซด์	– ก่อนและหลังการเปลี่ยนแปลง – ๑ ครั้งต่อเดือน
๓ Database Server	– ค่า Configure – ระบบ e-Manage – ข้อมูลในฐานข้อมูลของระบบที่สำคัญ	– ก่อนและหลังการเปลี่ยนแปลง – ๒ ครั้ง / วัน – ๑ ครั้ง / วัน
๔ Firewall Server	– ค่า Configure – ข้อมูล Rule ของ Firewall	– ก่อนและหลังการเปลี่ยนแปลง – ๑ ครั้งต่อเดือน
๕ Server ของระบบงานต่าง ๆ	– ค่า Configure – ระบบ e-Manage – ข้อมูลบน Server อื่น ๆ	– ก่อนและหลังการเปลี่ยนแปลง – ๑ ครั้ง / วัน – ๑ ครั้ง / เดือน

๑.๒ การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๑) การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อย ดังนี้

[๑] มีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบ สำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

[๒] มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อ ลดความเสี่ยงเหล่านั้น

[๓] มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

[๔] มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

[๕] มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก ได้แก่ ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

[๖] มีการสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๒) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่าง เหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

(๓) มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อม กรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

(๔) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อ สภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๑.๓ การกำหนดหน้าที่และความรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

มีการจัดหน่วยปฏิบัติการฉุกเฉินหรือสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน ดังนี้

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

(๑.๑) กำหนดนโยบายให้ศูนย์เทคโนโลยีสารสนเทศ

(๑.๒) ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศในฐานะผู้ควบคุมดูแล

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๒.๑) เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

(๒.๒) มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

(๒.๓) มีอำนาจสั่งทำลายกุญแจอาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

(๒.๔) ประชุมหารือกับคณะกรรมการที่เกี่ยวข้อง

(๒.๕) ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

(๒.๖) รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริการเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

(๓) ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย (หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต)

(๓.๑) วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

(๓.๒) มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

(๓.๓) สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

(๓.๔) ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ท่านผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

(๓.๕) ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้ายานพาหนะและหน่วยดับเพลิงเป็นต้น

(๓.๖) รายงานให้ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ ทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

(๓.๗) กำหนดอัตรากำลังพลวัสดุอุปกรณ์และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

(๓.๘) ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

(๔) ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administor and Staffs)

(๔.๑) กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

(๔.๒) พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย

(๔.๓) ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

(๔.๔) ป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

(๔.๕) หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ มีดังนี้

[๑] ทำการตรวจสอบระบบ Firewall

[๒] ทำการตรวจสอบ Virus, Worm, Spyware

[๓] ทำการตรวจสอบ UPS

[๔] ทำการตรวจสอบ Transaction log files

[๕] ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ

[๖] ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ

[๗] ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล

[๘] ทำการตรวจสอบค่า Configuration ของระบบ

(๔.๖) เตรียมเครื่องมืออุปกรณ์ทั้งทางด้านHardwareและsoftwareตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

(๔.๗) ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) และสำรองข้อมูลทั้งระบบ วันละ ๑ ครั้ง

(๔.๘) ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และแฟ้มข้อมูล Tape Backup รายชื่อโปรแกรม เอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรองสำเนาคู่มือ

(๔.๙) นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

(๕) ที่ปรึกษาด้านเทคนิค (วิศวกรที่ปรึกษา และเจ้าหน้าที่บริษัท)

(๕.๑) ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

(๕.๒) ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญ หรือหน่วยงานราชการที่เกี่ยวข้อง

(๕.๓) ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

(๖) หัวหน้าหน่วยงานที่เกิดเหตุ (On-site Manager)

(๖.๑) แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

(๖.๒) ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบสารสนเทศ

(๖.๓) นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๑.๔ การทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉิน

ให้มีการทดสอบสภาพพร้อมใช้งานของระบบ ต่อไปนี้

(๑) ระบบสารสนเทศ ปีละ ๑ ครั้ง

(๒) ระบบสำรอง ปีละ ๑ ครั้ง

(๓) ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ ๑ ครั้ง

๒. แนวปฏิบัติการกู้คืนระบบ

(๑) ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์หรือผู้ดูแลระบบเครือข่ายดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึก และรายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

(๒) ให้ใช้ข้อมูลทันสมัยที่สุด (Lastest Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

(๓) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

(๔) ต้องมีการซักซ้อมการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง

แนวปฏิบัติการสร้างความรู้ความเข้าใจการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

๑. การสร้างความรู้ ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วิธีแนวปฏิบัติ มีดังนี้

(๑) จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย ปีละ ๑ ครั้ง หรือทุกครั้งที่มีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

(๒) จัดทำคู่มือหรือสื่อดิวิทัศน์การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ และมีการเผยแพร่ทางเว็บไซต์ของมหาวิทยาลัย

(๓) จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหา แนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของมหาวิทยาลัย

(๔) จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน

(๕) ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับปรุงความรู้อยู่เสมอ

(๖) ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการผู้ใช้งาน

๒. หัวข้อความรู้ความเข้าใจในการในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์

๒.๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

(๑) การใช้งานทั่วไป

[๑] ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

[๒] เครื่องคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยแม่โจ้เป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น

[๓] โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

[๔] การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

[๕] ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

[๖] ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

[๗] ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการ ตกกระทบกระเทือน

[๘] การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

[๙] ไม่วางของทับบนหน้าจอและแป้นพิมพ์

[๑๐] การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

[๑๑] ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น

[๑๒] ผู้ใช้งานมีหน้าที่รับผิดชอบ ต้องล๊อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เพื่อป้องกันการสูญหาย

[๑๓] ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

[๑๔] ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

[๑๕] ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต ด้วยการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าตนไม่ได้เป็นผู้กระทำความผิด

[๑๖] ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่มหาวิทยาลัยแม่โจ้ กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

[๑๗] หากผู้ใช้งานกระทำการล่วงละเมิด หรือ พยามยามจะล่วงละเมิด ศูนย์เทคโนโลยีสารสนเทศ ในฐานะผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย ขอสงวนสิทธิที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ และ/หรือ การใช้งานใดๆ ตามความเหมาะสม

[๑๘] ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

[๑๙] ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

[๒๐] ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง

[๒๑] ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน

[๒๒] ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

[๒๓] ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาติจากผู้บังคับบัญชา หรือศูนย์เทคโนโลยีสารสนเทศ

[๒๔] ห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ หากตรวจพบถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

[๒๕] ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟท์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

[๒๖] ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

[๒๗] ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

[๒๘] ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาติจากผู้บังคับบัญชา

(๒) การสำรองข้อมูลและการกู้คืน

[๑] ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ได้แก่ CD, DVD และ External Hard Disk

[๒] ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๒.๒ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยแม่โจ้ ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

(๑) แนวทางการควบคุมการใช้งาน สำหรับผู้ดูแลระบบ

[๑] ต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยแม่โจ้ ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ

[๒] ต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยแม่โจ้

[๓] รหัสจดหมายอิเล็กทรอนิกส์ เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น ในการพิมพ์แต่ละตัวอักษร

[๔] ต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิด ได้ไม่เกิน ๕ ครั้ง

[๕] ต้องกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์ มีการล็อกเอ้าท์ออกจากหน้าจอตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลา ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้และรหัสผ่านอีกครั้ง

(๒) การใช้งานสำหรับผู้ใช้

[๑] ต้องไม่ตั้งค่า การใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

[๒] ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก ๓–๖ เดือน

[๓] ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยหรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย ละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาติให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยแม่โจ้

[๔] ต้องไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail Address) ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

[๕] ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยแม่โจ้ เพื่อการทำงานของมหาวิทยาลัยแม่โจ้เท่านั้น

[๖] หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

[๗] ทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส

[๘] ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

[๙] ต้องไม่ใช้ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยแม่โจ้ ทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์

[๑๐] ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

[๑๑] ทำการตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

๒.๓ การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัย ถูกระงับ ชะลอ ขัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้ มีแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต ดังนี้

(๑) ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยแม่โจ้ จัดสรรไว้เท่านั้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาติจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

(๒) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรม ป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

(๓) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัส เพื่อป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

(๔) ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยแม่โจ้ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม

(๕) ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยแม่โจ้

(๖) ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัยแม่โจ้

(๗) ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยแม่โจ้ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

(๘) ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

(๙) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

(๑๐) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

(๑๑) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรม ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

(๑๒) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยแม่โจ้ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

(๑๓) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๔ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

ปัจจุบันมีแหล่งให้บริการเครือข่ายทางสังคมเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจำนวนมาก ได้แก่ Facebook, Twitter, LinkedIn, Google Plus, MySpace, YouTube, Blog, Wiki รวมทั้งเว็บไซต์ต่างๆ ทั้งในประเทศและต่างประเทศ ที่เป็นการให้บริการ File Sharing, Photo Sharing, Video Sharing และกระดานข่าว (Webboard) และเนื่องจากสื่อสังคมออนไลน์ เป็นเครื่องมือที่มีทั้งประโยชน์และโทษที่ควรระวัง โดยเฉพาะข้อมูลข่าวสารบางอย่างที่เผยแพร่ออกสู่สาธารณะไปแล้วอาจไม่สามารถเรียกกลับคืนได้ และอาจก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อองค์กร ดังนั้น เพื่อให้ผู้ปฏิบัติงานในมหาวิทยาลัย สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ทางมหาวิทยาลัยแม่โจ้ จึงมีแนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อสังคมออนไลน์ (Social Network) และแสดงตนในฐานะบุคลากรหรือนักศึกษาในสังกัดมหาวิทยาลัยแม่โจ้ ดังนี้

(๑) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น

(๒) ควรแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ หากพบว่ามีข้อความบน Social Network ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงของหน่วยงาน ส่วนงานของมหาวิทยาลัยแม่โจ้ได้

(๓) พึงระลึกว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ และข้อบังคับว่าด้วยจรรยาบรรณของบุคลากรและนักศึกษามหาวิทยาลัยแม่โจ้ และข้อบังคับว่าด้วยวินัยนักศึกษา มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบน Social Network ด้วย ทั้งนี้การละเมิดจรรยาบรรณอย่างร้ายแรงดังที่กำหนดไว้ในข้อบังคับดังกล่าว

ได้แก่ การเปิดเผยความลับของนักศึกษาหรือผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่นักศึกษาหรือรับผู้รับบริการ หรือการทำให้เกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของมหาวิทยาลัยแม่โจ้ ถือเป็นความผิดทางวินัยอย่างร้ายแรงและผู้ที่ละเมิดสามารถถูกดำเนินการทางวินัยได้ด้วย

(๔) ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว พึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์

(๕) พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บน Social Network เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้

(๖) การนำเสนอข้อมูลข่าวสาร การแสดงความคิดเห็น ผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามจริยธรรมวิชาชีพและแนวปฏิบัติจริยธรรม

(๗) การใช้สื่อสังคมออนไลน์ (Social Media) พึงระมัดระวังการใช้ถ้อยคาและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง

(๘) ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

(๙) ผู้ใช้งาน พึงระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้าน และควรอ้างอิงแหล่งที่มาเมื่อนาเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง

(๑๐) ผู้ใช้งาน สามารถใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาได้ แต่ควรแสดงให้ชัดเจนว่า ข้อความใดเป็น “ข่าว” ข้อความใดเป็น “ความคิดเห็นส่วนตัว” ทั้งนี้พึงตระหนักว่าการใช้ Social Network นั้นการแบ่งแยกระหว่างเรื่องส่วนตัว และเรื่องหน้าที่การงาน เป็นสิ่งที่ทำได้ยาก หากประสงค์จะใช้ Social Network เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน

(๑๑) หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือมหาวิทยาลัยต้องแจ้ง ชื่อ Page หรือ Accout และ รายชื่อผู้ดูแล (Admin) ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และงานประชาสัมพันธ์ของสำนักงานอธิการบดีทราบ และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้นคืนแก่

ส่วนงานหรือมหาวิทยาลัย เมื่อพ้นจากหน้าที่ที่ต้องดูแล หรือพ้นสภาพจากการเป็นบุคลากรของมหาวิทยาลัยแม่โจ้

(๑๒) ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือสื่อสารข้อมูลในกิจการของมหาวิทยาลัยหรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ควรแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูลโปรไฟต์ (Profile) และพึงใช้ด้วยความสุภาพ และมีวิจารณญาณ

(๑๓) การเผยแพร่ข้อมูล หรือแสดงความเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง

(๑๔) ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ใต้บังคับบัญชาได้ ทั้งนี้ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจน ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงานอย่างแท้จริง

(๑๕) ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของมหาวิทยาลัย หรือข้อมูลที่ใช้ภายในมหาวิทยาลัยก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ

(๑๖) ในการสื่อสารข้อมูลในกิจการขององค์กรทางสื่อสังคมออนไลน์ (Social Media) ห้ามแสดงสัญลักษณ์พรรคการเมือง กลุ่มกดดันรณรงค์ทางสังคม กลุ่มลัทธิทางศาสนา และพึงระมัดระวังในการใช้สัญลักษณ์ที่ก่อให้เกิดความเข้าใจผิดและไม่ควรนำรูปบุคคลอื่น มาแสดงว่าเป็นรูปของตนเอง

(๑๗) การส่งต่อข้อมูลในสื่อสังคมออนไลน์ (Social Media)

[๑] พึงละเว้นการส่งต่อข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคลหรือสังคม

[๒] พึงระมัดระวังการส่งต่อข้อมูลในสถานการณ์ภัยพิบัติธรรมชาติ การก่อการร้าย การจลาจล วินาศกรรมหรือภาวะสงคราม

[๓] พึงระมัดระวังการส่งต่อข้อมูลเรื่อง บุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ

[๔] พึงระมัดระวังการส่งต่อข้อมูลที่กระทบต่อสิทธิ ความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์

(๑๘) ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อหน่วยงานส่วนงาน และมหาวิทยาลัยได้ด้วย

(๑๙) หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรอื่น ทางองค์กรหรือผู้ใช้งานที่รับผิดชอบข้อความนั้น ไม่ว่าจะเป็นการส่งข้อความเองหรือรับส่งข้อมูลต่อ ต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือองค์กรที่ได้รับความเสียหาย ทั้งนี้ต้องให้ผู้ที่ได้รับความเสียหายมีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

๒.๕ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (สำหรับผู้ดูแลระบบ)

ภายใต้บังคับของมาตรา ๒๖ แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ กำหนดประเภทของผู้ให้บริการ ไว้ดังนี้

๑. ผู้ให้บริการแก่บุคคลทั่วไปในการเข้าสู่อินเทอร์เน็ต หรือให้สามารถติดต่อถึงกันโดยประการอื่นทั้งนี้ โดยผ่านทางระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการให้บริการในนามของตนเองหรือเพื่อประโยชน์ของบุคคลอื่น สามารถจำแนกได้ ๔ ประเภท ดังนี้

   ก. ผู้ประกอบกิจการโทรคมนาคมและการกระจายภาพและเสียง (Telecommunication and Broadcast Carrier)

   ข. ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ (Access Service Provider) ได้แก่ผู้ให้บริการอินเทอร์เน็ต (Internet Service Provider) ทั้งมีสายและไร้สาย ผู้ประกอบการซึ่งให้บริการในการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ในห้องพัก ห้องเช่า โรงแรม หรือร้านอาหารและเครื่องดื่ม ในแต่ละกลุ่มอย่างหนึ่งอย่างใด และผู้ให้บริการเข้าถึงระบบเครือข่ายคอมพิวเตอร์สำหรับองค์กร เช่น หน่วยงานราชการ บริษัท หรือสถาบันการศึกษา

   ค. ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ (Host Service Provider) ได้แก่ ผู้ให้บริการเช่าระบบคอมพิวเตอร์ (Web Hosting) การให้บริการเช่า Web Server ผู้ให้บริการแลกเปลี่ยนแฟ้มข้อมูล (File Server หรือ File Sharing) ผู้ให้บริการการเข้าถึงจดหมายอิเล็กทรอนิกส์ (Mail Server Service Provider) และผู้ให้บริการศูนย์รับฝากข้อมูลทางอินเทอร์เน็ต (Internet Data Center)

   ง. ผู้ให้บริการร้านอินเทอร์เน็ต

๒. ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล (Content Service Provider) เช่น ผู้ให้บริการข้อมูลคอมพิวเตอร์ผ่านแอพพลิเคชั่นต่างๆ (Application Service Provider) ได้แก่

ก. ผู้ให้บริการเว็บบอร์ด (Web Board) หรือผู้ให้บริการบล๊อค (Blog)

ข. ผู้ให้บริการการทำธุรกรรมทางการเงินทางอินเทอร์เน็ต (Internet Banking) และผู้ให้บริการชำระเงินทางอิเล็กทรอนิกส์ (Electronic Payment Service Provider)

ค. ผู้ให้บริการเว็บเซอร์วิส (Web Services)

ง. ผู้ให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-Commerce) หรือธุรกรรมทางอิเล็กทรอนิกส์ (e-Transactions)

"ผู้ให้บริการ" มีหน้าที่ต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ โดยให้ผู้ให้บริการเก็บเพียงเฉพาะในส่วนที่เป็นข้อมูลจราจรที่เกิดจากส่วนที่เกี่ยวข้องกับบริการของตนเท่านั้น ด้วยวิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

๑. เก็บในสื่อ (Media) ที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง (Integrity) และระบุตัวบุคคล (Identification) ที่เข้าถึงสื่อดังกล่าวได้

๒. มีระบบการเก็บรักษาความลับของขอมูลที่จัดเก็บ และกำหนดชั้นความลับในการเขาถึงข้อมูลดังกลาว เพื่อรักษาความนาเชื่อถือของขอมูล และไมใหผูดูแลระบบสามารถแกไขข้อมูลที่เก็บรักษาไว เชน การเก็บไวใน Centralized Log Server หรือการทำ Data Archiving หรือทำ Data Hashing เปนตน เวนแต ผูมีหนาที่เกี่ยวของที่เจาของหรือผูบริหารองคกร กำหนดใหสามารถเขาถึงขอมูลดังกลาวได เชน ผูตรวจสอบระบบสารสนเทศขององคกร(IT Auditor) หรือบุคคลที่องคกรมอบหมาย เปนตน รวมทั้งพนักงานเจาหนาที่ตามพระราชบัญญัตินี้

๓. จัดใหมีผูมีหนาที่ประสานงานและใหขอมูลกับพนักงานเจาหนาที่ซึ่งไดรับการแตงตั้งตามพระราชบัญญัติวาดวยการกระทำความผิดเกี่ยวกับคอมพิวเตอร พ.ศ. ๒๕๕๐ เพื่อใหการส่งมอบขอมูลนั้น เปนไปดวยความรวดเร็ว

๔. ในการเก็บขอมูลจราจรนั้น ตองสามารถระบุรายละเอียดผูใชบริการเปนรายบุคคลได (Identification and Authentication) เชน ลักษณะการใชบริการ Proxy Server, Network Address Translation (NAT) หรือ Proxy Cache หรือ Cache Engine หรือบริการ Free Internet หรือ บริการ ๑๒๒๒ หรือ Wi-Fi Hotspot ตองสามารถระบุตัวตนของผูใช บริการเปนรายบุคคลไดจริง

๕. ในกรณีที่ผูใหบริการประเภทหนึ่งประเภทใด ในขอ ๑ ถึงขอ ๔ ขางตน ไดใหบริการในนามตนเอง แตบริการดังกลาวเปนบริการที่ใชระบบของผูใหบริการซึ่งเปนบุคคลที่สาม เปนเหตุให้ผูใหบริการในขอ ๑ ถึงขอ ๔ ไมสามารถรูไดวา ผูใชบริการที่เขามาในระบบนั้นเปนใคร ผูให

บริการ เชนวานั้นตองดำเนินการใหมีวิธีการระบุและยืนยันตัวบุคคล (Identification and Authentication) ของผูใชบริการผานบริการของตนเองดวย

เพื่อใหขอมูลจราจรมีความถูกตองและนำมาใชประโยชนไดจริงผูใหบริการตองตั้งนาฬิกาของอุปกรณบริการทุกชนิดใหตรงกับเวลาอางอิงสากล (Stratum ๐) โดยผิดพลาดไมเกิน ๑๐ มิลลิวินาที

มหาวิทยาลัยแม่โจ้ เป็นผูใหบริการบุคคลทั่วไป ข้อ ข, ค (“ผู้ให้บริการการเข้าถึงระบบเครือข่ายคอมพิวเตอร์”, “ผู้ให้บริการเช่าระบบคอมพิวเตอร์ หรือให้เช่าบริการโปรแกรมประยุกต์ต่างๆ”) และเป็นผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล มีหนาที่ต้องเก็บรักษาขอมูลจราจรทางคอมพิวเตอร ตามหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ โดยเริ่มเก็บข้อมูลเมื่อพ้นหนึ่งร้อยแปดสิบวันนับจากวันประกาศกระทรวงเทคโนโลยีสารสนเทศและการสื่อสาร เรื่องหลักเกณฑ์การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ของผู้ให้บริการ พ.ศ. ๒๕๕๐ ในราชกิจจานุเบกษา (๒๑ สิงหาคม ๒๕๕๐) มีรายการดังต่อไปนี้

ประเภท	รายการ
๑. ผู้ให้บริการทั่วไป ข้อ ข, ค	
ก. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย	๑) ข้อมูล Log ที่มีการบันทึกไว้เมื่อมีการเข้าถึงระบบเครือข่าย ซึ่งระบุถึงตัวตนและสิทธิในการเข้าถึงเครือข่าย (Access Logs Specific to Authentication and Authorization Servers เช่น TACACS (Terminal Access Controller Access–Control System) or RADIUS (Remote Authentication Dial–In User Service) or DIAMETER (Used to Control Access to IP Routers or Network Access Servers)
	๒) ข้อมูลเกี่ยวกับวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server)
	๓) ข้อมูลเกี่ยวกับชื่อที่ระบุตัวตนผู้ใช้ (User ID)

ประเภท	รายการ
	๔) ข้อมูลหมายเลขอินเทอร์เน็ตที่ถูกกำหนดให้โดยระบบผู้ให้บริการ (Assigned IP Address) ๕) ข้อมูลที่บอกถึงหมายเลขสายที่เรียกเข้า (Calling Line Identification)
ข. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail Server)	๑) ข้อมูล Log ที่บันทึกไว้เมื่อเข้าถึงเครื่องให้บริการไปรษณีย์อิเล็อกทรอนิกส์ (Simple Mail Transfer Protocol : SMTP Log) ซึ่งได้แก่ - ข้อมูลหมายเลขของข้อความที่ระบุในจดหมายอิเล็กทรอนิกส์ (Message ID) - ข้อมูลที่อยู่อิเล็กทรอนิกส์ของผู้ส่ง (Sender e-mail Address) - ข้อมูลชื่อที่อยู่อิเล็กทรอนิกส์ของผู้รับ (Receiver e-mail Address) - ข้อมูลที่บอกถึงสถานะในการตรวจสอบ (Status Indicator) ซึ่งได้แก่ จดหมายอิเล็กทรอนิกส์ที่ส่งสำเร็จ จดหมายอิเล็กทรอนิกส์ที่ส่งคืน จดหมายอิเล็กทรอนิกส์ที่มีการส่งล่าช้า เป็นต้น ๒) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้ใช้บริการที่เชื่อมต่ออยู่ขณะเข้ามาใช้บริการ (IP Address of Client Connected to Server) ๓) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and time of connection of Client Connected to server)

ประเภท	รายการ
	๔) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องบริการจดหมายอิเล็กทรอนิกส์ ที่ถูกเชื่อมต่ออยู่ในขณะนั้น (IP Address of Sending Computer)

	๕) ชื่อผู้ใช้งาน (User ID) (ถ้ามี) ๖) ข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ ผ่านโปรแกรมจัดการจากเครื่องของสมาชิก หรือการเข้าถึงเพื่อเรียกข้อมูลจดหมายอิเล็กทรอนิกส์ไปยังเครื่องสมาชิก โดยยังคงจัดเก็บข้อมูลที่บันทึกการเข้าถึงข้อมูลจดหมายอิเล็กทรอนิกส์ที่ดึงไปนั้น ไว้ที่เครื่องให้บริการ (POP๓ [Post Office Protocol Version ๓] Log or IMAP๔ [Internet Message Access Protocol Version ๔] Log)
ค. ข้อมูลอินเทอร์เน็ตจากการโอนแฟ้มข้อมูลบนเครื่อง	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องให้บริการโอนแฟ้มข้อมูล ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ (Date and Time of Connection of Client to Server) ๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น (IP Source Address) ๔) ข้อมูลชื่อผู้ใช้งาน (User ID) (ถ้ามี) ๕) ข้อมูลตำแหน่ง (Path) และชื่อไฟล์ที่อยู่บนเครื่องให้บริการโอนถ่ายข้อมูลที่มีการส่งขึ้นมาบันทึก หรือให้ดึงข้อมูลออกไป (Path and Filename of Data Object Uploaded or Downloaded)

ประเภท	**รายการ**
ง. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครื่องผู้ให้บริการเว็บและเครื่องให้บริการ ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการและเครื่องให้บริการ

	๓) ข้อมูลหมายเลขชุดอินเทอร์เน็ตของเครื่องคอมพิวเตอร์ผู้เข้าใช้ที่เชื่อมต่ออยู่ในขณะนั้น ๔) ข้อมูลคำสั่งการใช้งานระบบ ๕) ข้อมูลที่บ่งบอกถึงเส้นทางในการเรียกดูข้อมูล (URI : Uniform Resource Identifier) เช่น ตำแหน่งเว็บเพ็จ
จ. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)	๑) ข้อมูล Log ที่บันทึกเมื่อมีการเข้าถึงเครือข่าย (NNTP [Network News Transfer Protocol] Log) ๒) ข้อมูลวัน และเวลาการติดต่อของเครื่องที่เข้ามาใช้บริการ และเครื่องให้บริการ (Date and Time of Connection of Client to Server) ๓) ข้อมูลหมายเลข Port ในการใช้งาน (Protocol Process ID) ๔) ข้อมูลชื่อเครื่องให้บริการ (Host Name)
ฉ. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) หรือ Instance Messaging (IM) เป็นต้น	ข้อมูล Log เช่นข้อมูลเกี่ยวกับวัน เวลา การติดต่อของผู้ใช้บริการ (Date and Time of Connection of Client to Server) และข้อมูลชื่อเครื่องบนเครือข่ายและหมายเลขเครื่องของผู้ให้บริการที่เครื่องคอมพิวเตอร์เชื่อมต่ออยู่ในขณะนั้น (Hostname and IP Address) เป็นต้น
๒) ผู้ให้บริการในการเก็บรักษาข้อมูลคอมพิวเตอร์เพื่อประโยชน์ของบุคคล	
ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเก็บรักษาข้อมูลคอมพิวเตอร์ (Content Service Provider)	๑) ข้อมูลรหัสประจำตัวผู้ใช้หรือข้อมูลที่สามารถระบุตัวผู้ใช้บริการได้ หรือเลขประจำตัว (Use ID) ของผู้ขายสินค้าหรือบริการ หรือเลขประจำตัวผู้ใช้บริการ (Use ID) และที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้ใช้บริการ ๒) บันทึกข้อมูลการเข้าใช้บริการ ๓) กรณีผู้ให้บริการเว็บบอร์ด (Web board) หรือผู้ให้บริการบล็อค (Blog) ให้เก็บข้อมูลของผู้ประกาศ (Post) ข้อมูล

การบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ ให้ปฏิบัติดังต่อไปนี้

(๑) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

(๒) ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (IT Auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

(๓) กำหนดให้มีการบันทึกให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(๔) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment)

๑. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(๑) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง มีวิธีการปฏิบัติ ดังนี้

[๑] มีการอนุมัติให้ดำเนินการประเมินความเสี่ยงด้านสารสนเทศ

[๒] มีการวางแผนสำหรับการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

[๓] มีการตรวจสอบและประเมินความเสี่ยงของระบบให้บริการ

[๔] มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations)อย่างน้อย ๑ ครั้งต่อปี เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้

(๒) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงาน ได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ มีวิธีการปฏิบัติ ดังนี้

[๑] กำหนดให้มีคณะทำงานตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ซึ่งประกอบด้วยหน่วยตรวจสอบภายใน ของมหาวิทยาลัย (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เป็นผู้ตรวจสอบและประเมินความเสี่ยงระบบสารสนเทศ และให้ตรวจสอบและประเมินความเสี่ยงอย่างน้อย ๑ ครั้งต่อปี

[๒] มีข้อตกลงร่วมกันสำหรับขอบเขตการตรวจสอบ ระหว่างผู้ตรวจสอบกับผู้รับการตรวจ

[๓] มีข้อจำกัดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้ ในลักษณะที่อ่านได้เพียงอย่างเดียว

[๔] มีวิธีการที่ปลอดภัยสำหรับการอนุญาตให้ผู้ตรวจสามารถเข้าถึงข้อมูล ชนิดที่สามารถเขียนหรือบันทึกข้อมูลได้

[๕] มีการสร้างสำเนาข้อมูลเพื่อให้ผู้ตรวจสอบทำงานบนข้อมูลสำเนา

[๖] มีการทำลาย หรือลบข้อมูลที่ทำสำเนาทิ้งโดยทันทีที่ตรวจสอบเสร็จ

[๗] มีวิธีการแบบปลอดภัยสำหรับจัดเก็บหลักฐานข้อมูลที่ใช้อ้างอิงในการตรวจสอบ

[๘] มีการกำหนดหน้าที่ความรับผิดชอบของผู้ตรวจสอบและขั้นตอนปฏิบัติสำหรับการตรวจสอบ

[๙] มีการกำหนดเจ้าหน้าที่ที่ทำหน้าที่เป็นผู้ตรวจสอบให้เป็นเอกเทศ จากกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่จะดำเนินการตรวจสอบ (ผู้ตรวจสอบจะต้องไม่ตรวจสอบกิจกรรมหรือระบบเทคโนโลยีสารสนเทศที่ตนดูแล หรือรับผิดชอบ)

๒. แนวทางในการตรวจสอบและประเมินความเสี่ยง

(๑) แนวทางในการตรวจสอบและประเมินความเสี่ยง

[๑] มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

[๒] มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

[๓] มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ ให้ผู้บริหารพิจารณาระดับความเสี่ยงที่เป็นอยู่และกำหนดแนวทางการปรับปรุง และแจ้งให้หน่วยงานภายในที่เกี่ยวข้องทราบเพื่อนำไปปฏิบัติ

(๒) มาตรการในการตรวจประเมินระบบสารสนเทศ

[๑] ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

[๒] ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งดำเนินการทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

[๓] ต้องมีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

[๔] ต้องมีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

[๕] ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ต้องแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

(๓) รายการที่สอบทาน

[๑] การป้องกันการบุกรุกระบบ

[๒] การสำรองข้อมูล

[๓] การควบคุมการเข้าห้องควบคุมระบบเครือข่าย

[๔] การควบคุมผู้เข้า–ออกอาคาร

[๕] การซ้อมรับสถานการณ์ฉุกเฉิน

[๖] สอบทานการเข้าถึงระบบสารสนเทศ

[๗] สอบทานการกำหนดการใช้งานตามภารกิจ

(๔) การกำกับดูแลการปฏิบัติตามด้านเทคนิค

[๑] ผู้บริหารต้องกำกับดูแลเพื่อให้มั่นใจว่าเจ้าหน้าที่ทราบถึงความรับผิดชอบด้านการรักษาความปลอดภัยสารสนเทศและได้มีการปฏิบัติในทางที่เหมาะสม ซึ่งอาจรวมถึงการจัดให้มีมาตรการในการวัดผลการปฏิบัติงานของเจ้าหน้าที่จากการปฏิบัติตามมาตรฐานความปลอดภัยของสารสนเทศ

[๒] มหาวิทยาลัยต้องสอบทานต้องตรวจสอบการควบคุมทางด้านเทคนิคของระบบสารสนเทศ เพื่อตรวจสอบว่ามีความเพียงพอและเหมาะสมหรือไม่ รวมทั้งการปฏิบัติตามการควบคุมเหล่านั้น

[๓] ในระบบสารสนเทศโดยเฉพาะระบบที่สำคัญและมีความเสี่ยงสูง ต้องมีการทดสอบระดับมาตรฐานความปลอดภัยของระบบสารสนเทศอย่างสม่ำเสมอ เพื่อตรวจสอบถึงจุดเปราะบางของระบบและประสิทธิผลของการควบคุมด้านความปลอดภัย

[๔] เครื่องมือที่ใช้ในการตรวจสอบระบบคอมพิวเตอร์ทั้งหมด ซึ่งรวมถึงซอฟต์แวร์ระบบงานและเอกสาร ที่จำเป็นสำหรับงานตรวจสอบระบบคอมพิวเตอร์ ต้องได้รับการปกป้อง จากการลักลอบใช้งานหรือใช้ในทางที่ผิดวัตถุประสงค์ และการควบคุมจำกัดการเข้าใช้งานให้เฉพาะแผนกที่เกี่ยวข้องกับการตรวจสอบเท่านั้น

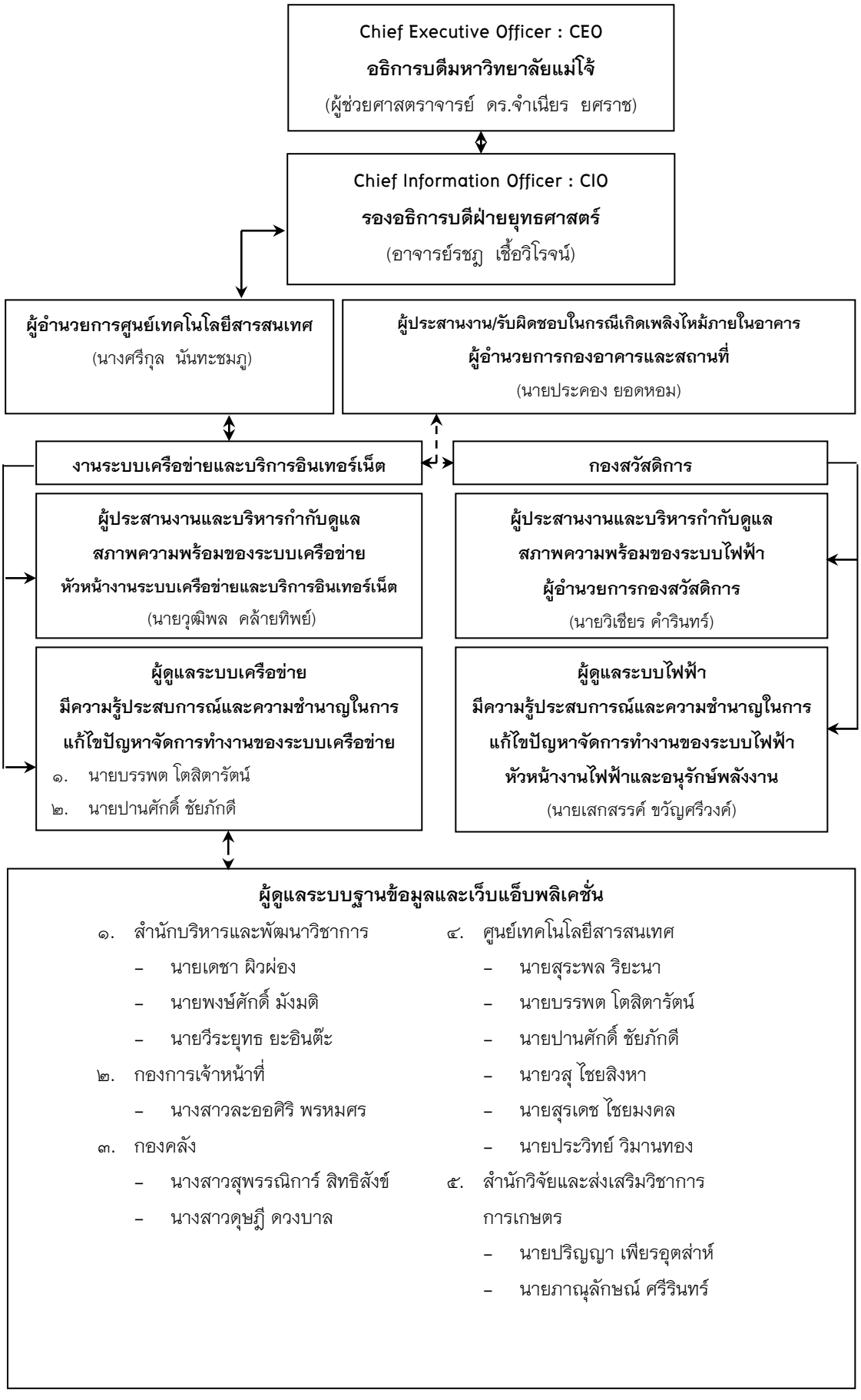
แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ (Contingency Plan)

แผนการแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจเกิดขึ้นกับระบบ Server และเครือข่ายมหาวิทยาลัยแม่โจ้ ปัจจุบันภัยที่เกิดแก่ระบบเทคโนโลยีสารสนเทศมีอัตราการเกิดเพิ่มขึ้นตามความก้าวหน้าของเทคโนโลยีสารสนเทศภัยอันตรายที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศอาจเกิดขึ้นได้โดยคน ซึ่งได้แก่เจ้าหน้าที่บุคลากรของหน่วยงานที่เกี่ยวข้องกับการใช้งานเทคโนโลยีสารสนเทศสถานการณ์หรือเหตุการณ์ ทั้งเจตนาและไม่เจตนาอันเป็นเหตุให้ข้อมูลข่าวสารในระบบเทคโนโลยีสารสนเทศถูกเปิดเผยหรือเปลี่ยนแปลง ทำลายปฏิเสธการทำงานหรือการกระทำอื่น ๆ ดังนั้นเพื่อเป็นการลดภัยดังกล่าวที่จะเกิดขึ้นในระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ จึงเห็นว่ามีความจำเป็นอย่างยิ่งที่มหาวิทยาลัยฯ จะต้องมีแผนรองรับสถานการณ์ฉุกเฉินจากภัยพิบัติระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยแม่โจ้ เพื่อรองรับสถานการณ์ดังกล่าวที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยแม่โจ้ แผนนี้จัดแบ่งออกเป็น ๓ ด้าน ได้แก่ แผนรองรับสถานการณ์ฉุกเฉิน จากภัยพิบัติที่เกิดขึ้นกับระบบเครือข่ายคอมพิวเตอร์ (Contingency Plan), แผนดำเนินการเพื่อให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานได้อย่างต่อเนื่อง (Continuity of Operationplan), และแผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

วัตถุประสงค์

๑) เพื่อลดความเสียหายที่จะเกิดแก่ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้
๒) เพื่อให้ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ สามารถดำเนินการได้อย่างต่อเนื่อง
๓) เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้

๑. ผู้รับผิดชอบดำเนินการเพื่อให้ระบบสารสนเทศใช้งานได้อย่างต่อเนื่อง



๒. การจัดหน่วยปฏิบัติการฉุกเฉินหรือสายการบังคับบัญชา (Lines of Authority) เมื่อเกิดเหตุฉุกเฉิน

(๑) ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)

[๑] กำหนดนโยบายให้ศูนย์เทคโนโลยีสารสนเทศ

[๒] ให้คำปรึกษาแก่ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศในฐานะผู้ควบคุมดูแล

(๒) ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

[๑] เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินระบบสารสนเทศ

[๒] มีอำนาจสั่งการให้ทุกหน่วยหยุดหรือปฏิบัติการระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบสารสนเทศ

[๓] มีอำนาจสั่งทำลายกุญแจอาคารเก็บวัตถุอันตรายเพื่อการระงับเหตุฉุกเฉิน

[๔] ประชุมหารือกับคณะกรรมการที่เกี่ยวข้อง

[๕] ประเมินสถานการณ์และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

[๖] รายงานข้อมูลและผลการปฏิบัติงานให้ผู้บริการเทคโนโลยีสารสนเทศระดับสูง (CIO) ทราบ

(๓) ผู้ประสานงานและบริหารกำกับดูแลสภาพความพร้อมของระบบเครือข่าย (หัวหน้างานระบบเครือข่ายและบริการอินเทอร์เน็ต)

[๑] วิเคราะห์สถานการณ์ในที่เกิดเหตุแล้วแจ้งเหตุต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

[๒] มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉินขั้นต้นจนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

[๓] สั่งการให้ผู้ที่เกี่ยวข้องมาปฏิบัติตามแผนฯ

[๔] ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมายหรือขณะที่ท่านผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

[๕] ประสานงานกับหัวหน้าหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้ายานพาหนะและหน่วยดับเพลิงเป็นต้น

[๖] รายงานให้ผู้อำนวยศูนย์เทคโนโลยีสารสนเทศ ทราบถึงสถานการณ์และขั้นตอนการดำเนินงานที่ได้กระทำไปแล้ว

[๗] กำหนดอัตรากำลังพลวัสดุอุปกรณ์และเครื่องมือที่จำเป็นต้องขอเพิ่มเติมในอนาคต

[๘] ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

(๔) ผู้ดูแลระบบเครือข่ายและผู้ช่วยดูแลระบบเครือข่าย (LAN Administor and Staffs)

[๑] กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

[๒] พิจารณาแจ้งสถานีดับเพลิงหรือหน่วยงานภายนอกอื่น ๆ มาช่วย

[๓] ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

[๔] ป้องกันชีวิตทรัพย์สินและสิ่งแวดล้อมให้ได้รับความเสียหายน้อยที่สุด

[๕] หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบวัสดุอุปกรณ์ที่ชำรุดเสียหายแล้วรายงานให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ อุปกรณ์ที่ต้องตรวจสอบ มีดังนี้

- ทำการตรวจสอบระบบ Firewall
- ทำการตรวจสอบ Virus, Worm, Spyware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

[๖] เตรียมเครื่องมืออุปกรณ์ทั้งทางด้านHardwareและsoftwareตลอดจนอุปกรณ์ที่เกี่ยวข้องเพื่อดำเนินการกู้ระบบโดยเร็ว

[๗] ทำการสำรองข้อมูลในส่วนของข้อมูล (Data) และสำรองข้อมูลทั้งระบบ วันละ ๑ ครั้ง

[๘] ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัยโดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบโปรแกรม และแฟ้มข้อมูล Tape Backup รายชื่อโปรแกรม เอกสารที่เกี่ยวกับระบบปฏิบัติและโปรแกรม รายการฮาร์ดแวร์สำรองสำเนาคู่มือ

[๙] นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

(๕) ที่ปรึกษาด้านเทคนิค (วิศวกรที่ปรึกษา และเจ้าหน้าที่บริษัท)

[๑] ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศและวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

[๒] ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญ หรือหน่วยงานราชการที่เกี่ยวข้อง

[๓] ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

(๖) หัวหน้าหน่วยงานที่เกิดเหตุ (On-site Manager)

[๑] แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเองและผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

[๒] ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัยระบบสารสนเทศ

[๓] นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

๓. แผนการสำรองข้อมูลและกู้คืนข้อมูล (Backup and Recovery Procedure)

การกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณ (System Recovery) ระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณโดยปกติจะต้องอยู่ในสภาพความพร้อมรองรับการให้บริการเครื่องลูกข่ายต่าง ๆ ได้ตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้จำเป็นต้องกู้ระบบคืนให้ได้เร็วที่สุดเท่าที่จะทำได้ เนื่องจากเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณต้องทำงานด้านบริการ (Service) แก่เครื่องลูกข่ายให้สามารถใช้งานได้ปกติการกู้คืนระบบเครื่องแม่ข่ายและอุปกรณ์กระจายสัญญาณจำเป็นต้องทำอย่างรวดเร็วเพื่อให้ใช้งานได้อย่างรวดเร็วที่สุด

แผนการนี้เป็นวิธีการที่ทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และแฟ้มข้อมูลกลับสู่สภาพเดิมเมื่อระบบเสียหายหรือหยุดทำงาน

๓.๑ Backup Plan

(๑) ระบบงานที่ต้องทำการสำรอง มีรายการ ดังนี้

(๑.๑) ระบบสารสนเทศเพื่อการบริหารจัดการ (e-Manage)

(๑.๒) ระบบฐานข้อมูล ๕ ด้านของมหาวิทยาลัย

[๑] ฐานข้อมูลนักศึกษาและหลักสูตร

[๒] ฐานข้อมูลบุคลากร

[๓] ฐานข้อมูลด้านการเงินและบัญชี

[๔] ฐานข้อมูลอาคารและสถานที่

[๕] ฐานข้อมูลงานวิจัย

(๒) บุคลากรผู้รับผิดชอบดูแลระบบฐานข้อมูลและเว็บแอ็บพลิเคชั่น

(๒.๑) เจ้าหน้าที่ดูแลระบบงานและฐานข้อมูล รับผิดชอบดูแล บำรุงรักษาระบบงานและฐานข้อมูล โดยมีหน้าที่ ตรวจสอบ บำรุงรักษา แก้ไขข้อบกพร่องต่างๆ ของระบบงานคอมพิวเตอร์ และการสำรองระบบงาน/ฐานข้อมูล

(๒.๒) เจ้าหน้าที่ดูแลระบบรับผิดชอบ ดูแล บำรุงรักษา ระบบเครือข่ายคอมพิวเตอร์ และความปลอดภัยของฐานข้อมูลทั้งหมด โดยมีหน้าที่ตรวจสอบ บำรุง รักษา แก้ไขข้อบกพร่องต่างๆ ของระบบเครือข่าย

(๒.๓) รายชื่อผู้ดูแลระบบ ดังนี้

๑) ศูนย์เทคโนโลยีสารสนเทศ

- นายบรรพต โตสิตารัตน์
- นายปานศักดิ์ ชัยภักดี
- นายสุระพล ริยะนา
- นายวสุ ไชยสิงหา
- นายสุรเดช ไชยมงคล

- นายประวิทย์ วิมานทอง

๒) สำนักบริหารและพัฒนาวิชาการ

- นายเดชา ผิวผ่อง
- นายพงษ์ศักดิ์ มังมติ
- นายวีระยุทธ ยะอินต๊ะ

๓) สำนักวิจัยและส่งเสริมวิชาการการเกษตร

- นายปริญญา เพียรอุตส่าห์
- นายภาณุลักษณ์ ศรีรินทร์

๔) กองการเจ้าหน้าที่

- นางสาวละออศิริ พรหมศร

๕) กองคลัง

- นางสาวสุพรรณิการ์ สิทธิสังข์
- นางสาวดุษฎี ดวงบาล

(๓) จัดเตรียม Storage ที่ใช้ในการเก็บข้อมูลที่ต้องการสำรอง รวมถึงระบบ/ซอฟต์แวร์ ที่ใช้ในการสำรองและกู้คืน

(๔) ทำการทดสอบความพร้อมของระบบ และดำเนินการสำรองระบบงานที่ได้คัดเลือกไว้

(๕) ตรวจสอบความถูกต้องของระบบงาน หลังจากที่ทำการสำรอง

(๖) บันทึกข้อมูลลงในแบบฟอร์มบันทึกการสำรองข้อมูล/แบบฟอร์มรายงานข้อผิดพลาดในการสำรองข้อมูล

(๗) หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการสำรองข้อมูล จนเป็นเหตุให้ไม่สามารถสำรองข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการสำรองข้อมูลอีกครั้ง

๓.๒ Recovery Plan

(๑) รายงานปัญหา/สาเหตุ ที่ต้องทำการกู้คืนข้อมูล ต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ

(๒) หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที

(๓) ใช้ข้อมูล ล่าสุด/ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

[๑] กรณีเกิดความเสียหายขึ้นกับระบบงาน (Source Code) จะทำการติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด

[๒] กรณีเกิดความเสียหายขึ้นกับฐานข้อมูล (Database) จะนำฐานข้อมูลที่เก็บไว้ล่าสุดกู้คืน เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด

[๓] กรณีเกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ Hardware ยังคงทำงานปกติ จะทำการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงทำการกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

[๔] กรณีเกิดความเสียหายขึ้นกับ Hardware ให้บริษัทผู้ดูแลทำการแก้ไขเบื้องต้นให้ Hardware สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับ OS และระบบงาน จะทำการติดตั้ง OS และระบบงานนั้นใหม่ จาก Source Code ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

(๔) ดำเนินการกู้คืนข้อมูลระบบงานที่มีปัญหา

(๕) ตรวจสอบความถูกต้องของระบบงาน หลังจากทำการกู้คืนระบบเสร็จเรียบร้อยแล้ว

(๖) หากพบปัญหาและข้อผิดพลาดระหว่างดำเนินการกู้คืนข้อมูล จนเป็นเหตุให้ไม่สามารถกู้คืนข้อมูลได้สำเร็จ ให้เรียกประชุมทีมงานผู้ดูแลระบบและผู้ที่เกี่ยวข้อง เพื่อปรึกษาและหาแนวทางในการกู้คืนข้อมูลอีกครั้ง

(๗) แจ้งผลการกู้คืนข้อมูลให้ผู้ใช้งานทราบ

๔. การเตรียมการป้องกันและการแก้ไข

(๑) การจัดเตรียมอุปกรณ์ที่จำเป็น ดังนี้

[๑] แผ่น Boot Disk

[๒] แผ่นติดตั้งระบบปฏิบัติการ/ระบบเครือข่าย/แผ่นติดตั้งระบบงานที่สำคัญ

[๓] แผ่นสำรองข้อมูลและระบบงานที่สำคัญ

[๔] แผ่นโปรแกรม Antivirus/Spyware

[๕] แผ่น Driver อุปกรณ์ต่าง ๆ

[๖] ระบบสำรองไฟฉุกเฉิน

[๗] Hard Disk สำรอง

[๘] สำเนารายละเอียดการบันทึกค่าต่าง ๆ ในการติดตั้งอุปกรณ์ที่จำเป็น

(๒) การป้องกันไวรัสคอมพิวเตอร์

[๑] ติดตั้งโปรแกรมป้องกันและตรวจจับไวรัส (Anti–Virus) ครอบคลุมทุกเครื่องแม่ข่ายและลูกข่ายเพื่อป้องกันความเสียหายของข้อมูล

[๒] Update ข้อมูลไวรัสอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง โดยเจ้าหน้าที่สามารถทำการ Update ไวรัสได้จากเครื่องคอมพิวเตอร์แม่ข่ายของมหาวิทยาลัย ซึ่งจะมีการแนะนำถึงขั้นตอนและวิธีการ Update ให้เจ้าหน้าที่สามารถดำเนินการได้ด้วยตนเอง

[๓] ตรวจสอบหาไวรัสทุกครั้งก่อนเปิดไฟล์จากแผ่นดิสก์หรือสื่อบันทึกข้อมูลต่างๆ

[๔] มีการแนะนำผู้ใช้คอมพิวเตอร์ให้ระวังภัยจากการเปิด File และ E-mail โดย Scan สื่อสำหรับจัดเก็บข้อมูลก่อนการใช้งาน ไม่เปิดอ่าน E-mail โดยไม่รู้ที่มาและให้ลบเมล์นั้นทิ้งทันที อย่าเปิดอ่าน

(๓) การป้องกันและแก้ไขปัญหาที่เกิดจากไฟฟ้าดับ

[๑] ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

[๒] เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ

[๓] กรณีระบบสำรองไฟฟ้าห้องควบคุมระบบเครื่องแม่ข่ายให้บริการของมหาวิทยาลัยขัดข้อง ให้เข้าสู่ระบบไฟฟ้าแบบ Bypass

(๔) การป้องกันความเสี่ยงจากไฟไหม้

[๑] ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซ ที่ห้องควบคุมระบบเครือแม่ข่ายให้บริการ เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) เพื่อการควบคุมเพลิงเบื้องต้นได้

[๒] ในกรณีที่เกิดไฟไหม้ภายในห้องปฏิบัติการระบบเครือข่ายคอมพิวเตอร์หลัก จะมีการตัดการจ่ายกระแสไฟฟ้าภายในบริเวณใกล้เคียง

[๓] จัดทำผังวางอุปกรณ์ระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์ และดำเนินการขนย้ายตามลำดับความสำคัญ เมื่อเกิดเหตุฉุกเฉิน

(๕) การป้องกันน้ำท่วมและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม

[๑] เปิดเครื่องปรับอากาศ สำหรับเครื่องแม่ข่ายให้บริการ ตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานอย่างสม่ำเสมอ

[๒] เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

[๓] ติดตามข่าวสารภัยพิบัติตามสถานการณ์ที่เกิดขึ้น

(๖) การป้องกันการบุกรุก และภัยคุกคามทางคอมพิวเตอร์ (Hacker) โดยการติดตั้งอุปกรณ์ Firewall เพื่อรักษาความปลอดภัยให้กับระบบเครือข่ายและป้องกันการใช้งานระบบเครือข่ายที่ผิดวัตถุประสงค์ ป้องกันการบุกรุกจากภายนอก

(๗) การป้องกันอุปกรณ์ระบบคอมพิวเตอร์แม่ข่ายชำรุด มีการทำระบบคอมพิวเตอร์แม่ข่ายให้บริการสำรอง เพื่อป้องกันข้อมูลเสียหายให้กับระบบงานต่างๆ

(๘) การป้องกันความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ จัดฝึกอบรมเสริมสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศเบื้องต้นในด้าน Hardware และ Software เพื่อลดความเสี่ยงในการปฏิบัติงานของเจ้าหน้าที่ให้น้อยที่สุด

(๙) การป้องกันความเสี่ยงในกรณีที่ระบบเครือข่ายคอมพิวเตอร์มีปัญหา

[๑] ดำเนินการติดตั้งเส้นทางสำรองสำหรับระบบงานบริการ ให้สามารถบริการได้อย่างต่อเนื่อง

[๒] ดำเนินการบำรุงรักษาอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์หลักอย่างสม่ำเสมอ

๕. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

(๑) กรณีระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์

[๑] ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายคอมพิวเตอร์ โดยพิจารณาตามลำดับความสำคัญของการให้บริการ และประสิทธิภาพของเครื่องสำรองไฟฟ้า

[๒] ในกรณีไฟไหม้ ให้ตัดระบบจ่ายไฟ ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว และทำการขนย้ายอุปกรณ์ไปไว้ในที่ปลอดภัย

[๓] ประสานขอความช่วยเหลือกับบริษัทที่รับผิดชอบดูแลบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายและ/หรือผู้เชี่ยวชาญระบบเครือข่ายคอมพิวเตอร์โดยเร็วที่สุด

[๔] ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบหาอุปกรณ์สำรอง หรือแจ้งให้บริษัทที่รับผิดชอบในการบำรุงรักษานำอุปกรณ์มาเปลี่ยนโดยเร็วที่สุด

(๒) กรณีเครื่องลูกข่าย

[๑] ในกรณีที่มีเหตุอันทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการใช้ระบบสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้น แจ้งให้นักวิชาการคอมพิวเตอร์ ของคณะ/หน่วยงาน/ศูนย์เทคโนโลยีสารสนเทศทราบ หรือกรณีมีเหตุอันทำให้การให้บริการระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายคอมพิวเตอร์ไม่สามารถให้บริการได้ ให้แจ้งเจ้าหน้าที่ผู้รับผิดชอบเพื่อดำเนินการประสานงานกับบริษัทที่รับผิดชอบในการบำรุงรักษารีบดำเนินการให้โดยด่วน

[๒] กรณีเกิดการขัดข้องเนื่องจากถูกไวรัสคอมพิวเตอร์ เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องอื่นในระบบเครือข่ายให้ทำการดึงสายเชื่อมโยงระบบเครือข่าย (สาย LAN) ออกจากเครื่องนั้นโดยเร็ว และแจ้งให้นักวิชาการคอมพิวเตอร์ ของคณะ/หน่วยงาน/ศูนย์เทคโนโลยีสารสนเทศ ดำเนินการแก้ไข

[๓] ในกรณีที่เกรงว่าเหตุที่เกิดจะเป็นอันตรายต่องาน/หน่วยงาน ภายในตึกที่ตั้งของคอมพิวเตอร์ที่พบการขัดข้องให้ดึงสาย LAN ออกจากจุดชุมสายในชั้นนั้นออกให้หมด

[๔] ปิดระบบไฟฟ้าที่เข้าเครื่องทั้งหมด

[๕] ขนย้ายเครื่องไปไว้ในที่ปลอดภัย

[๖] ให้เจ้าหน้าที่สำนักคอมพิวเตอร์แจ้งเหตุขัดข้องนั้นให้ผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยเร็วที่สุด

๖. แผนการนำระบบเทคโนโลยีสารสนเทศกลับสู่สภาพปกติ

การกู้คืนระบบคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบเครือข่ายคอมพิวเตอร์ โดยปกติจะต้องอยู่ในสภาพพร้อมให้บริการได้ตลอด ๒๔ ชั่วโมง หากไม่สามารถให้บริการ จะต้องดำเนินการกู้คืนระบบให้เร็วที่สุดเท่าที่จะทำได้ เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาวะปกติ เมื่อระบบเสียหาย หรือหยุดทำงาน ดังนี้

(๑) จัดหาอุปกรณ์ชิ้นส่วนใหม่เพื่อทดแทน

(๒) เปลี่ยนอุปกรณ์ชิ้นส่วนที่เสียหาย

(๓) ซ่อมอุปกรณ์ที่เสียหายให้เสร็จภายใน ๔๘ ชั่วโมง

(๔) สำรองอุปกรณ์ทดแทนหรือยืมอุปกรณ์จากหน่วยงานอื่นมาใช้ทดแทน

(๕) นำข้อมูลที่ได้ทำการสำรองไว้ (Backup) กลับมาใช้ (Restore) เพื่อกู้ระบบให้กลับมาภายใน ๔๘ ชั่วโมง

(๖) ตรวจสอบระบบปฏิบัติการ ระบบงานและฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลอื่นๆ ที่เกี่ยวข้อง

การประเมินสถานการณ์ความเสี่ยง

จากการติดตามตรวจสอบความเสี่ยงต่าง ๆ ในระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยแม่โจ้ พบว่าความเสี่ยงที่อาจเป็นอันตราย (Disaster) ต่อระบบเครือข่ายคอมพิวเตอร์ซึ่งเป็นองค์ประกอบหลักในระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ สามารถแยกเป็นภัยต่าง ๆ ได้ ๔ ประเภท ดังนี้

๑. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)
๒. ภัยที่เกิด Software
๓. ภัยจากไฟไหม้ หรือระบบไฟฟ้า
๔. ภัยจากน้ำท่วม (อุทกภัย)

๑. ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error)

ได้แก่ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และSoftware ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้เกิดการชะงักงันหรือหยุดทำงานและส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ มีวิธีการปฏิบัติ ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้นเพื่อลดความเสี่ยงด้าน Human Error ให้น้อยที่สุด ทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้นทำให้ความเสี่ยงที่เกิดจาก Human Error ลดน้อยลง

(๒) นำเสนอนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อพิจารณาในการประชุมคณะกรรมการนโยบายและพัฒนาระบบสารสนเทศ

(๓) จัดทำแนวปฏิบัติว่าด้วยการใช้งานคอมพิวเตอร์ทั่วไปและการเข้าถึงระบบเครือข่ายอินเทอร์เน็ต เผยแพร่ผ่านเว็บไซต์ของมหาวิทยาลัย เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

๒. ภัยที่เกิดจาก Software

เป็นภัยที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์ หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus) หนอนอินเทอร์เน็ต (Internet Worm) ม้าโทรจัน (Trojan Horse) และข่าวไวรัสหลอกลวง (Hoax) ซึ่ง Software ประเภทนี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ ถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยแม่โจ้ ใช้งานไม่ได้

มีแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้ง Firewall ที่เครื่องคอมพิวเตอร์แม่ข่ายทำหน้าที่ในการกำหนดสิทธิการเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์สแกนไวรัสที่เครื่องแม่ข่ายให้บริการ (Server) และเครื่องลูกข่าย (Client) ซึ่งทำหน้าที่เป็นซอฟต์แวร์ Antivirus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยแม่โจ้

(๓) แจ้งข้อมูลเตือนภัยไวรัสคอมพิวเตอร์ผ่านทางระบบอินทราเน็ตที่ http://www.it.mju.ac.th อย่างต่อเนื่องสม่ำเสมอ รวมทั้งแนะนำวิธีการป้องกันและการกำจัดภัยที่จะเกิดจาก Software ดังกล่าวให้เจ้าหน้าที่ได้ศึกษาและสามารถปฏิบัติการป้องกันและแก้ไขปัญหาในเบื้องต้นได้

๓. ภัยจากไฟไหม้หรือระบบไฟฟ้า

จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งศูนย์เทคโนโลยีสารสนเทศ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้เกิดภัยลักษณะดังกล่าวขึ้น มีแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากไฟไหม้หรือระบบไฟฟ้าขัดข้อง ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องแม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้อง โดยมีการสำรวจตรวจสอบระยะเวลาการสำรองไฟ กรณีที่เกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่ายอุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

๔. ภัยจากน้ำท่วม (อุทกภัย)

เนื่องจากห้องควบคุมระบบเครือข่ายอยู่บริเวณชั้น ๑ ของอาคาร ซึ่งมีความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ซึ่งมหาวิทยาลัยแม่โจ้ ได้ให้ความสำคัญและระมัดระวังเป็นอย่างยิ่งที่จะไม่ให้ภัยในลักษณะดังกล่าวเกิดขึ้น

มีแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจากน้ำท่วม (อุทกภัย) ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) เมื่อเกิดน้ำขังหรือมีการรั่วซึมจากน้ำ และมีแนวโน้มว่าน้ำท่วมขังเพิ่มขึ้นเรื่อย ๆ มาถึงบริเวณหน้าอาคาร ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครื่องแม่ข่ายทั้งหมด

(๓) ถอดเทป Back up ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย

(๔) ดำเนินการตัดระบบน้ำและไฟฟ้าในห้องควบคุม ปิดเบลคเกอร์เครื่องปรับอากาศ เพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(๕) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในชั้นที่สูงขึ้นไป

(๖) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๗) เมื่อระบบไฟฟ้าใช้งานได้ตามปกติผู้ดูแลระบบและเจ้าหน้าที่ผู้เกี่ยวข้องช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์ทำหน้าที่แม่ข่าย มาติดตั้ง ณ ห้องควบคุมระบบเครือข่ายชั้น ๑

(๘) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๙) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้วแจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้บริการได้ตามปกติ