



คู่มือวิธีปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ  
มหาวิทยาลัยแม่โจ้

จัดทำโดย ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้

## สารบัญ

หลักการ.....	2
วัตถุประสงค์ .....	2
นิยามศัพท์ .....	3
วิธีปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร .....	4
วิธีปฏิบัติในการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร.....	5
วิธีปฏิบัติในการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ .....	6
วิธีปฏิบัติในการบริหารจัดการระบบเครือข่าย .....	6
วิธีปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย.....	7
วิธีปฏิบัติในการควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ .....	8
วิธีปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ .....	8
วิธีปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน.....	9
วิธีปฏิบัติในการสำรองข้อมูล และกู้คืนระบบ.....	9
วิธีปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ .....	10
วิธีปฏิบัติของผู้ใช้งาน .....	11

## การปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้

### หลักการ

มหาวิทยาลัยแม่โจ้ ได้มีประกาศมหาวิทยาลัยแม่โจ้ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ เพื่อให้การบริหารจัดการและการใช้งานระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยแม่โจ้ เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศ ในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ประกอบด้วยนโยบายแต่ละด้าน ดังนี้ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ และกำหนดแนวปฏิบัติ เพื่อให้การดำเนินการบริหารจัดการรองรับนโยบายในแต่ละด้าน

ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยแม่โจ้ ซึ่งเป็นหน่วยงานหลักในการดูแลและให้บริการด้านระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของมหาวิทยาลัยแม่โจ้ จึงจัดทำคู่มือการปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ขึ้น เพื่อให้การดำเนินการด้านเทคโนโลยีสารสนเทศและการสื่อสาร มีความมั่นคงปลอดภัย และเป็นไปตามกฎระเบียบข้อปฏิบัติที่เกี่ยวข้อง

โดยวิธีปฏิบัติดังกล่าวต้องได้รับความร่วมมือจากผู้ดูแลระบบ ผู้ใช้งาน และผู้ที่เกี่ยวข้อง ในการถือปฏิบัติ ตามอย่างเคร่งครัด จึงหวังเป็นอย่างยิ่งว่า

วิธีปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ฉบับนี้ จะเป็นคู่มือให้กับผู้ดูแลระบบ และผู้ใช้บริการ ในการถือปฏิบัติ เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ต่อไป

### วัตถุประสงค์

- 1) เพื่อให้เกิดความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศและการสื่อสาร มหาวิทยาลัยแม่โจ้
- 2) เพื่อให้มีวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ในภาษาที่ง่ายต่อความเข้าใจ โดยสอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง สำหรับผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง ใช้เป็นคู่มือและถือปฏิบัติอย่างเคร่งครัด ตามหลักจริยธรรม
- 3) เพื่อสร้างความตระหนักและความสำคัญในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้แก่ผู้ดูแลระบบ ผู้ใช้บริการ และผู้ที่เกี่ยวข้อง
- 4) เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างสม่ำเสมอ

วิธีปฏิบัติตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มหาวิทยาลัยแม่โจ้ ประกอบด้วยวิธีการปฏิบัติในด้านต่างๆ ดังนี้

- 1) วิธีปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- 2) วิธีปฏิบัติในการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร
- 3) วิธีปฏิบัติในการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ
- 4) วิธีปฏิบัติในการบริหารจัดการระบบเครือข่าย
- 5) วิธีปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย
- 6) วิธีปฏิบัติในการบริหารจัดการระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ
- 7) วิธีปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ
- 8) วิธีปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน
- 9) วิธีปฏิบัติในการสำรองข้อมูล และกู้คืนระบบ
- 10) วิธีปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
- 11) วิธีปฏิบัติของผู้ใช้งาน

#### นิยามศัพท์

1) มหาวิทยาลัย	มหาวิทยาลัยแม่โจ้
2) ผู้ดูแลระบบ (System Administrator)	ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด
3) ผู้พัฒนาระบบ	ผู้ซึ่งได้รับมอบหมายให้รับผิดชอบในการพัฒนาระบบสารสนเทศ
4) เจ้าของข้อมูล	ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆหรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย ซึ่งหมายถึงข้อมูลส่วนบุคคล และข้อมูลของหน่วยงาน
5) เจ้าของระบบ	ผู้ได้รับมอบหมายให้เป็นหน่วยงานเจ้าภาพ ในการรับผิดชอบดูแลระบบสารสนเทศ โดยมีหน้าที่กำหนดสิทธิในการเข้าถึงข้อมูลในระดับหน่วยงาน
6) ผู้ใช้งาน	บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ที่กำหนดในการเข้าถึงสารสนเทศของมหาวิทยาลัยได้ ได้แก่ <b>ผู้บริหาร</b> หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี ผู้อำนวยการ สำนักฯ กองฯ ศูนย์ฯ คณบดี หัวหน้างาน

	<p><b>ผู้ดูแลระบบ (System Administrator)</b> หมายถึง ผู้ที่ได้รับมอบหมายจากผู้บริหาร ให้มีหน้าที่รับผิดชอบในการดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์</p> <p><b>เจ้าหน้าที่</b> หมายถึง ข้าราชการ พนักงานมหาวิทยาลัย พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ/จ้างเหมา</p> <p><b>นักศึกษา</b> หมายถึง นักศึกษามหาวิทยาลัยแม่โจ้ ระดับปริญญาตรี ปริญญาโท ปริญญาเอก</p> <p><b>บุคคลภายนอก</b> หมายถึง เจ้าหน้าที่จากหน่วยงานภายนอกที่ปฏิบัติการร่วมกับ มหาวิทยาลัยแม่โจ้</p>
--	---

### วิธีปฏิบัติของผู้ดูแลระบบเทคโนโลยีสารสนเทศและการสื่อสาร

- 1) กำหนดสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร แยกเป็นรายบุคคล โดยให้สามารถเข้าถึงได้ เฉพาะในส่วนที่เป็นหน้าที่ที่รับผิดชอบและหน้าที่ที่ได้รับมอบหมายเท่านั้น โดยต้องได้รับอนุญาตจากเจ้าของข้อมูลและเจ้าของระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร กรณีมีความจำเป็นต้องให้สิทธิพิเศษ ต้องกำหนดระยะเวลาการเข้าถึง และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาที่กำหนด โดยจำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่ม โดยอนุญาตให้ใช้ได้เท่าที่จำเป็น
- 2) ส่งมอบบัญชีรายชื่อและรหัสผ่านชั่วคราวให้กับผู้ใช้งาน ด้วยวิธีที่ปลอดภัย และแจ้งหน้าที่รับผิดชอบในการดูแลรักษาและใช้งานในทางที่ถูกต้อง โดยไม่ผิดต่อพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ให้ผู้ใช้งานทราบ
- 3) ดำเนินการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานะบุคลากร/นักศึกษา โดยกำหนดให้มีการยกเลิก เพิกถอน การอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสาร เมื่อมีการลาออก โอนย้าย สิ้นสุดการจ้าง ภายใน 24 ชั่วโมง หรือเมื่อมีการเปลี่ยนแปลงตำแหน่งงาน ภายใน 7 วัน โดยอ้างอิงข้อมูลบุคลากร จากเอกสารราชการของกองการเจ้าหน้าที่เป็นสำคัญ และข้อมูลนักศึกษาลาออก จากเอกสารราชการของสำนักบริหารและพัฒนาวิชาการ
- 4) เจ้าของข้อมูลบุคลากร โดยกองการเจ้าหน้าที่ ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบเป็นลายลักษณ์อักษร เมื่อบุคลากร
  - มีการว่าจ้างงาน
  - มีการเปลี่ยนแปลงสภาพการจ้างงาน
  - มีการลาออก หรือมีคำสั่งสิ้นสุดการเป็นผู้บริหาร บุคลากร และลูกจ้าง
  - มีการถึงแก่กรรม
  - มีการโอนย้ายข้ามหน่วยงานราชการ

- มีการฝึกงาน ลงโทษทางวินัย หรือถูกระงับการปฏิบัติหน้าที่
- 5) เจ้าของข้อมูลนักศึกษา โดยสำนักบริหารและพัฒนาระบบการศึกษา ต้องแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ เป็นลายลักษณ์อักษร เมื่อมีนักศึกษาลาออก
- 6) แจ้งเตือนให้ผู้ใช้งานเปลี่ยนรหัสผ่าน อย่างน้อยทุก 6 เดือน สำหรับผู้ใช้งานทั่วไป และอย่างน้อยทุก 3 เดือน สำหรับผู้บริหารและผู้ดูแลระบบ หรือตามระยะเวลาที่เหมาะสม
- 7) บริหารจัดการการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติเกิดขึ้นจากการใช้บริการของผู้ใช้งานที่ไม่เป็นไปตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้รีบแจ้งผู้ใช้งานยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบพิจารณา ระดับการให้บริการของผู้ใช้งานดังกล่าวทันที
- 8) ก่อนการติดตั้งอัปเดตระบบเทคโนโลยีสารสนเทศและการสื่อสารต่างๆ ต้องมีการแจ้งเตือนผู้ใช้งาน เพื่อเตรียมความพร้อมก่อนการดำเนินงาน
- 9) ติดตั้งและเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร ที่ได้รับมอบหมาย รวมทั้งการปรับปรุงซอฟต์แวร์ระบบปฏิบัติการให้เป็นปัจจุบัน โดยเปิดให้ใช้บริการ (Services) เท่าที่จำเป็นเท่านั้น และควรมีการจัดทำคู่มือปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่าย
- 10) บริหารจัดการข้อมูลคอมพิวเตอร์และโปรแกรมคอมพิวเตอร์ ที่เกี่ยวข้องกับกาปฏิบัติงานของหน่วยงาน สำหรับเครื่องคอมพิวเตอร์แม่ข่าย และอุปกรณ์ต่อพ่วงให้มีความมั่นคงปลอดภัย
- 11) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log File) ที่เกี่ยวข้องกับการให้บริการของหน่วยงาน เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้อย่างครบถ้วนถูกต้อง ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์
- 12) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งาน และเปิดเผยข้อมูลที่เป็นความลับ ให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากเจ้าของข้อมูลแล้วเท่านั้น

### วิธีปฏิบัติในการกำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ โดยแบ่งแยกบริเวณพื้นที่ใช้งาน ไว้ 2 ส่วน เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุมการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้น ดังนี้

- 1) พื้นที่ห้องควบคุมระบบ (Control Area) เป็นพื้นที่ที่จัดไว้สำหรับการเฝ้าระวังหรือสังเกตการณ์ระบบ
- 2) พื้นที่จำกัดการเข้าถึง (Restricted Area) เป็นพื้นที่สำหรับติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศ ระบบเครือข่าย และอุปกรณ์ต่อพ่วง รวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

### วิธีปฏิบัติในการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

- 1) ผู้ดูแลห้องควบคุมระบบเครือข่าย จัดทำเอกสาร “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่ห้องควบคุมระบบเครือข่าย” ซึ่งระบุรายละเอียด ชื่อ-นามสกุล, ตำแหน่ง, หน่วยงาน, รายละเอียดกิจกรรม, ระยะเวลา ดำเนินการ และสิทธิที่ได้รับ
- 2) ผู้ดูแลห้องควบคุมระบบเครือข่าย จัดทำแบบฟอร์มการบันทึกการเข้า-ออกพื้นที่ห้องควบคุมระบบเครือข่าย และมีการลง “บันทึกการเข้าออกพื้นที่ด้วยอุปกรณ์อุปกรณ์อิเล็กทรอนิกส์
- 3) บุคคลภายนอกต้องการเข้าห้องควบคุมระบบเครือข่าย ต้องแจ้งเหตุผลความจำเป็นเพื่อปฏิบัติงาน หรือมีหนังสือขอความอนุเคราะห์เข้าศึกษาดูงาน และมีเจ้าหน้าที่อยู่ด้วยตลอดเวลา โดยให้มีการจดบันทึกการเข้าออกพื้นที่ ไว้เป็นหลักฐาน ทั้งในกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่
- 4) ติดประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาต ให้รับทราบทั่วกัน

### วิธีปฏิบัติในการบริหารจัดการระบบเครือข่าย

- 1) ให้มีการจัดทำแผนผังระบบเครือข่าย (Network Diagram) ที่แสดงขอบเขตของเครือข่ายภายในและเครือข่ายนอกมหาวิทยาลัย พร้อมระบุอุปกรณ์ที่ติดตั้งในระบบเครือข่าย และปรับปรุงให้เป็นปัจจุบันอยู่เสมอ
- 2) โดยเครือข่ายภายในมหาวิทยาลัย แบ่งออกเป็นเครือข่ายย่อยๆ แยกตามกลุ่มอาคาร และจัดให้เครือข่ายไร้สายแยกออกจากเครือข่ายส่วนอื่นๆ ของมหาวิทยาลัย โดยระบบที่ไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่นๆ และมีการควบคุมสภาพแวดล้อมของระบบโดยเฉพาะ และมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย
- 3) ผู้ใช้บริการจะสามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น และผู้ที่อยู่ในวงเครือข่ายย่อยหนึ่ง จะไม่สามารถเข้าถึงข้อมูลที่อยู่อีกวงเครือข่ายหนึ่งได้โดยตรง โดยผู้ให้บริการสามารถติดต่อสื่อสารระหว่างเครือข่ายไร้สายและเครือข่ายภายในมหาวิทยาลัยได้ โดยผ่านระบบ VPN (Virtual Private Network)
- 4) ห้ามไม่ให้หน่วยงานทำการวางสายเครือข่ายรวมถึงการติดตั้งเครือข่ายไร้สายเองโดยไม่ได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ
- 5) ผู้ดูแลระบบ ต้องกำหนดหรือตั้งค่า Parameter Configurations ต่างๆ ของระบบเครือข่ายและอุปกรณ์ และทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละ 1 ครั้ง
- 6) ผู้ดูแลระบบต้องตรวจสอบการเปิดปิดพอร์ต (Remote Diagnostic and Configuration Port Protection) เพื่อควบคุมการเข้าถึงพอร์ตของอุปกรณ์เครือข่าย โดยจะปิดพอร์ตที่มีความเสี่ยงต่อการก่อให้เกิดความเสียหายต่อระบบ และปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นใช้งาน พร้อมทั้งมีการป้องกันการเข้าถึงพอร์ต ทั้งทางกายภาพและทางเครือข่าย โดยให้ทำการตรวจสอบอย่างน้อยสัปดาห์ละ 2 ครั้ง
- 7) ผู้ดูแลระบบต้องตรวจสอบการโจมตี บุกรุก การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่าย โดยบุคคลที่ไม่มีหน้าที่รับผิดชอบ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายและระบบ

เครือข่ายไร้สายอย่างสม่ำเสมอ โดยบันทึกการใช้งาน และเหตุการณ์ที่น่าสงสัยที่เกิดขึ้น หากตรวจสอบพบการใช้งานที่ผิดปกติ ให้รายงานต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ ทราบโดยทันที

- 8) การติดตั้ง เคลื่อนย้าย หรือทำการใดๆ กับอุปกรณ์ระบบเครือข่ายต่างๆ ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก ต้องได้รับการอนุญาตจากผู้ดูแลระบบ
- 9) ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่กำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน
- 10) ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point) เพื่อให้ยกต่อการดักจับข้อมูล
- 11) ผู้ดูแลระบบต้องกำหนดตำแหน่งวางอุปกรณ์ Access Point ให้เหมาะสม และควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้
- 12) ผู้ดูแลระบบ ควรเปลี่ยน ชื่อ Login และ Password สำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย
- 13) เลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address และชื่อผู้ใช้งาน รหัสผ่านที่กำหนดไว้เท่านั้น ใช้งานระบบเครือข่ายไร้สายได้อย่างถูกต้อง

### วิธีปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่าย

- 1) ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย โดยกำหนดชั้นตอนและแบบฟอร์มการใช้งานระบบเครือข่าย ประกอบด้วยรายละเอียดเพื่อระบุตัวตน ดังนี้ ชื่อผู้ใช้บริการ หมายเลขบัตรประชาชน หน่วยงาน กรณีเป็นบุคคลภายนอก ให้ระบุเหตุผลในการขอใช้ ระยะเวลาในการใช้บริการ
- 2) ผู้ดูแลระบบต้องควบคุมการจัดเส้นทางบนเครือข่าย ที่เชื่อมต่อกับระบบคอมพิวเตอร์ หรือระบบสารสนเทศ ที่มีการส่งข้อมูลหรือสารสนเทศ และควบคุมการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อควบคุมให้ผู้ใช้สามารถใช้บริการได้ตามภารกิจและบริการที่ได้รับอนุญาตเท่านั้น
- 3) ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายจากระยะไกล (Remote Access) โดยเข้ารหัสผ่านมาตรการที่เป็นมาตรฐานการรักษาความมั่นคงปลอดภัย เช่น SSL VPN เป็นต้น และผู้ใช้บริการต้องได้รับอนุมัติการเข้าถึงระบบจากผู้ดูแลระบบ โดยระบุเหตุผลความจำเป็นในการขอใช้บริการ
- 4) การอนุญาตให้ผู้ใช้เข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ต (Port) หรือโมเด็ม (Modem) โดยไม่จำเป็น และต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น



- 5) ให้มีการยุติการใช้งานระบบสารสนเทศ (Session Time Out) เมื่อไม่ได้ใช้งานเป็นเวลาเกิน 1 ชั่วโมง ยกเว้นในระบบที่มีความจำเป็นต้องใช้เป็นระยะเวลาที่นานขึ้น เช่น ระบบการประชุมออนไลน์ เป็นต้น ให้พิจารณาตามความเหมาะสม
- 6) ให้มีการจำกัดระยะเวลาการเชื่อมต่อระบบเครือข่าย (Limitation of Connection Time) เป็นระยะเวลา นานไม่เกิน 5 ชั่วโมง ต่อการเชื่อมต่อหนึ่งครั้ง หากต้องการเชื่อมต่อใหม่ ให้ทำการเข้ารหัสผ่านเพื่อยืนยัน ตัวตนอีกครั้ง
- 7) ผู้ใช้บริการระบบเครือข่ายมหาวิทยาลัยแม่โจ้ ต้องพิสูจน์ยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้ บริการ
- 8) ห้ามนำ IP Address ของมหาวิทยาลัยแม่โจ้ ไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน .mju.ac.th เว้นแต่ได้รับอนุญาต
- 9) ผู้ใช้งานที่ใช้ระบบเครือข่ายโดยขัดต่อพระราชบัญญัติว่าด้วยการกระทำผิดทางคอมพิวเตอร์ จะถูก พิจารณาระงับ และยกเลิกบัญชีผู้ใช้ โดยมหาวิทยาลัยแม่โจ้ จะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้น จากผู้ใช้

#### วิธีปฏิบัติในการควบคุมสิทธิ์สารสนเทศและการใช้งานระบบคอมพิวเตอร์

- 1) การจัดวางอุปกรณ์ต่างๆ ควรมีการแยกอุปกรณ์และระบบที่มีความสำคัญมากออกจากอุปกรณ์และระบบ ที่ใช้งานทั่วไป

#### วิธีปฏิบัติในการควบคุมการเข้าถึงระบบคอมพิวเตอร์ ระบบปฏิบัติการ ระบบสารสนเทศ

- 1) ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ให้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้งาน และตามสิทธิที่ได้รับอนุญาตให้เข้าถึง เท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
- 2) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ในห้อง ให้บริการสารสนเทศส่วนกลางของมหาวิทยาลัย และกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งาน ระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย
- 3) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีภัยคุกคามคาดเดารหัสผ่านจากเครื่อง ปลายทาง
- 4) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่จะเข้าสู่ระบบจะ เสร็จสมบูรณ์
- 5) จำกัดระยะเวลา และ จำนวนครั้งในการพิมพ์ผิด สำหรับใช้ในการป้องกันการคาดเดารหัสผ่าน
- 6) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหาย ให้กับระบบได้

- 7) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคล ที่ใช้ในการปฏิบัติงาน ผู้ใช้ต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่ตนรับผิดชอบ และตั้งให้มีการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เมื่อว่างเว้นจากการใช้งาน และต้องให้มีการใส่รหัสผ่านก่อนจึงจะเข้าใช้งานได้
- 8) ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ Username และ Password ทุกครั้ง และให้ทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่หน้าจอเป็นเวลานาน

### วิธีปฏิบัติในการบริหารจัดการการเข้าถึงของผู้ใช้งาน

- 1) ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงระบบ โดยกำหนดชื่อผู้ใช้บริการ รหัสผ่าน สิทธิที่ได้รับ เพื่อให้ผู้ใช้บริการสามารถใช้บริการได้ตามภารกิจของผู้ใช้งาน และตามสิทธิที่ได้รับอนุญาตให้เข้าถึงเท่านั้น รวมทั้งดำเนินการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ
- 2) ผู้ดูแลระบบต้องตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ
- 3) ผู้ใช้งานต้องรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร และต้องปฏิบัติตามอย่างเคร่งครัด
- 4) ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน ดังต่อไปนี้
  - 4.1) เปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
  - 4.2) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน และเมื่อผู้ใช้งานได้รับรหัสผ่านต้องตอบยืนยันการได้รับรหัสผ่าน
  - 4.3) กำหนดชื่อผู้ใช้งานและรหัสผ่าน ไม่ซ้ำกัน
  - 4.4) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวเมื่อพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดบ้าง และต้องกำหนดให้รหัสผู้ใช้งานนั้นต่างจากรหัสผู้ใช้งานตามปกติ
- 5) เจ้าของข้อมูลหรือเจ้าของระบบต้องบริหารจัดการการเข้าถึงข้อมูลสำคัญตามประเภทชั้นความลับ เพื่อควบคุมป้องกันข้อมูลที่มีความสำคัญ ข้อมูลส่วนบุคคล โดยการกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูล และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

### วิธีปฏิบัติในการสำรองข้อมูล และกู้คืนระบบ

- 1) ผู้ดูแลระบบจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย โดยคัดเลือกจากความสะดวกคล่องเชื่อมโยงกับภารกิจของมหาวิทยาลัย แผนปฏิบัติราชการ คำรับรองการปฏิบัติราชการและนโยบายของมหาวิทยาลัย ได้แก่ ฐานข้อมูล 5 ด้าน คือ นักศึกษาและหลักสูตร บุคลากร การเงินและบัญชี งานวิจัย และอาคารสถานที่

- 2) ผู้ดูแลระบบกำหนดเจ้าหน้าที่รับผิดชอบดำเนินการสำรองข้อมูล โดยจัดทำเป็นลายลักษณ์อักษร และให้เจ้าหน้าที่ลงนามรับทราบ
- 3) ผู้ดูแลระบบกำหนดขั้นตอนปฏิบัติ วิธีการสำรองข้อมูล ความถี่ ช่วงเวลา สื่อที่ใช้ สถานที่จัดเก็บข้อมูลในการสำรองข้อมูล และดำเนินการสำรองข้อมูล การกู้คืนข้อมูล ที่เหมาะสม และรองรับพระราชบัญญัติว่าด้วยการผิดเกี่ยวกับคอมพิวเตอร์ เพื่อให้ระบบอยู่ในสภาพพร้อมใช้งาน โดยแยกตามระบบสารสนเทศ แต่ละระบบ และจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม พร้อมทั้งมีการดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่จัดเก็บข้อมูลสำรอง
- 4) ผู้ดูแลระบบต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน ตามระยะเวลาที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน
- 5) ผู้ดูแลระบบ ต้องจัดให้มีรหัสก่อนเข้าถึงข้อมูลสำรองที่สำคัญ โดยการใช้วิธีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

#### วิธีปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

- 1) ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงาน
- 2) กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
- 3) การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
  1. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
  2. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
  3. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
- 4) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ 1 ครั้ง โดยผู้ตรวจสอบภายในของหน่วยงาน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน
- 5) กำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- 6) ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉิน ดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ
- 7) ผู้ดูแลระบบทดสอบและปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัย และสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

- 8) ผู้ดูแลระบบต้องบันทึกเหตุการณ์ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และหลักฐานสำหรับอ้างอิง เพื่อกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

## วิธีปฏิบัติของผู้ใช้งาน

เพื่อให้ผู้ใช้งานมีความรู้ในการใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายอย่างปลอดภัย และปฏิบัติตามเคร่งครัด ซึ่งประกอบด้วย การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและแบบพกพา การใช้งานจดหมายอิเล็กทรอนิกส์ การใช้งานระบบอินเทอร์เน็ต การใช้งานเครือข่ายสังคมออนไลน์

### 1. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อกำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ เป็นการป้องกันการเข้าถึงข้อมูลโดยบุคคลอื่นและเปิดเผยข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต มีข้อปฏิบัติดังนี้

#### ๑.๑ การใช้งานรหัสผ่าน (Password Use)

- (1) การตั้งและการเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย
  - (1.1) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที
  - (1.2) กำหนดรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น โดยมีเทคนิคที่ง่ายต่อการจดจำ
  - (1.3) เปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
  - (1.4) กำหนดรอบระยะเวลาการเปลี่ยนรหัสผ่าน ดังนี้
 

[1] ผู้ดูแลระบบและผู้บริหาร	ทุก ๓ เดือน
[2] ผู้ใช้งานทั่วไป	ทุก ๖ เดือน
- (2) คุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี
  - (2.1) กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
  - (2.2) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม
  - (2.3) หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน (123 , abcd) หรือกลุ่มของตัวอักขระที่เหมือนกัน (111 , aaa)
- (3) หน้าที่รับผิดชอบของผู้ดูแลระบบ
  - (4.1) ผู้ดูแลระบบทำหน้าที่เฝ้าระวังติดตามการใช้งานผิดวัตถุประสงค์
  - (4.2) ผู้ดูแลระบบมีหน้าที่รายงานเหตุการณ์ที่ผิดปกติให้กับผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO)
  - (4.3) ผู้ดูแลระบบต้องมีรหัสผ่าน 2 ชุด เพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

(4) การใช้งานรหัสผ่าน ของผู้ใช้ ต้องปฏิบัติดังนี้

- (3.1) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
- (3.2) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
- (3.3) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์
- (3.4) ไม่กำหนดให้มีการบันทึกช่วยจำรหัสผ่านส่วนบุคคล
- (3.5) ไม่อนุญาตให้ผู้อื่นใช้รหัสผ่านของตน หากเกิดปัญหาจากการใช้งานที่ผิดต่อกฎหมาย เจ้าของบัญชีต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ
- (3.6) ไม่ลับลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น
- (3.7) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้
- (3.8) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้ว ให้ทำการเปลี่ยนรหัสผ่านโดยทันที
- (3.9) ให้มีการรายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที
- (3.10) ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด และปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

๑.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ข้อปฏิบัติที่เหมาะสม เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของมหาวิทยาลัย ในขณะที่ไม่มีผู้ดูแล มีดังนี้

- (1) เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสำหรับผู้ใช้งานและผู้ดูแลระบบ
- (2) เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องติดตั้งระบบล็อกหน้าจอ (Screen Saver) หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงสามารถเปิดหน้าจอได้
- (3) ให้ทำการล็อกอุปกรณ์ที่สำคัญเมื่อไม่ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

๑.๓ การเข้ารหัสข้อมูลที่เป็นความลับ

ผู้ใช้อาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 ได้แก่

- (1) การสำรองข้อมูลที่เป็นข้อมูลลับต้องเข้ารหัสด้วยเทคโนโลยี Secured Socket Layer (SSL) ซึ่งเป็นเทคโนโลยีการเข้าสู่ข้อมูลผ่านรหัสที่ระดับ 128 bits (128 bits Encryption) เป็นอย่างน้อยเพื่อเข้ารหัสข้อมูลที่ถูกส่งผ่านเครือข่ายอินเทอร์เน็ตในทุกครั้ง
- (2) การอนุญาตให้เข้าถึงข้อมูลลับผ่านเครือข่ายต้องเข้ารหัสด้วยรหัสผ่าน กำหนดวันหมดอายุของการเข้าถึง และระบุให้เข้าถึงได้เฉพาะผู้มีสิทธิ
- (3) ไม่อนุญาตให้ส่งข้อมูลลับผ่านเครือข่าย หากต้องการส่งต้องขออนุญาตจากผู้บังคับบัญชาทุกครั้ง และในกรณีที่เป็นไฟล์แนบต้องเข้ารหัสด้วยรหัสผ่านทุกครั้ง

(4) การสำเนาข้อมูลขึ้นความลับ ต้องจดบันทึกจำนวนชุดที่ทำสำเนา รายละเอียดผู้ดำเนินการทุกครั้ง

## ๑.๔ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

### (1) การใช้งานทั่วไป

- [1] ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้
- [2] เครื่องคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยแม่โจ้เป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น
- [3] โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามี การติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว
- [4] การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจสอบจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศ หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น
- [5] ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส
- [6] ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้
- [7] ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ต้องใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการ ตก กระทบกระเทือน
- [8] การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง
- [9] ไม่วางของทับบนหน้าจอและแป้นพิมพ์
- [10] การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น
- [11] ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น
- [12] ผู้ใช้งานมีหน้าที่รับผิดชอบ ต้องล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เพื่อป้องกันการสูญหาย
- [13] ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายใน รวมถึงแบตเตอรี่
- [14] ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล
- [15] ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ ในส่วนที่มีใช้ของตนโดยไม่ได้รับอนุญาต ด้วยการบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือเข้าสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่

- ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็น การละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าตนไม่ได้เป็นผู้กระทำความผิด
- [16] ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่มหาวิทยาลัยแม่โจ้ กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม
  - [17] หากผู้ใช้งานกระทำการล่วงละเมิด หรือ พยายามจะล่วงละเมิด ศูนย์เทคโนโลยีสารสนเทศ ในฐานะ ผู้ดูแลระบบคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัย ขอสงวนสิทธิ์ที่จะยกเลิกการใช้งาน หรือ ระงับการเชื่อมต่อ และ/หรือ การใช้งานใดๆ ตามความเหมาะสม
  - [18] ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ
  - [19] ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล๊อคหน้าจอภาพ เมื่อไม่มีการใช้งาน หลังจากนั้น เมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน
  - [20] ในการเข้าใช้ระบบปฏิบัติการใส่ User และ Password ทุกครั้ง
  - [21] ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ร่วมกัน
  - [22] ผู้ใช้งานต้องทำการลงบันทึกออก (Logout) ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
  - [23] ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา หรือศูนย์เทคโนโลยีสารสนเทศ
  - [24] ห้ามมิให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากตรวจพบถือว่าเป็น ความผิดส่วนบุคคล ผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว
  - [25] ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟต์แวร์ที่มหาวิทยาลัย จัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น
  - [26] ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัด ต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์
  - [27] ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศ ภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

## (2) การสำรองข้อมูลและการกู้คืน

- [1] ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ได้แก่ CD, DVD และ External Hard Disk
- [2] ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

### ๑.๕ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail)

กำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยแม่โจ้ ซึ่งผู้ใช้งานจะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิหรือกระทำการใดๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

- (1) ต้องไม่ตั้งค่า การใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
- (2) ต้องเปลี่ยนรหัสผ่านอย่างเคร่งครัด ทุก 3-6 เดือน
- (3) ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยหรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย ละเมิดศีลธรรม จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยแม่โจ้
- (4) ต้องไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail Address) ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับขออนุญาตจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
- (5) ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยแม่โจ้ เพื่อการทำงานของมหาวิทยาลัยแม่โจ้เท่านั้น
- (6) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ต้องทำการล็อกเอาท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
- (7) ทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส
- (8) ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
- (9) ต้องไม่ใช่ข้อความที่ไม่สุภาพ หรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยแม่โจ้ ทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์
- (10) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
- (11) ทำการตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

### ๑.๖ การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

เพื่อให้ผู้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในราชกิจจานุเบกษา (18 มิถุนายน 2550) และพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในราชกิจจานุเบกษา (24 มกราคม 2560) ได้แก่ การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของ



บุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัย ถูกกระจัด ชะลอ ชัดขวาง หรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้ มีแนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต ดังนี้

- (1) ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยแม่โจ้ จัดสรรไว้เท่านั้น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร
- (2) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรม ป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราว์เซอร์
- (3) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัสเพื่อป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
- (4) ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยแม่โจ้ เพื่อทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม
- (5) ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยแม่โจ้
- (6) ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัยแม่โจ้
- (7) ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยแม่โจ้ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
- (8) ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
- (9) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
- (10) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ต ก่อนนำข้อมูลไปใช้งาน
- (11) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรม ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
- (12) ในการเสนอความคิดเห็น ผู้ใช้ต้องไม่ใช้ข้อความที่ยั่ว ให้อาย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยแม่โจ้ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ
- (13) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราว์เซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

### ๑.๗ 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 โดยเฉพาะข้อมูลข่าวสารบางอย่างที่เผยแพร่ไปสู่สาธารณะไปแล้วอาจไม่สามารถเรียกกลับคืนได้ และอาจก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อองค์กร ดังนั้น เพื่อให้ผู้ปฏิบัติงานในมหาวิทยาลัย สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ทางมหาวิทยาลัยแม่โจ้ จึงมีแนวทางปฏิบัติสำหรับผู้ใช้สื่อสังคมออนไลน์ (Social Network) และแสดงตนในฐานะบุคลากรหรือนักศึกษาในสังกัดมหาวิทยาลัยแม่โจ้ ดังนี้

- (1) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น
- (2) ควรแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ หากพบว่ามีข้อความบน Social Network ที่อาจก่อให้เกิดความเสื่อมเสียชื่อเสียงของหน่วยงาน ส่วนงานของมหาวิทยาลัยแม่โจ้ได้
- (3) พึงระลึกว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ในราชกิจจานุเบกษา (18 มิถุนายน 2550) พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ. 2560 ในราชกิจจานุเบกษา (24 มกราคม 2560) ข้อบังคับว่าด้วยจรรยาบรรณของบุคลากรและนักศึกษามหาวิทยาลัยแม่โจ้ และข้อบังคับว่าด้วยวินัยนักศึกษา มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบน Social Network ด้วย ทั้งนี้การละเมิดจรรยาบรรณอย่างร้ายแรงดังที่กำหนดไว้ในข้อบังคับดังกล่าว ได้แก่ การเปิดเผยความลับของนักศึกษาหรือผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่นักศึกษาหรือรับผู้รับบริการ หรือการทำให้เกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของมหาวิทยาลัยแม่โจ้ ถือเป็นความผิดทางวินัยอย่างร้ายแรงและผู้ละเมิดสามารถถูกดำเนินการทางวินัยได้ด้วย
- (4) ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว และพึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรได้
- (5) พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บน Social Network เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้
- (6) การนำเสนอข้อมูลข่าวสาร การแสดงความคิดเห็น ผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามจริยธรรมวิชาชีพ และแนวปฏิบัติจริยธรรม
- (7) การใช้สื่อสังคมออนไลน์ (Social Media) พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ทำร้าย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
- (8) ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน

- (9) ผู้ใช้งาน พึงระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้าน และควรอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
- (10) ผู้ใช้งาน สามารถใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาได้ แต่ควรแสดงให้เห็นชัดเจนว่า ข้อความใดเป็น “ข่าว” ข้อความใดเป็น “ความคิดเห็นส่วนตัว” ทั้งนี้พึงตระหนักว่าการใช้ Social Network นั้นการแบ่งแยกระหว่างเรื่องส่วนตัว และเรื่องหน้าที่การงาน เป็นสิ่งที่ทำได้ยาก หากประสงค์จะใช้ Social Network เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน
- (11) หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือมหาวิทยาลัยต้องแจ้ง ชื่อ Page หรือ Account และ รายชื่อผู้ดูแล (Admin) ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศทราบ โดยผู้ดูแลมีหน้าที่ต้องขอสิทธิในการดูแล Page หรือ Account นั้นคืนแก่มหาวิทยาลัย เมื่อพ้นจากหน้าที่ที่ต้องดูแล หรือพ้นสภาพจากการเป็นบุคลากรของมหาวิทยาลัยแม่โจ้
- (12) ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือสื่อสารข้อมูลในกิจการของมหาวิทยาลัยหรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ควรแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูลโปรไฟล์ (Profile) และพึงใช้ด้วยความสุภาพ และมีวิจารณญาณ
- (13) การเผยแพร่ข้อมูล หรือแสดงความคิดเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงาน ที่ตนสังกัด เว้นแต่จะเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง
- (14) ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความคิดเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ได้บังคับบัญชาได้ ทั้งนี้ ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนว่าเป็นความเห็นส่วนตัว มิใช่ความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงานอย่างแท้จริง
- (15) ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของมหาวิทยาลัย หรือข้อมูลที่ใช้ภายในมหาวิทยาลัยก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ
- (16) ในการสื่อสารข้อมูลในกิจการขององค์กรทางสื่อสังคมออนไลน์ (Social Media) ห้ามแสดงสัญลักษณ์พรรคการเมือง กลุ่มกดดันรณรงค์ทางสังคม กลุ่มลัทธิทางศาสนา และพึงระมัดระวังในการใช้สัญลักษณ์ที่ก่อให้เกิดความเข้าใจผิดและไม่ควรนำรูปบุคคลอื่นมาแสดงว่าเป็นรูปของตนเอง
- (17) การส่งต่อข้อมูลในสื่อสังคมออนไลน์ (Social Media)
- [1] พึงละเว้นการส่งต่อข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคลหรือสังคม

- [2] พังระมัดระวังการส่งต่อข้อมูลในสถานการณ์ภัยพิบัติธรรมชาติ การก่อการร้าย การจลาจล วิศวกรรมหรือภาวะสงคราม
- [3] พังระมัดระวังการส่งต่อข้อมูลเรื่อง บุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
- [4] พังระมัดระวังการส่งต่อข้อมูลที่กระทบต่อสิทธิ ความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
- (18) ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสม นอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลกระทบต่อหน่วยงาน ส่วนงาน และมหาวิทยาลัยได้ด้วย
- (19) หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรอื่น ทางองค์กรหรือผู้ใช้งานที่รับผิดชอบข้อความนั้น ไม่ว่าจะเป็นการส่งข้อความเองหรือรับส่งข้อมูลต่อ ต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือองค์กรที่ได้รับ ความเสียหาย ทั้งนี้ต้องให้ผู้ที่มีความเสียหายมีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย