แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2558
สำหรับผู้ใช้บริการเครือข่ายและระบบสารสนเทศมหาวิทยาลัยแม่โจ้

คำนำ

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของมหาวิทยาลัยแม่โจ้ นี้เป็นแนวปฏิบัติที่มีรายละเอียดบรรจุไว้ในนโยบายและแนวปฏิบัติความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย ซึ่งได้จัดทำขึ้นตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.2549 มาตรา 5 “หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้” และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. 2553 ที่กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร โดยมีวัตถุประสงค์ ดังนี้

1) เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยแม่โจ้ ให้ดำเนินไปได้อย่างมีประสิทธิภาพและประสิทธิผล

2) เพื่อกำหนดขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ อ้างอิงตามมาตรฐาน ISO/IEC27001 และมีการปรับปรุงอย่างต่อเนื่อง

3) เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร ข้าราชการ เจ้าหน้าที่ ผู้ดูแลระบบ นักศึกษาและบุคคลภายนอกที่ปฏิบัติงานร่วมกับมหาวิทยาลัยแม่โจ้ ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย ในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยแม่โจ้ ในการดำเนินงานและถือปฏิบัติตามอย่างเคร่งครัด

4) เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

5) เพื่อเผยแพร่และส่งเสริมให้กับข้าราชการ เจ้าหน้าที่ บุคลากรทุกระดับ และนักศึกษาในมหาวิทยาลัยแม่โจ้ โจ้ มีความรู้ ความเข้าใจในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศและการสื่อสาร และถือปฏิบัติอย่างเคร่งครัด

โดยมีเนื้อหาครอบคลุมแนวปฏิบัติในการเข้าถึงและใช้งานระบบสารสนเทศของผู้ใช้บริการเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยแม่โจ้

สารบาญ

การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

1. วิธีการปฏิบัติการใช้งานรหัสผ่าน (Password Use)

1) แนวปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

[1] ผู้ใช้งานควรเปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันที

[2] เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

[3] กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อย ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

[4] ผู้ใช้งานควรตั้งรหัสผ่านที่มีเทคนิคที่ง่ายต่อการจดจำ

[5] ผู้ใช้งานควรเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด และผู้ดูแลระบบควรเปลี่ยนรหัสผ่านด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป โดยกำหนดอย่างน้อยทุก 6 เดือนสำหรับผู้ใช้งานทั่วไป และอย่างน้อยทุก 3 เดือน สำหรับผู้บริหารและผู้ดูแลระบบ หรือตามระยะเวลาที่เหมาะสม

[6] ผู้ใช้งานควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

2) คุณสมบัติพื้นฐานสำหรับรหัสผ่านที่ดี

[1] กำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ 8 ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

[2] ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

[3] หลีกเลี่ยงการตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน หรือกลุ่มของตัวอักขระที่เหมือนกัน

3) ข้อระวังการใช้งานรหัสผ่านที่ปลอดภัย

[1] ผู้ใช้งานไม่ควรใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

[2] ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

[3] ต้องไม่กำหนดให้มีการบันทึกหรือช่วยจำรหัสผ่านส่วนบุคคล

[4] ผู้ใช้งานควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

2. การป้องกันอุปกรณ์ ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

1) ให้ผู้ใช้งานออกจากระบบเทคโนโลยีสารสนเทศ อุปกรณ์คอมพิวเตอร์ทันที เมื่อใช้งานเสร็จ

2) ผู้ใช้งาน ควรล็อกอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน

3) ให้ผู้ใช้งานป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบเทคโนโลยีสารสนเทศของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

4) ให้มีการตั้งล๊อกหน้าจอเครื่องคอมพิวเตอร์หลังจากไม่ได้ใช้งานเป็นเวลาไม่เกิน 30 นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

3. การเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ

ผู้ใช้งานสามารถนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2544 และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

4. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

1) การใช้งานทั่วไป

[1] ผู้ใช้งานต้องยอมรับทราบกฎระเบียบหรือนโยบายต่างๆ ที่กำหนดขึ้น โดยจะอ้างว่าไม่ทราบกฎระเบียบหรือนโยบาย มิได้

[2] เครื่องคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยแม่โจ้เป็นสมบัติของทางราชการ ผู้ใช้งานควรใช้เพื่อประโยชน์ทางราชการเท่านั้น

[3] โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติม และก่อให้เกิดความเสียหายหรือการละเมิดลิขสิทธิ์ ถือเป็นความผิดส่วนบุคคล ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

[4] การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของศูนย์หรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

[5] ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบหาไวรัสโดยโปรแกรมป้องกันไวรัส

[6] ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์หรือ และ/หรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

[7] ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น ตกหรือหลุดมือ ฯลฯ

[8] การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัด ควรปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

[9] ไม่วางของทับบนหน้าจอและแป้นพิมพ์

[10]การเคลื่อนย้ายเครื่อง ขณะที่เครื่องเปิดใช้งานอยู่ ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

[11]ไม่ใช้หรือวางเครื่องคอมพิวเตอร์แบบพกพาใกล้สิ่งที่เป็นของเหลว ความชื้น เช่น อาหาร น้ำ กาแฟ และเครื่องดื่มต่าง ๆ ฯลฯ

[12]ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล๊อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

[13]ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

[14]ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

[15]ผู้ใช้งานจะต้องไม่ละเมิดต่อผู้อื่น (อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใดๆ) ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น หรือสู่เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น การเผยแพร่ข้อความใดๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาหรือรูปภาพไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงฝ่ายเดียว

[16]ผู้ใช้งานสัญญาว่าจะปฏิบัติตามเงื่อนไข/นโยบาย/กฎ/ระเบียบ/คำแนะนำที่มหาวิทยาลัยแม่โจ้กำหนดไว้และที่จะกำหนดขึ้นในอนาคตตามความเหมาะสม

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

[18]ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

[19]ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน 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]ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาซอฟท์แวร์ที่มหาวิทยาลัยจัดเตรียมไว้ให้ผู้ใช้งาน เพื่อนำไปใช้งานที่อื่น

[25]ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

[26]ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

[27]ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

5. การใช้งานระบบจดหมายอิเล็กทรอนิกส์

1) ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์
2) ควรมีการเปลี่ยนรหัสผ่านอย่างเคร่งครัด เช่น ควรเปลี่ยนรหัสผ่านทุก 3-6 เดือน
3) ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยแม่โจ้ หรือละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย ละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยแม่โจ้
4) ข้อห้าม ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของผู้อื่น เพื่ออ่าน รับ-ส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน
5) ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยแม่โจ้ เพื่อการทำงานของมหาวิทยาลัยแม่โจ้ เท่านั้น
6) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์
7) ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable File เช่น .exe .com เป็นต้น
8) ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก
9) ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยแม่โจ้ ผ่านทางจดหมายอิเล็กทรอนิกส์
10) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์
11) ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูล และจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด
12) ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

13) ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้

6. การใช้งานระบบอินเทอร์เน็ต (Use of the Internet)

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ดังนี้

1) เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรม ป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์
2) ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัส (Virus Canning) ป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง
3) ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยแม่โจ้ เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น
4) ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยแม่โจ้
5) ผู้ใช้งาน ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัว ข้อมูลที่ไม่เหมาะสมทางศีลธรรม ข้อมูลที่ละเมิดสิทธิของผู้อื่น และข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัยแม่โจ้
6) ผู้ใช้งาน ต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยแม่โจ้ ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต
7) ผู้ใช้งาน ต้องไม่นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร การก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต
8) ผู้ใช้งาน ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ เติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย
9) ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของก่อนนำข้อมูลไปใช้งาน
10) ผู้ใช้งาน ต้องระมัดระวังการดาวน์โหลดโปรแกรม ใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา
11) ในการเสนอความคิดเห็น ผู้ใช้งาน ต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยแม่โจ้ รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น

12) หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้จากบุคคลอื่น

7. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

ปัจจุบันมีแหล่งให้บริการเครือข่ายทางสังคมเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ตเป็นจำนวนมาก ตัวอย่างเช่น Facebook, Twitter, LinkedIn, Google Plus, Myspace, YouTube, Blog, Wiki รวมทั้งเว็บไซต์ต่างๆ ทั้งในประเทศและต่างประเทศ ที่เป็นให้บริการ File Sharing, Photo Sharing, Video Sharing และกระดานข่าว (Web board) เป็นต้น และเนื่องจากสื่อสังคมออนไลน์ เป็นเครื่องมือที่มีทั้งประโยชน์และโทษที่ควรระวัง โดยเฉพาะข้อมูลข่าวสารบางอย่างที่เผยแพร่ออกสู่สาธารณะไปแล้วอาจไม่สามารถเรียกกลับคืนได้ และอาจก่อให้เกิดความเสียหายทั้งต่อตนเอง ต่อผู้อื่น และต่อองค์กร ดังนั้น เพื่อให้ผู้ปฏิบัติงานในมหาวิทยาลัย สามารถใช้สื่อสังคมออนไลน์ได้อย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ทางมหาวิทยาลัยแม่โจ้ จึงมีนโยบายและแนวทางปฏิบัติสำหรับผู้ที่ใช้สื่อสังคมออนไลน์ (Social Network) และแสดงตนในฐานะบุคลากรหรือนักศึกษาในสังกัดมหาวิทยาลัยแม่โจ้ ดังนี้

1) อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น
2) ควรแจ้งให้ศูนย์เทคโนโลยีสารสนเทศทราบ หากพบว่ามีข้อความบน Social Network ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงของหน่วยงาน ส่วนงานของมหาวิทยาลัยได้
3) พึงระลึกว่า พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 และข้อบังคับว่าด้วยจรรยาบรรณของบุคลากรและนักศึกษามหาวิทยาลัยแม่โจ้ และข้อบังคับว่าด้วยวินัยนักศึกษา มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบน Social Network ด้วย ทั้งนี้การละเมิดจรรยาบรรณอย่างร้ายแรงดังที่กำหนดไว้ในข้อบังคับดังกล่าว เช่น การเปิดเผยความลับของนักศึกษาหรือผู้รับบริการที่ได้มาจากการปฏิบัติหน้าที่หรือจากความไว้วางใจ ที่ก่อให้เกิดความเสียหายแก่นักศึกษาหรือรับผู้รับบริการ หรือการทำให้เกิดความเสียหายอย่างร้ายแรงแก่ทรัพย์สิน เกียรติ และชื่อเสียงของมหาวิทยาลัย ถือเป็นความผิดทางวินัยอย่างร้ายแรงและผู้ที่ละเมิดสามารถถูกดำเนินการทางวินัยได้ด้วย
4) ผู้ใช้งานพึงตระหนักว่าพื้นที่บนสื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ซึ่งข้อมูลที่มีการรายงานจะถูกบันทึกไว้และอาจมีผลทางกฎหมาย ถึงแม้จะเป็นการแสดงความคิดเห็นในนามชื่อบัญชีส่วนตัว พึงตระหนักถึงผลกระทบที่อาจเกิดขึ้นกับองค์กรได้ และพึงระมัดระวังเรื่องผลประโยชน์ในเชิงพาณิชย์
5) พึงตระหนักว่า ข้อความหรือความเห็นที่เผยแพร่บน Social Network เป็นข้อความที่สามารถเข้าถึงได้โดยสาธารณะ ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคม และด้านกฎหมาย นอกจากนี้ยังอาจมีผลกระทบต่อชื่อเสียง การทำงานและอนาคตของวิชาชีพของตนได้
6) การนำเสนอข้อมูลข่าวสาร การแสดงความคิดเห็น ผ่านสื่อสังคมออนไลน์ ต้องเป็นไปตามจริยธรรมวิชาชีพและแนวปฏิบัติจริยธรรม

7) การใช้สื่อสังคมออนไลน์ (Social Media) พึงระมัดระวังการใช้ถ้อยคำและภาษาที่อาจเป็นการดูหมิ่น ยุยง ท้าทาย หรือเป็นการละเมิดต่อบุคคลอื่น กรณีบุคคลอื่นมีความคิดเห็นที่แตกต่าง พึงงดเว้นการโต้ตอบด้วยถ้อยคำรุนแรง
8) ต้องไม่ละเมิดทรัพย์สินทางปัญญาของผู้อื่น หากต้องการกล่าวอ้างถึงแหล่งข้อมูลที่สนับสนุนข้อความของตน ควรให้การอ้างอิงถึงแหล่งข้อมูลนั้นอย่างชัดเจน
9) ผู้ใช้งาน พึงระมัดระวังกระบวนการหาข่าว หรือภาพจากสื่อสังคมออนไลน์ โดยมีการตรวจสอบอย่างถี่ถ้วนรอบด้าน และควรอ้างอิงแหล่งที่มาเมื่อนำเสนอ เว้นแต่สามารถตรวจสอบและอ้างอิงจากแหล่งข่าวได้โดยตรง
10) ผู้ใช้งาน สามารถใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือในการรายงานข่าวในนามของบุคคลธรรมดาได้ แต่ควรแสดงให้ชัดเจนว่า ข้อความใดเป็น “ข่าว” ข้อความใดเป็น “ความคิดเห็นส่วนตัว” ทั้งนี้พึงตระหนักว่าการใช้ Social Network นั้นการแบ่งแยกระหว่างเรื่องส่วนตัว และเรื่องหน้าที่การงาน เป็นสิ่งที่ทำได้ยาก หากประสงค์จะใช้ Social Network เพื่อเผยแพร่ข้อมูลเกี่ยวกับเรื่องหน้าที่การงานหรือข้อมูลเกี่ยวกับหน่วยงาน ควรแยกบัญชีผู้ใช้ ระหว่างการใช้เพื่อเรื่องส่วนตัว และเรื่องหน้าที่การงานออกจากกัน ยกตัวอย่างเช่น การใช้ Facebook ของผู้ที่ทำหน้าที่ประชาสัมพันธ์ของส่วนงาน ควรมีการแยก Facebook Profile ที่ใช้สำหรับติดต่อเครือข่ายของตนในเรื่องส่วนตัว เรื่องครอบครัว ออกจาก Facebook Profile ที่ใช้ประชาสัมพันธ์ส่วนงาน หรืออาจตั้งเป็น Facebook Page ประจำส่วนงานขึ้นแทนที่จะใช้ Profile ส่วนตัว
11) หากต้องการสร้าง Page หรือ Account ที่เป็นช่องทางในการเผยแพร่ข้อมูลอย่างเป็นทางการของส่วนงานหรือมหาวิทยาลัยต้องแจ้งให้หัวหน้าส่วนงาน ศูนย์เทคโนโลยีสารสนเทศทราบ และ/หรืองานประชาสัมพันธ์ของสำนักงานอธิการบดี แล้วแต่กรณี และต้องแจ้งรายชื่อของผู้ดูแล Page (Admin) หรือเจ้าของ Account นั้นให้หัวหน้าส่วนงาน ศูนย์เทคโนโลยีสารสนเทศทราบ และ/หรืองานประชาสัมพันธ์ของสำนักงานอธิการบดีทราบด้วย และผู้ดูแลมีหน้าที่ต้องมอบสิทธิ์ในการดูแล Page หรือ Account นั้นคืนแก่ส่วนงานหรือมหาวิทยาลัย เมื่อพ้นจากหน้าที่ที่ต้องดูแล หรือพ้นสภาพจากการเป็นบุคลากรของมหาวิทยาลัย
12) ผู้ใช้งานที่ใช้สื่อสังคมออนไลน์ (Social Media) เป็นเครื่องมือสื่อสารข้อมูลในกิจการของมหาวิทยาลัย หรือชื่อบุคคลที่ทำให้เข้าใจได้ว่าเป็นบุคคลในสังกัด ควรแสดงภาพ และข้อมูลให้ถูกต้องชัดเจนในข้อมูลโปรไฟต์ (Profile) และพึงใช้ด้วยความสุภาพ และมีวิจารณญาณ
13) การเผยแพร่ข้อมูล หรือแสดงความเห็นที่อาจทำให้เข้าใจว่าเป็นความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงาน ต้องมีการแสดงข้อความจำกัดความรับผิดชอบ (Disclaimer) ว่าเป็นความเห็นส่วนตัว มิใช่

ความเห็นของมหาวิทยาลัย ส่วนงาน หรือหน่วยงานที่ตนสังกัด เว้นแต่จะเป็นความเห็นของมหาวิทยาลัย ส่วนงานหรือหน่วยงานอย่างแท้จริง หรือได้รับอนุญาตจากผู้มีอำนาจที่เกี่ยวข้อง

14) ผู้บริหารในระดับใดๆ พึงระมัดระวังในการเผยแพร่ข้อมูล หรือการแสดงความเห็นเนื่องจากจะถูกมองว่าเป็นความเห็นของหน่วยงานของตนได้ง่าย และอาจมีผลกระทบต่อความเข้าใจของผู้ใต้บังคับบัญชาได้ ทั้งนี้ให้มีการแสดงข้อความจำกัดความรับผิดชอบอย่างชัดเจนเช่นเดียวกับข้อ 12
15) ห้ามเผยแพร่ข้อมูลที่เป็นทรัพย์สินทางปัญญาของมหาวิทยาลัย หรือข้อมูลที่ใช้ภายในมหาวิทยาลัย ก่อนได้รับอนุญาตอย่างเป็นทางการจากผู้มีอำนาจ
16) ในการสื่อสารข้อมูลในกิจการขององค์กรทางสื่อสังคมออนไลน์ (Social Media) ห้ามแสดงสัญลักษณ์พรรคการเมือง กลุ่มกดดันรณรงค์ทางสังคม กลุ่มลัทธิทางศาสนา และพึงระมัดระวังในการใช้สัญลักษณ์ที่ก่อให้เกิดความเข้าใจผิดและไม่ควรนำรูปบุคคลอื่น มาแสดงว่าเป็นรูปของตนเอง
17) การส่งต่อข้อมูลในสื่อสังคมออนไลน์ (Social Media)
    [1] พึงละเว้นการส่งต่อข้อมูลที่เป็นเท็จ ข่าวลือ ข่าวไม่ปรากฏที่มา เป็นเพียงการคาดเดา หรือส่งผลเสียหายกับบุคคลหรือสังคม
    [2] พึงระมัดระวังการส่งต่อข้อมูลในสถานการณ์ภัยพิบัติธรรมชาติ การก่อการร้าย การจลาจล วินาศกรรมหรือภาวะสงคราม
    [3] พึงระมัดระวังการส่งต่อข้อมูลเรื่อง บุคคลเสียชีวิต เด็กและเยาวชน ผู้สูญหาย ผู้ต้องหา เว้นเสียแต่ตรวจสอบข้อเท็จจริงแล้วและเห็นว่าเป็นประโยชน์ต่อสาธารณะ
    [4] พึงระมัดระวังการส่งต่อข้อมูลที่กระทบต่อสิทธิ ความเป็นส่วนตัว และศักดิ์ศรีความเป็นมนุษย์
18) ศึกษาการใช้ “การตั้งค่าความเป็นส่วนตัว” หรือ “Privacy Settings” ให้เข้าใจเป็นอย่างดี และปรับแต่งการตั้งค่าความเป็นส่วนตัวให้เหมาะสมกับบริบท การถูกละเมิดความเป็นส่วนตัวโดยไม่เหมาะสมนอกเหนือจากส่งผลกระทบต่อตนเองแล้ว อาจส่งผลต่อหน่วยงาน ส่วนงาน และมหาวิทยาลัยได้ด้วย
19) หากการนำเสนอข้อมูลข่าวสารหรือการแสดงความคิดเห็นผ่านสื่อสังคมออนไลน์ เกิดความผิดพลาด จนก่อให้เกิดความเสียหายต่อบุคคลหรือองค์กรอื่น ทางองค์กรหรือผู้ใช้งานที่รับผิดชอบข้อความนั้น ไม่ว่าจะเป็นการส่งข้อความเองหรือรับส่งข้อมูลต่อ ต้องดำเนินการแก้ไขข้อความที่มีปัญหาโดยทันที พร้อมทั้งแสดงถ้อยคำขอโทษต่อบุคคลหรือองค์กรที่ได้รับความเสียหาย ทั้งนี้ต้องให้ผู้ที่ได้รับความเสียหายมีโอกาสชี้แจงข้อมูลข่าวสารในด้านของตนด้วย

การใช้งานรหัสผ่าน

- เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับทันที
- ควรตั้งให้มีเทคนิคที่ง่ายต่อการจำ
- เก็บรหัสผ่านไว้เป็นความลับ
- เปลี่ยนรหัสผ่านทุก 3 เดือน และเปลี่ยนรหัสผ่านทันทีที่ทราบว่ารหัสถูกเปิดเผย
- การเปลี่ยนรหัสผ่านต้องไม่ใช้รหัสผ่านที่เคยตั้งมาแล้ว
- ไม่จดรหัสผ่านไว้ในสถานที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น และไม่กำหนดให้ระบบมีการบันทึกช่วยจำรหัสผ่าน

ข้อแนะนำในการตั้งรหัสผ่าน

- ตั้งรหัสผ่านอย่างน้อย 8 ตัวอักษร มีการผสมกันระหว่างตัวอักษร ตัวเลข และสัญลักษณ์
- ไม่ใช้ชื่อ-สกุลของตนหรือคนใกล้ชิดหรือคำจากพจนานุกรม
- หลีกเลี่ยงการตั้งรหัสผ่านด้วยอักขระที่เรียงกันหรือกลุ่มตัวอักขระที่เหมือนกัน

การใช้งานเครื่องคอมพิวเตอร์

- ต้องมีการใส่รหัสผ่านให้ถูกต้องก่อนใช้งานเครื่องคอมพิวเตอร์
- ให้มีการตั้งล็อกหน้าจอเครื่องคอมพิวเตอร์ หลังจากไม่ได้ใช้งานเกิน 30 นาที และต้องใส่รหัสผ่านให้ถูกต้อง จึงจะสามารถเปิดหน้าจอได้
- โปรแกรมที่ติดตั้งต้องถูกลิขสิทธิ์ หากมีการตรวจพบถือเป็นความผิดส่วนบุคคล

การใช้งานระบบอินเทอร์เน็ต

- ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส
- ไม่ใช้เครือข่ายอินเทอร์เน็ตเพื่อหาประโยชน์ในเชิงธุรกิจ
- ไม่เผยแพร่ส่งต่อข้อมูลอันเป็นเท็จ ซึ่งเกี่ยวกับความมั่นคง ภาพที่มีลักษณะอันลามก และข้อมูลที่ทำให้ผู้อื่นเสียชื่อเสียง
- เมื่อใช้งานอินเทอร์เน็ตเสร็จ ให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้จากบุคคลอื่น

การใช้งานระบบจดหมายอิเล็กทรอนิกส์ e-Mail MJU

- ระมัดระวังในการใช้งาน และไม่ละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือกระทำผิดกฎหมาย ละเมิดศีลธรรม และการแสวงหาประโยชน์ในเชิงธุรกิจ
- ไม่ใช้ที่อยู่ e-Mail ของผู้อื่น เว้นแต่จะได้รับการยินยอมจากเจ้าของ
- ใช้ e-Mail MJU เพื่อการทำงานของมหาวิทยาลัยแม่โจ้เท่านั้น
- ควรตรวจสอบไวรัสก่อนเปิดอ่านเอกสารแนบทุกครั้ง

การใช้งานเครือข่ายสังคมออนไลน์ Social Network

- ควรแจ้งศูนย์ IT หากพบข้อความบน Social Network ที่อาจทำให้เกิดความเสื่อมเสียชื่อเสียงของมหาวิทยาลัย
- พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ข้อบังคับว่าด้วยจรรยาบรรณของบุคลากรและนักศึกษา มหาวิทยาลัยแม่โจ้ และข้อบังคับว่าด้วยวินัยนักศึกษา มีผลผูกพันต่อการเผยแพร่ข้อมูลและแสดงความคิดเห็นบน Social Network
- พื้นที่สื่อสังคมออนไลน์เป็นพื้นที่สาธารณะ ข้อความที่เผยแพร่สามารถเข้าถึงได้โดยสาธารณะ ไม่ใช่พื้นที่ส่วนบุคคล ผู้เผยแพร่ต้องรับผิดชอบ ทั้งทางด้านสังคมและกฎหมาย
- ควรศึกษาการตั้งค่าความเป็นส่วนตัวเพื่อปรับแต่งให้เหมาะสม