นโยบายความมั่นคงปลอดภัย
ของระบบเทคโนโลยีสารสนเทศ

มหาวิทยาลัยราชภัฏอุดรธานี

อนุมัติให้ใช้ตั้งแต่วันที่ ๕ พ.ค ๒๕๕๕

(ลงชื่อ).....(ผู้อนุมัติ)

(นายณัติเทพ พิทักษานุรัตน์)

อธิการบดีมหาวิทยาลัยราชภัฏอุดรธานี

สารบัญ

นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ
มหาวิทยาลัยราชภัฏอุดรธานี ปีพ.ศ. ๒๕๕๕

บทนำ

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี มีความมั่นคง ปลอดภัย และมิให้ผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจารซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยราชภัฏอุดรธานี และเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ได้จัดทำขึ้นเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากอธิการบดีมหาวิทยาลัยราชภัฏอุดรธานี โดยผ่านความเห็นชอบของคณะกรรมการพัฒนาระบบสารสนเทศ และผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ และได้เผยแพร่ให้บุคลากรทุกคนที่เกี่ยวข้องทราบและปฏิบัติตามอย่างมีประสิทธิภาพ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ทบทวนปรับปรุงให้ทันสมัยอย่างน้อยปีละ ๑ ครั้ง

วัตถุประสงค์

๑. สร้างความมั่นใจว่าการใช้และการรักษาความมั่นคงปลอดภัยสารสนเทศภายในมหาวิทยาลัยราชภัฏอุดรธานี เป็นไปอย่างถูกต้องตามกฎหมายและข้อบังคับที่เกี่ยวข้อง

๒. มีข้อปฏิบัติที่รัดกุมและทำได้ในทางปฏิบัติเพื่อรักษาความมั่นคงปลอดภัยสารสนเทศ

๓. ให้บุคลากรในสังกัดมหาวิทยาลัยราชภัฏอุดรธานี ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงสารสนเทศทราบและเข้าใจถึงข้อปฏิบัติ ข้อห้าม และความรับผิดชอบถึงการใช้งานนั้น ๆ ที่จะส่งผลให้เกิดความมั่นคงปลอดภัยต่อระบบสารสนเทศ และเกิดการใช้งานตรงตามวัตถุประสงค์ของการใช้งานระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี รวมทั้งไม่ละเมิดระเบียบกฎหมาย หรือทำให้เกิดความเสียหายในการปฏิบัติงาน

๔. ปกป้องสารสนเทศให้ปลอดภัยจากความสูญเสียในรูปแบบใด ๆ เช่น การสูญหาย การถูกทำลาย การแก้ไขโดยไม่ได้รับอนุญาต การลักลอบนำข้อมูลไปใช้หรือเปิดเผย ตลอดจนสร้างความมั่นใจว่าสารสนเทศมีความถูกต้อง น่าเชื่อถือ และสามารถให้บริการได้

ขอบเขต

นโยบายนี้มีผลบังคับใช้กับผู้ใช้งาน ระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี ทุกระดับชั้น ทุกตำแหน่ง โดยไม่มีการยกเว้น โดยผู้ใช้งานรวมถึง ข้าราชการ พนักงานราชการ ลูกจ้าง สัญญาจ้าง ที่ต้องใช้งานระบบสารสนเทศ ของมหาวิทยาลัยราชภัฏอุดรธานี ตลอดถึงบุคคลภายนอกหรือผู้ใช้บริการที่ได้รับอนุญาตเข้าถึงทรัพยากรสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี โดยให้ถือว่านโยบายนี้ครอบคลุมไปยังสารสนเทศที่อยู่ภายใต้การปกป้องคุ้มครอง อาจเป็นสารสนเทศที่จัดเก็บอยู่ในคอมพิวเตอร์ส่วนบุคคลหรือเซิร์ฟเวอร์หรืออุปกรณ์สื่อสารโทรคมนาคม ตลอดจนสารสนเทศที่ส่งผ่านระบบเครือข่าย รวมทั้งสารสนเทศที่บันทึกไว้ในสื่อบันทึกข้อมูลใด ๆ

นิยามศัพท์

๑ “หน่วยงาน” หมายถึง คณะ สถาบัน สำนัก หรือส่วนงานอื่นที่มีฐานะเทียบเท่าคณะ

๒ “ศูนย์คอมพิวเตอร์” หมายถึง ศูนย์คอมพิวเตอร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏอุดรธานี

๓ “ผู้อำนวยการ” หมายถึง ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๔ “สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี ภายใต้การกำกับดูแลของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๕ “ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยราชภัฏอุดรธานี ภายใต้การกำกับดูแลของสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๖ “คณะกรรมการ” หมายถึง คณะกรรมการดูแลพัฒนาระบบสารสนเทศ มหาวิทยาลัยราชภัฏอุดรธานี

๗ “ผู้ใช้งาน” หมายถึง ข้าราชการ พนักงาน ลูกจ้างของมหาวิทยาลัยราชภัฏอุดรธานี และนักศึกษา รวมถึงบุคคลอื่นที่มหาวิทยาลัย มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

๘ “สิทธิของผู้ใช้งาน” หมายถึง สิทธิของผู้ใช้งานในการเข้าถึงระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

๙ “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๑๐ “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำเนินการในด้านต่าง ๆที่เกี่ยวข้อง เพื่อให้มั่นใจว่าระบบเครือข่าย และระบบสารสนเทศมีความปลอดภัย สามารถให้บริการได้ตลอดเวลา

๑๑ “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง สาเหตุที่อาจจะเป็นไปได้ที่จะเกิดขึ้นและมีผลกระทบต่อการให้บริการกับระบบเครือข่ายและระบบสารสนเทศ

๑๒ “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เหตุการณ์ที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่จะเกิดขึ้น และมีผลกระทบต่อการให้บริการกับระบบเครือข่ายและระบบสารสนเทศ

๑๓ “ผู้ดูแลระบบ” หมายถึง ข้าราชการหรือพนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

ผู้รับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๑. ระดับมหาวิทยาลัย

ผู้บริหารระดับสูงเป็นผู้รับผิดชอบการบริหารจัดการกำกับดูแล ภาพรวมความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย แต่ทั้งนี้ให้ คณะ/สถาบัน/สำนัก ที่เป็นเจ้าของข้อมูลทั้งที่อยู่ในระบบส่วนกลาง และในระบบที่ได้จัดสร้างขึ้นเอง ต้องรับผิดชอบกำกับดูแลความมั่นคงปลอดภัยให้เป็นไปตามนโยบายและแนวปฏิบัติที่ดีของมหาวิทยาลัย

๒. ระดับคณะ/สถาบัน/สานัก

คณะ/สถาบัน/สานัก ต้องแต่งตั้งผู้บริหารของหน่วยงานทำหน้าที่ในฐานะเจ้าของข้อมูลและเป็นผู้รับผิดชอบด้านประสานความร่วมมือและกำกับดูแลให้มีการปฏิบัติตามนโยบายและแนวปฏิบัติที่ดีของมหาวิทยาลัย

ภาระความรับผิดชอบด้านความมั่นคงปลอดภัยของสารสนเทศ

๑. **สำหรับอธิการบดี**

เป็นผู้ลงนามอนุมัติ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ

๒. **สำหรับผู้บริหาร**

ผู้บริหารทุกหน่วยงานต้องช่วยกันกำกับดูแล บุคลากรและนักศึกษาให้ตระหนัก และปฏิบัติตามนโยบายและแนวปฏิบัติที่ดีในเรื่องความมั่นคงปลอดภัยของสารสนเทศ

๓. **สำหรับคณะกรรมการ** มีหน้าที่ดังนี้

๓.๑ ทบทวนนโยบาย และปรับปรุงให้ทันสมัยสอดคล้องกับผลการประเมินความเสี่ยงในระบบสารสนเทศ

๓.๒ ผลักดันให้ผู้ใช้งานทุกคนตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูล ในระบบสารสนเทศ และปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๓.๓ สนับสนุนด้านสินทรัพย์ต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบเครือข่ายมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายฉบับนี้

๓.๔ คณะกรรมการ ต้องทบทวนประสิทธิภาพของการให้บริการระบบสารสนเทศและนโยบายด้านความมั่นคงปลอดภัย เพื่อวางแผนในการปรับปรุงแก้ไขและพัฒนาระบบให้มีประสิทธิภาพ ทุก ๆ ๑ ปี

๓.๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ ผู้อำนวยการจะเป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น

๔. สำหรับบุคลากรและนักศึกษา

บุคลากรและนักศึกษาทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติที่ดีของมหาวิทยาลัย ในกรณีที่พบปัญหาหรือช่องโหว่ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศมหาวิทยาลัยให้รายงานต่อมหาวิทยาลัย

๕. สำหรับผู้พัฒนาและดูแลระบบ

ผู้พัฒนาระบบสารสนเทศทุกระบบของมหาวิทยาลัยต้องพิจารณาถึงประเด็นที่เกี่ยวข้องกับความมั่นคงปลอดภัยของมหาวิทยาลัย และผ่านการพิจารณาและการให้คำแนะนำจากผู้บริหารระบบความมั่นคงปลอดภัยของสารสนเทศระดับสูง ผู้ดูแลระบบสารสนเทศมหาวิทยาลัยต้องมีภาระงานในส่วนเกี่ยวกับบทบาทความรับผิดชอบในเรื่องความมั่นคงปลอดภัยของสารสนเทศทั้งด้านเทคนิค ด้านการตรวจสอบ ด้านการเฝ้าระวัง และด้านการประเมินความเสี่ยงต่อมหาวิทยาลัย

ข้อกำหนดเกี่ยวกับประเภทข้อมูล

๑ ประเภทข้อมูล แบ่งได้ดังนี้

๑.๑ เอกสารกระดาษ

๑.๒ แฟ้มข้อมูลอิเล็กทรอนิกส์

๑.๓ ฐานข้อมูล

๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๓ เวลาและช่องทางการเข้าถึงข้อมูล

๓.๑ เอกสารกระดาษ จัดเก็บในตู้เอกสารพร้อมการป้องกันการเข้าถึง จัดทำแฟ้มระบุชื่อแฟ้มให้ชัดเจน เพื่อความรวดเร็วในการให้บริการ

๓.๒ แฟ้มข้อมูลอิเล็กทรอนิกส์ จัดเก็บบนเครื่องแม่ข่าย โดยกำหนดสิทธิการเข้าถึงสามารถเข้าถึงได้ตลอดเวลา

๓.๓ ฐานข้อมูล จัดเก็บบนเครื่องแม่ข่าย โดยกำหนดสิทธิการเข้าถึง สามารถเข้าถึงได้ตลอด เวลา

นโยบาย ๑ การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ (Acceptable Use Policy)

การใช้งานทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี ต้องมีการวางระเบียบแนวทางปฏิบัติทั้งทางด้านจริยธรรม จรรยาบรรณ และให้ถูกต้องตามกฎหมายเพื่อป้องกันความเสียหายอันเกิดจากกระทำที่ไม่ถูกต้อง เพื่อรักษาภาพลักษณ์ขององค์กร เพื่อให้บุคลากรและนักศึกษาในองค์กรใช้เป็นแนวทางในการปฏิบัติงานเป็นไปอย่างมีประสิทธิภาพ นโยบายความมั่นคงปลอดภัยระบบสารสนเทศ ของมหาวิทยาลัยราชภัฏอุดรธานี ประกอบด้วย ๗ หมวด โดยมีรายละเอียดดังต่อไปนี้

หมวด ๑ว่าด้วยการพิสูจน์ตัวตน(Accountability, Identification and Authentication)

ข้อ ๑ ผู้ที่มีความประสงค์ใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยให้นำบัตรแสดงตน มาทำการลงทะเบียนเพื่อขอบัญชีผู้ใช้งานและรหัสผ่านที่ห้องให้บริการของศูนย์คอมพิวเตอร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ข้อ ๒ ผู้ใช้งานมีหน้าที่ในการป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

ข้อ ๓ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใดๆ ที่เกิดจากบัญชีของผู้ใช้งาน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม

ข้อ ๔ ผู้ใช้งานต้องตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๔ ตัวอักษร ซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

ข้อ ๕ ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ทุกๆ ๖๐ วันหรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน จากผู้ดูแลระบบ

ข้อ ๖ ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่าน การถูกล็อคก็ดี หรือเกิดจากความผิดพลาดใดๆ ก็ดี ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที โดย

(๑) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

หมวด ๒ ว่าด้วยการบริหารจัดการสินทรัพย์ (Assets Management)

ข้อ ๗ ผู้ใช้งานต้องไม่เข้าไปในห้องคอมพิวเตอร์แม่ข่าย (Server) ของมหาวิทยาลัยที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๘ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องคอมพิวเตอร์แม่ข่าย (Server) เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๙ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๑๐ ผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๑๑ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต

ข้อ ๑๒ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่มหาวิทยาลัย มอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง การรับหรือคืนสินทรัพย์จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ ที่มหาวิทยาลัยมอบหมาย

ข้อ ๑๓ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของมหาวิทยาลัยที่ได้รับมอบหมาย

ข้อ ๑๔ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๑๕ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืม คอมพิวเตอร์ หรือโน๊ตบุ๊ค ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้มีอำนาจ

ข้อ ๑๖ สินทรัพย์และระบบสารสนเทศต่างๆ ที่มหาวิทยาลัยจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานของมหาวิทยาลัยเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่มหาวิทยาลัยไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัย

ข้อ ๑๗ ความเสียหายใดๆ ที่เกิดจากการละเมิดตามข้อ ๑๖ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

หมวด ๓ ว่าด้วยการบริหารจัดการข้อมูลองค์กร (Corporate Management)

ข้อ ๑๘ ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของมหาวิทยาลัยราชภัฏอุดรธานี หรือเป็นข้อมูลของบุคคลภายนอก

ข้อ ๑๙ ข้อมูลทั้งหลายที่อยู่ภายในสินทรัพย์ของมหาวิทยาลัยราชภัฏอุดรธานี ถือเป็นสินทรัพย์ของมหาวิทยาลัยราชภัฏอุดรธานี ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๒๐ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัยราชภัฏอุดรธานีหรือข้อมูลของผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๑ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๒๒ ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร มหาวิทยาลัย จะให้การสนับสนุนและเคารพต่อสิทธิ์ส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่มหาวิทยาลัย ต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับมหาวิทยาลัย ซึ่ง

มหาวิทยาลัยอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

หมวด ๔ ว่าด้วยการบริหารจัดการระบบสารสนเทศ (IT Infrastructure Management)

ข้อ ๒๓ ผู้ใช้งานมีสิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ แต่ต้องไม่ดำเนินการดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้มีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้อื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๔) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย กรณีที่ผู้ใช้สร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

ข้อ ๒๔ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๒๕ ห้ามเปิดหรือใช้งาน (Run) โปรแกรม ออนไลน์ทุกประเภท เพื่อความบันเทิง เช่น การดูหนังฟังเพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติราชการ

ข้อ ๒๖ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๒๗ ห้ามใช้ทรัพยากร ระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๒๘ ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของมหาวิทยาลัยราชภัฏอุดรธานีเพื่อประโยชน์ทางการค้า

ข้อ ๒๙ ห้ามกระทำการใดๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี โดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใดๆก็ตาม

ข้อ ๓๐ ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานีต้องหยุดชะงัก

ข้อ ๓๑ ห้ามใช้ระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๓๒ ห้ามกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลของ ผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๓ ห้ามติดตั้งอุปกรณ์หรือกระทำการใดเพื่อให้สามารถเข้าถึงระบบสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานีโดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

หมวด ๕ ว่าด้วยการปฏิบัติตามกฎหมายและข้อบังคับ (Law and Compliance)

ข้อ ๓๔ บรรดากฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทยรวมทั้งกฎระเบียบ ของมหาวิทยาลัยราชภัฏอุดรธานี ถือเป็นสิ่งสำคัญที่ผู้ใช้งานต้องตระหนักและปฏิบัติตามอย่างเคร่งครัด และไม่กระทำความผิดนั้น ดังนั้น หากผู้ใช้งานกระทำผิดตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

หมวด ๖ ว่าด้วยซอฟต์แวร์และลิขสิทธิ์ (Software Licensing and intellectual property)

ข้อ ๓๕ มหาวิทยาลัยเทคโนโลยีราชภัฏอุดรธานี ได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญาดังนั้นซอฟต์แวร์ที่มหาวิทยาลัยราชภัฏอุดรธานีอนุญาตให้ใช้งานหรือที่มหาวิทยาลัยราชภัฏอุดรธานี มีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และมหาวิทยาลัยราชภัฏอุดรธานีห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ มหาวิทยาลัยราชภัฏอุดรธานี ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๓๖ ซอฟต์แวร์ (Software) ที่มหาวิทยาลัยราชภัฏอุดรธานี ได้จัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นต่อการทางาน ห้ามมิให้ผู้ใช้งานทำการติดตั้ง ถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสาเนาเพื่อนำไปใช้งานที่อื่น

หมวด ๗ ว่าด้วยการป้องกันโปรแกรมไม่ประสงค์ดี (Preventing MalWare)

ข้อ ๓๗ คอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่มหาวิทยาลัยราชภัฏอุดรธานี ได้ประกาศให้ใช้ เว้นแต่คอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาพัฒนา ระบบป้องกัน โดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ ๓๘ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๓๙ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๔๐ ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๔๑ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และ ต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๔๒ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆที่เป็นสินทรัพย์ของมหาวิทยาลัยราชภัฏอุดรธานี หรือของผู้อื่น โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๔๓ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ มัลแวร์ หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของมหาวิทยาลัยราชภัฏอุดรธานี

นโยบาย ๒ การควบคุมการเข้าถึงระบบ (Access control Policy)

สำหรับการควบคุมการเข้าถึงระบบสารสนเทศ หมายถึง การเข้าถึงระบบของผู้ใช้ และรวมถึงการกำหนดหน้าที่ของผู้ใช้ การเข้าถึงเครือข่าย การใช้งานระบบที่ให้บริการ และระบบสารสนเทศ การเฝ้าดูการใช้งานระบบ คอมพิวเตอร์ประเภทพกพา และการปฏิบัติงานนอกสถานที่ เป็นต้น ซึ่งการออกนโยบายนี้ควรครอบคลุมหัวข้อหลักดังต่อไปนี้ โดยมีจุดประสงค์เพื่อควบคุมการเข้าถึงระบบสารสนเทศให้มีความมั่นคงปลอดภัย ดังนี้

หมวด ๑ ข้อกำหนดสำหรับการควบคุมการเข้าถึงสารสนเทศ

ข้อ ๑ มหาวิทยาลัยราชภัฏอุดรธานี กำหนดมาตรการควบคุมการเข้าใช้งาน ระบบสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน จะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ข้อ ๒ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ ๓ ผู้ดูแลระบบ (System Administrator) ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๔ ผู้ดูแลระบบ (System Administrator) ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

หมวด ๒ การบริหารจัดการการเข้าถึงระบบสารสนเทศ

ข้อ ๕ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการลงทะเบียนบุคลากรและนักศึกษาใหม่ของมหาวิทยาลัยราชภัฏอุดรธานี ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิ์ต่างๆในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

ข้อ ๖ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

ข้อ ๗ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน(Password)

(๓) ควรกำหนดให้ผู้ใช้บริการตอบยืนยันการได้รับรหัสผ่าน (Password)

(๔) ควรกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๕) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๖) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๘ ผู้ดูแลระบบ (System Administrator) ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(๔) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๕) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

หมวด ๓ การควบคุมการเข้าถึงระบบเครือข่าย

ข้อ ๙ ผู้ใช้งาน ต้องทำการยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการผ่านอุปกรณ์ Internet Access Management

ข้อ ๑๐ ผู้ดูแลระบบ ต้องตรวจสอบการโจมตี บุกรุก การใช้งานในลักษณะที่ผิดปกติ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอ บันทึกผลการตรวจสอบและเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย

ข้อ ๑๑ มีการติดตั้งอุปกรณ์หรือโปรแกรมป้องกันการบุกรุกในระบบเครือข่าย

ข้อ ๑๒ มีการปิดพอร์ตที่ไม่มีการใช้งานเครือข่ายทุกพอร์ต หากหน่วยงานที่ต้องการเชื่อมต่อระบบเครือข่ายเพิ่มเติมจะต้องได้รับอนุญาตจากผู้อำนวยการเป็นลายลักษณ์อักษร เพื่อให้สิทธิการใช้งาน

ข้อ ๑๓ มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control)โดยการกำหนดจากส่วนกลาง

ข้อ ๑๔ การบริหารจัดการรหัสผ่าน ดำเนินการผ่าน Web Portal

หมวด ๔ การควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๑๕ การจำกัดระยะเวลาการใช้งาน ผู้ดูแลระบบสารสนเทศ ต้องจำกัดระยะเวลาการใช้งานสำหรับระบบสารสนเทศ ที่มีความสำคัญสูงหรือมีความเสี่ยงสูง

ข้อ ๑๖ การพิสูจน์ตัวตนสำหรับผู้ใช้ ผู้ดูแลระบบสารสนเทศ ต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

ข้อ ๑๗ การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบสารสนเทศ ต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่าน และมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

ข้อ ๑๘ กระบวนการในการเข้าสู่ระบบให้บริการอย่างมั่นคงปลอดภัย ผู้ดูแลระบบสารสนเทศ ต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการ เพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการจะปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน ๓ ครั้ง เป็นต้น

ข้อ ๑๙ การพิสูจน์ตัวตนสำหรับเครื่องลูกข่าย ผู้ดูแลระบบสารสนเทศต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ก่อนที่จะอนุญาตให้เข้ามาใช้งานเครือข่ายของมหาวิทยาลัย

ข้อ ๒๐ การตัดเวลาการใช้งานเครื่องลูกข่าย ผู้ดูแลระบบสารสนเทศต้องมีวิธีการตัดเวลาการใช้งานเครื่องลูกข่าย เมื่อเครื่องลูกข่ายนั้นไม่ได้มีการใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอและต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

ข้อ ๒๑ การควบคุมการใช้งานโปรแกรมยูทิลิตี้ ผู้ดูแลระบบสารสนเทศต้องกำหนดให้มีการควบคุมการใช้โปรแกรมยูทิลิตี้สำหรับระบบเพื่อป้องกันการเข้าถึง โดยผู้ที่ไม่ได้รับอนุญาต ได้แก่

(๑) ก่อนใช้ต้องทำการพิสูจน์ตัวตนก่อน

(๒) ให้ทำการแยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

(๓) จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

(๔) ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน

ข้อ ๒๒ การติดตั้งระบบเตือนภัยสำหรับระบบที่มีความสำคัญสูง

หมวด ๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ข้อ ๒๓ ระบบที่มีผลกระทบและความสำคัญสูงต่อมหาวิทยาลัย เช่น ระบบงบประมาณ พัสดุ การเงิน และบัญชีกองทุนโดยเกณฑ์พึงรับ-พึงจ่าย ระบบทะเบียนและสถิติ นักศึกษา ต้องมีการควบคุมแยกเครื่องใช้งาน (Server) จากระบบอื่น ๆ

ข้อ ๒๔ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๒๕ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ ศูนย์คอมพิวเตอร์ สำนักวิทยบริการและเทคโนโลยีสารสนเทศได้กำหนดช่องทางการเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่สำคัญ โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน

ข้อ ๒๖ ผู้ดูแลระบบ ต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

หมวด ๖ การควบคุมอุปกรณ์สื่อสารพกพาและการปฏิบัติงานจากภายนอกมหาวิทยาลัย

กำหนดขึ้นด้วยวัตถุประสงค์เพื่อควบคุมการใช้งานอุปกรณ์คอมพิวเตอร์ประเภทเคลื่อนที่ได้ รวมทั้งการปฏิบัติงานนอกสำนักงานให้เป็นไปอย่างปลอดภัย

ข้อ ๒๗ การป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา ผู้ใช้ บุคลากรผู้ใช้ ต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา (Notebook, palmtops, laptop) เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่

(๑) ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

(๒) ต้องเข้ารหัสข้อมูลที่สำคัญไว้เป็นต้น

ข้อ ๒๘ การปฏิบัติงานนอกสำนักงาน ผู้ใช้ บุคลากรผู้ใช้ ต้องปฏิบัติในการใช้งานนอกสำนักงาน เช่น ใช้วิธีการป้องกันสำหรับเครื่องคอมพิวเตอร์พกพา การติดต่อผ่านทางเครือข่าย จากนอกสำนักงานต้องได้รับการป้องกันการถูกลักลอบดูข้อมูล เป็นต้น

หมวด ๗ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

ข้อ ๒๘ ผู้ดูแลระบบ จะทำการทบทวนสิทธิการใช้งาน เมื่อบุคลากรมีการเปลี่ยนแปลงตำแหน่ง เลื่อนขั้น ย้ายส่วนงาน

ข้อ ๒๙ เมื่อบุคลากร ลาออก หรือนักศึกษา พ้นสภาพนักศึกษา ระบบจะทำการยกเลิกบัญชีผู้ใช้งานโดยอัตโนมัติ

นโยบาย ๓ การใช้งานอินเทอร์เน็ต (Internet Security Policy)

ข้อ ๑ ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยราชภัฏอุดรธานีไว้เท่านั้น เช่น Proxy,Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำงานขออนุญาตจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ ๒ เครื่องคอมพิวเตอร์ส่วนบุคคล และเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บบราวเซอร์ (Web browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและเว็บบราวเซอร์

ข้อ ๓ ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ต จะต้องมีการทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

ข้อ ๔ ผู้ใช้งาน ห้ามใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยราชภัฏอุดรธานี เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่มีผล กระทบต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

ข้อ ๕ ผู้ใช้งาน จะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๖ ผู้ใช้งาน ห้ามเผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรม หรือข้อมูลที่ละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

ข้อ ๗ ห้ามผู้ใช้งาน เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยราชภัฏอุดรธานี ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านทางอินเทอร์เน็ต

ข้อ ๘ ห้ามผู้ใช้งาน นำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

ข้อ ๙ ห้ามผู้ใช้งาน นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

ข้อ ๑๐ ผู้ใช้งาน มีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

ข้อ ๑๑ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ จากผู้ขาย ต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

ข้อ ๑๒ ในการเสนอความคิดเห็น ผู้ใช้งานต้องไม่ใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยราชภัฏอุดรธานี รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่น ๆ

ข้อ ๑๓ หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ทำการปิดเว็บบราวเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

นโยบาย ๔ การเข้าถึงระบบเครือข่ายไร้สาย (Wireless Policy)

ผู้ดูแลระบบและผู้ใช้งานระบบเครือข่ายแบบไร้สาย (Wireless Policy) ของมหาวิทยาลัยราชภัฏอุดรธานีมีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

ข้อ ๑ การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องมีการกำหนดรหัสผ่านในการเข้าใช้งาน

ข้อ ๒ ห้ามผู้ใช้งาน (User) นำอุปกรณ์ Wireless มาติดตั้งหรือเปิดใช้งานเองในหน่วยงานไม่ว่าจะเป็น Access point ,Wireless Routers, Wireless USB client หรือ Wireless card

ข้อ ๓ ห้ามผู้ใช้งาน (User) เปิดระบบเครือข่ายไร้สายแบบจุดต่อจุด (ad-hoc) หรือpeer-to-peer Network

ข้อ ๔ ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยราชภัฏอุดรธานี จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตอย่างเป็นลายลักษณ์อักษร

ข้อ ๕ ผู้ดูแลระบบ ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

ข้อ ๖ ผู้ดูแลระบบ ต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

ข้อ ๗ ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์กระจายออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

ข้อ ๘ ผู้ดูแลระบบ ต้องเลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งานและควรสำรวจว่าสัญญาณกระจายออกไปภายนอกหรือไม่ นอกจากนี้ การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

ข้อ ๙ ผู้ดูแลระบบ ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

ข้อ ๑๐ ผู้ดูแลระบบ ต้องกำหนด ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

ข้อ ๑๑ ผู้ดูแลระบบ ต้องกำหนดค่าให้ WEP หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Access Point และ Wireless LAN Client เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

ข้อ ๑๒ ผู้ดูแลระบบ ต้องเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้งาน(Username) รหัสผ่าน (Passworsd) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address ชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้

ข้อ ๑๓ ผู้ดูแลระบบ ต้องมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๑๔ ผู้ดูแลระบบ ต้องตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

นโยบาย ๕ การใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail Policy)

ข้อ ๑ ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยราชภัฏอุดรธานี ให้เหมาะสมกับการใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออกเป็นต้น

ข้อ ๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้ใหม่ และรหัสผ่านสำหรับการใช้งานครั้งแรก เพื่อใช้ในการทดสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๓ การกำหนดรหัสผ่านที่ดี (good password) มีแนวทางปฏิบัติตามที่ระบุไว้ในนโยบายการใช้ทรัพยากรเครือข่ายคอมพิวเตอร์และระบบสารสนเทศ (Acceptable Use Policy)

ข้อ ๔ รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาป้อนรหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญญาลักษณ์แทนตัวอักษรนั้น เช่น ‘X’หรือ ‘O’ ในการพิมพ์แต่ละอักษร

ข้อ ๕ ผู้ดูแลระบบ ต้องมีกำหนดให้ระบบจดหมายอิเล็กทรอนิกส์มีการล๊อกเอ้าท์ออก จากหน้าจอตัดการใช้งานผู้ใช้ เมื่อผู้ใช้ไม่ได้ใช้งานระบบเป็นระยะเวลาตามที่กำหนดไว้ เช่น ๑๕ นาที เมื่อต้องการเข้าใช้งานต่อต้องใส่ชื่อผู้ใช้ และรหัสผ่านอีกครั้ง

ข้อ ๖ ผู้ใช้งาน ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๗ ผู้ใช้งาน ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยราชภัฏอุดรธานีหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๘ ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับยินยอมจากเจ้าของผู้ใช้ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

ข้อ ๙ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการล็อกเอ้าท์ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ ๑๐ ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิดเพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็นExecutable file เช่น .exe .com เป็นต้น

ข้อ ๑๑ ผู้ใช้งาน ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ ๑๒ ผู้ใช้งาน ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม อันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัยราชภัฏอุดรธานี หรือทำให้เกิดความแตกแยกผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ ๑๓ ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

ข้อ ๑๔ ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

ข้อ ๑๕ ผู้ใช้งาน ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ ระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๑๖ ผู้ใช้งาน ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

นโยบาย ๖ การใช้งานไฟร์วอลล์ (Firewall Policy)

ไฟร์วอลล์เป็นอุปกรณ์ที่มีความสำคัญในการบริหารความปลอดภัยของมหาวิทยาลัย เนื่องจากไฟร์วอลล์จะทำหน้าที่ควบคุมข้อมูลที่ผ่านเข้าออก เพื่อสร้างความปลอดภัยให้กับเครือข่ายขององค์กร ทั้งในด้านของการจำกัดการเชื่อมต่อ และการจำกัดการใช้งาน ไฟร์วอลล์จะทำหน้าที่กำหนดขอบเขตที่ควบคุมการเข้าถึงระบบเครือข่ายคอมพิวเตอร์ ข้อมูลที่ผ่านเข้าออกไฟร์วอลล์ จะเป็นข้อมูลที่ตรงตามที่นโยบายขององค์กรกำหนดเท่านั้น นโยบายการใช้งานไฟร์วอลล์ มีไว้เพื่อใช้เป็นแนวทางปฏิบัติในการบริหาร และดูแลรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๑ ไฟร์วอลล์ต้องกำหนดเงื่อนไขของการเชื่อมต่อหรือการให้บริการที่ได้รับอนุญาตเท่านั้น โดยกำหนดเงื่อนไขของกฎเป็น Deny All Allow Some คือ ห้ามทุกการเชื่อมต่อผ่านไฟร์วอลล์

ข้อ ๒ กฎการเชื่อมต่อหรือการให้บริการที่กำหนดว่าได้รับอนุญาตให้ผ่านไฟร์วอลล์ได้จะต้องบันทึกเป็นเอกสาร และสำเนาให้กับผู้ดูแลระบบเครือข่ายทุกคนรับทราบ โดยเงื่อนไขของการอนุญาตจะต้องได้รับความเห็นชอบจากผู้ดูและระบบ และรายงานให้ผู้อำนวยการทราบ

ข้อ ๓ ในทุกเส้นทางการสื่อสารคอมพิวเตอร์ที่เข้าและออกจากมหาวิทยาลัยราชภัฏอุดรธานีจะต้องได้รับการติดตั้งไฟร์วอลล์ในทุกเส้นทาง

ข้อ ๔ เครื่องคอมพิวเตอร์แม่ข่ายที่มีการเชื่อมต่อไปยังภายนอกองค์กร จะต้องจัดให้อยู่ใน DMZ (De-Militarize Zone) เสมอ

ข้อ ๕ ต้องไม่มีกฎที่อนุญาตให้การสื่อสารจากภายนอกองค์กรใด ผ่านเข้าไปในองค์กรได้โดยจะยอมให้เข้ามาในส่วน DMZ ได้เท่านั้น

ข้อ ๖ หากมีการเพิ่มเติมหรือเปลี่ยนแปลงเส้นทางการสื่อสารคอมพิวเตอร์ จะต้องได้รับการอนุญาตจากผู้ดูแลระบบเครือข่ายก่อน และต้องมีการตรวจสอบผลกระทบ และกฎที่ตั้งให้กับไฟร์วอลล์

ข้อ ๗ อุปกรณ์ไฟร์วอลล์ที่นำมาใช้งาน จะต้องเป็นอุปกรณ์ที่ทำหน้าที่เป็นไฟร์วอลล์เพียงอย่างเดียวโดยไม่ทำหน้าที่อื่น ๆ เช่น Anti Virus Gateway

ข้อ ๘ ผู้ดูแลระบบจะต้องตรวจสอบการทำงานของไฟร์วอลล์ จากบันทึกการทำงาน (logfile) อย่างสม่ำเสมอ อย่างน้อยทุกวันสุดสัปดาห์ และรายงานให้ผู้อำนวยการทราบเป็นรายเดือน

ข้อ ๙ การเปลี่ยนแปลงใด ๆ ที่เกี่ยวกับไฟร์วอลล์จะต้องได้รับการบันทึก และรายงานให้ผู้อำนวยการทราบ

ข้อ ๑๐ อุปกรณ์ไฟร์วอลล์จะต้องได้รับการป้องกันจากการเข้าถึงทางกายภาพ โดยจะต้องติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อก โดยอนุญาตให้ผู้ดูแลระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

ข้อ ๑๑ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บที่อุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๑๒ จะต้องมีการสำรองข้อมูลการกำหนดค่าต่าง ๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งที่มีการเปลี่ยนแปลงค่า

ข้อ ๑๓ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่าง ๆ จะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็น โดยจะต้องกำหนดเป็นกรณีไป

ข้อ ๑๔ มหาวิทยาลัยราชภัฏอุดรธานี มีสิทธิที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มี ความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไข

ข้อ ๑๕ การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องแม่ข่ายหรืออุปกรณ์เครือข่ายภายใน จะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบมหาวิทยาลัยราชภัฏอุดรธานี ก่อน

ข้อ ๑๖ ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตทันที

นโยบาย ๗ การใช้งานระบบตรวจจับและป้องกันผู้บุกรุก
(Intrusion Detection System and Intrusion Prevention System Policy)

ข้อ ๑ มหาวิทยาลัยราชภัฏอุดรธานี ต้องติดตั้งระบบตรวจจับและป้องกันการบุกรุกเอาไว้ในตำแหน่งที่ มีการเชื่อมต่อกับภายนอกทุกจุด หรือ อย่างน้อยจะต้องติดตั้งเอาไว้ในจุดที่ให้มีการให้บริการไปสู่ภายนอก องค์กร เช่น เครื่องคอมพิวเตอร์แม่ข่าย

ข้อ ๒ ในการติดตั้งระบบตรวจจับและป้องกันการบุกรุก ให้ติดตั้งไว้ที่ตำแหน่งหลัง ไฟร์วอลล์ และที่ด้านหน้าของกลุ่มของเครื่องคอมพิวเตอร์แม่ข่าย (Server Farm)

ข้อ ๓ ต้องมีการปรับแต่ง (Tuning) การทำงานของระบบตรวจจับและป้องกันการบุกรุก โดยบุคลากรของมหาวิทยาลัยราชภัฏอุดรธานี ที่ได้รับการอบรม หรือ โดยผู้เชี่ยวชาญ โดยให้ปรับแต่งให้ป้องกันได้มาก ที่สุดและเกิดการตรวจจับที่ผิดพลาด (False Positive) น้อยที่สุด ทุกครั้งที่มีการปรับแต่งจะต้องบันทึก ข้อมูลทุกครั้ง

ข้อ ๔ ต้องมีการตั้งระบบตรวจจับและป้องกันการบุกรุกให้สามารถอัปเดต Signature ได้โดยอัตโนมัติหรือผู้ดูแลระบบเครือข่ายจะต้องอัปเดต Signature ทุกสัปดาห์

ข้อ ๕ หากมีการเพิ่มเติมหรือเปลี่ยนแปลงเส้นทางการสื่อสารคอมพิวเตอร์ จะต้องได้รับการอนุญาตจากผู้ดูแลระบบเครือข่ายก่อน และต้องมีการตรวจสอบผลกระทบกับระบบตรวจจับและป้องกันการบุกรุก

ข้อ ๖ จะต้องตรวจสอบการทำงานของระบบตรวจจับและป้องกันการบุกรุก และ ตรวจสอบ Log ทดสอบการทำงานทุกเดือน

ข้อ ๗ การเปลี่ยนแปลงใด ๆ ที่เกี่ยวกับระบบตรวจจับและป้องกันการบุกรุก จะต้องได้รับการบันทึก และรายงานให้ผู้อำนวยการทราบ

ข้อ ๘ อุปกรณ์ระบบตรวจจับและป้องกันการบุกรุก จะต้องได้รับการป้องกันจากการ เข้าถึงทางกายภาพ โดยจะต้องติดตั้งในห้องที่มีการรักษาความปลอดภัย มีการล็อก โดยอนุญาตให้ผู้ดูแล ระบบเครือข่ายเท่านั้นที่สามารถเข้าถึงได้

นโยบาย ๘ การสำรองข้อมูลและการกู้คืนระบบ (Backup Policy)

หมวด ๑ การจัดให้มีระบบสำรองข้อมูล

นโยบายนี้จัดทำขึ้นด้วยวัตถุประสงค์เพื่อจัดทำระบบสำรองข้อมูล เพื่อให้มีข้อมูลสารสนเทศและระบบคอมพิวเตอร์ ระบบเครือข่าย สำหรับการใช้งานได้อย่างต่อเนื่องอย่างมีประสิทธิภาพและใช้งานได้ในเวลาที่ต้องการ (availability risk)

ข้อ ๑ ผู้ดูแลระบบคอมพิวเตอร์ ต้องจัดให้มีการสำรองและทดสอบข้อมูลที่สำรองเก็บไว้อย่างสม่ำเสมอ และให้เป็นไปตามนโยบายการสำรองข้อมูลของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๒ ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีกระบวนการในการสร้างความต่อเนื่องให้กับการดำเนินงาน การบริหารจัดการและการปรับปรุงกระบวนการที่ต้องใช้ข้อมูลสารสนเทศดังกล่าวอย่างสม่ำเสมอ กระบวนการนี้จะต้องระบุข้อกำหนดที่เกี่ยวข้องกับความมั่นคงปลอดภัยที่จำเป็นสำหรับการสร้างความต่อเนื่องให้กับการดำเนินงานตามวัตถุประสงค์ของมหาวิทยาลัยราชภัฏอุดรธานี

ข้อ ๓ การสำรองข้อมูลภายในองค์กร หมายถึง การทำสำรองข้อมูลทั้งหมด(Full backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องสำรองข้อมูลที่สำคัญไว้ตามระยะเวลาที่เหมาะสมและกำหนดไว้ชัดเจน เช่น สำรองข้อมูลอย่างน้อย ๑ ครั้งในรอบทุก ๆ สัปดาห์ เป็นต้น

ข้อ ๔ การจัดทำบันทึกการสำรองข้อมูล (Operator logs) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำบันทึกรายละเอียดการสำรองข้อมูล ได้แก่ เวลาเริ่มต้นและสิ้นสุด ชื่อผู้สำรอง ชนิดของข้อมูลที่บันทึก เป็นต้น และรายงานให้ผู้อำนวยการทราบ

ข้อ ๕ การรายงานข้อผิดพลาด (Fault logging) ผู้ดูแลระบบคอมพิวเตอร์ต้องทำรายงานข้อผิดพลาดจากการสำรองข้อมูลที่เกิดขึ้น รวมทั้งวิธีการที่ใช้แก้ไขด้วย

ข้อ ๖ ให้ผู้ดูแลระบบคอมพิวเตอร์มอบหมายหน้าที่การสำรองข้อมูลแก่เจ้าหน้าที่คนอื่นไว้สำรอง ในกรณีที่ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่ายไม่สามารถปฏิบัติงานได้

ข้อ ๗ ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้ ให้ดำเนินการแก้ไขปัญหาและรายงานต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศทราบ

ข้อ ๘ ให้ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายกำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

ข้อ ๙ การสำรองข้อมูลภายนอกสำนักงาน (Off-site backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการสำรองข้อมูลภายนอกสำนักงานตามความเหมาะสมของหน่วยงาน เพื่อให้สามารถกู้ระบบกลับคืนได้อย่างรวดเร็ว และเพื่อป้องกันระบบจากการถูกดโจมตี หรือความหายนะที่อาจเกิดขึ้น

ข้อ ๑๐ การเข้ารหัสข้อมูลสำคัญในการสำรองข้อมูล (Encrypted backup) ผู้ดูแลระบบคอมพิวเตอร์ต้องจัดให้มีการเข้ารหัสข้อมูลสำรองที่สำคัญ โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสมเพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

ข้อ ๑๑ นโยบายที่ต้องปฏิบัติเกี่ยวข้องกับการสำรองข้อมูล (Backup Policy) ผู้ดูแลระบบคอมพิวเตอร์ต้องปฏิบัติตามขั้นตอนปฏิบัติ Backup Procedure โดยเคร่งครัด

ข้อ ๑๒ ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายต้องทำการสำรอง ข้อมูลแต่ละรายการเช่น Mail servers, Web servers, Database servers, Firewall servers และ Server อื่นๆ โดยมีการกำหนดความถี่ในการสำรองข้อมูลและใช้วิธีแบคอัพแบบ Full Backup

ข้อ ๑๓ ผู้ดูแลระบบคอมพิวเตอร์ต้องตรวจสอบผลการสำรองข้อมูลด้วยตนเองว่าการแบคอัพตามรายละเอียดในตารางข้างต้นนั้นถูกต้องสมบูรณ์หรือไม่

ข้อ ๑๔ กรณีที่สมบูรณ์ ผู้ดูแลระบบคอมพิวเตอร์ นำสื่อบันทึกข้อมูลแบคอัพไปเก็บไว้นอกสำนักงานในสถานที่ปลอดภัย

ข้อ ๑๕ กรณีที่ไม่สมบูรณ์ ผู้ดูแลระบบคอมพิวเตอร์ต้องแก้ไขให้แบคอัพสมบูรณ์และกลับไปทำการตรวจสอบทั้งหมดใหม่อีกครั้ง

หมวด ๒ การกู้คืนระบบ

ข้อ ๑๖ ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือผู้ดูแลระบบเครือข่าย ดำเนินการแก้ไข รายงานผลการแก้ไขพร้อมทั้งบันทึกและให้รายงานสรุปผลการปฏิบัติงานต่อผู้อำนวยการทราบโดยเร็ว

ข้อ ๑๗ ให้ใช้ข้อมูลที่ทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

ข้อ ๑๘ หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงานความคืบหน้าการกู้คืนระบบเป็นระยะ จนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

หมวด ๓ การจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน

นโยบายเกี่ยวกับการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน (Business Continuity Management Policy) ผู้บริหารต้องมอบหมายให้บุคลากรที่เกี่ยวข้องดำเนินการดังต่อไปนี้

ข้อ ๑๙ กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

ข้อ ๒๐ กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูงและจำเป็นต้องวางแผนรับมือ

ข้อ ๒๑ ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูง ติดขัดหรือไม่สามารถใช้งานได้ อันเป็นผลจากภัยพิบัติที่กำหนดไว้

ข้อ ๒๒ จัดทำแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

ข้อ ๒๓ ทดสอบ/ประเมินและปรับปรุงแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ ๑ ครั้ง

นโยบาย ๙ ความมั่นคงทางกายภาพห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

หมวด ๑ การจัดแบ่งพื้นที่

ข้อ ๑ ห้องควบคุมระบบแบ่งเป็นสองพื้นที่ ได้แก่ พื้นที่ควบคุม (Control Area)และพื้นที่จำกัดการเข้าถึง (Restricted Area)

ข้อ ๒ พื้นที่ควบคุมเป็นพื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบส่วนพื้นที่จำกัดการเข้าถึงเป็นห้องที่มีระบบคอมพิวเตอร์และเครือข่ายติดตั้งอยู่

หมวด ๒ ข้อกำหนดการป้องกันห้องควบคุมระบบและระบบเครือข่าย

ข้อ ๓ ข้อกำหนดทางด้านกายภาพของห้องควบคุมระบบ

(๑) แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไปโดยกำหนดลำดับความสำคัญของอุปกรณ์แต่ละชนิดไว้เช่น Server, Router, Network Switch ต่าง ๆ

(๒) การติดตั้งอุปกรณ์ควรติดตั้งภายในตู้ Rack ที่เหมาะสมเพื่อสะดวกในการบำรุงรักษา

(๓) ตำแหน่งของการวางอุปกรณ์ต่าง ๆ ไม่ควรวางใกล้ประตู หน้าต่างเพื่อป้องกันอุบัติเหตุที่อาจเกิดขึ้น ไม่ควรวางอุปกรณ์ให้เครื่องปรับอากาศเป่าถูกโดยตรงเพื่อหลีกเลี่ยงความชื้น

(๔) การจัดวางสายเครือข่ายและสายไฟฟ้าควรมีการเก็บสายให้เรียบร้อยเพื่อป้องกันการเดินสะดุด

(๕) ติดประกาศบันทึกการบำรุงรักษา ชื่อและหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

(๖) ติดตั้งระบบรักษาความปลอดภัยในห้องเช่น กล้องวงจรปิด (CCTV)ระบบการเข้าออกห้องโดยระบบตรวจสอบลายนิ้วมือ (Fingerprint Scan) หรือบัตรผ่านเข้าออก (RFID)เป็นต้น

(๗) มีระบบป้องกันอัคคีภัย

(๘) มีระบบไฟฟ้าสำรองเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบไฟฟ้าสำรอง เป็นต้น

(๙) มีระบบป้องกันไฟฟ้าจากฟ้าผ่า

(๑๐) ระบบปรับอากาศแบบควบคุมอุณหภูมิ (๕๐-๘๐°F) และความชื้น(๒๐ – ๘๐%)

(๑๑) ติดตั้งฉนวนกันไฟไหม้ ที่ฝ้าเพดานและกำแพง

ข้อ ๔ ข้อกำหนดการเข้าไปในพื้นที่ควบคุม

(๑) ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม

(๒) บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศและต้องมีเจ้าหน้าที่นำเยี่ยมชมอยู่ด้วยตลอดเวลา

(๓) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้

เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๔) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

ข้อ ๕ ข้อกำหนดการเข้าไปในพื้นที่จำกัดการเข้าถึง

(๑) ไม่อนุญาตให้บุคคลเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ

(๒) หรือในกรณีที่บุคคลอื่นมีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศและต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

(๓) หรือบุคคลที่ได้รับคำสั่งจากผู้บริหารให้เข้าปฏิบัติหน้าที่ในพื้นที่ควบคุมซึ่งต้องมีเจ้าหน้าที่รับผิดชอบอย่างน้อย ๑ คน เข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้งและให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

(๔) ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า ๑๕ ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

(๕) ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

(๖) ไม่อนุญาตให้มีการเข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

(๗) ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้โดยได้รับความเห็นชอบจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

นโยบาย ๑๐ นโยบายการวางแผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติและการกู้ฟื้น

แผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติและการกู้ฟื้นนี้ได้จัดทำขึ้นเพื่อเป็นแนวทางและขั้นตอนสำหรับผู้ปฏิบัติงานสามารถรับมือภัยพิบัติ ติดตั้งและกู้คืนระบบคอมพิวเตอร์ ส่วนประกอบของแผนฯ มีรายละเอียดดังต่อไปนี้

หมวด ๑ การเตรียมรับมือภัยพิบัติ

ข้อ ๑ ความเสี่ยงและชนิดของภัยพิบัติ

ภัยพิบัติ หมายถึง เหตุการณ์ที่สร้างความเสียหายอย่างสิ้นเชิงกับระบบคอมพิวเตอร์ ระบบเครือข่ายและระบบสื่อสารภายใต้การดูแลของมหาวิทยาลัยราชภัฏอุดรธานี โดยเรียงลำดับตามความเป็นไปได้ที่จะเกิดจากมากไปหาน้อยดังนี้

(๑) การโจมตีของผู้บุกรุกคอมพิวเตอร์ ซึ่งมีผลทำให้ ระบบคอมพิวเตอร์ ระบบเครือข่าย หรือระบบสื่อสารเกิดความเสียหายอย่างสิ้นเชิงทั้งหมด

(๓) การเชื่อมโยงเครือข่ายล้มเหลว ซึ่งมีผลทำให้ระบบเครือข่าย หรือระบบสื่อสารล้มเหลวอย่างสิ้นเชิงทั้งหมด

(๓) อุปกรณ์จัดเก็บข้อมูลเสียหายอย่างสิ้นเชิงทั้งหมดและไม่สามารถกู้คืนได้

(๔) เกิดอัคคีภัย ที่ทำให้สร้างความเสียหายแก่ห้องควบคุมระบบหรือระบบอื่นที่กระทบต่อการให้บริการ

(๔) โจรกรรม ซึ่งเป็นเหตุการณ์ที่ทำให้ระบบไม่สามารถให้บริการได้เป็นจำนวนมาก

(๕) อุทกภัย การเกิดน้ำท่วม หรือเกิดน้ำขัง อันเนื่องมาจากธรรมชาติหรือไม่ใช่เกิดจากธรรมชาติ เช่น ท่อส่งน้ำรั่ว จนเป็นเหตุทำให้ระบบคอมพิวเตอร์ เครือข่าย หรือระบบสื่อสารเสียหายเป็นจำนวนมาก

(๖) ธรณีพิบัติ การเกิดแผ่นดินไหวจนเป็นเหตุทำให้เกิดความเสียหายจำนวนมากต่อระบบคอมพิวเตอร์ เครือข่าย หรือระบบสื่อสาร

(๘) วาตภัย ภัยที่เกิดขึ้นจากลมจนเป็นเหตุให้เกิดความเสียหายจำนวนมากต่อระบบคอมพิวเตอร์ เครือข่าย หรือระบบสื่อสาร

ข้อ ๒ การเตรียมแผน อุปกรณ์และเครื่องมือ มหาวิทยาลัยจัดให้มีการปฏิบัติการรับมือภัยพิบัติจัดเตรียมกล่องฉุกเฉิน (Lock Box) จำนวน ๒ กล่อง ภายในกล่องฉุกเฉินประกอบด้วย

(๑) รหัสผ่านสำหรับเข้าสู่ระบบคอมพิวเตอร์ที่มีสิทธิ์เท่าผู้ดูแลระบบ

(๒) แผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติ

(๓) ข้อมูลเกี่ยวกับการปรับตั้งค่าอุปกรณ์

(๔) ซอฟต์แวร์ที่มีความสำคัญสูง

ผู้ที่สามารถเปิดกล่องฉุกเฉินได้มีจำนวน ๔ คน คือ

(๑) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๒) หัวหน้าศูนย์คอมพิวเตอร์

(๓) ฝ่ายพัฒนาระบบเครือข่าย

(๔) ฝ่ายพัฒนาระบบสารสนเทศ

(๕) ฝ่ายห้องปฏิบัติและซ่อมบำรุง

ข้อ ๓ การสำรองข้อมูล ผู้ดูแลระบบคอมพิวเตอร์และผู้ดูแลระบบเครือข่ายมีหน้าที่ในการสำรองข้อมูลเพื่อให้สามารถนำมาใช้ในการกู้คืนระบบและติดตั้งระบบในกรณีที่เกิดภัยพิบัติ ทั้งนี้ให้ปฏิบัติตามนโยบายการสำรองข้อมูลและการกู้คืนระบบ ข้อมูลที่มีความสำคัญอื่น ๆ เช่น ค่าติดตั้งระบบของอุปกรณ์เครือข่าย ซอฟต์แวร์ที่มีความสำคัญให้เก็บไว้ในกล่องฉุกเฉิน

หมวด ๒ การรับมือเร่งด่วนขณะเกิดภัยพิบัติ

ข้อ ๔ การรายงานเหตุการณ์ ผู้ที่ทราบเหตุการณ์ภัยพิบัติมีหน้าที่รายงานเหตุการณ์เกิดภัยพิบัติให้กับผู้ใดผู้หนึ่งตามข้อมูลดังต่อไปนี้

(๑) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

(๒) หัวหน้าศูนย์คอมพิวเตอร์

(๓) ฝ่ายพัฒนาระบบเครือข่าย

(๔) ฝ่ายพัฒนาระบบสารสนเทศ

(๕) ฝ่ายห้องปฏิบัติและซ่อมบำรุง

ข้อ ๕ ขั้นตอนการปฏิบัติงาน

(๑) ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ สั่งการให้มีการปฏิบัติงานเพื่อรับมือเร่งด่วนขณะเกิดภัยพิบัติ หากผู้อำนวยการไม่สามารถปฏิบัติงานได้ ให้หัวหน้าศูนย์คอมพิวเตอร์ปฏิบัติราชการแทน โดยสั่งการให้ผู้มีสิทธิ์ในการเปิดกล่องฉุกเฉินหากไม่สามารถใช้กุญแจได้ให้ทำลายกุญแจและเปิดโดยวิธีการใดก็ได้ และดำเนินการตามขั้นตอนการปฏิบัติงานที่เก็บในกล่อง

(๒) หัวหน้าศูนย์คอมพิวเตอร์ สำรวจสถานะของบุคลากรหรือผู้ที่อยู่ในเหตุการณ์ขณะเกิดภัยพิบัติ หากมีการบาดเจ็บให้โทรศัพท์แจ้งโรงพยาบาล

(๓) หัวหน้าศูนย์คอมพิวเตอร์ สำรวจจำนวนเจ้าหน้าที่ศูนย์คอมพิวเตอร์หรือผู้ที่อยู่ในเหตุการณ์ขณะเกิดภัยพิบัติ เพื่อประชุมเร่งด่วนเพื่อชี้แจงหน้าที่และการดำเนินการรับมือภัยพิบัติ หากเจ้าหน้าที่ไม่ได้อยู่ในเหตุการณ์ ให้โทรศัพท์เพื่อเรียกตัวปฏิบัติงานโดยเร่งด่วนทั้งในและนอกเวลาราชการ

(๔) หัวหน้าศูนย์คอมพิวเตอร์ เรียกประชุมเจ้าหน้าที่ในฝ่ายเพื่อ วิเคราะห์ความเสียหายและกำหนดแผนปฏิบัติการกู้คืนระบบ โดยต้องประกอบด้วยหลักเกณฑ์ต่าง ๆ ดังนี้

(๑) เก็บรวบรวมแหล่งเก็บข้อมูลสำรองทั้งหมดหรือที่มีความสำคัญ

(๒) ติดตั้งฮาร์ดแวร์/ซอฟต์แวร์สำหรับการใช้งานระบบ

(๓) ใช้ข้อมูลสำรองเพื่อกู้ระบบ หากไม่สามารถทำได้อาจต้องติดตั้งซอฟต์แวร์ระบบใหม่ หลังจากนั้นจึงปรับแก้ค่าติดตั้ง

(๔) แก้ไขและปรับค่าข้อมูลของระบบงานต่าง ๆ ที่ทำงานบนระบบ

(๕) เปิดระบบและทดสอบ

(๖) เปิดระบบเพื่อทดสอบการทำงานพื้นฐาน

(๗) ให้ระบบทำงานให้เป็นปัจจุบันและเริ่มการทำงานอย่างสมบูรณ์

(๘) ให้ระบบทำงานเพื่อกลับสู่สถานะเดิมก่อนเกิดความเสียหาย หลังจากนั้นจึงเปิดให้ใช้งานได้อย่างสมบูรณ์

(๙) เฝ้าระวังระบบ

ข้อ ๖ การจัดเก็บและป้องกันทรัพย์สิน หัวหน้าศูนย์คอมพิวเตอร์กำหนดให้มีการจัดเก็บและป้องกันทรัพย์สินหลังจากเกิดภัยพิบัติแล้ว โดยป้องกันมิให้เกิดความเสียหายและสามารถนำมาใช้เพื่อกู้คืนระบบได้ โดยทรัพย์สินต่าง ๆ จะจัดเก็บดังนี้

(๑) อุปกรณ์คอมพิวเตอร์หรือเครือข่ายที่มีความสำคัญ ให้เก็บรวบรวมไว้ในห้องที่มิดชิดและมีกุญแจปิดเพื่อป้องกันการเข้าออก และให้ผู้มีสิทธิ์ถือกุญแจกล่องฉุกเฉิน

(๒) ห้องเก็บทรัพย์สินต้องหลีกเลี่ยงจากน้ำ สารเคมี และวัตถุไวไฟทั้งหมด

(๓) อุปกรณ์เก็บข้อมูลต้องจัดเก็บในตู้ที่มีกุญแจป้องกันการเปิดทุกครั้ง

(๔) เอกสารที่มีความสำคัญต้องจัดเก็บแยกจากอุปกรณ์อื่น ๆ หากเป็นไปได้ให้เก็บในตู้ที่มีกุญแจป้องกันการเปิดทุกครั้ง

ข้อ ๗ การประเมินความเสียหาย หัวหน้าศูนย์คอมพิวเตอร์ต้องจัดทำรายงานประเมินความเสียหายจากการเกิดภัยพิบัติ โดยเสนอต่อผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศในระหว่างการปฏิบัติงาน หรือหากไม่สามารถดำเนินการได้ให้เสนอ หลังจากการกู้ฟื้นระบบเสร็จสิ้นสมบูรณ์

ข้อ ๘ การจัดหาระบบทดแทนเร่งด่วน ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศกำหนดให้ฝ่ายที่เกี่ยวข้อง เพื่อจัดซื้อจัดหาระบบทดแทนเร่งด่วน หรือเร่งการจัดซื้อจัดหาระบบอย่างเร่งด่วนในกรณีที่มีความจำเป็นต่อการปฏิบัติงานกู้ฟื้นภัยพิบัติหรือการให้บริการที่มีความสำคัญ

หมวด ๓ การฟื้นฟูระบบหลังจากเกิดภัยพิบัติ

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศสั่งการให้หัวหน้างานมีหน้าที่รับผิดชอบในการดำเนินการฟื้นฟูระบบอย่างสมบูรณ์หลังจากการรับมือเร่งด่วน โดยกำหนดขั้นตอน งบประมาณที่ใช้ และระยะเวลาในการฟื้นฟูระบบอย่างสมบูรณ์

หมวด ๕ การปรับปรุงแผน

การปรับปรุงข้อมูลในแผนคณะทำงานกรรมการด้านความปลอดภัยสารสนเทศ มีหน้าที่ในการปรับปรุงข้อมูลในแผนปฏิบัติการรับมือความเสียหายจากภัยพิบัติเป็นประจำทุกเดือนหากมีข้อมูลที่เปลี่ยนแปลงไป โดยหลังจากที่มีการแก้ไข ให้บันทึกการแก้ไขทุกครั้ง

ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ
วันที่ 3 พ.ย 55 .....
(ผู้ช่วยศาสตราจารย์ประสิทธิ์ รางศรี)

อธิการบดีมหาวิทยาลัยราชภัฏอุดรธานี
วันที่ 5 พ.ย 55 .....
(ดร.ณัติเทพ พิทักษานุรัตน์)