ส่วนที่ 1
แนวปฏิบัติการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย
(Network System Control Room)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมและป้องกัน การรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบเครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบเทคโนโลยีสารสนเทศ มิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่ เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลง ระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูล และระบบข้อมูลของมหาวิทยาลัย โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่าย

2. แนวปฏิบัติการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

ข้อ 1. ภายในสำนักคอมพิวเตอร์และเครือข่าย มีการติดตั้งระบบกล้องวงจรปิด เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

ข้อ 2. ผู้ที่เกี่ยวข้อง บทบาท และหน้าที่รับผิดชอบ

(1) หัวหน้าฝ่ายพัฒนาเครือข่าย

- อนุมัติสิทธิเข้าออกพื้นที่ห้องควบคุมระบบเครือข่าย
- อนุมัติกระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(2) ผู้ดูแลห้องควบคุมระบบเครือข่าย

- ตรวจสอบดูแลบุคคลที่ขออนุญาตเข้ามาภายในห้องควบคุมระบบเครือข่าย ให้ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมระบบเครือข่ายอย่างเคร่งครัด

ข้อ 3. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

(1) ผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่มหาวิทยาลัยมีแนวทางปฏิบัติดังนี้

1.1) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้อง และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูและระบบ (System Administrator) เป็นต้น

1.2) ต้องจัดทำระบบเก็บบันทึกการเข้าออกห้องควบคุมระบบเครือข่าย ตามกระบวนการที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกห้องควบคุมระบบเครือข่าย”

1.3) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายต้องมีการควบคุมอย่างรัดกุม

(2) จัดให้มีเจ้าหน้าที่ทำหน้าที่ตรวจสอบประวัติการเข้าออกพื้นที่ห้องควบคุมระบบเครือข่ายเป็นประจำ และให้มีการปรับปรุงรายการผู้มีสิทธิเขาออกพื้นที่ห้องควบคุมระบบเครือข่าย ปีละ 1 ครั้ง เป็นอย่างน้อย

ส่วนที่ 2
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย
(Wireless LAN Access Control)

1. วัตถุประสงค์

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) ของมหาวิทยาลัย โดยการกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ข้อ 1. ผู้ใช้ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับอนุญาตจากผู้อำนวยการ โดยกรอกข้อมูลลงใน ” แบบฟอร์มการขอ Username และ Password”

ข้อ 2. ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

ข้อ 3. ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

ข้อ 4. ผู้ดูแลระบบควรเปลี่ยนค่าชื่อ login และรหัสผ่าน สำหรับการตั้งค่าการทำงานของอุปกรณ์ ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อ login และรหัสผ่านที่มีความคาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

ข้อ 5. ผู้ดูแลระบบ ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกไปนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอก หรือบริเวณขอบเขตที่ควบคุมไม่ได้

ข้อ 6. ผู้ดูแลระบบ ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในของมหาวิทยาลัย

ข้อ 7. ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

ส่วนที่ 3
การกำหนดผู้รับผิดชอบ

1. วัตถุประสงค์

กำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่มหาวิทยาลัยหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

- **ระดับนโยบาย**

ให้อธิการบดี (ผู้บริหารสูงสุดของหน่วยงาน, CEO) และ ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ CIO เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้อำนวยการสำนักคอมพิวเตอร์และเครือข่าย ติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติ

- **ระดับปฏิบัติ** ได้แก่

ข้อ 1. รักษาราชการแทนหัวหน้าฝ่ายพัฒนาเครือข่าย รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติอย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบเครือข่าย วางแผนการปฏิบัติงาน ติดตามการปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของระบบเครือข่าย พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

(1) ควบคุมการเข้า-ออกห้อง Server ตามการกำหนดสิทธิการเข้าถึง Server

(2) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยง

เครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยอุบลราชธานีให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

(3) กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN , Internet , Intranet ที่ให้บริการในมหาวิทยาลัยอุบลราชธานี

(4) แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

(5) รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

(6) กับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

(7) กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

(8) กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมดที่ให้บริการในเว็บไซต์มหาวิทยาลัยอุบลราชธานี ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม.

(9) กำกับดูแล ตรวจสอบในการกำ หนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบ

(10) อื่น ๆ ตามที่ได้รับมอบหมาย

ข้อ 2. นาย..... นักวิชาการคอมพิวเตอร์ รับผิดชอบ ดังนี้

(1) ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

(2) บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

(3) อื่น ๆ ตามที่ได้รับมอบหมาย

ข้อ 3. นาย.....นักวิชาการคอมพิวเตอร์ รับผิดชอบ ดังนี้

(1) ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

(2) รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

(3) อื่น ๆ ตามที่ได้รับมอบหมาย

ข้อ 4. นาย.....นักวิชาการคอมพิวเตอร์ รับผิดชอบดังนี้

(1) แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

(2) กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบเครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

(3) รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูลและสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

(4) บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยอุบลราชธานี ให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชม. แก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายในมหาวิทยาลัย

(5) อื่น ๆ ตามที่ได้รับมอบหมาย

ส่วนที่ 4
แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟล์วอลล์ (Firewall Policy)

1. วัตถุประสงค์

เหตุผลหลักที่มีการใช้ไฟร์วอลล์ (Firewall) ก็เพื่อให้ผู้ใช้ที่อยู่ภายในมหาวิทยาลัย สามารถใช้บริการเครือข่ายภายในได้เต็มที่และใช้บริการเครือข่ายภายนอก เช่น อินเตอร์เน็ตได้ในขณะที่ไฟร์วอลล์จะป้องกันไม่ให้ผู้ใช้ภายนอกเข้ามาใช้บริการเครือข่ายที่อยู่ข้างใน ไฟร์วอลล์สามารถควบคุมการใช้เครือข่ายได้โดยอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่านได้ซึ่งแพ็กเก็ตที่อนุญาตให้ผ่านหรือไม่นี้จะขึ้นอยู่กับนโยบายการรักษาความปลอดภัย (Security Policy) ของเครือข่าย ไฟร์วอล์เป็นระบบที่บังคับใช้นโยบายการรักษาความปลอดภัยระหว่างเครือข่าย โดยหลักการแล้วไฟร์วอลล์จะทำงานอยู่ 2 กลไก คือ การอนุญาตหรือไม่อนุญาตให้แพ็กเก็ตผ่าน ถ้าเครือข่ายมหาวิทยาลัยนั้นมีการเชื่อมต่อโดยตรงกับอินเตอร์เน็ตโดยที่ไม่มีไฟร์วอลล์ จะเป็นการเปิดช่องโหว่ให้เครือข่ายสามารถถูกโจมตีหรือบุกรุกได้อย่างง่ายดาย ตัวอย่างเช่น เครือข่ายมีโฮสต์หรือเซิรฟ์เวอร์เป็นร้อยๆ เครื่อง ถ้าผู้บุกรุกเครือข่ายสามารถบุกรุกเข้าเครื่องใดเครื่องหนึ่งได้ ต่อไปนี้ก็ไม่เป็นการยากที่จะบุกรุกเข้าไปยังเครื่องอื่นๆ การติดตั้งไฟร์วอลล์จะเป็นการป้องกันผู้บุกรุกได้ในระดับหนึ่ง

2. แนวปฏิบัติการใช้งานระบบรักษาความปลอดภัยเครือข่ายคอมพิวเตอร์ไฟร์วอลล์

ผู้ใช้งานระบบรักษาความปลอดภัยไฟร์วอลล์ (Firewall) ของมหาวิทยาลัย มีหน้าที่และความรับผิดชอบที่ต้องปฏิบัติ ดังนี้

ข้อ 1. ผู้ดูแลระบบต้องเฝ้าระวังและบริหารจัดการระบบรักษาความปลอดภัย (Firewall)

ข้อ 2. ผู้ดูแลระบบต้องจัดให้มีระบบตรวจสอบตัวตนจริง และสิทธิ์การเข้าใช้งานของผู้ใช้งาน (Identification and Authentication) ก่อนเข้าสู่ระบบงานคอมพิวเตอร์ที่รัดกุมเพียงพอ เช่น การกำหนดรหัสผ่าน (Password) ให้ยากแก่การคาดเดา เป็นต้น

ข้อ 3. ผู้ดูแลระบบต้องกำหนดค่า (Configuration) เพื่อกลั่นกรองข้อมูลที่มาทางเว็บไซต์ให้มีความปลอดภัยต่อระบบสารสนเทศและเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ป้องกันผู้บุกรุก ไวรัส รวมทั้ง malicious code ต่างๆ มิให้เข้าถึง (Access Risk) หรือสร้างความเสียหาย (Availability Risk) แก่ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์

ข้อ 4. ผู้ดูแลระบบต้องกำหนดขั้นตอนหรือวิธีปฏิบัติ ในการตรวจสอบการรักษาความปลอดภัยระบบเครือข่ายคอมพิวเตอร์ไฟร์วอลล์ และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่า Parameter ในลักษณะที่ผิดปกติต้องดำเนินการแก้ไข รวมทั้งมีการรายงานผู้บังคับบัญชาโดยทันที

ข้อ 5. การเปิดใช้บริการ (Service) ต้องได้รับอนุญาตจากผู้อำนวยการ ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ผู้ดูแลระบบต้องกำหนดมาตรการป้องกันเพิ่มเติม

ข้อ 6. ผู้ดูแลระบบต้องเปิดใช้งานไฟร์วอลล์ตลอดเวลา

ข้อ 7. ผู้ดูแลระบบต้องออกจากระบบงาน (Log Out) ในช่วงเวลาที่มิได้อยู่ปฏิบัติงานที่หน้าเครื่องคอมพิวเตอร์

ข้อ 8. ผู้ดูแลระบบต้องกำหนดให้มีการควบคุมการใช้งาน โดยการจัดให้มีบัญชีผู้ใช้งาน

ข้อ 9. ผู้ดูแลระบบการใช้งานต้องบันทึกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อเป็นการตรวจสอบผู้ใช้ก่อนเข้าใช้งานระบบ (Authentication) และควบคุมบุคคลที่ไม่เกี่ยวข้องมิให้เข้าถึง ล่วงรู้ (Access Risk) หรือแก้ไข เปลี่ยนแปลง (Integrity Risk) ข้อมูลหรือการทำงานของระบบคอมพิวเตอร์ในส่วนที่มิได้มีอำนาจหน้าที่เกี่ยวข้อง

ข้อ 10. ผู้บังคับบัญชาต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ อย่างชัดเจน

ข้อ 11. ผู้ขอใช้งานต้องยอมรับและปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

ข้อ 12. วัตถุประสงค์ในการขอใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่างๆ ของมหาวิทยาลัยและต่อกฎหมายที่เกี่ยวข้อง

ข้อ 13. ผู้ขอใช้งานต้องขออนุญาตเป็นลายลักษณ์อักษร ต่อผู้อำนวยการ โดยระบุข้อมูลดังนี้

(1) หมายเลข Port ที่ต้องการขอให้เปิด
(2) หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสาร
(3) วัตถุประสงค์ หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ
(4) วันที่เริ่มใช้และวันที่สิ้นสุดการขอใช้

ข้อ 14. ในการขอใช้งานหากพบว่าการขัดต่อนโยบาย ประกาศ ระเบียบของมหาวิทยาลัยหรือกฎหมาย หรืออาจทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ จะไม่อนุญาตให้ใช้งาน

ข้อ 15. ภายหลังการอนุญาตให้ใช้งานหากพบว่ามีการใช้งานที่ขัดต่อนโยบายประกาศระเบียบของมหาวิทยาลัย หรือกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของมหาวิทยาลัย จะยกเลิกการให้บริการทันที

ส่วนที่ 5
แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์
(Use of Electronic Mail)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่างๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิ์หรือกระทำการใดๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวปฏิบัติการใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ 1. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย ให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก เป็นต้น

ข้อ 2. ผู้ดูแลระบบต้องกำหนดสิทธิ์บัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรกเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

ข้อ 3. ผู้ใช้ไม่ควรตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) ของระบบจดหมายอิเล็กทรอนิกส์

ข้อ 4. ผู้ใช้ควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยหรือละเมิดสิทธิ์ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัย

ข้อ 5. ผู้ใช้ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่ง ข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

ข้อ 6. ผู้ใช้ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อการทำงานของมหาวิทยาลัยเท่านั้น

ข้อ 7. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการ Logout ออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ 8. ผู้ใช้ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

ข้อ 9. ผู้ใช้ไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

ข้อ 10. ผู้ใช้ไม่ควรใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ที่ไม่เหมาะสม ข้อมูลอันอาจทำให้เสียชื่อเสียงของมหาวิทยาลัย ทำให้เกิดความแตกแยกระหว่างมหาวิทยาลัยผ่านทางจดหมายอิเล็กทรอนิกส์

ข้อ 11. ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

ข้อ 12. ผู้ใช้ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

ข้อ 13. ผู้ใช้ควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

ข้อ 14. ผู้ใช้ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลัง มายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูล หรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

ข้อ 15. ผู้ใช้ควรทำการสำรองข้อมูลในจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอเลือกสำรองจดหมายอิเล็กทรอนิกส์ที่มีความสำคัญมาก โดยอาจทำการส่งต่อไปยังจดหมายอิเล็กทรอนิกส์แอดเดรสอื่น หรือทำการสำรองไว้ที่เมล์เซิร์ฟเวอร์ของมหาวิทยาลัย

ข้อ 16. ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ ควรให้ความรู้เกี่ยวกับการรักษาความปลอดภัยในจดหมายอิเล็กทรอนิกส์แก่ผู้ใช้งานจดหมายอิเล็กทรอนิกส์อย่างสม่ำเสมอ การให้ความรู้ถือเป็นการป้องกันเบื้องต้นเพื่อมิให้ผู้ใช้งานตกเป็นเหยื่อของผู้ไม่หวังดี และเป็นการป้องกันไม่ให้เกิดปัญหา ในกรณีที่ทำผิดพลาดแม้เพียงครั้งเดียว อาจส่งผลกระทบทำให้ระบบไม่สามารถทำงานได้

ข้อ 17. ในการใช้จดหมายอิเล็กทรอนิกส์ในการติดต่อสื่อสารนั้น ผู้ใช้ควรให้เกียรติกับผู้รับปลายทางเหมือนการสนทนาด้วยวาจา ควรตรวจสอบตัวสะกดไวยากรณ์ อ่านทวนเนื้อหาก่อนส่ง ใช้ข้อความที่กระชับเข้าถึงประเด็นอย่างรวดเร็ว แต่ข้อความต้องไม่สั้นเกินจนดูแล้วห้วน และให้ตระหนักอยู่เสมอว่าข้อความใด ๆ ที่ส่งผ่านเครือข่ายอินเทอร์เน็ตนั้นเป็นข้อความที่สามารถมองเห็นและอ่านได้โดยผู้อื่น ดังนั้นการส่งข้อความที่เป็นความลับจะต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์เพื่อเข้ารหัสข้อมูลนั้นก่อนส่งออกไป

ข้อ 18. ผู้ใช้ต้องไม่ทำการเปลี่ยนแปลง หรือแก้ไขข้อความจดหมายอิเล็กทรอนิกส์ต้นฉบับที่ได้รับมาและต้องการส่งต่อไป หากจดหมายอิเล็กทรอนิกส์นั้นถูกส่งถึงผู้รับเป็นการส่วนตัวต้องขออนุญาต ผู้ส่งก่อนที่จะส่งต่อจดหมายอิเล็กทรอนิกส์นั้นไปจดหมายอิเล็กทรอนิกส์ที่มีข้อมูลส่วนบุคคลควรได้รับการเข้ารหัสอย่างปลอดภัย (Encryption)

ข้อ 19. ผู้ใช้ควรใส่ชื่อหัวข้อเรื่องใน Subject ของจดหมายอิเล็กทรอนิกส์ เพื่อแสดงถึงเรื่องของจดหมายอิเล็กทรอนิกส์ที่ต้องการหารือหรือแจ้งให้ทราบ และควรส่งจดหมายอิเล็กทรอนิกส์ตอบกลับสั้น ๆ หากไม่มีเวลาพอเพื่อให้ผู้ส่งได้รับทราบว่าผู้รับได้รับจดหมายอิเล็กทรอนิกส์นั้นแล้วและจะตอบกลับอย่างสมบูรณ์ในภายหลัง

ข้อ 20. ผู้ใช้ไม่ควรส่งต่อจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์ ซึ่งเป็นสิ่งที่ไม่สมควรทำบนเครือข่ายอินเทอร์เน็ต หากได้รับจดหมายอิเล็กทรอนิกส์ลูกโซ่หรือสแปมจดหมายอิเล็กทรอนิกส์และมีข้อความขอให้ส่งต่อจดหมายอิเล็กทรอนิกส์นั้นให้ติดต่อหรือแจ้งผู้ดูแลระบบโดยทันที

ข้อ 21. ผู้ใช้ไม่ควรส่งจดหมายอิเล็กทรอนิกส์ที่เกี่ยวกับการล่วงละเมิดหรือข่มขู่ หรือมีเนื้อหาข้อความที่ขัดต่อกฎหมายและศีลธรรม และใช้จดหมายอิเล็กทรอนิกส์เป็นเครื่องมือในการกระจายข่าวสาร เว้นแต่เป็นการประกาศที่เหมาะสม

ข้อ 22. ผู้ใช้ควรพิจารณาใช้ “BCC” (blind carbon copy - สำเนาโดยที่ผู้รับไม่ทราบ) ในการส่งจดหมายอิเล็กทรอนิกส์ถึงผู้รับเป็นจำนวนมาก เพื่อไม่ให้รายชื่อผู้รับทั้งหมดปรากฏในลักษณะที่ยาวมากเกินไป

ข้อ 23. ผู้ใช้ควรทำตามนโยบายอย่างเคร่งครัด และแจ้งผู้ดูแลระบบเมื่อพบการใช้จดหมายอิเล็กทรอนิกส์ที่ไม่ถูกต้อง

ข้อ 24. ผู้ใช้จะต้องกรอกข้อมูลในช่องข้อมูลส่วนตัว (identity) โดยจะต้องใช้ชื่อผู้ส่ง (Sender) ที่เป็นจริง ตามที่มีบัญชีรายชื่ออยู่จริง เพื่อให้สามารถอ้างอิงในกรณีที่มีปัญหาเกิดขึ้น

ข้อ 25. ผู้ใช้ต้องไม่ตั้งชื่อผู้ส่ง (Sender) หรือข้อมูลอื่น ในลักษณะที่ส่อว่าเป็นผู้ดูแลระบบ (administrator) เช่น webmaster, host master, administrator, postmaster เป็นต้นโดยไม่ได้รับอนุญาต

ข้อ 26. ผู้ใช้ต้องไม่ทำการส่งจดหมายอิเล็กทรอนิกส์ในลักษณะของจดหมายลูกโซ่จดหมายชี้ชวนหรืออื่น ๆ อันเป็นการกระทำที่เข้าข่าย spam หรือ unsolicited electronic mailอย่างเด็ดขาด

ข้อ 27. ผู้ใช้บริการมีหน้าที่จะต้องรักษาชื่อผู้ใช้ และรหัสผ่านเป็นความลับ ไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

ข้อ 28. จดหมายของผู้ใช้บริการ ถือเป็นข้อมูลส่วนบุคคล ผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์ไม่สามารถจะทำการเก็บ กู้ หรือ ดึงข้อมูลส่วนตัวขึ้นมาได้ ดังนั้นผู้ใช้บริการจะต้องดูแลรักษาข้อมูลดังกล่าวอย่างระมัดระวัง โดยเฉพาะการลบจดหมายที่ไม่ต้องการ รวมทั้งจะต้องดูแลรักษาไม่ให้ขนาดของจดหมายที่จัดเก็บเกินกว่าจำนวนพื้นที่ที่ได้รับอนุญาต

ข้อ 29. ผู้ใช้ต้องมีความรับผิดชอบ และระมัดระวังในการใช้บริการตามสมควร ไม่ให้ล่วงละเมิดบุคคลอื่น รวมถึงศีลธรรม หรือกฎหมายใด ๆ อันเป็นผลให้เกิดความไม่สงบเรียบร้อยในมหาวิทยาลัยและสังคมถูกต้อง

ส่วนที่ 6
แนวปฏิบัติการใช้งานอินเตอร์เน็ต
(Internet Policy)

1. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูลข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของมหาวิทยาลัย ถูกระงับ ชะลอขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานตามปกติได้

2. แนวปฏิบัติในการใช้งานอินเทอร์เน็ต

ข้อ 1. ผู้ใช้งานต้องเป็นบุคลากรของมหาวิทยาลัย สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการ หรือผู้ที่ได้รับมอบหมาย

ข้อ 2. ผู้ใช้งานต้องใช้ทรัพยากรเครือข่ายอย่างมีประสิทธิ์ภาพ เช่น ไม่ดาวน์โหลดไฟล์ที่มีขนาดใหญ่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

ข้อ 3. ผู้ใช้งานต้องรับผิดชอบต่อข้อมูลของตนเอง ไม่ว่าจะเก็บไว้ในเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แม่ข่าย (Server) หรือการส่งข้อมูลผ่านเครือข่ายคอมพิวเตอร์

ข้อ 4. ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านรหัสผู้ใช้ (User Account) ของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของรหัสผู้ใช้ (User Account) ต้องเป็นผู้รับผิดชอบ

ข้อ 5. ผู้ใช้งานต้องไม่ใช้งาน เพื่อการกระทำการดังต่อไปนี้

(1) เพื่อการกระทำผิดกฎหมาย หรือเพื่อก่อให้เกิดความเสียหายแก่สถาบันชาติ ศาสนา พระมหากษัตริย์ มหาวิทยาลัย หน่วยงานอื่น และบุคคลอื่น

(2) เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(3) เพื่อการกระทำทางพาณิชย์

(4) เพื่อการเปิดเผยข้อมูลที่เป็นความลับซึ่งได้มาจากการปฏิบัติงาน

(5) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญา

(6) เพื่อให้ทราบข้อมูลข่าวสารของบุคคลอื่นโดยไม่ได้รับอนุญาตจากผู้เป็นเจ้าของ หรือผู้ที่มีสิทธิ์ในข้อมูลดังกล่าว

(7) เพื่อการรับหรือส่งข้อมูลซึ่งก่อหรืออาจก่อให้เกิดความเสียหายให้แก่มหาวิทยาลัย

(8) เพื่อขัดขวางการใช้งานเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย หรือของผู้ใช้อื่น หรือเพื่อให้เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ไม่สามารถใช้งานได้ตามปกติ

(9) เพื่อแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัยไปยังที่อยู่ของเว็บ (website) ใด ๆ ในลักษณะที่ก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

(10) เพื่อการอื่นใดที่อาจขัดต่อผลประโยชน์หรืออาจก่อให้เกิดความขัดแย้งหรือความเสียหายของมหาวิทยาลัย

ข้อ 6. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าเครือข่ายเพื่อประกอบธุรกิจส่วนบุคคล

ข้อ 7. ผู้ใช้งานต้องปฏิบัติตามนโยบายและแนวทางการใช้ระบบเครือข่ายที่มหาวิทยาลัย

ส่วนที่ 7
แนวปฏิบัติการควบคุมการเข้าถึง
(Access Control Policy)

1. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุม ป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องในการปฏิบัติหน้าที่เข้าถึง ล่วงรู้ แก้ไข เปลี่ยนแปลงระบบเทคโนโลยีสารสนเทศและการสื่อสารที่สำคัญ ซึ่งจะทำให้เกิดความเสียหายต่อข้อมูลและระบบข้อมูลของมหาวิทยาลัย โดยมีการกำหนดกระบวนการควบคุมการเข้าออกที่แตกต่างกันของกลุ่มบุคคลต่าง ๆ ที่มีความจำเป็นต้องเข้าออกห้องสำนักคอมพิวเตอร์และเครือข่าย

2. แนวปฏิบัติในการควบคุมการเข้าถึง

ข้อ 1. กระบวนการควบคุมการเข้าออกห้องควบคุมระบบ Network (ห้อง Server)

(1) ผู้ดูแลระบบ และเจ้าหน้าที่มหาวิทยาลัย มีแนวปฏิบัติดังนี้

1.1) ผู้ดูแลระบบ ควรจัดระบบเทคโนโลยีสารสนเทศและการสื่อสารให้เป็นสัดส่วนชัดเจน เช่น ส่วนระบบเครือข่าย (Network Zone) ส่วนเครื่องแม่ข่าย (Server Zone)เป็นต้น

1.2) ผู้ดูแลระบบ ต้องทำการกำหนดสิทธิ์บุคคลในการเข้า-ออกห้อง Server โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายใน

1.3) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้อง มีความจำเป็นต้องเข้า-ออกห้องServer ต้องมีมาตรการการควบคุมอย่างรัดกุม

ข้อ 2. กระบวนการหลักในการควบคุมการเข้าถึงระบบ

(1) สถานที่ตั้งของระบบเทคโนโลยีสารสนเทศและการสื่อสาร มีระบบรักษาความปลอดภัย (Security) ควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิ์และมีความจำเป็นผ่านเข้าใช้งานได้เท่านั้น

(2) ผู้ดูแลระบบกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูล เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ทั้งนี้ผู้ใช้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

(3) ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้น ที่สามารถแก้ไขเปลี่ยนแปลงสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลได้

(4) ผู้ดูแลระบบ จัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูลสำคัญ

(5) ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

ข้อ 3. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

(1) ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบ ให้แก่ผู้ใช้

(2) เจ้าของข้อมูล และ เจ้าของระบบ จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงานต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

(3) ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

ข้อ 4. การบริหารจัดการการเข้าถึงข้อมูลของผู้ใช้

(1) การลงทะเบียนเจ้าหน้าที่ใหม่ กำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการสำหรับการลงทะเบียนเจ้าหน้าที่ใหม่เพื่อให้มีสิทธิ์ต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน เช่น เมื่อเปลี่ยนตำแหน่งงานภายในมหาวิทยาลัย ลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน เป็นต้น

(2) การบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่าน๕.๒.๑ ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ กำหนดสิทธิ์ของเจ้าหน้าที่ในการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

2.1) มีการกำหนดให้ผู้ใช้ลงนามในเอกสารยอมรับเงื่อนไข ที่จะเก็บรักษารหัสผ่านให้เป็นความลับเฉพาะตนใน *“แบบฟอร์มสมัครเป็นสมาชิกระบบเครือข่าย LDD Network”*

2.2) การกำหนดชื่อผู้ใช้ต้องเป็นหนึ่งเดียวคือไม่ซ้ำกัน๕.๓ กำหนดสิทธิ์การใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย(Wireless LAN) ระบบอินเตอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

(3) ผู้ใช้ต้องลงนามรับทราบสิทธิ์และหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษรและต้องปฏิบัติตามอย่างเคร่งครัด

(4) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

4.1) ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงการทำลายข้อมูลแต่ละประเภทชั้นความลับ

4.2) ต้องกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

4.3) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส(Encryption) ทีเป็นมาตรฐานสากล

4.4) ควรมีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(5) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้ ผู้ดูแลระบบทบทวนสิทธิตามรอบระยะเวลาที่กำหนดไว้ หรือเมื่อมีการเปลี่ยนแปลงใด ๆ เช่น เมื่อเปลี่ยนตำแหน่งงานภายในมหาวิทยาลัยลดตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน หมดวาระ เกษียณอายุราชการ เป็นต้น

(6) ควรมีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของมหาวิทยาลัย

ข้อ 5. การบริหารจัดการการเข้าถึงระบบเครือข่าย

(1) ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของผู้ใช้ เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

(2) การเข้าสู่ระบบเครือข่ายภายในของมหาวิทยาลัย โดยผ่านทางอินเทอร์เน็ตจะต้องได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหน่วยงานที่ดูแลรับผิดชอบด้านโครงข่ายระบบเทคโนโลยีสารสนเทศและการสื่อสารก่อนที่จะสามารถใช้งานได้ในทุกกรณี

(3) ผู้ดูแลระบบ ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(4) ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

(5) ระบบเครือข่ายทั้งหมดของมหาวิทยาลัยที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกมหาวิทยาลัยควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ

(6) ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของมหาวิทยาลัยในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย

(7) การเข้าสู่ระบบงานเครือข่ายภายในมหาวิทยาลัย โดยผ่านทางอินเทอร์เน็ตจำเป็นต้องมีการ login และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้อง

(8) IP address ภายในของระบบงานเครือข่ายภายในของมหาวิทยาลัย จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

(9) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(10) การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักคอมพิวเตอร์และเครือข่ายเท่านั้น

(11) ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือกระทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความความเสียหายแก่ระบบเครือข่ายหลักของมหาวิทยาลัย

(12) ในกรณีที่ ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของมหาวิทยาลัย อาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

(13) ห้ามทำการวางสายเครือข่ายเพิ่มเติมโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สาย (Wireless Network) ด้วย

ข้อ 6. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

(1) ควรกำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

(2) ต้องมีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานโดยทันที

(3) ต้องเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ ftp, ssh หรือ ping เป็นต้น

(4) ควรดำเนินการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบันเพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น web server เป็นต้น

(5) การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยเจ้าหน้าที่สำนักคอมพิวเตอร์และเครือข่ายเท่านั้น

ข้อ 7. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

(1) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(2) การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(3) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(4) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

(5) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ 8. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application Information Access Control)

(1) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของมหาวิทยาลัย ควรกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มี สิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

(2) ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเตอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(3) ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร

3.1) กำหนดเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

3.2) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

3.3) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ

พิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(4) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชั่น (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น

(5) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อมหาวิทยาลัย ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกมหาวิทยาลัย (MobileComputing and Teleworking)

(6) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสาร

๙.๗ การควบคุมการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) กำหนดข้อปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของมหาวิทยาลัยจากภายนอกสำนักงาน

ข้อ 9. การควบคุมการเข้าใช้งานระบบจากภายนอก

(1) การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของมหาวิทยาลัย การควบคุมบุคคลที่เข้าสู่ระบบของมหาวิทยาลัยจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(2) ก่อนทำการให้สิทธิ์ในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัย อย่างเพียงพอและต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

(3) ต้องมีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม การเข้าสู่ระบบโดยการโทรศัพท์เข้ามหาวิทยาลัยนั้นต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบและวิธีการหมุนเข้าต้องได้รับการอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น

(4) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่ควรเปิดพอร์ตและโมเด็มที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วและจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

ข้อ 10. การพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอก

(1) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยนั้น จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตนอย่างน้อย ๑ วิธี

(2) การเข้าสู่ระบบสารสนเทศของมหาวิทยาลัยจากอินเทอร์เน็ตนั้น ควรมีการตรวจสอบผู้ใช้งานด้วย

(3) การเข้าสู่ระบบจากระยะไกล (Remote access) เพื่อเพิ่มความปลอดภัยจะต้องมีการ ตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน เช่น รหัสผ่าน เป็นต้น

ส่วนที่ 8
การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (log)

1. วัตถุประสงค์

เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ (log) มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้

2. แนวปฏิบัติในการจัดเก็บข้อมูลการจราจรคอมพิวเตอร์

ข้อ 1. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง ระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดขั้นตอนความลับในการเข้าถึง

ข้อ 2. ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (IT auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

ข้อ 3. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ใช้ในการตรวจสอบและเก็บบันทึกไว้ 90 วัน นับตั้งแต่การใช้งานสิ้นสุดลง

ข้อ 4. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ส่วนที่ 9
แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and Information Access Control)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ ขององค์กร โดยการกำหนดสิทธิ์ของผู้ใช้งานระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการอนุญาตและกำหนดสิทธิ์การเข้าใช้งานจากผู้ดูแลระบบ

2. แนวปฏิบัติการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ

ข้อ 1. ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ระบบ

(1) กำหนดเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(2) กำหนดชื่อผู้ใช้หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(3) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุดผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ 2. การจำกัดการเข้าถึงระบบ (Information access restriction) จะอนุญาตให้ผู้ใช้งานและบุคลากรฝ่ายสนับสนุนเข้าสู่ระบบ เฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิ์เกินความจำเป็นในการใช้งาน จะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่

ข้อ 3. ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบเทคโนโลยีสารสนเทศ

ข้อ 4. ผู้ดูแลระบบควรมีการทบทวนสิทธิ์การเข้าใช้งานอย่างสม่ำเสมอ

ข้อ 5. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (Mobile Computing and Teleworking)

ส่วนที่ 10
แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control)

1. วัตถุประสงค์

เพื่อกำหนดแนวทางควบคุมการเข้าถึงระบบปฏิบัติการ ขององค์กร โดยผู้ใช้งานต้องมีการยืนยันตัวตนก่อนเข้าใช้งานระบบตลอดจนกำหนดระยะเวลาในการเชื่อมต่อ เพื่อสร้างความปลอดภัยในการเข้าถึงระบบปฏิบัติการ

2. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ 1. กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดย วิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

ข้อ 2. การระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

ข้อ 3. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

ข้อ 4. เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)

ข้อ 5. การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคง

ส่วนที่ 11
แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

1. วัตถุประสงค์

เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

2. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ 1. มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

(1) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit assessment) ปีละ 1 ครั้ง

(2) ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยหน่วยตรวจสอบภายใน เพื่อให้มหาวิทยาลัยได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 2. มีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึงดังนี้

(1) มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง ปีละ 1 ครั้ง

(2) มีการทบทวนนโยบายและมาตรการในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศปีละ 1 ครั้ง

(3) มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ

(4) มีมาตรการในการตรวจประเมินระบบสารสนเทศ ดังนี้

4.1) ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว

4.2) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือจัดเก็บไว้โดยมีการป้อนกันเป็นอย่างดี

4.3) ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

4.4) ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

4.5) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

(5) มีการรายงานผลการประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง ต่อคณะกรรมการบริหารสารสนเทศมหาวิทยาลัยอุบลราชธานี และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

(6) มีการแสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เป็นส่วนหนึ่งของการรายงานผลการติดตาม ตรวจสอบและประเมินผลงาน ด้านเทคโนโลยีสารสนเทศและการสื่อสาร

ส่วนที่ 12
แนวปฏิบัติการระบบสารสนเทศและระบบสำรองของสารสนเทศ

1. วัตถุประสงค์

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยสามารถให้บริการได้อย่างต่อเนื่อง และเพื่อมาตรฐานในการปฏิบัติและความรับผิดชอบของผู้ดูแลระบบ โดยตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยเป็นสำคัญ

2. แนวปฏิบัติการระบบสารสนเทศและระบบสำรองของสารสนเทศ

ข้อ 1. ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

(1) มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของมหาวิทยาลัย พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

(2) กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

2.1) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

2.2) กำหนดรูปแบบสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup) ฯลฯ

2.3) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ

2.4) ตรวจสอบข้อมูลทั้งหมดระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน (configuration) ข้อมูลในฐานข้อมูล ฯลฯ

2.5) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บสำรองกับมหาวิทยาลัยควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับมหาวิทยาลัย เช่น ไฟไหม้ น้ำท่วม ฯลฯ

2.6) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

2.7) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

2.8) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

2.9) ตรวจสอบและทดสอบประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

2.10) กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลที่ได้สำรองเก็บไว้

ข้อ 2. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจตามแนวทางต่อไปนี้

(1) มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

1.1) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

1.2) มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบได้ ฯลฯ

1.3) มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

1.4) มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้

1.5) มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ ซอฟต์แวร์ ฯลฯ เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

1.6) มีการสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือสิ่งที่ทำเมื่อเกิดเหตุเร่งด่วน

(2) มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ปีละ 1 ครั้ง

ข้อ 3. ต้องการการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ 4. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ปีละ 1 ครั้ง

ข้อ 5. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงานในมหาวิทยาลัย ปีละ 1 ครั้ง