ประกาศมหาวิทยาลัยราชภัฏพิบูลสงคราม

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยสารสนเทศ

การการกำหนดมาตาฐานแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ เป็นเครื่องมือในการดำเนินการจัดทำนโยบายรักษาความปลอดภัยสารสนเทศของมหาวิทยาลัยราชภัฏพิบูลสงคราม ให้เป็นไปตามแนวนโยบายในการรักษาความปลอดภัยของหน่วยงานภาครัฐ และเพื่อให้ผู้ปฏิบัติงานในมหาวิทยาลัยราชภัฏพิบูลสงครามทุกท่าน ปฏิบัติเป็นแนวทางเดียวกันอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุด ทางมหาวิทยาลัยฯ จึงต้องกำหนดประกาศมหาวิทยาลัยราชภัฏพิบูลสงคราม แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ โดยกำหนดเป็นแนวปฏิบัติ ดังนี้

1. แนวปฏิบัติการรักษาความปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1.กำหนดให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารต่างๆให้ชัดเจน และมีการประกาศให้ทราบโดยทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรืออุปกรณ์ระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สายเป็นต้น

2. กำหนดให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นทีใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร รวมถึงการใช้ช่องสัญญาณการสื่อสารต่างๆ ภายในเขตพื้นที่มหาวิทยาลัย

3. กำหนดให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการในการควบคุมการเข้า-ออกพื้นและการเชื่อมต่อบริการที่ใช้

4. กำหนดให้หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานติดตั้งระบบเครือข่ายภายในมหาวิทยาลัยจะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์เครือข่าย และต้องมีเจ้าหน้าที่ควบคุมการปฏิบัติงานที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ผู้รับผิดชอบ : งานบริหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

2. แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ตามที่นโยบายในหมวดที่ว่าด้วยการปฏิบัติตามข้อกำหนด ซึ่งกำหนดขึ้นเพื่อให้มั่นใจว่านักศึกษาและบุคลากรของมหาวิทยาลัยรับทราบ และปฏิบัติตามนโนบาย กฎ ระเบียบ ข้อปฏิบัติ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยจึงได้กำหนดแนวปฏิบัติเพื่อให้มีการเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

1. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมอบรมของหน่วยงาน

2. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาปีละไม่น้อยกว่า 1 ครั้ง จัดเป็นกิกรรมเสริมในงานอบรมและสัมมนาอื่นๆ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

3. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในการให้เกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย

4. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการจากหน่วยงานต่างๆภายในมหาวิทยาลัย และประกาศให้รับทราบผ่านเว็บมหาวิทยาลัยที่ http://www.psru.ac.th

ผู้รับผิดชอบ : งานบริหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

3. แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

1.ผู้ดูระบบต้องกำหนดการลงทะเบียนบุคลากรและนักศึกษาใหม่ของมหาวิทยาลัย และกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่างๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน ดังต่อไปนี้

1.1 การลงทะเบียนเพื่อรับสิทธิการใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

1.1.1 กรณีนักศึกษาลงทะเบียนสำเร็จจะได้รับรหัสผู้ใช้(รหัสนักศึกษา) งานภายใน 1 วัน หลังจากรายงานตัวกรอกประวัติและชำระเงินเรียบร้อยแล้ว

1.1.2 กรณีบุคลากรจะได้รับบัญชีและรหัสผู้ใช้งานภายใน 1 วัน หลังจากรายงานตัวกรอกประวัติและกองบริหารงานบุคคลทำการบันทึกข้อมูลบุคลากรในระบบสมบูรณ์

1.2 การยกเลิกสิทธิการใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

1.2.1กรณีนักศึกษาจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 15 วัน หลังจากการขึ้นทะเบียนพ้นสภาพการเป็นนักศึกษาในระบบสมบูรณ์แล้ว

1.2.2 กรณีบุคลากรจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 15 วัน หลังจากกองบริหารงานบุคคลที่จัดทำคำสั่งให้พ้นสภาพการเป็นบุคลากร และบันทึกข้อมูลในระบบสมบูรณ์แล้ว

2. ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บริหารของหน่วยงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

3. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งาน ดังต่อไปนี้

3.1 กำหนดประเภทของสิทธิกับผู้ใช้งานระบบสารสนเทศ โดยจำแนกประเภทสิทธิตามหน้าที่และความรับผิดชอบ และต้องจัดเก็บและมอบหมายสิทธิให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

3.2 กรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

3.3 กรณีมีการว่าจ้างผู้รับจ้างจากภายนอกเข้าใช้งานระบบสารสนเทศจะต้องกำหนดระยะเวลาการใช้งานของผู้รับจ้างภายนอกและระงับการใช้งานทันทีเมื่องานดังกล่าวเสร็จสิ้นหรือสิ้นสุดสัญญา

4. ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้บริการ ดังต่อไปนี้

4.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

4.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งมอบให้กับบุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

4.3 ห้ามมอบให้ผู้ใช้งานบันทึก หรือเก็บรหัสผ่านไว้บนระบบคอมพิวเตอร์ในแบบที่มิได้ป้องกันการเข้าถึง

4.4 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารของหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ในระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานสูงสุดต่างจากรหัสผู้ใช้งานปกติ

5. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานตามประเภทของข้อมูล ความสำคัญของข้อมูล ความลับของข้อมูล และลำดับชั้นการเข้าถึงของข้อมูลโดยการเข้าถึงนั้นจะต้องเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น

5.1 ต้องมีการกำหนดประเภทของข้อมูล ซึ่งมีการจัดแบ่งไว้เป็น 3 ประเภท คือ

5.1.1 ข้อมูลสารสนเทศด้านการบริหารงาน เช่น ระบบคลังข้อมูลมหาวิทยาลัย ระบบภาระงานบุคลากรสายวิชาการ

5.1.2 ข้อมูลสารสนเทศด้านการบริการอาจารย์ นักศึกษา และบุคลากร เช่น ระบบบริการการศึกษา ระบบทรัพยากรบุคคล

5.1.3 ข้อมูลสารสนเทศด้านการบริการบุคคลทั่วไป เช่น ระบบรับนักศึกษาใหม่ ระบบประชาสัมพันธ์

5.2 ต้องมีการจัดลำดับความสำคัญของข้อมูลโดยแบ่งออกเป็น 3 ลำดับ คือ

5.2.1 ข้อมูลที่มีระดับความสำคัญมากที่สุด

5.2.2 ข้อมูลที่มีระดับความสำคัญปานกลาง

5.2.3 ข้อมูลที่มีระดับความสำคัญน้อย

5.3 ต้องมีการกำหนดระดับชั้นของการเข้าถึงข้อมูล โดยมีการพิสูจน์สิทธิในการเข้าถึงข้อมูลแต่ละระดับชั้นและต้องกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวจริงของผู้ใช้ข้อมูลในแต่ละชั้นการเข้าถึงข้อมูล โดยแบ่งระดับชั้นออกเป็น 3 ระดับชั้นคือ

5.3.1 ระดับชั้นสำหรับผู้บริหาร

5.3.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

5.3.3 ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ได้รับมอบหมาย

5.4 ต้องกำหนดระยะเวลาในการเข้าถึง และวิธีการในการระงับการใช้งานเมื่อพ้นระยะเวลาดังกล่าวและกำหนดระยะเวลาไม่มีการใช้งานต่อเนื่องเป็นระยะเวลาติดต่อกันไม่เกิน

5.5 ต้องกำหนดช่องทางในการเข้าถึงข้อมูลในแต่ละประเภท ว่ามีการเข้าถึงข้อมูลแต่ละประเภทได้โดยตรงหรือการเข้าถึงผ่านระบบงาน

5.6 ต้องกำหนดให้มีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น ในกรณีการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ

5.7 ผู้ดูแลระบบต้องจัดเตรียมเครื่องมือที่ใช้ในการเข้ารหัสให้กับผู้ใช้สำหรับการเข้ารหัสข้อมูลที่เป็นความลับ

5.8 ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2554

5.9 ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ในการส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

4. แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

1. มหาวิทยาลัยต้องกำหนดให้มีมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัยในกรณีบุคคลจากหน่วยงานภายนอกหรือผู้รับจ้างจากภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรตามสายงานต่อผู้บริหารของหน่วยงานหรือผู้อำนวยการ

2. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

3. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศที่มีต่อระบบข้อมูล

4. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่างๆ

5. ผู้ดูแลระบบต้องจัดให้มีการตรวจสอบการกำหนดสิทธิตามลำดับความสำคัญของระบบสารสนเทศ

6. ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนสำหรับผู้ใช้ที่อยู่ภายในและภายนอกองค์กร และกำหนดสิทธิการเข้าใช้งานระบบสารสนเทศจากภายนอก(User authentication for external connections)

7. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการเข้าใช้งานระบบสารสนเทศจากภายนอกองค์กร

8. ผู้ดูแลระบบต้องกำหนดความสำคัญของระบบสารสนเทศ และมีการควบคุมอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร เพื่อให้ระบบสารสนเทศที่สำคัญมีความปลอดภัยมากที่สุด

9. ผู้ดูแลระบบต้องติดตั้งระบบสารสนเทศที่มีความสำคัญสูงไว้บนเครื่องคอมพิวเตอร์แม่ข่ายในห้องคอมพิวเตอร์กลาง หรือห้องคอมพิวเตอร์ซึ่งมีสภาพแวดล้อมที่เหมาะสม เช่น ระบบสำรองไฟฟ้า และระบบปรับอากาศ เป็นต้น

10. ผู้ดูแลระบบต้องกำหนดสิทธิและให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยกำหนดมาตรการและข้อปฏิบัติที่เหมาะสมเพื่อปกป้องสารสนเทศจากภาวะความเสี่ยงอันเนื่องมาจากการใช้อุปกรณ์เหล่านั้น

11. ผู้ดูแลระบบต้องกำหนดสิทธิและให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องทำการยืนยันตัวตนโดยใช้ (iPASSPORT ID)ก่อนเข้าสู่ระบบของมหาวิทยาลัย

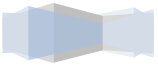
12. ผู้ดูแลระบบจะต้องมีระบบบริหารจัดการรหัสผ่านที่ทำงานในลักษณะอัตโนมัติ เพื่อให้รหัสผ่านของผู้ใช้มีคุณภาพ

13. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงบริการสารสนเทศตามสิทธิที่ได้รับอนุญาตเท่านั้น

14. ผู้รับจ้างภายนอกต้องมีการลงนามรับรองว่าจะไม่นำข้อมูลของมหาวิทยาลัยออกไปเปิดเผยภายนอก

15. ผู้ดูแลระบบต้องมีการกำหนดให้ใช้ฐานข้อมูลผู้ใช้จากระบบ (iPASSPORT ID) เป็นบานข้อมูลกลางในการกำหนดสิทธิการเข้าถึงเท่านั้น

ผู้รับผิดชอบ : งานบริหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ



5. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

1. ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้า-ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

3.การขอใช้งานพื้นที่เครื่องให้บริการเว็บ (Web Sever) และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและจะต้องไม่ลงโปรแกรมที่เป็นอันตรายและส่งผลกระทบต่อการใช้งานของผู้ใช้บริการอื่นๆ

4. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกณ์ส่วนกลาง ซึ่งได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์สวิตช์ อุปกรณ์เชื่อมต่อกับระบบเครือข่ายหลัก โดยมิได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

5. ผู้ดูแลระบบจะต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้การบริหารจัดการระบบเครือข่ายเป็นไปอย่างมีประสิทธิภาพ ดังต่อไปนี้

5.1 มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.2 มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

5.3 กำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่นๆ ได้

5.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกณ์ป้องกันการบุกรุกซึ่งต้องสามารถตรวจจับโปรแกรมประสงค์ร้ายได้

5.5 ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่อาจเข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติ

5.6 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน เพื่อผ่านออกสู่อินเทอร์เน็ตต้องทำการบันทึกเข้า (Logon) โดยระบุชื่อผู้ใช้และรหัสผ่านโดยใช้ (iPASSPORT ID) ของผู้ใช้บริการเพื่อใช้ยืนยันผ่านระบบพิสูจน์ตัวตนของมหาวิทยาลัยเพื่อใช้และรหัสผ่านโดยใช้ติดตามตรวจสอบความถูกต้องของการใช้บริการ

5.7 หมายเลขไอพี (IP Address) ที่ให้บริการระบบเครือข่ายภายในของหน่วยงานต่างๆ จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

5.8 จัดทำแผนผังระบบเครือข่าย (Network Diagram) โดยระบุรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันแม็คแอดเดส (Physical Address) พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.9 การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเท่าที่จำเป็น

6. ผู้ดูแลระบบต้องดูแลรับผิดชอบระบบคอมพิวเตอร์เครื่องแม่ข่าย โดยควบคุมในเรื่องข้อกำหนดในการแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

7. ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์ครบถ้วน ถูกต้อง เพื่อให้สามารถระบุถึงตัวตนได้ตามแนวทาง ดังต่อไปนี้

7.1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล ผู้ดูแลระบบมิได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ให้เป็นไปตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550

7.2 กำหนดให้มีการบันทึกการทำงานของระบบปฏิบัติการของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งานคำสั่ง (Command line) และบันทึกไฟล์วอลล์ (Firewall log) เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

7.3 ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

7.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

8. ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

8.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำหนังสือถึงผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่ออนุญาตก่อน

8.2 ผู้ดูแลระบบควบคุมช่องทางพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องไม่เปิดช่องทางที่ใช้ทิ้งไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อโดยอัตโนมัติเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

8.3 วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศก่อน

8.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

8.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนโดยใช้(iPASSPORT ID)ของมหาวิทยาลัย

8.6 การเข้าสู่ระบบต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานเข้าสู่ระบบภายใน เช่น การใช้วีพีเอ็น เอสเอสแอล เป็นต้น

8.7 ผู้ดูแลระบบจะต้องกำหนดช่องทาง ที่ใช้ในการเข้าสู้ระบบ และจะต้องตรวจสอบและติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

9.ผู้ดูแลระบบต้องกำหนดวิธีการปกปิดหมายเลขไอพีของระบบงานภายในเครือข่ายของหน่วยงาน เพื่อป้องกันมิให้บุคคลภายนอกสามารถทราบข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้ โดยทำการแบ่งแยกเป็นหมายเลขไอพีสาธารณะ (public IP Address) และหมายเลขไอพีภายใน (private IP Address) เพื่อยกเครือข่ายย่อย และให้มีการจัดทำการแปลงหมายเลขเครือข่าย (NAT Network Address Translation)

ผู้รับผิดชอบ : งานระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

6. แนวปฏิบัติการใช้รหัสผ่าน

1. รหัสผ่าน (Password) จะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะมีการผสมผสานกันระหว่างตัวเลขหรือตัวอักษรพิมพ์เล็กหรือตัวพิพมใหญ่ หรือตัวอักขระพิเศษ

2. รหัสผ่านต้องไม่เป็นคำที่มีความหมายทั้งภาษาไทยและภาษาอังกฤษ และเป็นคำที่ไม่มีความหมายในพจนานุกรม

3. ห้ามตั้งรหัสผ่านเหมือนกับชื่อหรือนามสกุล หรือสิ่งที่ง่ายต่อการคาดเดา

4. ห้ามจดบันทึกรหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถมองเห็นได้

5. ทำการเปลี่ยนแปลงรหัสผ่านใหม่ในทุกๆ 3 เดือน เป็นอย่างน้อย

6. ห้ามนำรหัสผ่านที่เคยใช้งานมาแล้วกลับมาใช้งานอีก

7. รหัสผ่านจะต้องเป็นความลับเฉพาะบุคคล และจะไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยมิได้รับอนุญาต

ผู้รับผิดชอบ : งานพัฒนาระบบสารสนเทศและเครือข่าย งานบริการวิชาการ ศูนย์เทคโนโลยีสารสนเทศ

7.แนวปฏิบัติการใช้งาน iPASSPORT

1. ผู้ ใช้บริการจะต้องเก็บรักษารหัส (iPASSPORT ID) ไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยมิได้รับอนุญาต

2. ผู้ใช้บริการที่เป็นเจ้าของ (iPASSPORT ID) ต้องเป็นผู้รับผิดชอบต่อผลต่างๆ ที่เกิดขึ้นจากการใช้บริการเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3. ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้ (iPASSPORT ID) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อหยุดการใช้งานชั่วคราว หรือเสร็จสิ้นการใช้งาน

4. ผู้ใช้บริการลงทะเบียนอุปกรณ์เครือข่ายด้วย (Physical Address) ไว้กับระบบ (iPASSPORT) จะต้องทำการแจ้งยกเลิกการใช้งานในกรณีอุปกรณ์ (Physical Address) ทุกครั้งเมื่อไม่ใช้งาน (Physical Address)

5. ผู้ใช้งานหยุดใช้งานอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์เครือข่ายเป็นระยะเวลาตามที่กำหนดให้ถือว่า ออกจากระบบ (Logout)

6. ผู้ใช้งานรหัส (iPASSPORT ID) ที่ไม่ใช้งานติดต่อกันเป็นระยะเกิน 90 วัน ระบบจะระรับการใช้บริการ

7. ผู้ใช้งานรหัส (iPASSPORT ID) จะต้องไม่สามารถใช้งานได้ ในกรณีผู้ใช้งานสิ้นสุดการเป็นนักศึกษาหรือเป็นเจ้าหน้าที่ของมหาวิทยาลัย

8. กรณีผู้ใช้งานชั่วคราม (iPASSPORT Card) ระยะเวลาการใช้งานและรหัสการเข้าใช้ ให้เป็นไปตามที่ผู้ดูแลระบบกำหนดเท่านั้นและผู้ใช้งานต้องลงชื่อ พร้อมเลขบัตรประจำตัวประชาชน วัน เวลา การเปิดใช้งานไว้เป็นหลักฐาน

ผู้รับผิดชอบ : งานพัฒนาระบบสารสนเทศและเครือข่าย งานบริการวิชาการ ศูนย์เทคโนโลยีสารสนเทศ

8. แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ

ให้ศูนย์เทคโนโลยีสารสนเทศกำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแลดังต่อไปนี้

1. ผู้ใช้บริการต้องออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบสารสนเทศ เครื่องคอมพิวเตอร์ เป็นต้น อุปกรณ์ใช้งานระบบเครือข่าย

2. ผู้ใช้บริการจะต้องป้องกันไม่ให้ผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน โดยใส่รหัสผ่านให้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน

3. ผู้ใช้บริการต้องล็อคอุปกรณ์คอมพิวเตอร์และอุปกรณ์เครือขายที่สำคัญ เมื่อไม่ได้ใช้งาน หรือปล่อยทิ้งไว้โดยไม่มีผู้ดูแล ด้านทางกายภาพและด้านซอฟแวร์

4. สร้างความตระหนักและให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกณ์ในขณะที่ไม่มีผู้ใช้งาน

5. ออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งานประจำวัน หรือต้องพักหน้าจอไว้เป็นเวลานานๆ

6. ระบบสารสนเทศจะต้องมีการกำหนดค่าการตัดการใช้งานระบบ (Idle timeout) ภายใน 15 นาทีหลังจากที่ไม่มีการใช้งาน

7. เครื่องคอมพิวเตอร์ที่ใช้งานส่วนบุคคล ไม่ได้ใช้งานให้ทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงทันทีเมื่อเสร็จสิ้นงาน

ผู้รับผิดชอบ : งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

9.แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

จุดประสงค์เพื่อจัดทำแนวปฏิบัติให้ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงหน้าที่ความรับผิดชอบด้านการจัดการและการใช้ระบบคอมพิวเตอร์และเครือข่ายสารสนเทศ และสามารถปฏิบัติตามอย่างเคร่งครัด โดยให้มีส่วนร่วมในการช่วยกันป้องกันสินทรัพย์และข้อมูลของมหาวิทยาลัยให้อยู่ในสภาพมีความมั่นคงปลอดภัย ซึ่งควบคุมด้านการรักษาความลับ ความถูกต้องคนรบถ้วน ความปลอดภัยจากภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด และสภาพสารสนเทศพร้อมใช้งาน

1. การติดตั้งเครื่องคอมพิวเตอร์ลูกข่ายต้องดำเนินการตามแนวปฏิบัติซึ่งครอบคลุมประเด็นต่างๆ ดังนี้

1.1 การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti-virus)

1.2 การติดตั้งโปรแกรมปรับปรุงการอุดช่องโหว่ของวินโดว์ (Window update Patch)

1.3 การลงทะเบียนเครื่องในระบบ (iPASSPORT) ลงทะเบียน (MAC address)

1.4 การติดตั้งซอฟต์แวร์พื้นฐาน

2. ให้มีการทบทวนค่าแม็คแอดเดส (MAC address หรือ Media Access Control Address) ที่บันทึกไว้อย่างน้อยปีละ 1 ครั้ง ในกรณีการซ่อมบำรุงเครื่องคอมพิวเตอร์ลูกข่าย และอาจมีผลต่ออุปกรณ์ที่เชื่อมต่อเครือข่าย ผู้ซ่อมบำรุงต้องแจ้งศูนย์เทคโนโลยีสารสนเทศเพื่อการปรับปรุง (MAC address)

3. เครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องสามารถใช้งานระบบเครือข่ายทั้งเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศของมหาวิทยาลัยได้เท่าที่มีการอนุญาตให้ใช้งานหรือที่ได้มีการกำหนดสิทธิไว้เท่านั้น

4. ในการเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่าย ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติ เกี่ยวกับการระบุและพิสูจน์ตัวตนและการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

5. การใช้แฟ้มข้อมูลร่วมกัน (Shared File) ต้องมีการกำหนดให้ใช้วิธีการระบุชื่อผู้ใช้งานและรหัสผ่านถูกต้องก่อนจึงจะสามารถเรียกใช้งานได้ ทั้งเครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งชื่อผู้ใช้งานจะต้องเป็นไปตามแนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

6. ห้ามมิให้มีการใช้อุปกรณ์ต่อพ่วงโดยไม่ผ่านการยืนยันตัวตนโดยการแชร์ผ่านออกเครื่องเดียว (Shared Internet) หรือการนำอุปกรณ์ต่อพ่วง เช่น โทรศัพท์มือถือมาเชื่อมต่อยังเครื่องคอมพิวเตอร์ลูกข่ายเพื่อใช้เป็นช่องทางในการใช้อินเทอร์เน็ตและเชื่อมต่อระบบเครือข่ายของมหาวิทยาลัย

7. ห้ามเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม หรือไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

8. ห้ามทำการเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงานโดยมิได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศ

9. ห้ามมิให้ทำการปรับแต่งไบออส (Bios) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจจะส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นสาเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

10. ห้ามมิให้ทำการติดตั้งโปรแกรมที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

11. เครื่องคอมพิวเตอร์จะต้องมีการกำหนดค่าการพักจอภาพ (screen saver) เพื่อให้มีการป้องกันการเข้าถึงระบบปฏิบัติการในขณะที่ไม่มีผู้ใช้งาน

12. ห้ามมิให้ทำการติดตั้งโปรแกรมควบคุมระยะไกล (Remote Computer) เครื่องคอมพิวเตอร์บริการส่วนกลาง เว้นแต่ได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ : งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

10.แนวปฏิบัติการติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย

1.ติดตั้งและใช้งานระบบปฏิบัติการที่มีลิขสิทธิถูกต้องตามกฎหมาย

2.จัดทำรายงานตรวจสอบ (Checklist) สำหรับการติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย และปรับปรุงรายการตรวจสอบนั้นอย่างน้อยปีละ 1 ครั้ง โดยให้มีการระบุรุ่นเวอร์ชั่นของรายการตรวจสอบอย่างชัดเจนเพื่อป้องกันความสับสนของการนำไปใช้งาน

3. ให้หน่วยงานที่รับผิดชอบดำเนินการติดตั้งเครื่องคอมพิวเตอร์ลุกข่ายตามรายการตรวจสอบที่ได้จัดทำขึ้นมีข้อมูลดังนี้ ชื่อคอมพิวเตอร์, โปรแกรม, รุ่นเวอร์ชั่น, เบอร์โทรติดต่อ, ผู้รับผิดชอบ, หน่วยงาน, ค่าอุปกรณ์เครือข่าย (Physical Address)

4. ให้ดำเนินการปรับปรุงระบบปฏิบัติการ (Update หรือ Service Pack หรือ Patch หรือ Hot fix ของระบบปฏิบัติการนั้น

5. ให้มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus) ไดๆ ตามผู้ใช้ต้องการ โดยขั้นต่ำกำหนดให้ใช้ Microsoft Security Essentials Free Software เป็นอย่างน้อย

6. ให้มีการกำหนดและติดตั้งซอฟต์แวร์เฉพาะที่จำเป็นต่อการปฏิบัติงานของมหาวิทยาลัยเท่านั้น โดยให้มีการทบทวนรายการซอฟต์แวร์พื้นฐานนั้นเพื่อให้เหมาะสมและสอดคล้องกับการปฏิบัติงานตามภารกิจของมหาวิทยาลัย

7. ต้องติดตั้งซอฟต์แวร์ที่ถูกลิขสิทธิและเป็นซอฟต์แวร์พื้นฐานที่จำเป็นต่อการใช้งานของมหาวิทยาลัยเท่านั้น

8. ศูนย์เทคโนโลยีสารสนเทศจะดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์ลูกข่ายอย่างน้อยปีละ 1 ครั้ง

9. เครื่องคอมพิวเตอร์ที่ใช้ในการปฏิบัติงานจะต้องอยู่ในรายการมาตรฐานเครื่องคอมพิวเตอร์ลูกข่ายเท่านั้น

10. ผู้ใช้งานทำการลงทะเบียนคอมพิวเตอร์ลูกข่ายเพื่อเก็บค่า (Physical Address) ในระบบ (iPASSPORT) เพื่อเก็บข้อมูลเครื่องคอมพิวเตอร์ให้สามารถบอกได้ว่าเครื่องนั้นตั้งอยู่ที่ใดภายในมหาวิทยาลัยและผู้ใดเป็นเจ้าของเครื่องคอมพิวเตอร์เครื่องนั้น

11. เครื่องคอมพิวเตอร์จะต้องมีการกำหนดค่ารหัสการเข้าใช้งานเพื่อป้องกันการเข้าถึงระบบปฏิบัติการในขณะที่ไม่มีผู้ใช้งาน

12. เครื่องคอมพิวเตอร์จะต้องทำการตั้งค่ารหัสการเข้าใช้งานการพักจอภาพเมื่อมิได้มีการใช้งาน

13. เครื่องคอมพิวเตอร์จะต้องถูกล็อคหน้าจอทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

14. เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องมีการตั้งค่าการยืนยันตัวตนก่อนเข้าใช้งานระบบปฏิบัติการ และระบบเครือข่าย

15. จัดทำรายงานเกี่ยวกับรายละเอียดของเครื่องคอมพิวเตอร์ลูกข่ายปีละ 1 ครั้ง

16. เครื่องคอมพิวเตอร์ที่ใช้งานส่วนบุคคล มิได้ใช้งานให้ทำการปิดเครื่องคอมพิวเตอร์และอุปกรณ์ต่อพ่วงทันทีเมื่อเสร็จสิ้นสุดการใช้งาน

ผู้รับผิดชอบ: งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

11.แนวปฏิบัติการควบคุมการใช้สินทรัพย์สารสนเทศ

1. ผู้ดูแลระบบและผู้ใช้งานจะต้องออกจากระบบ (Logout) ทุกครั้งเมื่อเลิกการใช้งาน

2. ผู้ใช้งานจะต้องปิดเครื่อง (Shut Down) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน ณ สิ้นวัน

3. เอกสารที่เป็นความลับทางราชการ จะต้องเก็บอยู่ในลิ้นชักตู้เก็บเอกสารที่ปลอดภัย และไม่วางเอกสารความลับทางราชการไว้ที่โต๊ะหลังเลิกงาน

4. เอกสารที่เป็นความลับทางราชการจะต้องเก็บอยู่ในลิ้นชักที่สามารถล็อคได้

5. กุญแจที่สามารถเปิดลิ้นชักเอกสารลับจะต้องมีผู้รับผิดชอบและอยู่ในที่ปลอดภัย

6. ผู้ใช้งานจะต้องไม่บันทึกรหัสผ่านเก็บไว้ที่โต๊ะหรือเครื่องคอมพิวเตอร์ที่ใช้งาน

7. เมื่อมีการพิมพ์เอกสารความลับทางราชการออกผ่านทางเครื่องพิมพ์จะต้องรีบนำออกจากเครื่องพิมพ์ทันที

8. เมื่อได้รับเอกสารความลับทางราชการผ่านเครื่องโทรสารจะต้องรีบนำออกจากเครื่องโทรสารทันที

9. กรณีที่มีการแทงจำหน่ายอุปกรณ์คอมพิวเตอร์ หรือ อุปกรณ์จัดเก็บข้อมูลที่มีข้อมูลที่เป็นความลับทางราชการจะต้องดำเนินการทำลายข้อมูลนั้นก่อนทุกครั้ง โดยวิธีการทำลายข้อมูลจะต้องดำเนินการดังตารางนี้

	การทำลายข้อมูล		
ฮาร์ดดิสก์ (Hard Disk)	**ระดับที่ 1 ลบล้างข้อมูล (Clear)**	**ระดับที่ 2 (Purge)**	**ระดับที่ 3 (Destroy)**
ขั้นตอนการดำเนินงาน	ทำการเขียนข้อมูลทับข้อมูลเดิมและต้องได้รับอนุญาตจากผู้ที่มีสิทธิเท่านั้น	ทำการใช้เครื่องมือในการทำลายล้างข้อมูล เช่น โปรแกรม Secure Erase เป็นต้น	ทำการทุบเพื่อทำลาย
สื่อบันทึกข้อมูลแบบพกพา (USB Drives)	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ขั้นตอนการดำเนินงาน	ทำการเขียนข้อมูลทับข้อมูลเดิมและต้องได้รับอนุญาตจากผู้ที่มีสิทธิเท่านั้น	ทำการใช้เครื่องมือในการทำลายล้างข้อมูล เช่น โปรแกรม Secure Erase เป็นต้น	ทำการทุบเพื่อทำลาย
ซีดีรอม หรือ ดีวีดีรอม	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ขั้นตอนการดำเนินงาน	-	-	-
อุปกรณ์พกพา (cell PDA)	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ขั้นตอนการดำเนินงาน	ทำการล้างข้อมูลของผู้ใช้และข้อมูลการใช้งานทั้งหมดและรีเซตค่าไปยังค่าเริ่มต้นที่ออกจากโรงงาน	เหมือนระดับที่ 1	ทำการทุบเพื่อทำลาย
เครื่องถ่ายเอกสารหรือโทรสาร	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ขั้นตอนการดำเนินงาน	รีเซตตามบริษัทผู้ผลิต	เหมือนระดับที่ 1	-
อุปกรณ์เครือข่าย (Network Devices)	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ขั้นตอนการดำเนินงาน	ทำการรีเซตค่าไปยังค่าเริ่มต้นที่ออกจากโรงงาน	เหมือนระดับที่ 1	ทุบเพื่อทำลาย

หมายเหตุ ระดับที่ 1 สำหรับผู้ดูแลระบบของหน่วยงาน
ระดับที่ 2 และ ระดับที่ 3 สำหรับผู้ดูแลระบบของมหาวิทยาลัย เช่น ศูนย์เทคโนโลยีสารสนเทศ หรือ หน่วยงานที่ดูแลระบบของมหาวิทยาลัย

ผู้รับผิดชอบ: งานบริการวิชาการ งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

12. แนวปฏิบัติการบริหารจัดการสิทธิและการแบ่งแยกเครือข่าย

1. แบ่งแยกและควบคุมเครือข่ายอุปกรณ์ไฟร์วอลล์ (Firewall) และทำงานร่วมกันกับอุปกรณ์เครือข่ายสวิตช์ซึ่งสามารถกำหนดเครือข่ายเสมือน (VLAN) ได้

2. การจัดแบ่งเครือข่ายผู้ใช้งานภายในทำการจัดแบ่งตามภารกิจ กลุ่มงาน การใช้ทรัพยากรร่วมกัน และหน้าที่ โดยจำกัดการเข้าถึงข้ามส่วนงานหรือกลุ่มงาน เพื่อป้องกันข้อมูลรั่วไหล หรือการโจมตีในเครือข่าย

3. การใช้งานบนเครือข่ายหลักต้องมีการแบ่งแยกพื้นที่โซนการทำงานตามความเหมาะสม โดยอย่างน้อยให้เป็นส่วนๆ ดังนี้

3.1 โซนผู้ใช้งาน (Intranet)

3.2 โซนเครือข่ายไร้สาย (Wireless)

3.3 โซนเจ้าหน้าที่ดูแลระบบ (Administrator)

3.4 โซนเครื่องคอมพิวเตอร์แม่ข่ายให้บริการสาธารณะ (Public Server)

3.5 โซนเครื่องคอมแม่ข่ายโปรแกรมประยุกต์ เฉพาะงาน (Application Server)

3.6 โซนเครื่องคอมพิวเตอร์แม่ขายให้บริการเฉพะภายในกรม เท่านั้น (Internal Server)

3.7 โซนเครือข่ายส่วนขยายของมหาวิทยาลัย

3.8 โซนอาคารหรือพื้นที่วิทยาเขตของมหาวิทยาลัย

4. โซนผู้ใช้งานมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

4.1 สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

4.2 สามารถเข้าใช้งานบนระบบสารสนเทศภายในได้โดยไม่มีการจำกัดด้านเวลา

4.3 สามารถใช้งานอินเทอร์เน็ตได้ต่อเมื่อมีการ login โดยใช้ (iPASSPORT)เท่านั้น

5. โซนเครือข่ายไร้สาย มีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

5.1 สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

5.2 สามารถใช้งานระบบเครือข่ายได้ต่อเมื่อมีการ login โดยใช้(iPASSPORT ID) เท่านั้น

5.3 สิทธิในการเข้าใช้งานสามารถปรับเปลี่ยนได้ตามประกาศมหาวิทยาลัย โดยประกาศให้ทราบผ่านหน้าต่าง (Login) ระบบเครือข่ายไร้สาย

6. โซนเจ้าหน้าที่ภายนอก กำหนดให้เป็นกลุ่มของผู้รับจ้างดุแลระบบเครือข่ายของมหาวิทยาลัยโดยมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

6.1 ไม่สามารถเชื่อมต่อไปยังภายนอกโวนของตนเองเว้นแต่มีการขออนุญาตเป็นกรณีพิเศษ ซึ่งจะต้องได้รับความเห็นชอบจากศูนย์เทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

7. โซนเจ้าหน้าที่ดูแลระบบมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

7.1 สามารถเชื่อมต่อเข้าไปยังระบบเครือข่ายของมหาวิทยาลัยได้ทุกที่และตลอดเวลา

8. โซนเครื่องคอมพิวเตอร์แม่ข่ายโดยต้องมีการกำหนดระดับความสำคัญ และความต้องการเพื่อจำแนกเครื่องแม่ข่ายไปยังตำแหน่งที่เหมาะสม ไม่ว่าจะเป็นกลุ่มของเครื่องแม่ข่ายที่ให้บริการสาธารณะ ระบบโปรแกรมประยุกต์ และเครื่องแม่ข่ายที่ให้บริการเฉพาะภายในเท่านั้น

8.1 สามารถเชื่อมต่อจากโซนต่างๆ ของมหาวิทยาลัยที่ได้กำหนดไว้ เพื่อเข้ามาใช้บริการเครื่องคอมพิวเตอร์แม่
ข่าย

8.2 เครื่องคอมพิวเตอร์ภายนอกเครือข่ายจะต้องไม่สามารถติดต่อเข้ามายังเครื่องแม่ข่ายที่อยู่ในกลุ่มเพื่อให้บริการภายในเท่านั้น

8.3 เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถเรียกออกไปยังอินเทอร์เน็ตได้เว้นแต่มีเหตุจำเป็นที่จะต้องเชื่อมต่อเช่น การใช้งานดีเอ็นเอส (DNS) ของเครื่องคอมพิวเตอร์แม่ข่าย การปรับปรุงเรื่องไวรัส เป็นต้น

9. ศูนย์เทคโนโลยีสารสนเทศสามารถทักท้วง หรือไม่อนุญาตให้มีการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย หรือเครื่องคอมพิวเตอร์แม่ข่ายได้ หากตรวจพบความผิดปกติซึ่งอาจก่อให้เกิดความเสี่ยกาย หรือมีความไม่เหมาะสมกับระบบเครือข่ายหรือต่อมหาวิทยาลัย

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

13. แนวปฏิบัติการจัดการไฟร์วอลล์

1.ศูนย์เทคโนโลยีสารสนเทศมีหน้าที่ในการบริหารจัดการและกำหนดค่าใช้งานของอุปกรณ์รักษาความปลอดภัย (firewall) ส่วนกลางบนเครือข่ายบัวศรีของมหาวิทยาลัย

2. บริการต่างๆ จะถูกปฏิเสธทั้งหมด ยกเว้นแต่บริการที่ทางศูนย์เทคโนโลยีสารสนเทศเปิดให้บริการเท่านั้น

3. ก่อนการใช้งานอินเทอร์เน็ตทุกครั้ง ผู้ใช้งานจะต้องทำการล็อกอินโดยใช้(iPASSPORT ID)

4. การเปลี่ยนแปลงการกำหนดต่างๆ บนอุปกรณ์รักษาความปลอดภัยจะต้องดำเนินการโดยผู้ที่ได้รับมอบหมายเท่านั้น โดยทุกครั้งที่มีการเปลี่ยนแปลงต้องบันทึกข้อมูล และสำรองข้อมูลต่างๆ ไว้ก่อนเสมอ

5. การให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตที่เป็นการใช้งานพื้นฐานโปรแกรมทั่วไปเท่านั้น กรณีผู้ใช้ต้องการเชื่อมต่อผ่านพอร์ตอื่นนอกเหนือจากที่กำหนดไว้ต้องได้รับอนุญาตจากศูนย์เทคโนโลยีสารสนเทศก่อน

6. พอร์ตที่ใช้สำหรับตรวจสอบและการปรับแต่งระบบจะถูกปิดทั้งหมดและจะต้องเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

7. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายจะต้องกำหนดค่าการให้บริการที่จำเป็นต่อการให้บริการตามแบบฟอร์มขอเปิดใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น

8. เส้นทางการเชื่อมต่อระบบเครือข่ายจะต้องมีการควบคุมเพื่อป้องกันข้อมูลสารสนเทศที่มีความสำคัญสูง

9. ในกรณีตรวจพบว่าเครื่องคอมพิวเตอร์ลูกข่ายใดที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย หรือ มีการใช้งานอันจะก่อให้เกิดปัญหาต่อเครือข่าย ศูนย์เทคโนโลยีสารสนเทศขอสงวนสิทธิในการระงับ หรือ บล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายนั้นจนกว่าจะดำเนินการแก้ไขเสร็จสิ้น

10. ผู้ละเมิดนโยบายด้านความปลอดภัยของระบบเครือข่ายบัวศรีของมหาวิทยาลัยจะถูกระงับการใช้งานทันทีโดยมิต้องแจ้งให้ทราบล่วงหน้า

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

14. แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) ให้อยู่ในพื้นที่ใช้งานระบบเครือข่ายไร้สายของมหาวิทยาลัย โดยให้มีการรั่วไหลน้อยที่สุด

2. ผู้ดูแลระบบต้องทำการเปลี่ยนค่าเอสเอสไอดี (SSID หรือ Service Set Identifier) ตามที่ได้ถูกกำหนดเป็นค่าเริ่มต้นไว้ (default setting) โดยผู้ผลิต ทันทีที่นำอุปกรณ์กระจายสัญญาณมาติดตั้งใช้งาน

3. อุปกรณ์กระจายสัญญาณที่มีคุณสมบัติตามข้อกำหนดมาตรฐานของมหาวิทยาลัยจะต้องถูกติดตั้งระบบการยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่าย (iPASSPORT) ของมหาวิทยาลัย

4. กรณีอุปกรณ์กระจายสัญญาณที่จัดหาไม่สามารถติดตั้งระบบยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่าย (iPASSPORT) ข้อ 3 ได้นั้น ผู้ดูแลระบบจะต้องดำเนินการติดตั้งให้เป็นแบบบริดจ์ (bridge) เท่านั้นเพื่อให้ผู้ใช้งานยืนยันตัวตนผ่านระบบ (iPASSPORT) ของมหาวิทยาลัย

5. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งไฟร์วอลล์ (firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

6. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์ หรือ ฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยติดตามและบันทึกเหตุการณ์น่าสงสัยในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจพบความผิดปกติในการใช้งาน ผู้ดูแลระบบต้องรายงานต่อผู้บริหารของหน่วยงานให้ทราบทันที

7. ผู้ดูแลระบบต้องควบคุมดูแลมิให้บุคคล หรือหน่วยงานภายนอกที่มิได้รับอนุญาตเข้าใช้บริการระบบเครือข่ายไร้สายของมหาวิทยาลัยเพื่อผ่านเข้าสู้ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในของมหาวิทยาลัย

8. กรณีอุปกรณ์กระจายสัญญาณ (access point) ส่วนบุคคล จะต้องทำการลงทะเบียน MAC address ผู้รับผิดชอบ และหมายเลข (Serial Number) กับศูนย์เทคโนโลยีสารสนเทศเพื่อสามารถตรวจสอบผู้รับผิดชอบอุปกณ์นั้นได้

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

15. แนวปฏิบัติในการติดตั้งสวิซ์และฮับ

1. การเชื่อมต่ออุปกรณ์สวิตซ์ (switch) หรือ ฮับ (hub) หรืออุปกรณ์เชื่อมต่ออื่นใดที่นำมาพ่วงต่อกับระบบเครือข่ายของมหาวิทยาลัย จะต้องได้รับอนุญาตศูนย์เทคโนโลยีสารสนเทศก่อนเท่านั้น

2. การเดินสายยูทีพี (UTP) หรือดำเนินการติดตั้งยูทีพี บนอุปกรณ์สวิตซ์ หรือ ฮับในตู้แร็คที่ศูนย์เทคโนโลยีสารสนเทศดูแล จะต้องแจ้งศูนย์เทคโนโลยีสารสนเทศก่อนทุกครั้ง

3. หมายเลขไอพีที่ติดตั้งบนอุปกณ์สวิตซ์ จะต้องเป็นหมายเลขที่กำหนดให้โดยศูนย์เทคโนโลยีสารสนเทศเท่านั้น ห้ามดำเนินการโดยมิได้รับอนุญาต

4. อุปกณ์สวิตซ์ที่ติดตั้งจะต้องสามารถตรวจสอบผ่านโปรโตคอลเอสเอ็นเอ็มพี (SNMP) เพื่อศูนย์เทคโนโลยีสารสนเทศสามารถตรวจสอบการทำงานของอุปกณ์นั้นได้

5. อุปกรณ์สวิตซ์ที่ติดตั้งจะต้องลงทะเบียน MAC address หน่วยงานผู้รับผิดชอบ และหมายเลขครุภัณฑ์กับศูนย์เทคโนโลยีสารสนเทศเพื่อสามารถตรวจสอบผู้รับผิดชอบอุปกณ์นั้นได้

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

16. แนวปฏิบัติการควบคุมการเข้าออกห้องคอมพิวเตอร์กลาง

1. ผู้ดูแลระบบต้องกำหนดมาตรการการควบคุมและป้องกันบุคคลภายนอกในการเข้าถึงห้องคอมพิวเตอร์กลาง (data center) โดยจะต้องปฏิบัติอย่างน้อยดังนี้

1.1 ผู้เข้าออกใช้ห้องต้องขออนุญาตโดยระบุถึงกิจกรรม หรือความจำเป็นในการเข้าใช้

1.2 ผู้ขอเข้าใช้ห้องต้องปฏิบัติตามกฎระเบียบของศูนย์เทคโนโลยีสารสนเทศอย่างเคร่งครัด

1.3 ผู้ขอเข้าใช้ห้องต้องไม่ทำการใดๆ อันอาจก่อให้เกิดความเสียหายต่อทรัพย์สินของมหาวิทยาลัย

1.4 ผู้ขอเข้าใช้ห้องต้องคิดบัตรแสดงตนให้ชัดเจน พร้อมทั้งลงบันทึกรายละเอียดของการเข้าใช้ เวลาเข้า เวลาออก รวมทั้งกิจกรรมที่ดำเนินการ

1.5 กรณีที่มีการใช้งานนอกเวลาทำการ ผู้ขอเข้าใช้ห้องต้องได้รับอนุญาตจากผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและเพื่อการจัดเตรียมเจ้าหน้าที่ของศูนย์เทคโนโลยีสารสนเทศในการอำนวยความสะดวกสำหรับการปฏิบัติงานดังกล่าว

1.6 การเข้าดำเนินการกับระบบที่สำคัญจำเป็นต้องมีผู้รับผิดชอบระบบนั้นอยู่กำกับดูแลการปฏิบัติงานเสมอและหากมีการกระทำใดๆ ที่อาจส่งผลต่อระบบจะต้องได้รับความเห็นชอบจากเจ้าของระบบนั้นก่อน

1.7 ต้องจัดให้มีพื้นที่สำหรับการส่งมอบ หรือขนย้ายอุปกรณ์ต่างๆ เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ห้องคอมพิวเตอร์กลาง โดยไม่จำเป็น

2. ผู้ดูแลระบบต้องควบคุมดูแลสภาพแวดล้อมของระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตรวจสอบการทำงานของระบบที่ใช้ในการควบคุมสภาพแวดล้อมเพื่อให้สามารถใช้งานได้ตามปกติ โดยแบ่งออกเป็น 3 ระบบดังนี้

2.1 ระบบตรวจจับควัน (smoke detector system) เพื่อป้องกันการเกิดอัคคีภัยของห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2.2 ระบบเครื่องปรับอากาศ (air conditioning system) เพื่อป้องกันการเกิดความชื้นจากละอองน้ำในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2.3 ระบบไฟฟ้าสำรองฉุกเฉิน (UPS) เพื่อป้องกันอุปกรณ์ และเครื่องคอมพิวเตอร์แม่ข่ายหยุดทำงาน

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

17. แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

1. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (User) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของอุปกรณ์คอมพิวเตอร์

๒. ผู้ใช้บริการ (ผู้ใช้งาน) ต้องไม่อนุญาตให้ผู้ใช้งานอื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนเพื่อเข้าใช้งานระบบปฏิบัติการของอุปกรณ์คอมพิวเตอร์

๓. ผู้ใช้บริการต้องตั้งค่าการพักหน้าจอและต้องเช็ครหัสผ่าน(Password)ผู้ใช้งานเมื่อเปิดใช้งานระบบปฏิบัติการ

๔. ผู้ใช้ต้องทำการออกจากระบบระบบปฏิบัติการของอุปกรณ์คอมพิวเตอร์ (Logout) ทุกครั้งที่เลิกใช้งานระบบ

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

18. แนวปฏิบัติการพัฒนาระบบสารสนเทศ

1. การออกแบบระบบสารสนเทศต้องคำนึงถึงความต้องการในการใช้งานและความต้องการของผู้ใช้

2. การวิเคราะห์และออกแบบระบบสารสนเทศ ต้องคำนึงถึงความปลอดภัยในการเข้าถึงและจัดเก็บข้อมูล โดยระบบสารสนเทศหลักที่มีความสำคัญ ต้องมีการเข้ารหัสของการสื่อสารระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายด้วยมาตรฐานใบรับรอง (SSl)

3. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องมีกระบวนการระบุพิสูจน์ตัวตนตามนโยบาย และแนวปฏิบัติบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

4. ระบบสารสนเทศที่พัฒนาขึ้นต้องสามารถแบ่งแยกระดับของผู้ใช้งานได้ เช่น ผู้ใช้งานทั่วไป เจ้าหน้าที่ดูแลระบบ ผู้เยี่ยมชม เป็นต้น

5.การแบ่งแยกระดับของผู้ใช้งานต้องสามารถกำหนดสิทธิการเข้าใช้งานได้ชัดเจน เช่น สามารถมองเห็นเมนูใดได้บ้าง สามารถแก้ไขข้อมูลใดได้บ้าง สามารถลบข้อมูลใดได้บ้าง เป็นต้น

6. ต้องมีการจัดเก็บข้อมูลการเข้าใช้ระบบ (log) โดยมีรายละเอียดดังนี้เป็นอย่างน้อย เช่น (1) วันที่และเวลา (2) ผู้ใช้งาน

7. กำหนดให้การตัดการเชื่อมต่อระหว่างระบบกับผู้ใช้งานได้โดยอัตโนมัติ (Session Timeout) หากผู้ใช้งานมิได้มีการทำกิจกรรมใดๆ กับระบบนั้นเป็นเวลาเกินกว่า 10 นาที หรือตามความเหมาะสม

8. ระบบสารสนเทศทีมีความสำคัญสูงจะต้องมีการจำกัดระยะเวลาการเชื่อมต่อโดยให้มีการเชื่อมต่อครั้งละไม่เกิน 2 ชั่วโมง

9. ในการพัฒนาระบบ การทดสอบระบบ ต้องพัฒนาบนเครื่องคอมพิวเตอร์ที่จัดเตรียมไว้สำหรับการพัฒนาเท่านั้น

10. ผู้พัฒนาระบบต้องตรวจสอบระบบตั้งแต่การนำข้อมูลเข้า กระบวนการประมวลผล และตรวจสอบผลลัพธ์จากการประมวลผลทุกครั้งก่อนนำระบบขึ้นใช้งานจริง

11. ผู้พัฒนาระบบต้องทำการทดสอบระบบตั้งแต่การนำข้อมูลเข้า กระบวนการประมวลผล และตรวจสอบผลลัพธ์จากการประมวลผลทุกครั้งก่อนนำระบบขึ้นใช้งานจริง

12. ระบบที่พัฒนาขึ้นต้องมีการควบคุมเวอร์ชั่นของโปรมแกรม เพื่อใช้ในการควบคุมเปลี่ยนแปลงหรือ แก้ไขและต้องมีการทดสอบการทำงานทุกครั้งหลังการเปลี่ยนแปลง

13. มีการควบคุมการเข้าถึงซอร์สโค้ดของระบบ โดยจะสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้น

14. ต้องมีการปรับปรุงซอฟต์แวร์อย่างสม่ำเสมอหรือตามคำแนะนำของผู้ผลิตซอฟต์แวร์เพื่อป้องกันไม่ให้เกิดช่องโหว่ และต้องดำเนินการติดตั้งกับเครื่องทดสอบก่อนเท่านั้น จึงดำเนินการกับเครื่องที่ใช้งานหลัก

ผู้รับผิดชอบ :ฝ่ายระบบสารสนเทศ ศูนย์เทคโนโลยีสารสนเทศ

19. แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

1. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยมิได้รับอนุญาต

1.3 ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

1.5 ความเสี่ยงที่เกิดจากการลักลอบให้รหัสผ่านของผู้อื่นมิได้รับอนุญาต

2. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น โดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบในด้าน

2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

3. กำหนดมาตรการจัดการความเสี่ยง

3.1 ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT contingency plan)

3.2 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ 1 ครั้ง

3.3 การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศ (internal IT auditor) หรือโดยผู้ตรวจสอบด้านความมั่นคงปลอดภัยจากภายนอก (external IT auditor)

ผู้รับผิดชอบ : ฝ่ายงานบิหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

20. แนวปฏิบัติการสำรองข้อมูล

1. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

3. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างน้อยปีละ 2 ครั้ง

ผู้รับผิดชอบ :ฝ่ายงานบิหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

21. แนวปฏิบัติการจัดทำระบบสำรออง

1. พิจารณาคัดเลือกระบบสำรองที่เหมาะสมกับมหาวิทยาลัยให้พร้อมใช้งานอยู่เสมอ

2. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

3. กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูง และจำเป็นต้องมีแผนรับมือ

4. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลแต่ละระบบสารสนเทศ และระบบสำรองข้อมูล

5. ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญติดขัด หรือไม่สามารถใช้งานได้ อันเป็นผลจากภัยพิบัติที่ได้กำหนดไว้

6. กำหนดกระวนการรายงานผลต่อผู้ดูแลรับผิดชอบในแต่ละระดับชั้น เมื่อเกิดภัยพิบัติ

7.ทดสอบ ประเมิน และปรับปรุงแผนรับมือเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีล่ะ 1 ครั้ง

ผู้รับผิดชอบ :ฝ่ายงานบิหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

22. แนวปฏิบัติการจัดการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

1. ผู้ดูแลระบบจะต้องรายงานการเกิดปัญหาและความเสียหายต่อระบบแก่ผู้อำนวยการเป็นอันดับที่1เพื่อรับทราบปัญหาที่เกิดขึ้น

2. ผู้ดูแลระบบต้องดำเนินการตรวจสอบการใช้งานระบบเครือข่ายโดยใช้เครื่องมือในกาตรวจสอบแลจัดเก็บข้อมูลการให้บริการเครือข่าย

3. เมื่อมีเหตุการณ์ผิดปกติซึ่งทำให้ไม่สามารถให้บริการได้ หรือการใช้งานไม่สะดวกจะต้องดำเนินการแจ้งให้ผู้ใช้ทราบและจัดเก็บลงระบบรายงานปัญหาเครือข่าย

4. ผู้ดูแลระบบจะต้องเร่งดำเนินการแก้ไขปัญหาให้สามารถกลับมาใช้งานได้ตามปกติ ในกรณีที่ไม่สามารถใช้งานได้ตามช่วงเวลาดังกล่าวจะต้องดำเนินการแจ้งเป็นลำดับขั้นดังต่อไปนี้

5. หลังจากใช้งานไม่ได้ 10 นาที ต้องดำเนินการประกาศแจ้งที่หน้าประชาสัมพันธ์ข่าวประกาศเครือข่ายและแจ้งหัวหน้าฝ่ายที่เกี่ยวข้อง

6. หลังจากใช้งานไม่ได้ 3 ชั่วโมง ต้องดำเนินการแจ้งรองผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาแนวทางแก้ไขปัญหา

7. หลังจากใช้งานไม่ได้ 1 วัน ต้องดำเนินการแจ้งผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศเพื่อพิจารณาแนวทางการแก้ไขปัญหา

8. หลังจากใช้งานไม่ได้ 2 วัน ต้องดำเนินการแจ้งมหาวิทยาลัยเพื่อพิจารณาแนวทางแก้ไขปัญหา

9. เมื่อดำเนินการแก้ไขเสร็จสิ้น ต้องทำการรายงานผลการดำเนินการในระบบข่าวประกาศเครือข่าย และจัดทำคู่มือแนวปฏิบัติและวิธีการแก้ไขปัญหา

10. จัดรวบรวมข้อมูลรายงานการเกิดปัญหาประจำปีเพื่อเป็นข้อมูลในการปรับปรุงระบบ

23. แนวปฏิบัติของผู้ดูแลระบบ

1. ผู้ดูแลระบบ มีอำนาจหน้าที่ ดังต่อไปนี้

1.1 ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้บริการผู้นั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกัน หรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบ พิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

1.2 ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

1.3 ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย

1.4 ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

1.5 ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

1.6 ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน รวมทั้งการเก็บรักษารหัสผ่าน

1.7 ไม่ใช้อำนาจหน้าที่ของตนเองในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

1.8 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

1.9 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบโดยไม่มีเหตุผลอันสมควร

1.10 เมื่อผู้ดูแลระบบพ้นจากหน้าที่จะต้องคืนสินทรัพย์ของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

1.11 รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนการสำรองข้อมูล แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูลและการทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

2. ผู้ดูแลระบบจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่การใช้บริการสิ้นสุด การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

2.1 เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

2.2 มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน(Internal IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

2.3 ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

2.4 เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

ผู้รับผิดชอบ :ฝ่ายงานบิหาร งานพัฒนาระบบสารสนเทศและเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

24. แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย

1.เครื่องคอมพิวเตอร์ภายในหน่วยงานทุกเครื่องต้องทำการอัพเดท (Update Patch) ของระบบปฏิบัติการเว็บบราวเซอร์ และโปรแกรมการใช้งานอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability)ที่เกิดขึ้นจากซอฟต์แวร์

2. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการติดตั้งโปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย (malware) รวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

3. ห้ามมิให้ผู้ใช้บริการทำการปิด หรือยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

4. หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย และต้องดำเนินการแจ้งศูนย์เทคโนโลยีสารสนเทศหรือผู้ที่เกี่ยวข้องดำเนินการแก้ไขก่อนที่จะเชื่อมต่อเข้าระบบเครือข่ายอีกครั้ง

5. ก่อนการใช้งานสื่อบันทึกแบบพกพา ต้องมีการตรวจสอบเพื่อป้องกันและกำจัดโปรมแกรมประสงค์ร้าย

6. ผู้ใช้บริการต้องทำการตรวจสอบไฟล์ที่สามารถประมวลผลได้ (เช่น .exe .com .bat .vbs .scr .pif .hta) ผ่านทางโปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย ก่อนทำการเปิดทุกครั้ง

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายปฏิบัติการและบริการ ศูนย์เทคโนโลยีสารสนเทศ

25. แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต

1. ห้ามผู้ใช้งานปฏิบัติการใดๆ ที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดี โดยหากมีการกระทำดังกล่าวเกิดขึ้นถือเป็นความรับผิดชอบของผู้ใช้งาน ซึ่งอยู่นอกเหนือจากความรับผิดชอบของมหาวิทยาลัย

2. ห้ามผู้ใช้งานปฏิบัติการใดๆ ที่ไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

3. ผู้ใช้งานจะต้องไม่ละเมิดสิทธิผู้อื่น โดยการดัดแปลงแก้ไขข้อมูล โดยมิได้รับอนุญาต

4. ห้ามผู้ใช้งานใช้งานในทางที่ไม่เหมาะสม สร้างความเสียหายให้กับผู้อื่น หรือ การใช้ภาษาที่ไมสุภาพ หรือ กระทำใดๆ ที่จะทำให้ผู้อื่นเสียหาย

5. ห้ามผู้ใช้งานเข้าใช้งานระบบโดยมิได้รับอนุญาต การบุกรุก หรือพยายามเข้าใช้งานโดยมิได้รับอนุญาตถือเป็นความผิดตามระเบียบของมหาวิทยาลัย

6. มหาวิทยาลัยจะไม่รับประกันคุณภาพการเก็บข้อมูล การรับส่งข้อมูลข่าวสาร หรือการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมด และจะไม่รับผิดชอบเสียหายอันเนื่องมาจากวงจรสื่อสารชำรุด จานแม่เหล็กชำรุด หรือความล่าช้าที่เกิดขึ้นในการใช้งาน

7. มหาวิทยาลัยขอสงวนสิทธิ์ในการยกเลิก หรือระงับการเชื่อมต่อ ในกรณีตรวจสอบพบการพยายามบุกรุกหรือทำให้ระบบของมหาวิทยาลัยมีประสิทธิภาพลดลง

8. ผู้ใช้งานต้องทำความเข้าใจและยอมรับระเบียบปฏิบัติที่มหาวิทยาลัยกำหนดขึ้น โดยจะอ้างว่าไม่ทราบระเบียบปฏิบัตินั้นๆ มิได้

9. บัญชีผู้ใช้งาน ((iPASSPORT ID)) นั้นมหาวิทยาลัยมอบให้เพื่อการใช้งานตามภารกิจของมหาวิทยาลัยเท่านั้น และห้ามมิให้ผู้อื่นที่ไม่ได้เกี่ยวข้องกับมหาวิทยาลัยนำไปใช้

10. ถ้าเกิดความเสียหายขึ้นจากการใช้งานบัญชีผู้ใช้งาน ผู้เป็นเจ้าของต้องรับผิดชอบกับความเสียหายที่เกิดขึ้นเว้นแต่พิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ และฝ่ายปฏิบัติการและบริการ ศูนย์เทคโนโลยีสารสนเทศ

26. แนวทางปฏิบัติการบริหารจัดการระบบจดหมายอิเล็กทรอนิกส์

1. เครื่องคอมพิวเตอร์ที่เปิดให้บริการระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องเป็นเครื่องให้บริการของมหาวิทยาลัยที่ดูแลบริหารจัดโดยศูนย์เทคโนโลยีสารสนเทศเท่านั้น

2. ผู้ดูแลระบบต้องจัดให้มีระบบในการตรวจสอบจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ผ่านเข้าออกระบบบริการอิเล็กทรอนิกส์หลักของมหาวิทยาลัยเพื่อป้องกันปัญหาไวรัสและสแปม

3. การสำรองข้อมูล (e-mail) ส่วนบุคคลให้ผู้ใช้ดำเนินการสำรองโดยให้ใช้ Application ของมหาวิทยาลัยภายใต้โดเมน User@psru.ac.th (Google Cloud Platform)ที่ทางมหาวิทยาลัยจัดเตรียมไว้ในการเก็บข้อมูล (e-mail) ส่วนบุคคล

3. การสำรองข้อมูล (e-mail) หน่วยงาน ภายในมหาวิทยาลัยดำเนินการสำรองโดยให้ใช้ Application ของมหาวิทยาลัยภายใต้โดเมน @psru.ac.th ใช้งาน (Google Cloud Platform) ที่ทางมหาวิทยาลัยจัดเตรียมไว้ในการเก็บข้อมูล (e-mail) หน่วยงาน

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

27. แนวปฏิบัติการใช้บริการจดหมายอิเล็กทรอนิกส์

1. ผู้ใช้งานมีหน้าที่รับผิดชอบบัญชีบัวศรีที่ได้รับจากมหาวิทยาลัย ต้องระวังมิให้ผู้อื่นสามารถเข้าถึงรหัสผ่านเพื่อใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ของตนโดยมิชอบ

2. ผู้ใช้งานต้องรักษารหัสผ่านและไม่อนุญาตให้ผู้อื่นใช้รหัสผ่านของตน

3. ผู้ใช้งานพึ่งทราบว่าผู้ดูแลระบบไม่มีสิทธิถาม หรือร้องขอใช้ให้เปิดเผยรหัสผ่านเพื่อเข้าใช้งานบัญชีบัวศรี

4. ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

5. ห้ามเผยแพร่ หรือส่งต่อจดหมายลูกโซ่

6. ห้ามเผยแพร่ข้อมูลที่เป็นความลับของมหาวิทยาลัย

7. ห้ามปลอมแปลง หรือดัดแปลงชื่อผู้ส่งเพื่อให้บุคคลอื่นเข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นมาจากบุคคลอื่น

8. ห้ามปกปิด หรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

9. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่เผยแพร่ ข้อความ ภาพ วีดีโอ หรือเสียงที่ให้ร้ายต่อบุคคลหรือกลุ่มบุคคลหรือในลักษณะที่หยาบคาย หรือลามก อนาจาร

10. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรม หรือรหัสผ่านสำหรับการเข้าถึงโปรแกรมในลักษณะที่เป็นการละเมิดลิขสิทธิ์

11. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้ที่ไม่ต้องการ

12. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายไวรัส หรือโปรแกรมที่เป็นอันตรายกับความมั่นคงปลอดภัยของระบบเครือข่าย

13. ห้ามมิให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ที่ได้รับจากมหาวิทยาลัยไปสมัครสมาชิกตามเว็บไซต์ต่างๆ เพื่อประโยชน์ส่วนตัน และไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

14. เมื่อได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

15. ผู้ใช้งานเปลี่ยนรหัสผ่านทุกๆ 3-6 เดือน

16. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงบันทึกออก (Logout) ทุกครั้ง

17. ผู้ใช้งานหลีกเลี่ยงการแนบไฟล์ขนาดใหญ่ โดยมีขนาดไม่เกิน 20 MB

18. ห้ามส่งข้อมูลที่เป็นความลับผ่านทางจดหมายอิเล็กทรอนิกส์โดยมิได้เข้ารหัสลับ

19. การสำรองข้อมูลส่วนบุคคล มหาวิทยาลัยดำเนินการจัดเตรียม Application ภายใต้โดเมน @psru.ac.th โดยใช้งาน (Google Cloud Platform) ในการสำรองข้อมูลส่วนบุคคลโดยผู้ใช้ต้องดำเนินการด้วยตนเอง

20. มหาวิทยาลัยขอสงวนลิขสิทธิ์ในการระงับการใช้งานบัญชีผู้ใช้ได้ทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากผู้ดูแลระบบตรวจพบความผิดปกติซึ่งอาจจะเกิดจากบัญชีผู้ใช้นั้น

ผู้รับผิดชอบ :ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ศูนย์เทคโนโลยีสารสนเทศ

28. ข้อกำหนดการจัดการฐานข้อมูลและการควบคุมการเข้าถึงข้อมูล

โดยกำหนดให้ใช้งานฐานข้อมูลกลาง iPASSPORT เป็นระบบจัดการผู้ใช้งานรวมของมหาวิทยาลัยราชภัฏพิบูลสงคราม มีรายละเอียดดังต่อไปนี้

1. กลุ่มผู้ใช้งานจัดแบ่งเป็นกลุ่มดังนี้
   1.1 นักศึกษา
   1.2 เจ้าหน้าที่

1.3 อาจารย์

1.4 ผู้บริหาร

1.5 ผู้ดูแลระบบ

1.6 ผู้ใช้งานทั่วไป

2. การทำงานและสิทธิของกลุ่มผู้ใช้งาน

ตารางการให้สิทธิ์กลุ่มผู้ใช้งาน

การทำงาน	**นักศึกษา**	**เจ้าหน้าที่**	**อาจารย์**	**ผู้บริหาร**	**ผู้ดูแลระบบ**	**ผู้ใช้งานทั่วไป**
การเข้าสู่ระบบ	P	P	P	P	P	N
ตารางเรียน	R	R	R	R	R	R
ข้อมูลการเงิน	N	R/W	N	R	R	N
ข้อมูลทะเบียนนักศึกษา	R/W	R/W	R/W	R/W	R	N
ข้อมูลเจ้าหน้าที่	N	R/W	N	R/W	R	N
ข้อมูลอาจารย์	N	N	R/W	R/W	R	N
ข้อมูลผู้บริหาร	N	N	N	R/W	R	N
ข้อมูลผู้ดูแลระบบ	N	N	N	R/W	R/W	N
ข้อมูลผู้ใช้งานทั่วไป	R	R	N	R/W	R/W	R
หน้ารายงานผล(Report)						
-รายงานผลการเรียน	R	R/W	R/W	R	R/W	R
-ประวัติอาจารย์	R	R/W	R/W	R	R/W	R
-ตารางเวลาผู้บริหาร	N	R	R	R/W	R	R

หมายเหตุ : สิทธ์การใช้งาน ข้อกำหนดดังนี้

P = Password ใช้งานรหัสผ่านในการเข้าถึง

R = Read อ่าน

W = Write เขียน

G = Grant มอบสิทธิ์

N = No access ไม่มีสิทธิ์

R/W = สิทธ์เฉพาะเจ้าหน้าที่หน่วยงานที่รับผิดชอบ

3. การเป็นสมาชิกและถอดถอนสิทธิ์ให้เป็นไปตามนโยบายความมั่นคงปลอดภัยของสารสนเทศและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ เพื่อเป็นมาตรฐานในการจัดการผู้ใช้งาน

ผู้รับผิดชอบ : ศูนย์เทคโนโลยีสารสนเทศ

29. กำหนดความรับผิดชอบควบคุมและติดตาม ส่งเสริม ประเมินผลการปฏิบัติให้เป็นไปตามนโยบายสารสนเทศ ให้ศูนย์เทคโนโลยีสารสนเทศเป็นผู้ดำเนินการ โดยการแต่งตั้งคณะทำงานโดยผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศ

ผู้รับผิดชอบ : ศูนย์เทคโนโลยีสารสนเทศ

30. กำหนดความรับผิดชอบด้านความเสียหาย กรณีระบบเทคโนโลยีสารสนเทศ และการสื่อสาร หรือข้อมูลสารสนเทศของมหาวิทยาลัยเกิดความเสียหาย หรือเกิดอันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบาย และแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดให้ผู้บริหารระดับสูงสุดของมหาวิทยาลัยโดยตำแหน่งเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ผู้รับผิดชอบ : มหาวิทยาลัยราชภัฏพิบูลสงคราม