นโยบายความปลอดภัยสารสนเทศ
มหาวิทยาลัยราชภัฏพิบูลสงคราม

1. นิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

1.1. “มหาวิทยาลัย” หมายถึง มหาวิทยาลัยราชภัฏพิบูลสงคราม

1.2. “ศูนย์ IT” หมายถึง ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัย

1.3. “ผู้อำนวยการ” หมายถึง ผู้อำนวยการ ศูนย์ IT

1.4. “สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของมหาวิทยาลัย ภายใต้การกำกับดูแลของศูนย์ IT

1.5. “ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัย ภายใต้การกำกับดูแลของศูนย์ IT

1.6. “พนักงาน” หมายถึง ข้าราชการ พนักงานราชการ พนักงานมหาวิทยาลัย พนักงานประจำตามสัญญา ลูกจ้าง ของมหาวิทยาลัย ที่สังกัดศูนย์ IT

1.7. “ผู้ดูแลระบบ” หมายถึง พนักงานที่ผู้รับผิดชอบด้านการให้บริการระบบเครือข่าย ภายใต้การกำกับดูแลของศูนย์ IT

1.8. “หน่วยงาน” หมายถึง คณะ สำนัก กอง ศูนย์ ภายใต้การกำกับดูแลของมหาวิทยาลัย

1.9. “ผู้พัฒนาระบบ” หมายถึง พนักงานที่ผู้รับผิดชอบด้านการพัฒนาระบบสารสนเทศให้กับศูนย์ IT และหน่วยงาน ของมหาวิทยาลัย

1.10. “ผู้ใช้งาน” หมายถึง ข้าราชการ ผู้บริหาร พนักงาน เจ้าหน้าที่ ลูกจ้าง นักศึกษา ของมหาวิทยาลัย และ รวมถึงบุคคลอื่นที่มหาวิทยาลัยอนุญาตให้ใช้ระบบคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย

1.11. “บุคคลากร” หมายถึง ข้าราชการ ผู้บริหาร พนักงาน เจ้าหน้าที่ ลูกจ้าง ของมหาวิทยาลัย

1.12. “สิทธิของผู้ใช้งาน” หมายถึง สิทธิการใช้งานทั่วไป สิทธิการเข้าถึง สิทธิการใช้งานอ่านเขียนข้อมูล สิทธิจำเพาะเครือข่ายหรือฐานข้อมูล และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

1.13. “ความมั่นคงปลอดภัยของสารสนเทศ” หมายถึง การธำรงไว้ซึ่งความลับ ความถูกต้องครบถ้วน ความถูกต้องแท้จริง ความรับผิดชอบ การห้ามปฏิเสธความรับผิดชอบ ความหน้าชื้อถือ และสภาพพร้อมใช้งานของระบบสารสนเทศ

1.14. “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

1.15. “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่ายที่แสดงให้เป็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

1.16. “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

1.17. ความเสียง หมายถึง โอกาสของสินทรัพย์สารสนเทศถูกละเมิดความปลอดภัย

1.18. ผู้ใช้ iPASSPORT (User ID iPASSPORT) หมายถึง ชื่อและรหัสบัญชีผู้ใช้งานเพื่อใช้ในการพิสูจน์ตัวตนก่อนการเข้าใช้งานเครือข่ายและบริการระบบสารสนเทศของมหาวิทยาลัยและรวมถึงสิทธิของผู้ใช้งานระบบต่างๆ

2. บททั่วไป

2.1. วัตถุประสงค์ของนโยบายความปลอดภัยสารสนเทศนี้ถูกจัดทำขึ้นเพื่อให้การบริหารและการรักษาความปลอดภัยที่เกี่ยวกับสารสนเทศของมหาวิทยาลัยสามารถดำเนินการได้และเพื่อให้บุคลากรและนักศึกษาตระหนักถึงความสำคัญในเรื่องความมั่นคงปลอดภัยของสารสนเทศ โดยแต่งตั้งคณะกรรมการจัดทำร่างข้อกำหนดด้านความปลอดภัยของสารสนเทศบนระบบเครือข่ายซึ่งนโยบายฉบับนี้จะถูกปรับปรุงทบทวนให้มีความทันอย่างน้อยปีละครั้ง และดำเนินการประกาศให้ผู้ที่เกี่ยวข้องทราบที่ http://www.psru.ac.th/it_security/

2.2. นโยบายความปลอดภัยสารสนเทศ ต้องได้รับการจัดทำเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้อำนวยการ และต้องเผยแพร่ให้ผู้ใช้งานทุกคนทราบ

2.3. นโยบายความปลอดภัยสารสนเทศประกอบด้วย ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยให้เป็นไปตามแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม พ.ศ. 2556 ตามที่แนบท้ายประกาศนี้

3. ความรับผิดชอบระบบสารสนเทศ

3.1. อธิการบดีต้องเป็นผู้ลงนามอนุมัติประกาศใช้นโยบายความปลอดภัยสารสนเทศ

3.2. อธิการบดีออกคำสั่งแต่งตั้งคณะทำงานเพื่อทบทวนนโยบายให้ให้ทันสมัย และแต่งตั้งคณะทำงานต่างๆ อย่างน้อยปีละครั้ง

3.3. อธิการบดีต้องเป็นผู้ผลักดันให้พนักงานทุกคนตระหนักถึงความสำคัญในการรักษาความปลอดภัยของทรัพย์สินของศูนย์ IT

3.4. อธิการบดีการต้องเป็นผู้ผลักดันให้พนักงานของศูนย์ IT ทุกคนปฏิบัติตามนโยบายความปลอดภัยสารสนเทศและตามกฎหมาย

3.5. อธิการบดีต้องให้การสนับสนุนด้านทรัพยากรต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบเครือข่ายมีความปลอดภัยและสอดคล้องกับนโยบายฉบับนี้

3.6. สำหรับผู้บริหาร ผู้บริหารของทุกหน่วยงานต้องกำกับดูแลให้นักศึกษา และบุคลากรได้ตระหนักถึงความสำคัญของความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัย

3.7. สำหรับนักศึกษาและบุคลากร นักศึกษาและบุคลากรทุกคนต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวปฏิบัติของมหาวิทยาลัยและต้องรายงานต่อหาวิทยาลัยเมื่อเกิดปัญหาข้อผิดพลาดที่เกี่ยวกับความมั่นคงปลอดภัยของสารสนเทศ

3.8. สำหรับผู้พัฒนาระบบและผู้ดูแลระบบ ผู้พัฒนาระบบและผู้ดูแลระบบต้องตระหนักถึงความมั่นคงปลอดภัยของสารสนเทศ โดยผู้พัฒนาระบบและผู้ดูแลระบบต้องมีภารงานและความรับผิดชอบในการจัดการระบบสารสนเทศ โดยต้องผ่านการพิจารณาและได้รับคำแนะนำจากผู้บริหารเทคโนโลยีระดับสูง หรือผู้อำนวยการ

3.9. สำหรับบุคคลทั่วไปผู้ใช้งาน ผู้ใช้งานที่มีสิทธิในการเข้าถึงข้อมูลสารสนเทศ หรือทรัพยากรด้านสารสนเทศ ต้องรับผิดชอบในการปฏิบัติตามนโยบายและแนวทางปฏิบัติของมหาวิทยาลัย ใช้งานตามสิทธิที่ได้รับอนุญาต และต้องรับผิดชอบในการไม่เปิดเผยข้อมูลความลับของมหาวิทยาลัยโดยไม่ได้รับอนุญาต

4. โครงสร้างความปลอดภัยของศูนย์ IT

4.1. ศูนย์ IT ต้องมีคำสั่งแต่งตั้งคณะกรรมการจัดทำร่างข้อกำหนดด้านความปลอดภัยของข้อมูลสารสนเทศบนระบบเครือข่ายที่ผ่านการลงนามโดยผู้อำนวยการ โดยคณะกรรมการชุดนี้มีหน้าที่หลักในการร่างข้อกำหนดด้านความปลอดภัยสารสนเทศ และควบคุมพนักงานรวมไปถึงผู้ใช้งานให้ปฏิบัติตามนโยบายความปลอดภัยสารสนเทศฉบับนี้

4.2. กองบริหารงานบุคคลต้องจัดให้มีการลงนามข้อตกลงระหว่างผู้ใช้งานและศูนย์ IT ว่าจะไม่เปิดเผยความลับของศูนย์ IT

4.3. ศูนย์ IT ควรมีรายชื่อสำหรับติดต่อประสานงานด้านความมั่นคงปลอดภัย เช่น ผู้ให้บริการอินเทอร์เน็ต ศูนย์ประสานงานด้านความมั่นคงปลอดภัยสารสนเทศ เป็นต้น เพื่อให้เกิดความรวดเร็วในการแก้ไขปัญหา เมื่อมีเหตุการณ์ละเมิดความปลอดภัยสารสนเทศ

4.4. หัวหน้าผู้ดูแลระบบต้องประเมินความเสี่ยงอันเกิดจากการเข้าถึงระบบเครือข่ายโดยบุคคลภายนอก และมีมาตรการรองรับหรือแก้ไขที่ชัดเจน เป็นระยะ ๆ ตามที่กำหนด

4.5. ผู้ดูแลระบบต้องแจ้งนโยบายในการเข้าใช้งานระบบเครือข่าย และขั้นตอนปฏิบัติการเข้าใช้งานห้องควบคุมระบบเครือข่ายให้กับผู้ใช้งานและบุคคลภายนอกทราบก่อนอนุมัติให้ใช้งาน

5. การบริหารจัดการทรัพย์สินของศูนย์ IT

5.1. ศูนย์ IT ต้องจัดทำบัญชีทรัพย์สินระบบเครือข่ายโดยระบุผู้รับผิดชอบในทรัพย์สินแต่ละชิ้นอย่างชัดเจน และจัดหมวดหมู่ทรัพย์สินตามระดับความสำคัญ ความลับ คุณค่า เพื่อหาวิธีการบริหารจัดการที่เหมาะสม

5.2. ผู้ดูแลระบบต้องบริหารจัดการทรัพย์สินที่แยกตามหมวดหมู่ไว้แล้ว เพื่อป้องกันไม่ให้ทรัพย์สินเกิดความเสียหายใช้งานไม่ได้ หรือสูญหาย

6. **ความมั่นคงปลอดภัยของศูนย์ IT ที่เกี่ยวข้องกับพนักงาน**

6.1. หัวหน้าผู้ดูแลระบบและกองบริหารงานบุคคล ต้องกำหนดหน้าที่และความรับผิดชอบด้านความปลอดภัยสารสนเทศเป็นลายลักษณ์อักษรสำหรับผู้ใช้งาน และ หรือหน่วยงานภายนอกที่ว่าจ้างมาปฏิบัติงาน

6.2. กองบริหารงานบุคคลและหน่วยงานภายในที่เกี่ยวข้องต้องตรวจสอบคุณสมบัติของผู้สมัครเข้าเป็นพนักงานใหม่ โดยละเอียด เช่น ประวัติการทำงาน วุฒิการศึกษา และระดับความเสี่ยงในการเข้าถึงสารสนเทศ เป็นต้น

6.3. กองบริหารงานบุคคลและศูนย์ IT ต้องกำหนดเงื่อนไขการจ้างงาน รวมไปถึงหน้าที่ความรับผิดชอบด้านความปลอดภัยสารสนเทศ โดยพนักงานใหม่จะต้องเห็นชอบและลงนามในเงื่อนไขการจ้างงานด้วย

6.4. ศูนย์ IT ต้องสร้างความตระหนักให้พนักงานและผู้ที่มาปฏิบัติหน้าที่จากหน่วยงานภายนอกตระหนักถึงความปลอดภัย เกี่ยวกับลักษณะงานที่ต้องรับผิดชอบ

6.5. พนักงานและหน่วยงานภายนอกที่จะเข้ามาปฏิบัติงาน ต้องปฏิบัติตามนโยบายความปลอดภัยสารสนเทศของศูนย์ IT

6.6. พนักงานที่ฝ่าฝืนหรือละเมิดนโยบายด้านความปลอดภัยสารสนเทศของศูนย์ IT ต้องถูกลงโทษตามกระบวนการทางวินัย

6.7. พนักงานที่ลาออกจากงานหรือถูกเลิกจ้างงาน ต้องคืนทรัพย์สินของศูนย์ IT ที่อยู่ในความครอบครองของตน และถูกยกเลิกสิทธิในการเข้าถึงทรัพย์สินหรือข้อมูลสารสนเทศ

7. **การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม**

7.1. งานบริการระบบเครือข่าย งานพัฒนาระบบสารสนเทศ และหน่วยอาคารสถานที่ต้องจัดทำบริเวณรักษาความปลอดภัยและจัดให้มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาต รวมไปถึงการกำหนดบริเวณสำหรับบุคคลภายนอกในการเข้าถึงเพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต การก่อให้เกิดความเสียหาย การก่อกวน หรือแทรกแซงต่อทรัพย์สินของศูนย์ IT

7.2. ศูนย์ IT ต้องจัดทำแผนป้องกันอุบัติภัย เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือ หายนะอื่น ๆ ทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้โดยเร็วที่สุด

7.3. พนักงานต้องจัดวางและป้องกันทรัพย์สินให้ปลอดภัยจากภัยคุกคามด้านสิ่งแวดล้อม อันตรายต่าง ๆ รวมทั้งการเข้าถึงโดยไม่ได้รับอนุญาต

7.4. เพื่อลดความเสี่ยงในการล้มเหลวของระบบสนับสนุนการให้บริการระบบเครือข่าย ศูนย์ IT ต้องบำรุงรักษาระบบสาธารณูปโภค เช่น ระบบไฟฟ้า ระบบปรับอากาศ เป็นต้น ให้สามารถใช้งานได้อย่างต่อเนื่องและมีระบบสำรองหากเกิดเหตุการณ์ที่ระบบสาธารณูปโภคหลักไม่สามารถใช้งานได้

7.5. อุปกรณ์ระบบเครือข่ายที่ใช้งานภายนอกศูนย์ IT สายไฟ สายสื่อสาร และสายเคเบิลอื่น ๆ ต้องได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อสายสัญญาณ หรืออุปกรณ์ระบบเครือข่ายนั้น ๆ

7.6. ผู้ดูแลระบบต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟท์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือเขียนทับ ก่อนที่จะทิ้งอุปกรณ์ดังกล่าว เพื่อป้องกันข้อมูลหากอุปกรณ์นั้นถูกนำกลับมาใช้อีกครั้ง

7.7. พนักงานต้องไม่นำทรัพย์สินของศูนย์ IT ออกไปภายนอกศูนย์ IT ยกเว้นได้รับอนุญาต ซึ่งต้องปฏิบัติตามระเบียบการนำพัสดุออกภายนอกอาคารอย่างเคร่งครัด

8. **การบริหารจัดการระบบเครือข่ายของศูนย์ IT**

8.1. งานบริการระบบเครือข่ายต้องจัดทำระเบียบปฏิบัติด้านการให้บริการระบบเครือข่ายเป็นลายลักษณ์อักษร และเผยแพร่ให้กับผู้ใช้งานและผู้เกี่ยวข้องรับทราบ

8.2. ผู้ดูแลระบบต้องควบคุมการให้บริการของหน่วยงานภายนอกให้ปฏิบัติตามข้อตกลงด้านความปลอดภัยที่ทำไว้ระหว่างศูนย์ IT และหน่วยงานภายนอก

8.3. ศูนย์ IT ต้องวางแผนความต้องการทรัพยากรสารสนเทศเพื่อกำหนดความต้องการทรัพยากรสารสนเทศเพิ่มเติมในอนาคต เพื่อให้ระบบมีประสิทธิภาพที่เหมาะสมและเพียงพอต่อการใช้งาน

8.4. ระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือติดตั้งใหม่ ต้องผ่านการตรวจสอบว่าไม่มีผลกระทบต่อระบบเครือข่ายโดยรวม ก่อนนำระบบนั้นมาใช้งาน

8.5. ผู้ดูแลระบบต้องตรวจจับ ป้องกัน และกู้คืน เพื่อป้องกันทรัพย์สินจากโปรแกรมที่ไม่ประสงค์ดี หรือโปรแกรมชนิดเคลื่อนที่(โปรแกรมที่สามารถเคลื่อนย้ายจากหน่วยความจำคอมพิวเตอร์เครื่องหนึ่งไปยังหน่วยความจำคอมพิวเตอร์อีกเครื่องหนึ่งได้ด้วยตัวเอง) รวมทั้งมีการสร้างความตระหนักถึงอันตรายที่เกิดขึ้นจากโปรแกรมที่ไม่ประสงค์ดีเหล่านี้ รวมถึงเผยแพร่วิธีการใช้งานระบบเครือข่ายอย่างปลอดภัยให้ผู้ใช้งานทราบด้วย

8.6. ผู้ดูแลระบบต้องสำรองข้อมูลและทดสอบข้อมูลที่เก็บไว้อย่างสม่ำเสมอตามขั้นตอนการปฏิบัติงานเรื่องการสำรองข้อมูลและมีการซักซ้อมการกู้คืนระบบข้อมูลภายในระยะเวลาที่กำหนดแต่ละครั้งต้องไม่เกิน 15 นาที ทุก 45 วันเป็นอย่างน้อย

8.7. หัวหน้างานบริการระบบเครือข่ายต้องบริหารจัดการระบบเครือข่าย จัดระดับการให้บริการ กำหนดมาตรการเพื่อป้องกันภัยคุกคามต่าง ๆ ทางระบบเครือข่าย และดูแลรักษาระบบความปลอดภัยสำหรับระบบเครือข่ายและ Application ที่ใช้งานบนระบบเครือข่าย รวมทั้งข้อมูลสารสนเทศต่าง ๆ ที่ส่งผ่านทางระบบเครือข่าย

8.8. งานบริการระบบเครือข่ายต้องมีวิธีการจัดการสื่อที่ใช้ในการบันทึกข้อมูล เพื่อป้องกันการเปิดเผย การเปลี่ยนแปลงแก้ไข การลบหรือการทำลายทรัพย์สินสารสนเทศโดยไม่ได้รับอนุญาต

8.9. พนักงานทุกคนต้องปฏิบัติตามระเบียบปฏิบัติเรื่องการควบคุมเอกสาร

8.10. ศูนย์ IT ต้องกำหนดขั้นตอนปฏิบัติ และมาตรการรองรับ ในการแลกเปลี่ยนสารสนเทศ และซอฟท์แวร์ภายในศูนย์ IT หรือ ระหว่างหน่วยงาน

8.11. ก่อนการเผยแพร่ข้อมูลออกสู่สาธารณะ ผู้รับผิดชอบในการเผยแพร่ข้อมูลต้องตรวจสอบความถูกต้องของข้อมูลสารสนเทศ เพื่อข้อมูลมีความถูกต้อง ไม่ก่อให้เกิดความเข้าใจผิด อีกทั้งเมื่อเผยแพร่ออกไปแล้วต้องมีกลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาตอีกด้วย

8.12. ผู้ดูแลระบบต้องจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ โดยเก็บข้อมูลดังนี้

8.12.1. ข้อมูลอินเทอร์เน็ตที่เกิดจากการเข้าถึงระบบเครือข่าย (Network Access Systems) (Dial up services)

8.12.2. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการจดหมายอิเล็กทรอนิกส์ (e-mail servers)

8.12.3. ข้อมูลอินเทอร์เน็ตที่เกิดจากการถ่ายโอนข้อมูลบนเครื่องให้บริการถ่ายโอนข้อมูล (FTP servers)

8.12.4. ข้อมูลอินเทอร์เน็ตบนเครื่องผู้ให้บริการเว็บ (Web servers)

8.12.5. ชนิดของข้อมูลบนเครือข่ายคอมพิวเตอร์ขนาดใหญ่ (Usenet)

8.12.6. ข้อมูลที่เกิดจากการโต้ตอบกันบนเครือข่ายอินเทอร์เน็ต เช่น Internet Relay Chat (IRC) และ Instant Messaging (IM) เป็นต้น

9. **การควบคุมการเข้าถึงระบบสารสนเทศระบบเครือข่ายและทรัพย์สินสารสนเทศ**

9.1. เพื่อควบคุมการเข้าถึง (Access Control) ผู้บริหารแต่งตั้งผู้ดูแลระบบสารสนเทศเครือข่ายและทรัพย์สินสารสนเทศตามภารงานมหาวิทยาลัย

9.2. หัวหน้างานบริการระบบเครือข่ายและหัวหน้างานที่เกี่ยวข้องต้องมีการควบคุมและจำกัดสิทธิ์การใช้งานระบบตามความจำเป็นในการใช้งาน และมีการทบทวนสิทธิ์ตามระยะเวลาที่กำหนดอย่างเป็นทางการ

9.3. ผู้ดูแลระบบต้องบริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบเครือข่ายและระบบสารสนเทศได้ตามสิทธิ์ที่ได้รับ

9.4. ผู้ใช้งานต้องมีวิธีการป้องกันไม่ให้ผู้ที่ไม่มีสิทธิ์เข้าถึง สามารถเข้าถึงทรัพย์สินที่อยู่ในความรับผิดชอบของตนเองโดยไม่มีเจ้าหน้าที่ดูแลได้ เช่น เมื่อหยุดใช้งานเครื่องคอมพิวเตอร์ให้ทำการล็อคหน้าจอ หรือเมื่อออกจากห้องปฏิบัติงานให้ล็อคประตู เป็นต้น

9.5. ทรัพย์สินที่สำคัญ ไม่ว่าจะเป็นเอกสาร หรือสื่อบันทึกข้อมูล ต้องไม่อยู่ในสถานที่ที่ไม่ปลอดภัย เช่น สามารถเข้าถึงได้ทางกายภาพ หรืออยู่ในที่สาธารณะพบเห็นได้ง่าย เป็นต้น

9.6. ก่อนการใช้งานระบบเครือข่ายหรืออุปกรณ์บนระบบเครือข่าย จะต้องทำการระบุตัวตนผู้ขอใช้งานทุกครั้ง เพื่อทราบว่าใครเป็นผู้ขอใช้งานและสิทธิ์ในการใช้งาน

9.7. ผู้ดูแลระบบจะต้องการป้องกันการเข้าถึงพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ไม่ว่าจะเป็นจากทางกายภาพหรือผ่านระบบเครือข่าย

9.8. ผู้ดูแลระบบต้องแยกระบบเครือข่ายออกเป็นกลุ่มของผู้ใช้งาน และกลุ่มของเครื่องแม่ข่ายที่ให้บริการระบบสารสนเทศ รวมไปถึงระบบสารสนเทศที่มีความสำคัญสูง เพื่อให้ง่ายต่อการจำกัดการเข้าถึงและบริหารจัดการความปลอดภัยระบบเครือข่าย

9.9. ผู้ดูแลระบบต้องกำหนดเส้นทางการเชื่อมต่อระบบเครือข่าย เพื่อให้ข้อมูลสารสนเทศบนระบบเครือข่ายถูกจำกัดสิทธิ์ในการเข้าถึงจากผู้ใช้งานระบบเครือข่ายได้

9.10. ผู้ดูแลระบบต้องต้องมีการระบุตัวตน การควบคุมรหัสผ่าน และการจำกัดระยะเวลาในการเข้าถึงระบบปฏิบัติการ เช่น ระบบจะตัดเมื่อผู้ใช้งานไม่ได้ใช้งานมาเป็นระยะเวลาหนึ่ง เป็นต้น

9.11. ผู้ดูแลระบบต้องควบคุมอุปกรณ์สื่อสารชนิดพกพา เช่น Notebook mobile phone เป็นต้น และหาวิธีการป้องกันเพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากอุปกรณ์เหล่านี้ เมื่อถูกนำเข้ามาใช้งานในระบบเครือข่าย

9.12. การควบคุมการเข้าถึงห้องคอมพิวเตอร์กลางให้เป็นไปตามประกาศแนวปฏิบัติการเข้าถึงห้องคอมพิวเตอร์กลาง

10. การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

10.1. ผู้พัฒนาระบบขึ้นมาใหม่ หรือปรับปรุงจากของเดิมที่มีอยู่แล้ว จะต้องระบุข้อกำหนดความปลอดภัยของระบบใหม่นี้ก่อนใช้งาน เพื่อผู้ที่ใช้งานจะไม่ทำให้ระบบนี้ใช้งานไม่ได้หรือก่อกวนระบบเครือข่ายโดยรวม

10.2. ผู้พัฒนาระบบจะต้องตรวจสอบความถูกต้องของข้อมูลก่อนนำเข้าสู่กระบวนการประมวลผล และมีระบบตรวจสอบระหว่างการประมวลผลว่าเกิดความผิดพลาดหรือไม่ รวมทั้งตรวจสอบหลังจากที่ประมวลผลเรียบร้อยว่าข้อมูลสารสนเทศมีความถูกต้องหรือไม่ ก่อนนำไปใช้งาน

10.3. ผู้พัฒนาระบบต้องควบคุมการติดตั้งซอฟท์แวร์ต่าง ๆ ลงไปยังระบบที่ให้บริการ ทั้งนี้เพื่อลดความเสี่ยงที่จะทำให้ระบบบริการเสียหาย ผิดปกติ หรือไม่สามารถใช้งานได้ เช่น กรณีที่จะติดตั้งอุปกรณ์หรือพัฒนาระบบใด ๆ ที่จะส่งผลกับระบบโดยรวม จะต้องตัดตัวเองออกจากระบบโดยรวมเสียก่อน หรือทำการทดสอบในระบบจำลองก่อนที่จะนำมาใช้กับระบบจริง เป็นต้น

10.4. ผู้พัฒนาระบบต้องหลีกเลี่ยงการนำข้อมูลจริงที่ใช้อยู่บนระบบให้บริการมาทดสอบระบบ หากมีความจำเป็นต้องนำมาใช้ให้ทำการควบคุม เช่น การลบข้อมูลส่วนตัว การลบบางส่วนของข้อมูลที่เป็นความลับ เป็นต้น

10.5. หัวหน้างานพัฒนาระบบต้องมีระบบการจำกัดการเข้าถึงซอร์สโค้ดที่ระบบให้บริการอยู่ เพื่อป้องกันการเปลี่ยนแปลงที่เกิดขึ้น โดยไม่ได้รับอนุญาตหรือไม่ได้เจตนา

10.6. ผู้ดูแลระบบต้องมีวิธีปฏิบัติในการควบคุมหรือเปลี่ยนแปลงแก้ไขระบบสารสนเทศ โดยต้องมีการตรวจสอบทางเทคนิคว่าระบบยังทำงานดีอยู่หรือไม่หลังจากการเปลี่ยนแปลงแก้ไขระบบสารสนเทศเรียบร้อยแล้ว

10.7. หลีกเลี่ยงการแก้ไขซอฟท์แวร์ที่มาจากผู้ผลิต หากมีความจำเป็น ต้องมีการควบคุมการแก้ไขอย่างเข้มงวด

10.8. หัวหน้างานพัฒนาระบบต้องป้องกันการรั่วไหลของสารสนเทศ หรือลดโอกาสที่สารสนเทศจะรั่วไหลออกไป เพื่อไม่ให้ผู้อื่นนำข้อมูลสารสนเทศนี้ไปใช้งานโดยมิชอบได้

10.9. ผู้ดูแลระบบต้องวางแผนประเมินความเสี่ยงของระบบ ทำการทดสอบ และกำหนดมาตรการป้องกันช่องโหว่ของระบบ

11. การบริหารจัดการความเสี่ยงด้านความปลอดภัยของระบบสารสนเทศ

11.1. ผู้ดูแลระบบต้องจัดทำรายงานผลประเมินความเสี่ยงเป็นรายเดือน พร้อมคำแนะนำในการลดความเสี่ยงเหล่านั้น เพื่อให้ผู้บริหารพิจารณา ตามหัวข้อดังนี้

11.1.1. ด้านการใช้งานระบบสารสนเทศที่ไม่ถูกต้องตามนโยบาย ประกาศ หรือระเบียบปฏิบัติ

11.1.2. ด้านภัยคุกคามจากไวรัสคอมพิวเตอร์ หนอนคอมพิวเตอร์ และมัลแวร์

11.1.3. ด้านภัยคุกคามจากการโจมตีระบบโดยผู้ไม่ประสงค์ดี ที่อาจส่งผลให้ข้อมูลสารสนเทศ และการสื่อสาร

11.1.4. ด้านขีดจำกัดในการให้บริการของระบบสารสนเทศ ที่อาจส่งผลให้ไม่สามารถใช้งานหรือให้บริการได้

11.1.5. ด้านกายภาพ หรือ ภัยธรรมชาติ

11.1.6. หรือด้านอื่น ๆ ที่อาจเกิดขึ้นได้

11.2. ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติเพื่อรับมือเหตุการณ์ที่เกี่ยวข้องกับความปลอดภัยสารสนเทศ พร้อมทั้งกำหนดหน้าที่และผู้รับผิดชอบที่ชัดเจน

11.3. ผู้ดูแลระบบต้องบันทึกเหตุการณ์ละเมิดความปลอดภัยที่เกิดขึ้น โดยพิจารณาถึงประเภท ปริมาณ และค่าใช้จ่าย ที่เกิดจากการเสียหาย เพื่อเรียนรู้และป้องกันไม่ให้เกิดซ้ำขึ้นอีก

11.4. ผู้ดูแลระบบต้องเก็บรวบรวมหลักฐานสำหรับอ้างอิง ในกรณีที่เหตุการณ์ที่เกิดขึ้นมีความเกี่ยวข้องกับการดำเนินการทางกฎหมาย

12. การบริหารความต่อเนื่องในการดำเนินงานของศูนย์ IT

12.1. ศูนย์ IT ต้องมีระเบียบปฏิบัติในการบริหารจัดการระบบเครือข่าย เพื่อให้สามารถให้บริการได้อย่างต่อเนื่อง รวมทั้งมีแผนฉุกเฉินในการกู้คืนระบบกรณีที่ระบบเกิดความเสียหาย

12.2. หัวหน้างานบริการระบบเครือข่ายต้องมีการทดสอบและปรับปรุงแผนฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

13. การปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ

13.1. ศูนย์ IT ต้องระบุข้อกำหนดทางกฎหมาย และนโยบายการใช้งานระบบเครือข่ายเป็นลายลักษณ์อักษรชัดเจน และมีการปรับปรุงให้ทันสมัยอย่างน้อยปีละครั้ง

13.2. ศูนย์ IT ต้องควบคุมให้ผู้ใช้งานระบบเครือข่ายทุกคนปฏิบัติตามนโยบายความปลอดภัยสารสนเทศ นโยบายการเข้าใช้งานระบบเครือข่าย และไม่ละเมิดข้อกฎหมายว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

13.3. ศูนย์ IT ต้องมีแผนการตรวจประเมินความปลอดภัยของระบบสารสนเทศ โดยผู้ดูแลระบบเอง หรือโดยบุคคลภายนอก และต้องมีการควบคุมเครื่องมือหรือซอฟท์แวร์ที่ใช้ในการตรวจประเมิน เพื่อป้องกันการใช้งานผิดวัตถุประสงค์หรือการเปิดเผยข้อมูลตรวจประเมินโดยไม่ได้รับอนุญาต

14. ข้อตกลงในการให้บริการระบบเครือข่าย

14.1. บริการชื่อผู้ใช้งานและรหัสผ่านส่วนตัวสำหรับการเข้าใช้งานระบบเครือข่าย PIBUL NET

14.2. เมื่อผู้ใช้งานเป็นพนักงานใหม่จะต้องผ่านขั้นตอนการขอบัญชีผู้ใช้งาน การรับทราบนโยบายการใช้งานและรับทราบ Disclosure Agreement ของหน่วยงาน

14.3. ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านของตนเองทันที หลังจากได้รับรหัสผ่านจากผู้ดูแลระบบ โดยการตั้งรหัสผ่านใหม่จะต้องมีความยาวไม่น้อยกว่า 7 ตัวอักษร

14.4. ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านของตนเองอย่างน้อยทุก ๆ 3 เดือนโดยการตั้งรหัสผ่านใหม่จะต้องมีความยาวไม่น้อยกว่า 7 ตัวอักษร

14.5. ผู้ใช้งานต้องรับผิดชอบในการจัดเก็บและรักษารหัสผ่านของตนเองให้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้หากมีผู้อื่นล่วงรู้ข้อมูลอันเป็นความลับนี้ และนำไปใช้งานในทางที่ผิด ยกเว้นกรณีที่สอบสวนโดยตัวแทนของมหาวิทยาลัยหรือเจ้าพนักงานแล้วไม่ถือว่าเป็นความผิดของผู้ใช้งานคนนั้น ๆ

14.6. การเชื่อมต่อผ่านสายเข้าสู่ระบบเครือข่าย PIBUL NET

14.7. ผู้ใช้งานต้องมีบัญชีผู้ใช้งานระบบเครือข่าย เพื่อใช้ในการระบุตัวตนก่อนเข้าใช้งานระบบเครือข่าย PIBUL NET

14.8. การเชื่อมต่อแบบไร้สายเข้าสู่ระบบเครือข่าย PIBUL NET มีข้อกำหนดดังนี้

14.8.1. ผู้ใช้งานจะต้องมีบัญชีผู้ใช้งานระบบเครือข่าย จึงจะสามารถใช้งานระบบเครือข่าย ไร้สายนี้ได้

14.8.2. ระบบเครือข่ายไร้สายของมหาวิทยาลัย จะใช้ชื่อว่า PSRU-WIFI ซึ่งต้องระบุตัวตนก่อนเข้าใช้งาน

14.8.3. ผู้ใช้งานระบบเครือข่ายไร้สาย ต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายของมหาวิทยาลัยอย่างเคร่งครัด

14.9. บริการสืบค้นข้อมูลผ่านระบบเครือข่าย Internet และ Intranet

14.9.1 ผู้ใช้งานสืบค้นข้อมูลผ่านระบบเครือข่าย Internet และ Intranet จะต้องระบุตัวตนก่อนเข้าใช้งานทุกครั้ง

14.9.2 ผู้ใช้งานต้องระมัดระวังในการใช้งาน หลีกเลี่ยงการเข้าสืบค้นข้อมูลในแหล่งที่ไม่ปลอดภัย

14.9.3 ผู้ใช้งานต้องปฏิบัติตามคำแนะนำในคู่มือการใช้งานระบบเครือข่ายอย่างปลอดภัย

14.9.4 ผู้ใช้งานต้องปฏิบัติตามนโยบายการใช้งานระบบเครือข่ายอย่างเคร่งครัด

14.9.5 ผู้ใช้งานต้องไม่ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์อย่างเด็ดขาด

14.10. บริการสืบค้นข้อมูลผ่านระบบฐานข้อมูลออนไลน์

14.10.1. การใช้งานระบบฐานข้อมูลออนไลน์ของมหาวิทยาลัยนั้น ผู้ใช้งานจะต้องเชื่อมต่อระบบอินเทอร์เน็ตด้วยจึงจะสามารถใช้งานได้

14.10.2. ในกรณีที่ผู้ให้บริการอินเทอร์เน็ตของมหาวิทยาลัยไม่สามารถให้บริการได้ อาจจะส่งผลกระทบให้ไม่สามารถใช้งานระบบฐานข้อมูลออนไลน์ด้วย

14.11. บริการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับนักศึกษา

14.11.1 มหาวิทยาลัยเป็นผู้สร้างและอำนวยความสะดวกในการใช้งาน PSRU Live Mail ในระบบเดิมเพื่อใช้งานสนับสนุนการดำเนินงานของมหาวิทยาลัย

14.11.2 ผู้ใช้งานต้องปฏิบัติตามข้อกฎหมาย และไม่ใช้งานในลักษณะที่ก่อให้เกิดความเสียหายกับผู้อื่น หรือมหาวิทยาลัย โดยผู้ใช้งานต้องรับผิดชอบในการใช้งานทั้งหมด ยกเว้นผู้ใช้งานพิสูจน์ได้ว่าตนมิใช่ผู้กระทำ

14.11.3 ต้องไม่ใช้งานบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ร่วมกับผู้อื่น หรือแจกจ่ายบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ไปให้กับผู้อื่น

14.11.4 กล่องจดหมายที่ผู้ใช้งานได้รับหลังจากได้รับบัญชีผู้ใช้งานเรียบร้อยแล้วจะมีขนาด 2 GB และในการแนบไฟล์เพื่อทำการส่งจดหมายแต่ละครั้งต้องมีขนาดไม่เกิน 10 MB

14.11.5 ในกรณีที่ไม่ได้ทำการ login เข้าใช้งานเป็นเวลาเกิน 180 วัน กล่องจดหมายจะถูกปิด ไม่สามารถใช้งานได้ ต้องทำการติดต่อผู้ให้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย โดยข้อมูล ต่าง ๆ ที่ได้เก็บไว้ในระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยอาจไม่สามารถกู้คืนได้อีก

14.11.6 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้บริการเพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมายหรือเพื่อปกป้องสิทธิ์หรือทรัพย์สินของมหาวิทยาลัยหรือของผู้ใช้บริการอื่น

14.11.7 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบการให้บริการ

14.11.8 มหาวิทยาลัยจะไม่รับประกันความเสียหายหรือสูญหายของข้อมูลที่เก็บไว้ในระบบ

14.11.9 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจเปลี่ยนแปลงบริการหรือตัดทอนลักษณะใดของบริการ ไม่ว่าเหตุผลใดก็ตามได้ตลอดเวลา และอาจยกเลิกหรือระงับการบริการผู้ใช้บริการเมื่อพบว่าละเมิดข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

14.11.10 ข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์นี้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ดังนั้นผู้ให้บริการมีสิทธิ์ในการส่งข้อมูลการให้บริการเพิ่มเติมให้กับผู้ใช้บริการ ผ่านทางจดหมายอิเล็กทรอนิกส์หรือทางหน้าเว็บไซต์บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

14.12. บริการสื่อสารด้วยจดหมายอิเล็กทรอนิกส์สำหรับพนักงาน

14.12.1 มหาวิทยาลัยเป็นผู้สร้างและอำนวยความสะดวกในการใช้งาน PSRU Mail เพื่อใช้งานสนับสนุนการดำเนินงานของมหาวิทยาลัย

14.12.2 ผู้ใช้งานต้องปฏิบัติตามข้อกฎหมาย และไม่ใช้งานในลักษณะที่ก่อให้เกิดความเสียหายกับผู้อื่น หรือมหาวิทยาลัย โดยผู้ใช้งานต้องรับผิดชอบในการใช้งานทั้งหมด ยกเว้นผู้ใช้งานพิสูจน์ได้ว่าตนมิใช่ผู้กระทำ

14.12.3 ต้องไม่ใช้งานบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ร่วมกับผู้อื่น หรือแจกจ่ายบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ไปให้กับผู้อื่น

14.12.4 กล่องจดหมายที่ผู้ใช้งานได้รับหลังจากได้รับบัญชีผู้ใช้งานเรียบร้อยแล้วจะมีขนาด 5 GB และในการแนบไฟล์เพื่อทำการส่งจดหมายแต่ละครั้งต้องมีขนาดไม่เกิน 15 MB

14.12.5 ในกรณีที่ไม่ได้ทำการ login เข้าใช้งานเป็นเวลาเกิน 180 วัน กล่องจดหมายจะถูกปิด ไม่สามารถใช้งานได้ ต้องทำการติดต่อผู้ให้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย โดยข้อมูล ต่าง ๆ ที่ได้เก็บไว้ในระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยอาจไม่สามารถกู้คืนได้อีก

14.12.6 จดหมายอิเล็กทรอนิกส์ในกล่องจดหมายจะถูกเก็บไว้บนระบบสำรองข้อมูลสูงสุด 60 วัน โดยจดหมายที่ส่งเข้ามายังกล่องจดหมายก่อนวันสำรองข้อมูลประจำสัปดาห์จะสามารถกู้คืนได้หากสูญหาย โดยผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ต้องแจ้งให้ผู้ดูแลระบบทราบ

14.12.7 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้บริการ เพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิ์หรือทรัพย์สินของมหาวิทยาลัยหรือของผู้ใช้บริการอื่น

14.12.8 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจยุติการให้บริการชั่วคราว เพื่อเพิ่มระบบรักษาความปลอดภัยหรือหยุดยั้งการก่อกวนระบบการให้บริการ

14.12.9 มหาวิทยาลัยจะไม่รับประกันความเสียหายหรือสูญหายของข้อมูลที่เก็บไว้ในระบบ

14.12.10 ผู้ให้บริการจดหมายอิเล็กทรอนิกส์อาจเปลี่ยนแปลงบริการหรือตัดทอนลักษณะใดของบริการ ไม่ว่าเหตุผลใดก็ตามได้ตลอดเวลา และอาจยกเลิกหรือระงับการบริการผู้ใช้บริการเมื่อพบว่าละเมิดข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยโดยไม่ต้องแจ้งให้ทราบล่วงหน้า

14.12.11 ข้อตกลงการใช้งานจดหมายอิเล็กทรอนิกส์นี้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ดังนั้นผู้ให้บริการมีสิทธิ์ในการส่งข้อมูลการให้บริการเพิ่มเติมให้กับผู้ใช้บริการ ผ่านทางจดหมายอิเล็กทรอนิกส์หรือทางหน้าเว็บไซต์บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

14.13. บริการดาว์นโหลดซอฟท์แวร์ที่มีลิขสิทธิ์ถูกต้อง ฟรีซอฟท์แวร์ หรือซอฟท์แวร์แบบเปิดเผยรหัสที่มีให้บริการในระบบเครือข่าย PIBUL NET

14.13.1 บริการนี้จัดทำขึ้นเพื่ออำนวยความสะดวกให้กับ ผู้งาน ได้ใช้ซอฟท์แวร์ลิขสิทธิ์ที่ถูกต้องตามกฎหมาย ประกอบกับรัฐบาลได้กำหนดมาตรการป้องกันการละเมิดลิขสิทธิ์ซอฟท์แวร์ โดยขอความร่วมมือกับส่วนราชการต่าง ๆ ให้ดำเนินการจัดหาซอฟท์แวร์ถูกกฎหมายมาใช้งานต่อไป

14.13.2 สามารถใช้งานซอฟท์แวร์ลิขสิทธิ์ได้เฉพาะเครื่องคอมพิวเตอร์ที่ใช้งานภายในมหาวิทยาลัยเท่านั้น

14.13.3 หากผู้ใช้งานนำซอฟท์แวร์ลิขสิทธิ์ไปใช้งานกับเครื่องคอมพิวเตอร์ส่วนบุคคล มหาวิทยาลัยจะไม่รับผิดชอบผลจากการกระทำดังกล่าวใดๆทั้งสิ้น

14.13.4 ซอฟท์แวร์เหล่านี้จะให้บริการดาวน์โหลดผ่านระบบเครือข่าย PIBUL NET เท่านั้น ไม่มีบริการทำซ้ำ หรือคัดลอกลงบนสื่อบันทึกข้อมูลเพื่อแจกจ่ายใดๆทั้งสิ้น

14.14. บริการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับ World Wide Web

14.14.1 หากคณะหรือหน่วยงาน มีความต้องการในการมีโฮมเพจเป็นของตนเอง สามารถทำหนังสือเพื่อขอพื้นที่ของเว็บหลักมหาวิทยาลัยได้ โดยต้องอยู่ภายใต้โดเมน psru.ac.th เท่านั้น

14.14.2 หากคณะหรือหน่วยงาน มีเครื่องแม่ข่ายที่ให้บริการเว็บเป็นของตนเอง และต้องการจดทะเบียนภายใต้โดเมน psru.ac.th สามารถขออนุมัติจดชื่อโดเมนมาที่ศูนย์ IT โดยกรอกรายละเอียดชื่อเว็บไซต์ และ IP Address มาให้ครบถ้วน

14.15. บริการเว็บไซต์สำหรับนักศึกษาและบุคลากร

14.15.1. นักศึกษามหาวิทยาลัยสามารถมีพื้นที่เว็บไซต์สำหรับสร้างโฮมเพจของตนเองได้ โดยมี 2 ระบบ คือ ระบบ web hosting (student.psru.ac.th) และระบบ Live space

14.15.2. ต้องใช้ user account สำหรับใช้งานอินเทอร์เน็ตของมหาวิทยาลัยในการสมัครขอพื้นที่ใช้งาน student.psru.ac.th

14.15.3. ต้องใช้ e-mail address ของ Live mail ในการเข้าใช้งาน Live space สำรองข้อมูลส่วนบุคคล โดยผู้ใช้งานมีหน้าที่สำรองข้อมูลสุวนบุคคลด้วยตนเอง

14.15.4. ต้องไม่นำเสนอข้อมูลที่ผิดกฎหมาย หรือแสดงข้อความ รูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของไทย

14.15.5. ต้องไม่เผยแพร่ข้อความ ใช้ถ้อยคำที่ไม่สุภาพ ซึ่งส่งผลให้เกิดความเสื่อมเสียต่อบุคคลหรือหน่วยงานที่ถูกกล่าวอ้าง พาดพิงถึง

14.15.6. ต้องไม่กระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของมหาวิทยาลัยหรือของบุคคลอื่น

14.15.7. ศูนย์ IT สามารถเข้าไปตรวจสอบ Web site ของนักศึกษาและบุคลากร ตลอดจนมีอำนาจในการระงับการให้บริการ sub domain ได้ ในกรณีที่ตรวจพบการดำเนินงานที่ขัดแย้งกับนโยบายการใช้งานระบบเครือข่ายหรือพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์

14.16. บริการฝากเครื่องคอมพิวเตอร์แม่ข่ายสำหรับหน่วยงานในสังกัดมหาวิทยาลัย

14.16.1 หน่วยงานเจ้าของเครื่องคอมพิวเตอร์แม่ข่ายต้องยอมรับ และปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

14.16.2 เครื่องคอมพิวเตอร์แม่ข่ายที่นำมาฝากต้องผ่านการตรวจสอบจากผู้ดูแลระบบเพื่อให้มั่นใจว่าจะไม่รบกวนการทำงานของระบบอื่น ๆ และไม่เป็นช่องโหว่ต่อการจู่โจม โดยหากตรวจสอบแล้วพบความเสี่ยงที่อาจจะเป็นอันตรายต่อระบบอื่น ๆ จะไม่อนุญาตให้นำมาฝากไว้ในห้องควบคุมระบบเครือข่ายได้จนกว่าจะได้รับการแก้ไขโดยหน่วยงานเจ้าของเครื่องคอมพิวเตอร์แม่ข่าย

14.16.3 หากเครื่องคอมพิวเตอร์แม่ข่ายที่นำมาฝากเป็นสาเหตุที่ทำให้ระบบอื่น ๆ ทำงานผิดปกติหรือไม่สามารถให้บริการได้ ผู้ดูแลระบบจะสงวนสิทธิ์ในการยกเลิกการการเชื่อมต่อระหว่างเครื่องคอมพิวเตอร์แม่ข่ายดังกล่าวออกจากระบบเครือข่ายทันที โดยไม่จำเป็นต้องแจ้งล่วงหน้า เพื่อคงไว้ซึ่งมาตรการด้านความปลอดภัย

14.17. การขอใช้บริการพิเศษอื่นๆที่จำเป็นต้องเปิด Port Firewall ของมหาวิทยาลัยสำหรับบุคลากรในสังกัดมหาวิทยาลัย

14.17.1. บุคลากรผู้ขอต้องยอมรับ และปฏิบัติตามนโยบายด้านความปลอดภัยอย่างเคร่งครัด

14.17.2. วัตถุประสงค์ในการใช้งานจะต้องไม่ขัดต่อนโยบาย ประกาศ ระเบียบต่าง ๆ ของมหาวิทยาลัย และต้องไม่ขัดต่อกฎหมาย

14.18. บุคลากรผู้ขอต้องทำการขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการ ในการขอแต่ละครั้ง โดยต้องระบุข้อมูลทางเทคนิคโดยละเอียดดังต่อไปนี้

14.18.1. หมายเลข Port ที่ต้องการขอให้เปิด

14.18.2. หมายเลข IP Address ของปลายทางที่ต้องการติดต่อสื่อสารด้วย

14.18.3. วัตถุประสงค์หรือชื่อแอพพลิเคชั่นที่ต้องการใช้งานผ่าน Port นั้น ๆ

14.18.4. วันที่เริ่มใช้ และวันที่สิ้นสุดการขอใช้

14.19. ทางศูนย์ IT จะไม่อนุมัติให้ใช้งาน หากทำการพิจารณาแล้วพบว่าการขอใช้งานขัดต่อนโยบาย ประกาศ ระเบียบ ของมหาวิทยาลัย หรือขัดต่อกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ

14.20. ภายหลังการอนุมัติให้ใช้งานแล้วพบว่ามีการใช้งานที่ขัดต่อนโยบาย ประกาศ ระเบียบ ของมหาวิทยาลัย หรือขัดต่อกฎหมาย หรืออาจจะทำให้เกิดช่องโหว่ด้านความปลอดภัยต่อระบบสารสนเทศ หรือทำให้เกิดความเสียหายต่อระบบสารสนเทศของมหาวิทยาลัย ทางศูนย์ IT จะยกเลิกการให้บริการทันที

15. การเปิดเผยข้อมูล การยกเลิก หรือ สิ้นสุดการให้บริการระบบสารสนเทศ

15.1. ผู้อำนวยการอาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งาน เพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธ์หรือทรัพย์สิน หรือของผู้ใช้งานอื่น

15.2. ผู้อำนวยการอาจยกเลิกสิทธิการเข้าใช้งานระบบเครือข่าย หากผู้ใช้งานมิได้เข้าใช้งานระบบเครือข่ายภายในระยะเวลาติดต่อกันเกิน 90 วัน

15.3. ผู้อำนวยการอาจยกเลิกการให้บริการหากพบว่าผู้ใช้งานละเมิดข้อตกลงการใช้งาน หรือทำให้การให้บริการระบบเครือข่ายขัดข้อง โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

15.4. กรณีผู้ใช้งานเป็นข้าราชการ พนักงาน ลูกจ้าง นักศึกษา ของมหาวิทยาลัย พ้นสภาพการเป็นข้าราชการ พนักงาน ลูกจ้าง นักศึกษา ของมหาวิทยาลัย ศูนย์ IT จะยกเลิกสิทธิการใช้งานทันที

15.5. กรณีผู้ใช้งานเป็นบุคลากรจากภายนอกที่มหาวิทยาลัยอนุญาตให้ใช้ระบบคอมพิวเตอร์และระบบเครือข่ายของมหาวิทยาลัย จะสิ้นสุดสิทธิการใช้งาน เมื่อจบงานตามสัญญาการทำงาน

15.6. กรณีผู้ใช้งาน ฝ่าฝืนนโยบายความปลอดภัยสารสนเทศ การยกเลิกสิทธิผู้ใช้งานขึ้นอยู่กับดุลยพินิจของผู้อำนวยการ

16. มหาวิทยาลัยต้องจัดให้มีการสำรองข้อมูลที่สำคัญ

16.1. โดยต้องกำหนดรูปแบบ และวิธีการปฏิบัติ รวมทั้งแผนการสำรองข้อมูลที่เหมาะสมเพื่อป้องกันการสูญหายอันแดขึ้นจากภาวะคุกคาม และจากการเกิดภัยพิบัติ

16.2. จัดเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

16.3. จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์โดยใช้ระบบเอกสารแบบฟอร์ม

16.4. จัดทำแผนงบประมาณประจำปีปรับปรุงอุปกรณ์สำรองไฟฟ้า ระบบทำความเย็น ระบบสำรองข้อมูล และอุปกรณ์ป้องกันอัคคีภัย

17. กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยให้มีการตรวจสอบและควบคุมประสิทธิภาพของระบบงานเทคโนโลยีสารสนเทศและการสื่อสาร และดำเนินการตรวจประเมินระบบความมั่นคงปลอดภัยด้านระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยอย่างน้อยปีละ 1 ครั้ง

18. กำหนดให้มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ อย่างน้อยปีละ 1 ครั้ง

19. กรณีระบบเทคโนโลยีสารสนเทศและการสื่อสาร หรือข้อมูลสารสนเทศของมหาวิทยาลัยเกิดความเสียหาย หรือเกิดอันตรายใดๆ แก่องค์กร หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศกำหนดให้ผู้บริหารระดับสูงสุดของมหาวิทยาลัยเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

20. การกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของทางราชการ พ.ศ.2540 และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 หรือข้อกำหนดอื่นที่ได้ประกาศใช้ทดแทน

21. การตรวจสอบและประเมินความเสียงระบบสารสนเทศ จัดให้มีการตรวจสอบความเสี่ยงระบบสารสนเทศ และเทคโนโลยีสารสนเทศและการสื่อสาร โดยดำเนินการประเมินระบบอย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ : ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม

ศูนย์เทคโนโลยีสารสนเทศ มหาวิทยาลัยราชภัฏพิบูลสงคราม วันที่ 1 กุมภาพันธ์ 2559