แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ

มหาวิทยาลัยศรีนครินทรวิโรฒ

พ.ศ. 2557

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ
มหาวิทยาลัยศรีนครินทรวิโรฒ

มหาวิทยาลัยศรีนครินทรวิโรฒ ตระหนักถึงความสำคัญของสารสนเทศซึ่งนับเป็นสินทรัพย์ที่มีคุณค่าสูงสุดขององค์กร มหาวิทยาลัยจึงได้จัดทำนโยบายความมั่นคงปลอดภัยของสารสนเทศขึ้น เพื่อให้มั่นใจว่าสารสนเทศรวมทั้งระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยมีการดูแลด้านการบริหารจัดการอย่างมีประสิทธิภาพ ถูกต้องตามหลักมาตรฐานสากล และเป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง โดยมหาวิทยาลัยได้จัดทำแนวปฏิบัติขึ้นเพื่อใช้เป็นแนวทางสำหรับการกำหนดวิธีการปฏิบัติด้านการรักษาความมั่นคงปลอดภัยของสารสนเทศให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ ซึ่งแบ่งสาระสำคัญออกเป็น 7 ส่วน ประกอบด้วย

ส่วนที่ 1 การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
ส่วนที่2 การบริหารจัดการด้านการสื่อสารและเครือข่ายคอมพิวเตอร์สารสนเทศ
ส่วนที่ 3 การควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย
ส่วนที่ 4 การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ
ส่วนที่ 5 การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย
ส่วนที่ 6 การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย
ส่วนที่ 7 การปฏิบัติตามข้อกำหนด

ส่วนที่ 1
การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ตามนโยบายในหมวดที่ว่าด้วยการสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ซึ่งกำหนดขึ้นเพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์สารสนเทศ มหาวิทยาลัยจึงได้กำหนดมาตรการและแนวปฏิบัติในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและมีความจำเป็นที่ต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้บริการภายในมหาวิทยาลัยและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. ให้สำนักคอมพิวเตอร์ เป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน และมีการประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2. ให้สำนักคอมพิวเตอร์เป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

3. ให้สำนักคอมพิวเตอร์กำหนดมาตรการในการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

4. หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าออกห้องคอมพิวเตอร์กลาง

1. ผู้ดูแลระบบต้องกำหนดมาตรการการควบคุมและป้องกันบุคคลภายนอกในการเข้าถึงห้องคอมพิวเตอร์กลาง (data center) โดยจะต้องปฏิบัติอย่างน้อยดังนี้

1.1 ผู้ขอเข้าใช้ห้องต้องขออนุญาตโดยระบุถึงกิจกรรม หรือความจำเป็นในการเข้าใช้

1.2 ผู้ขอเข้าใช้ห้องต้องปฏิบัติตามกฎระเบียบของสำนักคอมพิวเตอร์อย่างเคร่งครัด

1.3 ผู้ขอเข้าใช้ห้องต้องไม่ทำการใด ๆ อันอาจก่อให้เกิดความเสียหายต่อทรัพย์สินของมหาวิทยาลัย

1.4 ผู้ขอเข้าใช้ห้องต้องติดบัตรแสดงตนให้ชัดเจน พร้อมทั้งลงบันทึกรายละเอียดของการเข้าใช้ เวลาเข้า เวลาออก รวมทั้งกิจกรรมที่ดำเนินการ

1.5 กรณีที่มีการใช้งานนอกเวลาทำการ ผู้ขอเข้าใช้ห้องต้องได้รับอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์ และเพื่อการจัดเตรียมเจ้าหน้าที่ของสำนักคอมพิวเตอร์ในการอำนวยความสะดวกสำหรับการปฏิบัติงานดังกล่าว

1.6 การเข้าดำเนินการกับระบบที่สำคัญจำเป็นต้องมีผู้รับผิดชอบระบบนั้นอยู่กำกับดูแลการปฏิบัติงานเสมอ และหากมีการกระทำการใด ๆ ที่อาจส่งผลต่อระบบจะต้องได้รับความเห็นชอบจากเจ้าของระบบนั้นก่อน

1.7 ต้องจัดให้มีพื้นที่สำหรับการส่งมอบ หรือขนย้ายอุปกรณ์ต่าง ๆ เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ห้องคอมพิวเตอร์กลาง โดยไม่จำเป็น

2. ผู้ดูแลระบบต้องควบคุมดูแลสภาพแวดล้อมของระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตรวจสอบการทำงานของระบบที่ใช้ในการควบคุมสภาพแวดล้อมเพื่อให้สามารถใช้งานได้ตามปกติ โดยแบ่งออกเป็น 3 ระบบดังนี้

2.1 ระบบตรวจจับควัน (smoke detector system) เพื่อป้องกันการเกิดอัคคีภัยของห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2.2 ระบบเครื่องปรับอากาศ (air conditioning system)เพื่อป้องกันการเกิดความชื้นจากละอองน้ำในห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2.3 ระบบไฟสำรองฉุกเฉิน (UPS) เพื่อป้องกันอุปกรณ์ และเครื่องคอมพิวเตอร์แม่ข่ายหยุดทำงาน

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

ส่วนที่ 2
การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ

ตามนโยบายในหมวดที่ว่าด้วยการบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ ซึ่งได้กำหนดขึ้นเพื่อให้การดำเนินงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติขึ้นเพื่อให้ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงหน้าที่ความรับผิดชอบด้านการจัดการและการใช้ระบบคอมพิวเตอร์และเครือข่ายสารสนเทศ และสามารถปฏิบัติตามอย่างเคร่งครัด โดยให้มี

ส่วนร่วมในการช่วยกันป้องกันสินทรัพย์และข้อมูลของมหาวิทยาลัยให้อยู่ในสภาพมีความมั่นคงปลอดภัย ซึ่งครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ

แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

1. การติดตั้งเครื่องคอมพิวเตอร์ลูกข่ายต้องดำเนินการตามแนวปฏิบัติซึ่งครอบคลุมประเด็นต่าง ๆ ดังนี้
    - การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (anti-virus)
    - การติดตั้งโปรแกรมปรับปรุงการอุดช่องโหว่ของวินโดว์ (Window update Patch)
    - การติดตั้งซอฟต์แวร์ลงทะเบียนเครื่อง
    - การติดตั้งซอฟต์แวร์พื้นฐาน

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

3. เครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องสามารถใช้งานระบบเครือข่ายทั้งเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศของมหาวิทยาลัยได้เท่าที่มีการอนุญาตให้ใช้งานหรือที่ได้มีการกำหนดสิทธิไว้เท่านั้น

4. ในการเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่าย ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติเกี่ยวกับการระบุและพิสูจน์ตัวตน และการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

5. การใช้แฟ้มข้อมูลร่วมกัน (shared file) ต้องมีการกำหนดให้ใช้วิธีการระบุชื่อผู้ใช้งานและรหัสผ่านให้ถูกต้องก่อนจึงจะสามารถเรียกใช้งานได้ ทั้งเครื่องคอมพิวเตอร์ลูกข่ายด้วยกันเอง และ เครื่องคอมพิวเตอร์ลูกข่ายกับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งชื่อผู้ใช้งานจะต้องเป็นไปตามแนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

6. ห้ามมิให้มีการใช้งานอุปกรณ์ต่อพ่วงโดยไม่ผ่านการยืนยันตัวตนโดยการแชร์ผ่านออกเครื่องเดียว (Shared Internet) หรือการนำอุปกรณ์ต่อพ่วง เช่น โทรศัพท์มือถือมาเชื่อมต่อยังเครื่องคอมพิวเตอร์ลูกข่ายเพื่อใช้เป็นช่องทางในการใช้งานอินเตอร์เน็ต

7. ห้ามเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม หรือไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

8. ห้ามทำการเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในหน่วยงานโดยมิได้รับอนุญาตจากสำนักคอมพิวเตอร์

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

10. ห้ามมิให้ทำการติดตั้งโปรแกรมที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์

11. เครื่องคอมพิวเตอร์จะต้องมีการกำหนดค่าการพักจอภาพ (screen saver) เพื่อให้มีการป้องกันการเข้าถึงระบบปฏิบัติการในขณะที่ไม่มีผู้ใช้งาน

ผู้รับผิดชอบ : ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย

1. ติดตั้งและใช้งานระบบปฏิบัติการที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

2. จัดทำรายการตรวจสอบ (checklist) สำหรับการติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย และปรับปรุงรายการตรวจสอบนั้นอย่างน้อยปีละ 1 ครั้ง โดยให้มีการระบุเวอร์ชั่นของรายการตรวจสอบอย่างชัดเจนเพื่อป้องกันความสับสนของการนำไปใช้งาน

3. ให้หน่วยงานที่รับผิดชอบดำเนินการติดตั้งเครื่องคอมพิวเตอร์ลูกข่ายตามรายการตรวจสอบที่ได้จัดทำขึ้น

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

5. ให้มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus)

6. ให้มีการกำหนดและติดตั้งซอฟต์แวร์เฉพาะที่จำเป็นต่อการปฏิบัติงานของมหาวิทยาลัยเท่านั้น โดยให้มีการทบทวนรายการซอฟต์แวร์พื้นฐานนั้นเพื่อให้เหมาะสมและสอดคล้องกับการปฏิบัติงานตามภารกิจของมหาวิทยาลัย

7. ต้องติดตั้งซอฟต์แวร์ที่ถูกลิขสิทธิ์และเป็นซอฟต์แวร์พื้นฐานที่จำเป็นต่อการใช้งานของมหาวิทยาลัยเท่านั้น

8. สำนักคอมพิวเตอร์จะดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์ลูกข่ายอย่างน้อยปีละ 1 ครั้ง

9. เครื่องคอมพิวเตอร์ที่ใช้ในการปฏิบัติงานจะต้องอยู่ในรายการมาตรฐานเครื่องคอมพิวเตอร์ลูกข่ายเท่านั้น

10. ต้องติดตั้งซอฟต์แวร์ลงทะเบียนคอมพิวเตอร์ลูกข่ายเพื่อเก็บแม็คแอดเดส ของเครื่องคอมพิวเตอร์เพื่อให้สามารถบอกได้ว่าเครื่องนั้นตั้งอยู่ที่ใดภายในมหาวิทยาลัยและผู้ใดเป็นเจ้าของเครื่องคอมพิวเตอร์เครื่องนั้น

11. เครื่องคอมพิวเตอร์จะต้องมีการกำหนดค่าเพื่อป้องกันการเข้าถึงระบบปฏิบัติการในขณะที่ไม่มีผู้ใช้งาน

12. เครื่องคอมพิวเตอร์จะต้องทำการตั้งค่าการพักจอภาพเมื่อมิได้มีการใช้งาน

13. เครื่องคอมพิวเตอร์จะต้องถูกล็อคหน้าจอทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

14. เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องมีการตั้งค่าการยืนยันตัวตนก่อนเข้าใช้งานระบบปฏิบัติการ

15. จัดทำรายงานเกี่ยวกับรายละเอียดของเครื่องคอมพิวเตอร์ลูกข่ายปีละ 1 ครั้ง

ผู้รับผิดชอบ : ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการใช้งานบัวศรีไอดี

1. ผู้ใช้บริการจะต้องเก็บรักษาบัวศรีไอดี (Buasri ID) ไว้เป็นความลับ ห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอนจำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยมิได้รับอนุญาต

2. ผู้ใช้บริการที่เป็นเจ้าของบัวศรีไอดี ต้องเป็นผู้รับผิดชอบต่อผลต่างๆ ที่เกิดขึ้นจากการใช้บริการเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3. ผู้ใช้บริการจะต้องลงบันทึกเข้า (Login) โดยใช้บัวศรีไอดีของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อหยุดการใช้งานชั่วคราว หรือเสร็จสิ้นการใช้งาน

ผู้รับผิดชอบ : ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการใช้รหัสผ่าน

1. รหัสผ่าน (password) จะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข หรือตัวอักษรพิมพ์เล็กหรือตัวพิมพ์ใหญ่ หรือตัวอักขระพิเศษ

2. รหัสผ่านต้องไม่เป็นคำที่มีความหมายทั้งภาษาไทยและภาษาอังกฤษ และเป็นคำที่ไม่มีความหมายในพจนานุกรม

3. ห้ามตั้งรหัสผ่านเหมือนกับชื่อหรือนามสกุล หรือสิ่งที่ง่ายต่อการคาดเดา

4. ห้ามจดบันทึกรหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถมองเห็นได้

5. ทำการเปลี่ยนแปลงรหัสผ่านใหม่ในทุกๆ 3 เดือน เป็นอย่างน้อย

6. ห้ามนำรหัสผ่านที่เคยใช้งานมาแล้วกลับมาใช้งานอีก

7. รหัสผ่านจะต้องความลับเฉพาะของบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยมิได้รับอนุญาต

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย

1. เครื่องคอมพิวเตอร์ภายในหน่วยงานทุกเครื่องต้องทำการอัพเดท (Update Patch) ของระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานอย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์

2. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการติดตั้งโปรแกรมป้องกันและกำจัดโปรแกรมประสงค์ร้าย (malware) รวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

3. ห้ามมิให้ผู้ใช้บริการทำการปิด หรือยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

4. หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย และต้องดำเนินการแจ้งสำนักคอมพิวเตอร์หรือผู้ที่เกี่ยวข้องดำเนินการแก้ไขก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่ายอีกครั้ง

5. ก่อนการใช้งานสื่อบันทึกแบบพกพา ต้องมีการตรวจสอบเพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย

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

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต

1. ห้ามผู้ใช้งานปฏิบัติการใด ๆ ที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดี โดยหากมีการกระทำดังกล่าวเกิดขึ้นถือเป็นความรับผิดชอบของผู้ใช้งาน ซึ่งอยู่นอกเหนือจากความรับผิดชอบของมหาวิทยาลัย

2. ห้ามผู้ใช้งานปฏิบัติการใด ๆ ที่ไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

3. ผู้ใช้งานจะต้องไม่ละเมิดสิทธิผู้อื่น โดยการดัดแปลงแก้ไขข้อมูล โดยมิได้รับอนุญาต

4. ห้ามผู้ใช้งานใช้งานในทางที่ไม่เหมาะสม สร้างความเสียหายให้กับผู้อื่น หรือ การใช้ภาษาที่ไม่สุภาพ หรือกระทำการใดๆ ที่จะทำให้ผู้อื่นเสียหาย

5. ห้ามผู้ใช้งานเข้าใช้งานระบบโดยมิได้รับอนุญาต การบุกรุก หรือพยายามเข้าใช้งานโดยมิได้รับอนุญาตถือเป็นความผิดตามระเบียบของมหาวิทยาลัย

6. มหาวิทยาลัยจะไม่รับประกันคุณภาพการเก็บข้อมูล การรับส่งข้อมูลข่าวสาร หรือการไม่สามารถใช้งานได้ของระบบบางส่วนหรือทั้งหมด และจะไม่รับผิดชอบความเสียหายอันเนื่องมาจากวงจรสื่อสารชำรุด จานแม่เหล็กชำรุด หรือความล่าช้าที่เกิดขึ้นในการใช้งาน

7. มหาวิทยาลัยขอสงวนสิทธิ์ในการยกเลิก หรือระงับการเชื่อมต่อ ในกรณีตรวจสอบพบการพยายามบุกรุกหรือทำให้ระบบของมหาวิทยาลัยมีประสิทธิภาพลดลง

8. ผู้ใช้งานต้องทำความเข้าใจและยอมรับระเบียบปฏิบัติที่มหาวิทยาลัยกำหนดขึ้น โดยจะอ้างว่าไม่ทราบระเบียบปฏิบัตินั้น ๆ มิได้

9. บัญชีผู้ใช้งาน (บัวศรีไอดี) นั้นมหาวิทยาลัยมอบให้เพื่อการใช้งานตามภารกิจของมหาวิทยาลัยเท่านั้น และห้ามมิให้ผู้อื่นที่ไม่ได้เกี่ยวข้องกับมหาวิทยาลัยนำไปใช้งาน

10. ถ้าเกิดความเสียหายขึ้นจากการใช้งานบัญชีผู้ใช้งาน ผู้เป็นเจ้าของต้องรับผิดชอบกับความเสียหายที่เกิดขึ้นเว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ และฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการบริหารจัดการระบบจดหมายอิเล็กทรอนิกส์

1. เครื่องคอมพิวเตอร์ที่เปิดให้บริการระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องเป็นเครื่องให้บริการของมหาวิทยาลัยที่ดูแลบริหารจัดโดยสำนักคอมพิวเตอร์เท่านั้น

2. ผู้ดูแลระบบต้องจัดให้มีระบบในการตรวจสอบจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ผ่านเข้าออกระบบบริการอิเล็กทรอนิกส์หลักของมหาวิทยาลัยเพื่อป้องกันปัญหาไวรัสและสแปม

แนวปฏิบัติการใช้บริการจดหมายอิเล็กทรอนิกส์

1. ผู้ใช้งานมีหน้าที่รับผิดชอบบัญชีบัวศรีที่ได้รับจากมหาวิทยาลัย ต้องระวังมิให้ผู้อื่นสามารถเข้าถึงรหัสผ่านเพื่อใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ของตนโดยมิชอบ

2. ผู้ใช้งานต้องรักษารหัสผ่านและไม่อนุญาตให้ผู้อื่นใช้รหัสผ่านของตน

3. ผู้ใช้งานพึงทราบว่าผู้ดูแลระบบไม่มีสิทธิถาม หรือร้องขอผู้ใช้ให้เปิดเผยรหัสผ่านเพื่อเข้าใช้งานบัญชีบัวศรี

4. ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

5. ห้ามเผยแพร่ หรือส่งต่อจดหมายลูกโซ่

6. ห้ามเผยแพร่ข้อมูลที่เป็นความลับของมหาวิทยาลัย

7. ห้ามปลอมแปลง หรือดัดแปลงชื่อผู้ส่งเพื่อให้บุคคลอื่นเข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นมาจากบุคคลอื่น

8. ห้ามปกปิด หรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

9. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่เผยแพร่ ข้อความ ภาพ วิดิโอ หรือเสียงที่ให้ร้ายต่อบุคคลหรือกลุ่มบุคคล หรือในลักษณะที่หยาบคาย หรือลามก อนาจาร

10. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรม หรือรหัสผ่านสำหรับการเข้าถึงโปรแกรมในลักษณะที่เป็นการละเมิดลิขสิทธิ์

11. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้ที่ไม่ต้องการ

12. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายไวรัส หรือโปรแกรมที่เป็นอันตรายกับความมั่นคงปลอดภัยของระบบเครือข่าย

13. ห้ามมิให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ที่ได้รับจากมหาวิทยาลัยไปสมัครสมาชิกตามเว็บไซต์ต่าง ๆ เพื่อประโยชน์ส่วนตน และไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

14. เมื่อได้รับรหัสผ่านครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

15. ผู้ใช้งานเปลี่ยนรหัสผ่านทุกๆ 3-6 เดือน

16. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงบันทึกออก (Logout) ทุกครั้ง

17. ผู้ใช้งานหลีกเลี่ยงการแนบไฟล์ขนาดใหญ่ โดยให้มีขนาดไม่เกิน 20 MB

18. ห้ามส่งข้อมูลที่เป็นความลับผ่านทางจดหมายอิเล็กทรอนิกส์โดยมิได้เข้ารหัสลับ

19. มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับการใช้งานบัญชีผู้ใช้ได้ทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากผู้ดูแลระบบตรวจพบความผิดปกติซึ่งอาจจะเกิดจากบัญชีผู้ใช้นั้น

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

ส่วนที่ 3
การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

ตามนโยบายในหมวดที่ว่าด้วยการควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย ซึ่งกำหนดขึ้นเพื่อให้เกิดมาตรการในควบคุมการเข้าถึงระบบ การบริหารการจัดการเข้าถึงของผู้ใช้ และการควบคุมการเข้าถึงเครือข่ายของมหาวิทยาลัย รวมถึงการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้ายที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้ มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติขึ้นเพื่อให้ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงความสำคัญของการควบคุม และได้ร่วมมือในการปฏิบัติอย่างถูกต้องเหมาะสมเพื่อช่วยกันการป้องกันการบุกรุกซึ่งจะส่งผลความเสียหายต่อระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย

แนวปฏิบัติของผู้ดูแลระบบ

1. ผู้ดูแลระบบ มีอำนาจหน้าที่ ดังต่อไปนี้

1.1 ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการที่ไม่เป็นไปตามนโยบายนี้ 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 ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

1.8 ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้บริการที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

1.9 ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

1.10 เมื่อผู้ดูแลระบบพ้นจากหน้าที่จะต้องคืนสินทรัพย์ของหน่วยงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการสำนักคอมพิวเตอร์ หรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

1.12 รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนการสำรองข้อมูล แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูลและการทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

2. ผู้ดูแลระบบจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้บริการเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่า 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

2.1 เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

2.2 มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ สามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่

ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (Internal IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

2.3 ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

2.4 เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยผิดพลาดไม่เกิน 10 มิลลิวินาที

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

1. มหาวิทยาลัยต้องกำหนดให้มีมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัย ในกรณีบุคคลจากหน่วยงานภายนอกหรือผู้รับจ้างจากภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรตามสายงานต่อผู้บริหารของหน่วยงานของมหาวิทยาลัย

2. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

3. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศที่มีต่อระบบข้อมูล

4. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ

5. ผู้ดูแลระบบต้องจัดให้มีการตรวจสอบการกำหนดสิทธิตามลำดับความสำคัญของระบบสารสนเทศ

6. ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร และกำหนดสิทธิการเข้าใช้งานระบบสารสนเทศจากภายนอก

7. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการเข้าใช้งานระบบสารสนเทศจากภายนอกองค์กร

8. ผู้ดูแลระบบต้องกำหนดความสำคัญของระบบสารสนเทศ และมีการควบคุมอุปกรณ์คอมพิวเตอร์ หรืออุปกรณ์สื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร เพื่อให้ระบบสารสนเทศที่สำคัญมีความปลอดภัยมากที่สุด

9. ผู้ดูแลระบบต้องติดตั้งระบบสารสนเทศที่มีความสำคัญสูงไว้บนเครื่องคอมพิวเตอร์แม่ข่ายในห้องคอมพิวเตอร์กลาง หรือห้องคอมพิวเตอร์ซึ่งมีสภาพแวดล้อมที่เหมาะสม เช่น ระบบสำรองไฟฟ้า และระบบปรับอากาศ เป็นต้น

10. ผู้ดูแลระบบต้องควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยกำหนดมาตรการและข้อปฏิบัติที่เหมาะสมเพื่อปกป้องสารสนเทศจากภาวะความเสี่ยงอันเนื่องมาจากการใช้อุปกรณ์เหล่านั้น

11. ผู้ดูแลระบบต้องกำหนดสิทธิและให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องทำการยืนยันตัวตนโดยใช้บัวศรีไอดีก่อนเข้าสู่ระบบของมหาวิทยาลัย

12. ผู้ดูแลระบบจะต้องมีระบบการบริหารจัดการรหัสผ่านที่ทำงานในลักษณะอัตโนมัติ เพื่อให้รหัสผ่านของผู้ใช้มีคุณภาพ

13. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงบริการสารสนเทศตามสิทธิที่ได้รับอนุญาตเท่านั้น

14. ผู้รับจ้างจากภายนอกต้องมีการลงนามรับรองว่าจะไม่นำข้อมูลของมหาวิทยาลัยออกไปเปิดเผยภายนอก

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

1. ผู้ดูแลระบบต้องกำหนดการลงทะเบียนบุคลากรและนิสิตใหม่ของมหาวิทยาลัย และกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน ดังต่อไปนี้

1.1 การลงทะเบียนเพื่อรับสิทธิการใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

1.1.1 กรณีนิสิตจะได้รับชื่อบัญชีและรหัสผู้ใช้งานภายใน 1 วัน หลังจากรายงานตัวและชำระเงินเรียบร้อยแล้ว

1.1.2 กรณีบุคลากรจะได้รับชื่อบัญชีและรหัสผู้ใช้งานภายใน 1 วัน หลังจากกองการเจ้าหน้าที่จัดทำคำสั่งบรรจุบุคลากร และบันทึกข้อมูลในระบบสมบูรณ์แล้ว

1.2 การยกเลิกสิทธิการใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

1.2.1 กรณีนิสิตจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 7 วัน หลังจากการขึ้นทะเบียนพ้นสภาพการเป็นนิสิตในระบบสมบูรณ์แล้ว

1.2.2 กรณีบุคลากรจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 30 วัน หลังจากกองการเจ้าหน้าที่จัดทำคำสั่งให้พ้นสภาพการเป็นบุคลากร 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 กรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุง ผู้ใช้งานจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานปกติ

3.3 กรณีมีการว่าจ้างผู้รับจ้างจากภายนอกจะต้องกำหนดระยะเวลาการใช้งานของผู้รับจ้างภายนอกและระงับการใช้งานทันทีเมื่องานดังกล่าวเสร็จสิ้นหรือสิ้นสุดสัญญา

4. ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้บริการ ดังต่อไปนี้

4.1 กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

4.2 ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งมอบให้กับบุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

4.3 ห้ามมิให้ผู้ใช้งานบันทึก หรือเก็บรหัสผ่านไว้บนระบบคอมพิวเตอร์ในแบบที่มิได้ป้องกันการเข้าถึง

4.4 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บริหารของหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที

เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ในระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานสูงสุดต่างจากรหัสผู้ใช้งานตามปกติ

5. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานตามประเภทของข้อมูล ความสำคัญของข้อมูล ความลับของข้อมูล และลำดับชั้นการเข้าถึงของข้อมูลโดยการเข้าถึงนั้นจะต้องเข้าถึงได้โดยผู้ที่ได้รับอนุญาตเท่านั้น

5.1 ต้องมีการกำหนดประเภทของข้อมูล ซึ่งมีการจัดแบ่งไว้เป็น 3 ประเภท คือ

5.1.1 ข้อมูลสารสนเทศด้านการบริหารงาน เช่น ระบบคลังข้อมูลมหาวิทยาลัย ระบบภาระงานบุคลากรสายวิชาการ

5.1.2 ข้อมูลสารสนเทศด้านการบริการอาจารย์ นิสิต และบุคลากร เช่น ระบบบริการการศึกษา ระบบทรัพยากรบุคคล

5.1.3 ข้อมูลสารสนเทศด้านการบริการบุคคลทั่วไป เช่น ระบบรับนิสิตใหม่ ระบบประชาสัมพันธ์

5.2 ต้องมีการจัดลำดับความสำคัญของข้อมูลโดยแบ่งออกเป็น 3 ลำดับคือ

5.2.1 ข้อมูลที่มีระดับความสำคัญมากที่สุด

5.2.2 ข้อมูลที่มีระดับความสำคัญปานกลาง

5.2.3 ข้อมูลที่มีระดับความสำคัญน้อย

5.3 ต้องมีการกำหนดระดับชั้นของการเข้าถึงข้อมูล โดยมีการพิสูจน์สิทธิในการเข้าถึงข้อมูลแต่ละระดับชั้น และต้องกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นการเข้าถึงข้อมูล โดยแบ่งระดับชั้นออกเป็น 3 ระดับชั้น คือ

5.3.1 ระดับชั้นสำหรับผู้บริหาร

5.3.2 ระดับชั้นสำหรับผู้ใช้งานทั่วไป

5.3.3 ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย

5.4 ต้องกำหนดระยะเวลาในการเข้าถึง และวิธีการในการระงับการใช้งานเมื่อพ้นระยะเวลาดังกล่าว

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

	- ข้อมูลการขอตำแหน่ง - ข้อมูลการเลื่อนขั้นเงินเดือน - คำสั่งพ้นราชการ - คำสั่งสอบทางวินัย - ทายาทบำเหน็จตกทอด ข้อมูลนิสิต ได้แก่ - ผลการเรียน - หลักฐานการจ่ายเงิน - เลขที่บัญชีธนาคาร	- สิทธิประโยชน์และสวัสดิการ - ประวัติครอบครัว - ประวัติการลา	- ตำแหน่ง - สาขาที่จบการศึกษา - รูปถ่ายที่ใช้ภายในมหาวิทยาลัย ข้อมูลนิสิต ได้แก่ - ชื่อ-นามสกุล - คณะ สาขาวิชา - ปีการศึกษา - ชั้นปี - สถานภาพ - ตารางสอน ข้อมูลทั่วไปของมหาวิทยาลัย - แผนที่มหาวิทยาลัย - ตำแหน่งงาน - ผลงานทางวิชาการ

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

1. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (username) และรหัสผ่าน (password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน
2. ผู้ใช้บริการต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และ รหัสผ่านของตนเพื่อการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน
3. ผู้ใช้บริการต้องตั้งค่าการพักจอภาพ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้ต้องใส่รหัสผ่านของผู้เข้าใช้งาน
4. ผู้ใช้ต้องทำการออกจากระบบปฏิบัติการ (logout) ทุกครั้งทันทีเมื่อเลิกใช้งาน

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ และฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) ให้อยู่ในพื้นที่ใช้งานระบบเครือข่ายไร้สายของมหาวิทยาลัย โดยให้มีการรั่วไหลน้อยที่สุด
2. ผู้ดูแลระบบต้องทำการเปลี่ยนค่าเอสเอสไอดี (SSID หรือ Service Set Identifier) ตามที่ได้ถูกกำหนดเป็นค่าเริ่มต้นไว้ (default setting) โดยผู้ผลิต ทันทีที่นำอุปกรณ์กระจายสัญญาณมาติดตั้งใช้งาน

3. อุปกรณ์กระจายสัญญาณที่มีคุณสมบัติตามข้อกำหนดมาตรฐานของมหาวิทยาลัยจะต้องถูกติดตั้งระบบการยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีของมหาวิทยาลัย

4. กรณีอุปกรณ์กระจายสัญญาณที่จัดหาไม่สามารถติดตั้งระบบการยืนยันการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีตามข้อ 3 ได้นั้น ผู้ดูแลระบบจะต้องดำเนินการติดตั้งให้เป็นแบบบริดจ์ (bridge) เท่านั้นเพื่อให้ผู้ใช้งานยืนยันตัวตนผ่านระบบบัวศรีของมหาวิทยาลัย

5. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งไฟร์วอลล์ (firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน

6. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์ หรือ ฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยติดตามและบันทึกเหตุการณ์น่าสงสัยในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจพบความผิดปกติในการใช้งาน ผู้ดูแลระบบต้องรายงานต่อผู้บริหารของหน่วยงานให้ทราบทันที

7. ผู้ดูแลระบบต้องควบคุมดูแลมิให้บุคคล หรือ หน่วยงานภายนอกที่มิได้รับอนุญาตเข้าใช้บริการระบบเครือข่ายไร้สายของมหาวิทยาลัยเพื่อผ่านเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในของมหาวิทยาลัย

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

แนวปฏิบัติในการติดตั้งสวิตช์และฮับ

1. การเชื่อมต่ออุปกรณ์สวิชต์ (switch) หรือ ฮับ (hub) หรืออุปกรณ์เชื่อมต่ออื่นใดที่จะนำมาพ่วงต่อกับระบบเครือข่ายของมหาวิทยาลัย จะต้องได้รับอนุญาตก่อนเท่านั้น

2. การเดินสายยูทีพี (UTP) หรือดำเนินการติดตั้งยูทีพี บนอุปกรณ์สวิชต์ หรือ ฮับในตู้แร็คที่ดูแลโดยสำนักคอมพิวเตอร์ จะต้องแจ้งสำนักคอมพิวเตอร์ก่อนทุกครั้ง

3. หมายเลขไอพีที่ติดตั้งบนอุปกรณ์สวิตช์ จะต้องเป็นหมายเลขที่กำหนดให้โดยสำนักคอมพิวเตอร์เท่านั้น ห้ามดำเนินการโดยมิได้รับอนุญาต

4. อุปกรณ์สวิตช์ที่ติดตั้งจะต้องสามารถตรวจสอบผ่านโปรโตคอลเอสเอ็นเอ็มพี (SNMP) เพื่อสำนักคอมพิวเตอร์สามารถตรวจสอบการทำงานของอุปกรณ์นั้นได้

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

1. ให้สำนักคอมพิวเตอร์กำหนดมาตรการควบคุมการเข้า-ออก ห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่าย

2. ผู้ใช้บริการจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

3. การขอใช้งานพื้นที่เครื่องให้บริการเว็บ (web server) และชื่อโดเมนย่อย (sub domain name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้อำนวยการสำนักคอมพิวเตอร์ และจะต้องไม่ลงโปรแกรมที่เป็นอันตรายและส่งผลกระทบต่อการใช้งานของผู้ใช้บริการอื่น ๆ

4. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ซึ่งได้แก่ อุปกรณ์จัดเส้นทาง (router) อุปกรณ์สวิตช์ อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

5. ผู้ดูแลระบบจะต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้การบริหารจัดการระบบเครือข่ายเป็นไปอย่างมีประสิทธิภาพ ดังต่อไปนี้

5.1 มีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

5.2 มีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

5.3 กำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้

5.4 ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกซึ่งต้องสามารถตรวจจับโปรแกรมประสงค์ร้ายได้

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

5.6 การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน เพื่อผ่านออกสู่อินเทอร์เน็ตต้องทำการบันทึกเข้า (Login) โดยระบุชื่อผู้ใช้และรหัสผ่านโดยใช้บัวศรีไอดีของผู้ใช้บริการเพื่อใช้ยืนยันผ่านระบบพิสูจน์ตัวตนของมหาวิทยาลัยเพื่อใช้ติดตามตรวจสอบความถูกต้องของการใช้บริการ

5.7 หมายเลขไอพี (IP Address) ภายในของระบบเครือข่ายภายในของหน่วยงาน จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

5.8 จัดทำแผนผังระบบเครือข่าย (network diagram) โดยระบุรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก ที่สามารถระบุบนระบบเครือข่ายและใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยันแม็คแอดเดส พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

5.9 การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

6. ผู้ดูแลระบบต้องดูแลรับผิดชอบระบบคอมพิวเตอร์เครื่องแม่ข่าย โดยควบคุมในเรื่องข้อกำหนดในการแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

7. ให้สำนักคอมพิวเตอร์ กำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีครบถ้วน ถูกต้อง เพื่อให้สามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

7.1 จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล ผู้ดูแลระบบมิได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน (Internal IT Auditor) หรือบุคคลที่หน่วยงานมอบหมาย

7.2 กำหนดให้มีการบันทึกการทำงานของระบบการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งานคำสั่ง (command line) และ บันทึกไฟร์วอลล์ (firewall log) เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

7.3 ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

7.4 ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

8. ให้สำนักคอมพิวเตอร์ กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

8.1 บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานจะต้องทำหนังสือถึงผู้อำนวยการสำนักคอมพิวเตอร์เพื่อขออนุญาตก่อน

8.2 ผู้ดูแลระบบควบคุมช่องทางพอร์ต (port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องไม่เปิดช่องทางที่ใช้ทิ้งไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อโดยอัตโนมัติเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

8.3 วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องได้รับอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์ก่อน

8.4 การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

8.5 การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนโดยใช้บัวศรีไอดีของมหาวิทยาลัย

8.6 การเข้าสู่ระบบต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น การใช้วีพีเอ็น เอสเอสแอล เป็นต้น

8.7 ผู้ดูแลระบบจะต้องกำหนดช่องทาง ที่ใช้ในการเข้าสู่ระบบ และจะต้องตรวจสอบและติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

9. ผู้ดูแลระบบต้องกำหนดวิธีการปกปิดหมายเลขไอพีของระบบงานภายในเครือข่ายของหน่วยงาน เพื่อป้องกันมิให้บุคคลภายนอกสามารถทราบข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้ โดยทำการแบ่งแยกเป็นหมายเลขไอพีสาธารณะ (public IP Address) และ หมายเลขไอพีภายใน (private IP Address) เพื่อแยกเครือข่ายย่อย และให้มีการจัดทำการแปลงหมายเลขเครือข่าย (NAT (Network Address Translation)

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ

ให้สำนักคอมพิวเตอร์กำหนดมาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแลดังต่อไปนี้

1. ผู้ใช้บริการต้องออกจากระบบสารสนเทศโดยทันทีเมื่อเสร็จสิ้นงาน เช่น ระบบสารสนเทศ เครื่องคอมพิวเตอร์ เป็นต้น

2. ผู้ใช้บริการป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตนโดยใส่รหัสผ่านได้ถูกต้องก่อนเข้าใช้งานเครื่องคอมพิวเตอร์

3. ผู้ใช้บริการต้องล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือปล่อยทิ้งไว้โดยไม่มีดูแล

4. สร้างความตระหนักและให้เกิดความเข้าใจในมาตรการป้องกันการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

5. ออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน หรือต้องพักหน้าจอไว้เป็นเวลานาน ๆ

6. ระบบสารสนเทศจะต้องมีการกำหนดค่าการตัดการใช้งานระบบ (idle timeout) ภายใน 20 นาทีหลังจากที่ไม่มีการใช้งาน

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการควบคุมการใช้สินทรัพย์สารสนเทศ

1. ผู้ดูแลระบบและผู้ใช้งานจะต้องออกจากระบบ (logout) ทุกครั้งเมื่อเลิกการใช้งาน
2. ผู้ใช้งานจะต้องปิดเครื่อง (shut down) เครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน ณ สิ้นวัน
3. เอกสารที่เป็นความลับทางราชการ จะต้องเก็บอยู่ในลิ้นชักที่ปลอดภัยและไม่วางเอกสารความลับทางราชการไว้ที่โต๊ะหลังเลิกงาน
4. เอกสารที่เป็นความลับทางราชการจะต้องเก็บอยู่ในลิ้นชักที่สามารถล๊อคได้
5. กุญแจที่สามารถเปิดลิ้นชักเอกสารลับจะต้องมีผู้รับผิดชอบและอยู่ในที่ปลอดภัย
6. ผู้ใช้งานจะต้องไม่บันทึกรหัสผ่านเก็บไว้ที่โต๊ะหรือเครื่องคอมพิวเตอร์ที่ใช้งาน
7. เมื่อมีการพิมพ์เอกสารความลับทางราชการออกผ่านทางเครื่องพิมพ์จะต้องรีบนำออกจากเครื่องพิมพ์ทันที
8. เมื่อได้รับเอกสารความลับทางราชการผ่านเครื่องโทรสารจะต้องรีบนำออกจากเครื่องโทรสารทันที
9. กรณีที่มีการแทงจำหน่ายอุปกรณ์คอมพิวเตอร์ หรือ อุปกรณ์จัดเก็บข้อมูลที่มีข้อมูลที่เป็นความลับทางราชการจะต้องดำเนินการทำลายข้อมูลนั้นก่อนทุกครั้ง โดยวิธีการทำลายข้อมูลจะต้องดำเนินการดังตารางนี้

	การทำลายข้อมูล		
ฮาร์ดดิสก์ (Hard Disk)	ระดับที่ 1 (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	-	-	ย่อยเพื่อทำลาย
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 สำนักคอมพิวเตอร์ หรือ หน่วยงานที่ดูแลระบบของมหาวิทยาลัย

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ ฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

แนวปฏิบัติการบริหารจัดการสิทธิและการแบ่งแยกเครือข่าย

1. แบ่งแยกและควบคุมเครือข่ายด้วยอุปกรณ์ไฟร์วอลล์ (firewall) และทำงานร่วมกันกับอุปกรณ์เครือข่ายสวิตช์ ซึ่งสามารถกำหนดเครือข่ายเสมือน (VLAN) ได้

2. การจัดแบ่งเครือข่ายผู้ใช้งานภายในให้ทำการจัดแบ่งตามภารกิจ และหน้าที่ โดยจำกัดการเข้าถึงข้ามส่วนงานหรือกลุ่มงาน เพื่อป้องกันข้อมูลรั่วไหล หรือการโจมตีในเครือข่าย

3. การใช้งานบนเครือข่ายหลักต้องมีการแบ่งแยกพื้นที่หรือโซนการทำงานตามความเหมาะสม โดยอย่างน้อยให้เป็นส่วน ๆ ดังนี้

   3.1 โซนผู้ใช้งาน (Intranet)

   3.2 โซนเครือข่ายไร้สาย (Wireless)

   3.3 โซนเจ้าหน้าที่ดูแลระบบ (Administrator)

   3.4 โซนเครื่องคอมพิวเตอร์แม่ข่ายให้บริการสาธารณะ (Public Server)

   3.5 โซนเครื่องคอมพิวเตอร์แม่ข่ายโปรแกรมประยุกต์ เฉพาะงาน (Application Server)

   3.6 โซนเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเฉพาะภายในกรม เท่านั้น (Internal Server)

   3.7 โซนเครือข่ายส่วนขยายของมหาวิทยาลัย

4. โซนผู้ใช้งานมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

   4.1 สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

   4.2 สามารถเข้าใช้งานบนระบบสารสนเทศภายในได้โดยไม่มีการจำกัดด้านเวลา

   4.3 สามารถใช้งานอินเทอร์เน็ตได้ต่อเมื่อมีการ login โดยใช้บัวศรีไอดีเท่านั้น

5. โซนเครือข่ายไร้สาย มีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้ (ให้ถือปฏิบัติ เมื่อมหาวิทยาลัยมีระบบดังกล่าวแล้ว)

   5.1 สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

   5.2 สามารถใช้งานอินเทอร์เน็ตได้ต่อเมื่อมีการ login โดยใช้บัวศรีไอดีเท่านั้น

6. โซนเจ้าหน้าที่ภายนอก กำหนดให้เป็นกลุ่มของผู้รับจ้างดูแลระบบเครือข่ายของมหาวิทยาลัยโดยมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

6.1 ไม่สามารถเชื่อมต่อไปยังภายนอกโซนของตนเองเว้นแต่มีการขออนุญาตเป็นกรณีพิเศษ ซึ่งจะต้องได้รับความเห็นชอบจากสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษร

7. โซนเจ้าหน้าที่ดูแลระบบมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

7.1 สามารถเชื่อมต่อเข้าไปยังระบบเครือข่ายของมหาวิทยาลัยได้ทุกที่และตลอดเวลา

8. โซนเครื่องคอมพิวเตอร์แม่ข่ายโดยต้องมีการกำหนดระดับความสำคัญ และความต้องการเพื่อจำแนกเครื่องแม่ข่ายไปยังตำแหน่งที่เหมาะสม ไม่ว่าจะเป็นกลุ่มของเครื่องแม่ข่ายที่ให้บริการสาธารณะ ระบบโปรแกรมประยุกต์ และเครื่องแม่ข่ายที่ให้บริการเฉพาะภายในเท่านั้น

8.1 สามารถเชื่อมต่อจากโซนต่างๆของมหาวิทยาลัยที่ได้กำหนดไว้ เพื่อเข้ามาใช้บริการบนเครื่องคอมพิวเตอร์แม่ข่าย

8.2 เครื่องคอมพิวเตอร์ภายนอกเครือข่ายจะต้องไม่สามารถติดต่อเข้ามายังเครื่องแม่ข่ายที่อยู่ในกลุ่มเพื่อให้บริการภายในเท่านั้น

8.3 เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถเรียกออกไปยังอินเทอร์เน็ตได้เว้นแต่มีเหตุจำเป็นที่จะต้องเชื่อมต่อ เช่น การใช้งานดีเอ็นเอส (DNS) ของเครื่องคอมพิวเตอร์แม่ข่าย การปรับปรุงเรื่องไวรัส เป็นต้น

9. สำนักคอมพิวเตอร์สามารถทักท้วง หรือไม่อนุญาตให้มีการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย หรือเครื่องคอมพิวเตอร์แม่ข่ายได้ หากตรวจพบความผิดปกติซึ่งอาจก่อให้เกิดความเสียหาย หรือมีความไม่เหมาะสมกับระบบเครือข่าย หรือต่อมหาวิทยาลัย

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

แนวปฏิบัติการจัดการไฟร์วอลล์

1. สำนักคอมพิวเตอร์มีหน้าที่ในการบริหารจัดการและกำหนดค่าการใช้งานของอุปกรณ์รักษาความปลอดภัย (firewall) ส่วนกลางบนเครือข่ายบัวศรีของมหาวิทยาลัย
2. บริการต่าง ๆ จะถูกปฏิเสธทั้งหมด ยกเว้นแต่บริการที่ทางสำนักคอมพิวเตอร์เปิดให้บริการเท่านั้น
3. ก่อนการใช้งานอินเทอร์เน็ตทุกครั้ง ผู้ใช้งานจะต้องทำการล็อกอินโดยใช้บัวศรีไอดี
4. การเปลี่ยนแปลงการกำหนดค่าต่าง ๆ บนอุปกรณ์รักษาความปลอดภัยจะต้องดำเนินการโดยผู้ที่ได้รับมอบหมายเท่านั้น โดยทุกครั้งที่มีการเปลี่ยนแปลงต้องบันทึกข้อมูล และสำรองข้อมูลค่าต่าง ๆ ไว้ก่อนเสมอ
5. การให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตที่เป็นการใช้งานพื้นฐานโปรแกรมทั่วไปเท่านั้น กรณีผู้ใช้ต้องการเชื่อมต่อผ่านพอร์ตอื่นนอกเหนือจากที่กำหนดไว้ต้องได้รับอนุญาตจากสำนักคอมพิวเตอร์ก่อน
6. พอร์ตที่ใช้สำหรับตรวจสอบและการปรับแต่งระบบจะถูกปิดทั้งหมดและจะต้องเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น
7. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายจะต้องกำหนดค่าการให้บริการที่จำเป็นต่อการให้บริการตามแบบฟอร์มขอเปิดใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น
8. เส้นทางการเชื่อมต่อระบบเครือข่ายจะต้องมีการควบคุมเพื่อป้องกันข้อมูลสารสนเทศที่มีความสำคัญสูง

9. ในกรณีตรวจพบว่าเครื่องคอมพิวเตอร์ลูกข่ายใดที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย หรือ มีการใช้งานอันจะก่อให้เกิดปัญหาต่อเครือข่าย สำนักคอมพิวเตอร์ขอสงวนสิทธิ์ในการระงับ หรือ บล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายนั้นจนกว่าจะดำเนินการแก้ไขเสร็จสิ้น
10. ผู้ละเมิดนโยบายด้านความปลอดภัยของระบบเครือข่ายบัวศรีของมหาวิทยาลัยจะถูกระงับการใช้งานทันทีโดยมิต้องแจ้งให้ทราบล่วงหน้า

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย สำนักคอมพิวเตอร์

ส่วนที่ 4
การจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ

ตามนโยบายในหมวดที่ว่าด้วยการจัดหาพัฒนาและบำรุงรักษาระบบสารสนเทศ ซึ่งกำหนดขึ้นเพื่อให้การพัฒนาและบำรุงระบบสารสนเทศสามารถดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัย และเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศ มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติสำหรับการดำเนินการพัฒนาระบบขึ้นเพื่อให้ผู้ออกแบบ ผู้พัฒนา รวมทั้งผู้ดูแลระบบได้ตระหนักถึงความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติอย่างเคร่งครัด

แนวปฏิบัติการพัฒนาระบบสารสนเทศ

1. การออกแบบระบบสารสนเทศต้องคำนึงถึงความต้องการในการใช้งานและความต้องการของผู้ใช้
2. การวิเคราะห์และออกแบบระบบสารสนเทศ ต้องคำนึงถึงความปลอดภัยในการเข้าถึงและจัดเก็บข้อมูล โดยระบบสารสนเทศหลักที่มีความสำคัญ ต้องมีการเข้ารหัสของการสื่อสารระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายด้วยมาตรฐานใบรับรอง (SSL)
3. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องมีกระบวนการระบุและพิสูจน์ตัวตนตามนโยบาย และแนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน
4. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องสามารถแบ่งแยกระดับของผู้ใช้งานได้ เช่น ผู้ใช้งานทั่วไป เจ้าหน้าที่ดูแลระบบ ผู้เยี่ยมชม เป็นต้น
5. การแบ่งแยกระดับของผู้ใช้งานต้องสามารถกำหนดสิทธิการเข้าใช้งานได้ชัดเจน เช่น สามารถมองเห็นเมนูใดได้บ้าง สามารถแก้ไขข้อมูลใดได้บ้าง สามารถลบข้อมูลใดได้บ้าง เป็นต้น
6. ต้องมีการจัดเก็บข้อมูลการเข้าใช้ระบบงาน (log) โดยมีรายละเอียดดังนี้เป็นอย่างน้อย เช่น (1) วันที่และเวลา (2) ผู้ใช้งาน
7. กำหนดให้มีการตัดการเชื่อมต่อระหว่างระบบกับผู้ใช้งานได้โดยอัตโนมัติ (Session Timeout) หากผู้ใช้งานมิได้มีการทำกิจกรรมใดๆ กับระบบนั้นเป็นเวลาเกินกว่า 10 นาที หรือตามความเหมาะสม
8. ระบบสารสนเทศที่มีความสำคัญสูงจะต้องมีการจำกัดระยะเวลาการเชื่อมต่อโดยให้มีการเชื่อมต่อครั้งละไม่เกิน 2 ชั่วโมง

9. ในการพัฒนาระบบ การทดสอบระบบ ต้องพัฒนาบนเครื่องคอมพิวเตอร์ที่จัดเตรียมไว้สำหรับการพัฒนาเท่านั้น

10. ผู้พัฒนาระบบต้องตรวจสอบและควบคุมเวอร์ชันของซอร์สโค้ด และต้องมีระบบการสำรองซอร์สโค้ด ก่อนการแก้ไขทุกครั้ง

11. ผู้พัฒนาระบบต้องทำการทดสอบระบบตั้งแต่การนำข้อมูลเข้า กระบวนการประมวลผล และตรวจสอบผลลัพธ์จากการประมวลผลทุกครั้งก่อนนำระบบขึ้นใช้งานจริง

12. ระบบที่พัฒนาขึ้นต้องมีการควบคุมเวอร์ชั่นของโปรแกรม เพื่อใช้ในการควบคุมเปลี่ยนแปลงหรือ แก้ไขและต้องมีการทดสอบการทำงานทุกครั้งหลังการเปลี่ยนแปลง

13. มีการควบคุมการเข้าถึงซอร์สโค้ดของระบบ โดยจะสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้น

14. ต้องมีการปรับปรุงซอฟต์แวร์อย่างสม่ำเสมอหรือตามคำแนะนำของผู้ผลิตซอฟต์แวร์เพื่อป้องกันไม่ให้เกิดช่องโหว่และต้องดำเนินการติดตั้งกับเครื่องทดสอบก่อนเท่านั้น จึงจะดำเนินการกับเครื่องที่ใช้งานหลัก

ผู้รับผิดชอบ : ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

ส่วนที่ 5
การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย

ตามนโยบายในหมวดที่ว่าด้วยการดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย ซึ่งกำหนดขึ้นเพื่อให้มีระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และใช้เป็นเครื่องมือที่ช่วยในการตรวจสอบและปรับปรุงแก้ไขระบบให้มีประสิทธิภาพมากยิ่งขึ้น มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติเพื่อการตรวจสอบ และจัดการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างเหมาะสม และมีประสิทธิภาพ

แนวปฏิบัติการจัดการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

1. ผู้ดูแลระบบต้องดำเนินการตรวจสอบการใช้งานระบบเครือข่ายโดยใช้เครื่องมือในการตรวจสอบและจัดเก็บข้อมูลการให้บริการเครือข่าย

2. เมื่อมีเหตุการณ์ผิดปกติซึ่งทำให้ไม่สามารถให้บริการได้ หรือการใช้งานไม่สะดวกจะต้องดำเนินการแจ้งให้ผู้ใช้ทราบและจัดเก็บลงระบบรายงานปัญหาเครือข่าย

3. ผู้ดูแลระบบจะต้องเร่งดำเนินการแก้ไขปัญหาให้สามารถกลับมาใช้งานได้ตามปกติ ในกรณีที่ไม่สามารถใช้งานได้ตามช่วงเวลาดังกล่าวจะต้องดำเนินการแจ้งเป็นลำดับขั้นดังต่อไปนี้

4. หลังจากใช้งานไม่ได้ 10 นาที ต้องดำเนินการประกาศแจ้งที่หน้าประชาสัมพันธ์ข่าวประกาศเครือข่ายและแจ้งหัวหน้าฝ่ายที่เกี่ยวข้อง

5. หลังจากใช้งานไม่ได้ 3 ชั่วโมง ต้องดำเนินการแจ้งรองผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อพิจารณาแนวทางแก้ไขปัญหา

6. หลังจากใช้งานไม่ได้ 1 วัน ต้องดำเนินการแจ้งผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อพิจารณาแนวทางการแก้ไขปัญหา

7. หลังจากใช้งานไม่ได้ 2 วัน ต้องดำเนินการแจ้งมหาวิทยาลัยเพื่อพิจารณาแนวทางการแก้ไขปัญหา

8. เมื่อดำเนินการแก้ไขเสร็จสิ้น ต้องทำการรายงานผลการดำเนินการในระบบข่าวประกาศเครือข่าย และจัดทำคู่มือแนวปฏิบัติและวิธีการแก้ไขปัญหา

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ และฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์

ส่วนที่ 6
การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย

ตามนโยบายในหมวดที่ว่าด้วยการบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย ซึ่งกำหนดขึ้นเพื่อมิให้การดำเนินงานตามภารกิจของมหาวิทยาลัยต้องเกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานตามภารกิจที่สำคัญของมหาวิทยาลัยต้องได้รับผลกระทบ หรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และเพื่อให้มั่นใจได้ว่าสามารถกู้ระบบคืนได้ในระยะเวลาที่เหมาะสม มหาวิทยาลัยจึงได้กำหนดแนวปฏิบัติเพื่อการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบบความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

1. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้

   1.1 ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)

   1.2 ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยมิได้รับอนุญาต

   1.3 ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

   1.4 ความเสี่ยงที่เกิดจากการลงบันทึกเข้า (Login) สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บริการคนเดียวกันมากกว่าหนึ่งจุด

   1.5 ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่านของผู้อื่นโดยมิได้รับอนุญาต

2. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น โดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบในด้าน

   2.1 ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

   2.2 ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

   2.3 จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

3. กำหนดมาตรการจัดการความเสี่ยง

   3.1 ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับ

ระบบสารสนเทศ (IT contingency plan)

3.2 ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ 1 ครั้ง

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

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการสำรองข้อมูล

1. จัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของหน่วยงานจากจำเป็นมากไปหาน้อย

2. มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

3. จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจนข้อมูลที่สำรองต้องจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ในสถานที่จัดทำระบบสำรอง และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างน้อยปีละ 2 ครั้ง

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

แนวปฏิบัติการจัดทำระบบสำรอง

1. พิจารณาคัดเลือกระบบสำรองที่เหมาะสมกับมหาวิทยาลัยให้พร้อมใช้งานอยู่เสมอ
2. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง
3. กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูง และจำเป็นต้องมีแผนรับมือ
4. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลแต่ละระบบสารสนเทศ และระบบสำรองข้อมูล
5. ทำการประเมินความเสี่ยงที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัด หรือไม่สามารถใช้งานได้ อันเป็นผลจากภัยพิบัติที่ได้กำหนดไว้
6. กำหนดกระบวนการรายงานผลต่อผู้ดูแลรับผิดชอบในแต่ละระดับชั้น เมื่อเกิดภัยพิบัติ
7. ทดสอบ ประเมิน และปรับปรุงแผนรับมือเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ สำนักคอมพิวเตอร์

ส่วนที่ 7
การปฏิบัติตามข้อกำหนด

ตามนโยบายในหมวดที่ว่าด้วยการปฏิบัติตามข้อกำหนด ซึ่งกำหนดขึ้นเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยรับทราบ และปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยจึงได้กำหนดแนวปฏิบัติเพื่อให้มีการเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

1. จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
2. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาปีละไม่น้อยกว่า 1 ครั้ง โดยอาจจัดร่วมกับการสัมมนาอื่นด้วยก็ได้ และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ มาถ่ายทอดความรู้
3. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
4. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

ผู้รับผิดชอบ : ฝ่ายระบบคอมพิวเตอร์และเครือข่าย ฝ่ายระบบสารสนเทศ และฝ่ายปฏิบัติการและบริการ สำนักคอมพิวเตอร์