เอกสารแนบท้ายประกาศมหาวิทยาลัยศรีนครินทรวิโรฒ
เรื่อง แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของสารสนเทศ

หมวด 1
การสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ตามนโยบายในหมวดที่ว่าด้วยการสร้างความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม ซึ่งกำหนดขึ้นเพื่อป้องกันการเข้าถึงทางกายภาพโดยมิได้รับอนุญาต ป้องกันความเสียหายและการคุกคามสินทรัพย์สารสนเทศ มหาวิทยาลัยจึงได้กำหนดมาตรการและแนวปฏิบัติในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและมีความจำเป็นที่ต้องรักษาความลับ โดยมาตรการนี้มีผลบังคับใช้กับผู้ใช้บริการภายในมหาวิทยาลัยและหน่วยงานภายนอกซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย

ส่วนที่ 1 แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

1. ให้ส่วนงานกำหนดพื้นที่ผู้ใช้บริการพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารให้ชัดเจน และมีการประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกเป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

2. ให้ส่วนงานกำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

3. ให้ส่วนงานกำหนดมาตรการในการควบคุมการเข้า-ออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสาร

4. หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในส่วนงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากหัวหน้าส่วนงานลงนาม

ผู้รับผิดชอบ

ผู้บริหารส่วนงานที่เกี่ยวข้อง

ส่วนที่ 2 แนวปฏิบัติการควบคุมการเข้าออกห้องคอมพิวเตอร์กลาง

1. ผู้ดูแลระบบต้องกำหนดมาตรการการควบคุมและป้องกันบุคคลภายนอกในการเข้าถึงห้องคอมพิวเตอร์กลาง (data center) โดยจะต้องปฏิบัติอย่างน้อยดังนี้

(1) การขออนุญาตเข้าใช้ห้องคอมพิวเตอร์กลางจะต้องระบุถึงกิจกรรม หรือความจำเป็นในการเข้าใช้

(2) ผู้ขอเข้าใช้ห้องต้องปฏิบัติตามกฎระเบียบของส่วนงานอย่างเคร่งครัด

(3) ผู้ขอเข้าใช้ห้องต้องไม่ทำการใด ๆ อันอาจก่อให้เกิดความเสียหายต่อทรัพย์สินของมหาวิทยาลัย

(4) ผู้ขอเข้าใช้ห้องต้องติดบัตรแสดงตนให้ชัดเจน พร้อมทั้งลงบันทึกรายละเอียดของการเข้าใช้ เวลาเข้า เวลาออก รวมทั้งกิจกรรมที่ดำเนินการ

(5) กรณีที่มีการใช้งานนอกเวลาทำการ ผู้ขอเข้าใช้ห้องต้องได้รับอนุญาตจากหัวหน้าส่วนงานและเพื่อการจัดเตรียมเจ้าหน้าที่ของส่วนงานในการอำนวยความสะดวกสำหรับการปฏิบัติงานดังกล่าว

(6) การเข้าดำเนินการกับระบบที่สำคัญจำเป็นต้องมีผู้รับผิดชอบระบบนั้นอยู่กำกับดูแลการปฏิบัติงาน และหากมีการกระทำการใด ๆ ที่อาจส่งผลต่อระบบจะต้องได้รับความเห็นชอบจากเจ้าของระบบนั้นก่อน

(7) ต้องจัดให้มีพื้นที่สำหรับการส่งมอบ หรือขนย้ายอุปกรณ์ต่าง ๆ เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ห้องคอมพิวเตอร์กลาง โดยไม่จำเป็น

2. ผู้ดูแลระบบต้องควบคุมดูแลสภาพแวดล้อมของห้องคอมพิวเตอร์กลาง โดยการตรวจสอบการทำงานของระบบที่ใช้ในการควบคุมสภาพแวดล้อมของห้องเพื่อให้สามารถใช้งานได้ตามปกติ ซึ่งแบ่งออกเป็น 3 ระบบ ดังนี้

(1) ระบบตรวจจับควัน (smoke detector system) เพื่อป้องกันการเกิดอัคคีภัยของห้องคอมพิวเตอร์กลาง

(2) ระบบเครื่องปรับอากาศ (air conditioning system) เพื่อป้องกันการเกิดความร้อนสะสมของอุปกรณ์และควบคุมความชื้นที่เกิดจากละอองน้ำในห้องคอมพิวเตอร์กลาง

(3) ระบบไฟสำรองฉุกเฉิน (UPS) เพื่อสำรองกระแสไฟฟ้าสำหรับป้องกันอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายหยุดทำงาน กรณีไฟฟ้าดับหรือไฟฟ้าไม่เพียงพอ

ผู้รับผิดชอบ

ผู้บริหารส่วนงานที่เกี่ยวข้อง

หมวด 2
การบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ

ตามนโยบายในหมวดที่ว่าด้วยการบริหารจัดการด้านการสื่อสารและเครือข่ายสารสนเทศ ซึ่งได้กำหนดขึ้นเพื่อให้การดำเนินงานที่เกี่ยวข้องกับโครงสร้างพื้นฐานด้านสารสนเทศ และอุปกรณ์ประมวลผลมีความถูกต้อง เหมาะสม และปลอดภัย มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติขึ้นเพื่อให้ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงหน้าที่ความรับผิดชอบด้านการจัดการและการใช้ระบบคอมพิวเตอร์และเครือข่าย

สารสนเทศ และสามารถปฏิบัติตามอย่างเคร่งครัด โดยให้มีส่วนร่วมในการช่วยกันป้องกันสินทรัพย์และข้อมูลของมหาวิทยาลัยให้อยู่ในสภาพมีความมั่นคงปลอดภัย ซึ่งครอบคลุมด้านการรักษาความลับ ความถูกต้องครบถ้วน และสภาพพร้อมใช้งานของสารสนเทศ

ส่วนที่ 1 แนวปฏิบัติการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย

1. การติดตั้งเครื่องคอมพิวเตอร์ลูกข่ายต้องดำเนินการตามแนวปฏิบัติซึ่งครอบคลุมประเด็นต่าง ๆ ดังนี้

- การติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (anti-virus)
- การติดตั้งโปรแกรมปรับปรุงการอุดช่องโหว่ของวินโดว์ (Window update Patch)
- การติดตั้งซอฟต์แวร์พื้นฐาน

2. เครื่องคอมพิวเตอร์ลูกข่ายทุกเครื่องสามารถใช้งานระบบเครือข่ายทั้งเครื่องคอมพิวเตอร์แม่ข่ายและระบบสารสนเทศของมหาวิทยาลัยได้เท่าที่มีการอนุญาตให้ใช้งานหรือที่ได้มีการกำหนดสิทธิไว้เท่านั้น

3. ในการเข้าใช้งานเครื่องคอมพิวเตอร์ลูกข่าย ผู้ใช้งานต้องปฏิบัติตามแนวปฏิบัติเกี่ยวกับการระบุและพิสูจน์ตัวตน และการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

4. การใช้แฟ้มข้อมูลร่วมกัน (shared file) ต้องกำหนดให้มีกระบวนการตรวจสอบสิทธิ โดยการระบุชื่อผู้ใช้งานและรหัสผ่านให้ถูกต้อง จึงจะสามารถเรียกใช้งานแฟ้มข้อมูลได้ ทั้งเครื่องคอมพิวเตอร์ลูกข่ายเชื่อมต่อกันเอง หรือเครื่องคอมพิวเตอร์ลูกข่ายเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย ซึ่งการกำหนดชื่อผู้ใช้งานและรหัสผ่านจะต้องปฏิบัติตามตามแนวปฏิบัติการใช้รหัสผ่านอย่างเคร่งครัด

5. ห้ามมิให้มีการใช้งานอุปกรณ์ต่อพ่วงโดยไม่ผ่านการกระบวนการพิสูจน์ตัวตน เช่น การแชร์อินเทอร์เน็ตผ่านออกเครื่องเดียว (Shared Internet) หรือการนำโทรศัพท์มือถือเชื่อมต่อกับเครื่องคอมพิวเตอร์เพื่อใช้เป็นช่องทางในการใช้งานอินเตอร์เน็ต

6. ห้ามเข้าใช้งานเว็บไซต์ที่ไม่เหมาะสม หรือไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

7. ห้ามทำการเปลี่ยนแปลงหมายเลขไอพี (IP Address) ของเครื่องคอมพิวเตอร์ภายในส่วนงานโดยมิได้รับอนุญาตจากสำนักคอมพิวเตอร์

8. ห้ามทำการติดตั้งโปรแกรมที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากหัวหน้าส่วนงาน

9. เครื่องคอมพิวเตอร์จะต้องมีการกำหนดค่าการพักภาพหน้าจอ (screen saver)และล็อคหน้าจอ เพื่อให้มีการป้องกันการเข้าถึงระบบปฏิบัติการในขณะที่ไม่มีผู้ใช้งาน

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 2 แนวปฏิบัติการติดตั้งเครื่องคอมพิวเตอร์ลูกข่าย

1. ติดตั้งและใช้งานระบบปฏิบัติการที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

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

3. ให้มีการติดตั้งซอฟต์แวร์ป้องกันไวรัสคอมพิวเตอร์ (Anti-Virus)

4. ให้มีการกำหนดและติดตั้งซอฟต์แวร์พื้นฐานที่สำนักคอมพิวเตอร์แนะนำต่อการปฏิบัติงานของมหาวิทยาลัย โดยให้มีการทบทวนรายการซอฟต์แวร์พื้นฐานนั้นเพื่อให้เหมาะสมและสอดคล้องกับการปฏิบัติงานตามภารกิจของมหาวิทยาลัย

5. ควรติดตั้งซอฟต์แวร์พื้นฐานและซอฟต์แวร์ที่ใช้งานที่มีลิขสิทธิ์ถูกต้องตามกฎหมายที่จำเป็นต่อการใช้งานของมหาวิทยาลัย

6. ควรดำเนินการบำรุงรักษาเครื่องคอมพิวเตอร์ลูกข่ายอย่างน้อยปีละ 1 ครั้ง

7. เครื่องคอมพิวเตอร์ที่ใช้ในการปฏิบัติงานจะต้องมีรายละเอียดคุณลักษณะไม่ต่ำกว่ามาตรฐานเครื่องคอมพิวเตอร์ลูกข่ายของมหาวิทยาลัย

8. เครื่องคอมพิวเตอร์จะต้องกำหนดค่าเพื่อป้องกันการเข้าถึงระบบปฏิบัติการขณะที่ไม่มีผู้ใช้งาน

9. เครื่องคอมพิวเตอร์จะต้องทำการตั้งค่าการพักจอภาพเมื่อมิได้มีการใช้งาน

10. เครื่องคอมพิวเตอร์จะต้องถูกล็อคหน้าจอทุกครั้งเมื่อเสร็จสิ้นการใช้งาน

11. เครื่องคอมพิวเตอร์ทุกเครื่องจะต้องมีการตั้งค่าการพิสูจน์ตัวตนก่อนเข้าใช้งานระบบปฏิบัติการ

12. จัดทำรายงานเกี่ยวกับรายละเอียดของเครื่องคอมพิวเตอร์ลูกข่ายปีละ 1 ครั้ง

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 3 แนวปฏิบัติการใช้งานรหัสบัวศรีไอดี

1. ผู้ถือครองรหัสบัวศรีไอดี (Buasri ID) จะต้องใช้รหัสบัวศรีไอดีของตนเอง เพื่อใช้พิสูจน์ตัวตนและตรวจสอบสิทธิก่อนเข้าใช้ระบบสารสนเทศ หรือเครือข่ายอินเทอร์เน็ตของมหาวิทยาลัย

2. ผู้ถือครองรหัสบัวศรีไอดีต้องเป็นผู้รับผิดชอบต่อผลต่างๆ ที่เกิดขึ้นจากการใช้บริการเครื่องคอมพิวเตอร์หรือระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

3. ผู้ถือครองรหัสบัวศรีไอดีต้องลงชื่อ (Login) เข้าสู่ระบบโดยใช้รหัสบัวศรีไอดีของตนเองและทำการลงชื่อออก (Logout) ทุกครั้งเมื่อหยุดการใช้งานชั่วคราว หรือเสร็จสิ้นการใช้งาน

4. ระบบสารสนเทศของมหาวิทยาลัยจะทำการบันทึกข้อมูลการใช้งาน ซึ่งสามารถบ่งบอกตัวบุคคลของผู้ถือครองรหัสบัวศรีไอดีได้

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 4 แนวปฏิบัติการใช้รหัสผ่าน

1. รหัสผ่าน (password) จะต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะประกอบด้วยตัวเลข (Numerical character) ตัวอักษรพิมพ์เล็ก ตัวอักษรพิมพ์ใหญ่ (Alphabet) และตัวอักขระพิเศษ (Special character)

2. รหัสผ่านต้องไม่เป็นคำที่มีความหมายทั้งภาษาไทยและภาษาอังกฤษ และเป็นคำที่ไม่มีความหมายในพจนานุกรม

3. ไม่ควรตั้งรหัสผ่านเหมือนกับชื่อหรือนามสกุล หรือสิ่งที่ง่ายต่อการคาดเดา

4. ไม่ควรจดบันทึกรหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถมองเห็นได้

5. ควรทำการเปลี่ยนแปลงรหัสผ่านใหม่ในทุกๆ 3 เดือน เป็นอย่างน้อย

6. รหัสผ่านสามารถแก้ไขได้ด้วยตนเองผ่านเว็บไซต์ https://account.swu.ac.th

7. ไม่ควรนำรหัสผ่านที่เคยใช้งานมาแล้วกลับมาใช้งานอีก

8. รหัสผ่านจะต้องเป็นความลับเฉพาะของบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยมิได้รับอนุญาต

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 5 แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย

1. เครื่องคอมพิวเตอร์ภายในส่วนงานทุกเครื่องต้องทำการอัพเดท (Update Patch) ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมที่ใช้งานให้เป็นปัจจุบัน เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์

2. เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการติดตั้งโปรแกรมป้องกันไวรัสและกำจัดโปรแกรมประสงค์ร้าย (malware) รวมทั้งอัพเดทให้เป็นปัจจุบัน

3. ห้ามมิให้ผู้ใช้บริการทำการปิด หรือยกเลิก หรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์ โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

4. หากผู้ใช้บริการพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามมิให้ผู้ใช้บริการเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่าย และต้องดำเนินการแจ้งสำนักคอมพิวเตอร์หรือผู้ที่เกี่ยวข้องดำเนินการแก้ไขก่อนที่จะเชื่อมต่อเข้ากับระบบเครือข่ายอีกครั้ง

5. ก่อนการใช้งานสื่อบันทึกแบบพกพาต้องมีการตรวจสอบป้องกัน กำจัดโปรแกรมประสงค์ร้าย

6. ผู้ใช้บริการต้องทำการตรวจสอบไฟล์ที่สามารถประมวลผลได้ (เช่น .exe .com .bat .vbs .scr .pif .hta) ผ่านทางโปรแกรมป้องกันไวรัสและกำจัดโปรแกรมประสงค์ร้าย ก่อนทำการปิดเครื่องคอมพิวเตอร์ทุกครั้ง

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 6 แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต

1. ห้ามผู้ใช้งานปฏิบัติการใด ๆ ที่เป็นการขัดต่อกฎหมาย หรือศีลธรรมอันดี โดยหากมีการกระทำดังกล่าวเกิดขึ้นถือเป็นความรับผิดชอบของผู้ใช้งาน ซึ่งอยู่นอกเหนือจากความรับผิดชอบของมหาวิทยาลัย

2. ผู้ใช้งานจะต้องไม่ละเมิดสิทธิผู้อื่น หรือทำการดัดแปลงแก้ไขข้อมูลผู้อื่น โดยมิได้รับอนุญาต

3. ห้ามผู้ใช้งานระบบอินเทอร์เน็ตในทางที่ไม่เหมาะสม เช่น การแสดงความคิดเห็นหรือการใช้ภาษาที่ไม่สุภาพ หรือกระทำการใด ๆ ที่จะทำให้ผู้อื่นเสียหาย

4. มหาวิทยาลัยจะไม่รับประกันคุณภาพการเก็บข้อมูล การรับส่งข้อมูลข่าวสารระบบบางส่วนหรือทั้งหมดที่ไม่สามารถใช้งานได้ และจะไม่รับผิดชอบความเสียหายอันเนื่องมาจากวงจรสื่อสารชำรุด จานแม่เหล็กชำรุด หรือความล่าช้าที่เกิดขึ้นในการใช้งาน

5. มหาวิทยาลัยขอสงวนสิทธิ์ในการยกเลิกหรือระงับการเชื่อมต่อ ในกรณีตรวจสอบพบการพยายามบุกรุก หรือทำให้ระบบสารสนเทศหรือระบบเครือข่ายของมหาวิทยาลัยมีประสิทธิภาพลดลง

6. ผู้ใช้งานต้องทำความเข้าใจและยอมรับระเบียบปฏิบัติที่มหาวิทยาลัยกำหนดขึ้น โดยจะอ้างว่าไม่ทราบระเบียบปฏิบัตินั้น ๆ มิได้

7. บัญชีผู้ใช้งาน (รหัสบัวศรีไอดี) นั้น มหาวิทยาลัยมอบให้เพื่อการใช้งานตามภารกิจของมหาวิทยาลัยเท่านั้น และห้ามมิให้ผู้อื่นที่ไม่ได้เกี่ยวข้องกับมหาวิทยาลัยนำไปใช้งาน

8. ถ้าเกิดความเสียหายขึ้นจากการใช้งานบัญชีผู้ใช้งาน ผู้เป็นเจ้าของต้องรับผิดชอบกับความเสียหายที่เกิดขึ้น เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 7 แนวปฏิบัติการบริหารจัดการระบบจดหมายอิเล็กทรอนิกส์

1. เครื่องคอมพิวเตอร์แม่ข่ายที่เปิดให้บริการระบบจดหมายอิเล็กทรอนิกส์ (E-mail Server) ต้องเป็นเครื่องคอมพิวเตอร์ของมหาวิทยาลัยหรือระบบจดหมายอิเล็กทรอนิกส์ภายนอกที่ดูแลบริหารจัดโดยสำนักคอมพิวเตอร์เท่านั้น

2. ผู้ดูแลระบบต้องจัดให้มีระบบในการตรวจสอบจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ผ่านเข้าออกระบบบริการอิเล็กทรอนิกส์หลักของมหาวิทยาลัยเพื่อป้องกันปัญหาไวรัสและสแปม

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์

ส่วนที่ 8 แนวปฏิบัติการใช้บริการจดหมายอิเล็กทรอนิกส์

1. ผู้ใช้งานมีหน้าที่รับผิดชอบบัญชีจดหมายอิเล็กทรอนิกส์ที่ได้รับจากมหาวิทยาลัย ต้องระวังมิให้ผู้อื่นสามารถเข้าถึงรหัสผ่านเพื่อใช้งานบัญชีจดหมายอิเล็กทรอนิกส์ของตนโดยมิชอบ

2. ผู้ใช้งานพึงทราบว่าผู้ดูแลระบบไม่มีสิทธิถาม หรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านเข้าใช้งานบัญชีจดหมายอิเล็กทรอนิกส์

3. ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

4. ห้ามเผยแพร่ หรือส่งต่อจดหมายลูกโซ่

5. ห้ามเผยแพร่ข้อมูลที่เป็นความลับของมหาวิทยาลัย

6. ห้ามปลอมแปลง หรือดัดแปลงชื่อผู้ส่งเพื่อให้บุคคลอื่นเข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้นมาจากบุคคลอื่น

7. ห้ามปกปิด หรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

8. ห้ามส่งจดหมายอิเล็กทรอนิกส์ที่เผยแพร่ ข้อความ ภาพ วิดีโอ หรือเสียงที่ให้ร้ายต่อบุคคลหรือกลุ่มบุคคล หรือในลักษณะที่หยาบคาย หรือลามก อนาจาร

9. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อเผยแพร่โปรแกรม หรือรหัสผ่านสำหรับการเข้าถึงโปรแกรมในลักษณะที่เป็นการละเมิดลิขสิทธิ์

10. ห้ามส่งจดหมายอิเล็กทรอนิกส์เพื่อกระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้ที่ไม่ต้องการ

11. ห้ามใช้จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย ในการแพร่กระจายไวรัส หรือโปรแกรมที่เป็นอันตรายกับความมั่นคงปลอดภัยของระบบเครือข่ายมหาวิทยาลัย

12. ห้ามมิให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ที่ได้รับจากมหาวิทยาลัยไปสมัครสมาชิกตามเว็บไซต์ต่าง ๆ เพื่อประโยชน์ส่วนตน และไม่เกี่ยวข้องกับภารกิจของมหาวิทยาลัย

13. เมื่อผู้ใช้งานได้รับรหัสผ่านและเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ครั้งแรก ผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านโดยทันที

14. ผู้ใช้งานเปลี่ยนรหัสผ่านทุกๆ 3-6 เดือน

15. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงชื่อออกจากระบบทุกครั้ง

16. ผู้ใช้งานหลีกเลี่ยงการแนบไฟล์ขนาดใหญ่ โดยให้มีขนาดไม่เกิน 20 MB

17. ห้ามส่งข้อมูลส่วนบุคคลที่มีความอ่อนไหวหรือเป็นความลับผ่านทางจดหมายอิเล็กทรอนิกส์โดยไม่ได้เข้ารหัสข้อมูล

18. มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับการใช้งานบัญชีผู้ใช้ได้ทันทีโดยไม่ต้องแจ้งให้ทราบล่วงหน้า หากตรวจพบความผิดปกติต่อความมั่นคงปลอดภัยซึ่งอาจจะเกิดจากบัญชีผู้ใช้รายนั้น

19. ผู้ใช้งานต้องใช้บริการจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย เพื่อใช้ในการติดต่อภารกิจของมหาวิทยาลัย

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

หมวด 3
การควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

ตามนโยบายในหมวดที่ว่าด้วยการควบคุมการเข้าถึงระบบสารสนเทศและเครือข่าย ซึ่งกำหนดขึ้นเพื่อให้เกิดมาตรการในควบคุมการเข้าถึงระบบ การบริหารการจัดการเข้าถึงของผู้ใช้ และการควบคุมการเข้าถึงเครือข่ายของมหาวิทยาลัย รวมถึงการป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้ายที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของส่วนงานได้ มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติขึ้น เพื่อให้ผู้ดูแลระบบและผู้ใช้บริการได้ตระหนักถึงความสำคัญของการควบคุม และการบูรณาการร่วมกันในการปฏิบัติงานอย่างถูกต้องเหมาะสม เพื่อป้องกันการบุกรุกที่อาจก่อให้เกิดความเสียหายต่อระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย

ส่วนที่ 1 แนวปฏิบัติของผู้ดูแลระบบ

1. ผู้ดูแลระบบ มีอำนาจหน้าที่ ดังต่อไปนี้

(1) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของส่วนงานให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์หรือระบบเครือข่ายให้ผู้ดูแลระบบรีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที และในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้บริการ ที่ไม่เป็นไปตามนโยบายให้รีบ

แจ้งผู้ใช้บริการผู้นั้นยุติการกระทำดังกล่าวในทันที และเพื่อป้องกัน หรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่ส่วนงาน ให้ผู้ดูแลระบบพิจารณาระงับการใช้ระบบเครือข่ายของผู้ใช้บริการดังกล่าวได้ทันที

(2) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและอัพเดตให้เป็นปัจจุบัน

(3) ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่าย

(4) ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(5) ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ให้ถูกต้องและเป็นปัจจุบัน โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้บริการที่พ้นสภาพการเป็นผู้ใช้บริการ

(6) ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้บริการให้มีการกำหนดรหัสผ่าน ก่อนเข้าใช้ระบบปฏิบัติการและกำหนดรหัสผ่านให้เป็นไปตามแนวปฏิบัติการใช้รหัสผ่าน

(7) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลส่วนบุคคลหรือเข้าใช้งานระบบคอมพิวเตอร์ของผู้อื่นโดยไม่มีเหตุผลอันสมควร

(8) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิข้อมูลส่วนบุคคลหรือเข้าใช้งานระบบคอมพิวเตอร์ที่มีข้อมูลส่วนบุคคลจัดเก็บไว้ในภายใน โดยไม่มีเหตุผลอันสมควร

(9) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลความลับหรือข้อมูลส่วนบุคคลให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

(10) เมื่อผู้ดูแลระบบพ้นจากหน้าที่จะต้องคืนสิทธิของผู้ดูแลส่วนงานที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้มีอำนาจหรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสิทธิ

(11) จัดทำแผนบำรุงรักษาระบบสารสนเทศ แผนสำรองและกู้คืนข้อมูล และแผนรับมือภัยพิบัติในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ มีการจัดทำแผนทดสอบความพร้อมใช้งานระบบสารสนเทศ ระบบสำรองข้อมูล และระบบกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

2. ผู้ดูแลระบบจะต้องบันทึกข้อมูลจราจรทางคอมพิวเตอร์ โดยจะต้องบันทึกข้อมูลของผู้ใช้บริการเท่าที่จำเป็น เพื่อให้สามารถระบุตัวผู้ใช้บริการนับตั้งแต่เริ่มใช้บริการ โดยต้องบันทึกข้อมูลไว้เป็นเวลาไม่น้อยกว่า 90 วันนับตั้งแต่การใช้บริการสิ้นสุดลง การบันทึกข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มีความมั่นคงและปลอดภัย ดังต่อไปนี้

(1) บันทึกลงในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่บันทึกไว้ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบ สามารถแก้ไขข้อมูลที่บันทึกไว้ เว้น

แต่ผู้ที่ได้รับสิทธิให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของส่วนงาน (Internal IT Auditor) หรือบุคคลที่ส่วนงานมอบหมาย

(3) ในการบันทึกมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้บริการเป็นรายบุคคลได้

(4) เพื่อให้ข้อมูลการจราจรทางคอมพิวเตอร์มีความถูกต้องและนำมาใช้ประโยชน์ได้จริง ผู้ดูแลระบบต้องตรวจสอบเวลาของอุปกรณ์ที่ให้บริการทุกชนิด ให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยคลาดเคลื่อนไม่เกิน 10 มิลลิวินาที

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 2 แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

1. มหาวิทยาลัยต้องกำหนดให้มีมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศเพื่อดูแลรักษาความปลอดภัย ในกรณีบุคคลจากหน่วยงานภายนอกหรือผู้รับจ้างจากภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของส่วนงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรตามสายงานต่อหัวหน้าส่วนงานของมหาวิทยาลัย

2. ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการปฏิบัติงานและหน้าที่ความรับผิดชอบของผู้ใช้ รวมทั้งมีขั้นตอนการทบทวนและปรับปรุงสิทธิให้สอดคล้องกับการเข้าถึงข้อมูลและระบบข้อมูลอย่างน้อยปีละ 1 ครั้ง

3. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศที่มีต่อระบบข้อมูล

4. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ

5. ผู้ดูแลระบบต้องจัดให้มีการตรวจสอบการกำหนดสิทธิตามลำดับความสำคัญของระบบสารสนเทศ

6. ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร และกำหนดสิทธิการเข้าใช้งานระบบสารสนเทศจากภายนอก

7. ผู้ดูแลระบบต้องมีการกำหนดขั้นตอนการเข้าใช้งานระบบสารสนเทศจากภายนอกองค์กร

8. ผู้ดูแลระบบต้องติดตั้งระบบสารสนเทศที่มีความสำคัญสูงและไวต่อการรบกวน ไว้บนเครื่องคอมพิวเตอร์แม่ข่ายที่แยกจากระบบสารสนเทศอื่น โดยติดตั้งที่ห้องคอมพิวเตอร์กลาง หรือห้องคอมพิวเตอร์ซึ่งมีสภาพแวดล้อมที่เหมาะสม เช่น ระบบรักษาความปลอดภัย ระบบสำรองไฟฟ้า และระบบปรับอากาศ เป็นต้น

9. ผู้ดูแลระบบต้องดูแลควบคุมเครื่องคอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ โดยกำหนดมาตรการและข้อปฏิบัติที่เหมาะสมในการเข้าถึงระบบสารสนเทศที่มีความสำคัญสูงและไวต่อการรบกวน เพื่อปกป้องระบบสารสนเทศจากภาวะความเสี่ยงอันเนื่องมาจากการใช้อุปกรณ์ดังกล่าว

10. ผู้ดูแลระบบต้องกำหนดสิทธิและให้ผู้ใช้งานอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ต้องทำการพิสูจน์ตัวตนโดยใช้รหัสบัวศรีไอดีก่อนเข้าสู่ระบบของมหาวิทยาลัย

11. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงบริการสารสนเทศตามสิทธิที่ได้รับอนุญาตเท่านั้น

12. ผู้รับจ้างจากภายนอกต้องปฏิบัติตามนโยบายและแนวปฏิบัตินี้ โดยให้มีการลงนามเป็นลายลักษณ์อักษรรับรองว่าจะไม่นำข้อมูลของมหาวิทยาลัยออกไปเปิดเผยภายนอก

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 3 แนวปฏิบัติการบริหารจัดการการเข้าถึงระบบสารสนเทศ

1. ผู้ดูแลระบบต้องกำหนดให้มีขั้นตอนการปฏิบัติการกำหนดสิทธิอย่างเป็นทางการ ให้แก่ผู้ใช้รายใหม่ของมหาวิทยาลัย เพื่อให้มีสิทธิในการใช้งานระบบสารสนเทศของมหาวิทยาลัยตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การเปลี่ยนสถานะ การเปลี่ยนตำแหน่ง การลาออก หรือการพ้นสภาพการปฏิบัติงาน ดังต่อไปนี้

(1) การได้รับสิทธิการเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

(1.1) กรณีนิสิตจะได้รับชื่อบัญชีและรหัสผู้ใช้งานภายใน 5 วัน หลังจากรายงานตัวและชำระเงินเรียบร้อยแล้ว

(1.2) กรณีบุคลากรจะได้รับชื่อบัญชีและรหัสผู้ใช้งานภายใน 1 วัน หลังจากส่วนทรัพยากรบุคคลจัดทำคำสั่งบรรจุบุคลากร และบันทึกข้อมูลในระบบ HURIS สมบูรณ์แล้ว

(2) การยกเลิกสิทธิการเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

(2.1) กรณีนิสิตจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 30 วัน หลังจากการขึ้นทะเบียนพ้นสภาพการเป็นนิสิตในระบบสมบูรณ์แล้ว โดยทำการยกเลิกทุกกรณี

(2.2) กรณีบุคลากรจะถูกยกเลิกสิทธิการใช้ชื่อบัญชีและรหัสผู้ใช้งานภายใน 30 วัน หลังจากส่วนทรัพยากรบุคคลจัดทำคำสั่งให้พ้นสภาพการเป็นบุคลากร และบันทึกข้อมูลในระบบ HURIS สมบูรณ์แล้ว ยกเว้นกรณีเกษียณยังสามารถใช้งานได้ต่อไป

2. ผู้ดูแลระบบต้องกำหนดการใช้งานระบบเสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบ

อินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะในการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าส่วนงานเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ 1 ครั้ง

3. ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งาน ดังต่อไปนี้

(1) กำหนดประเภทของสิทธิกับผู้ใช้งานระบบสารสนเทศ โดยจำแนกประเภทสิทธิตามหน้าที่และความรับผิดชอบ และต้องจัดเก็บและมอบหมายสิทธิให้แก่ผู้ใช้งานที่ได้รับอนุญาตเท่านั้น

(2) กรณีที่มีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าส่วนงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง

(3) กรณีมีการว่าจ้างผู้รับจ้างจากภายนอกจะต้องกำหนดระยะเวลาการใช้งานของผู้รับจ้างภายนอกและระงับการใช้งานทันทีเมื่องานดังกล่าวเสร็จสิ้นหรือสิ้นสุดสัญญา

4. ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้บริการ ดังต่อไปนี้

(1) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(2) การส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการส่งมอบรหัสผ่านให้กับบุคคลอื่น หรือการส่งรหัสผ่านด้วยจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(3) ห้ามมิให้ผู้ใช้งานบันทึกรหัสผ่านไว้บนระบบคอมพิวเตอร์ในแบบที่มิได้ป้องกันการเข้าถึง

5. ผู้ดูแลระบบต้องบริหารจัดการระดับชั้นการเข้าถึงข้อมูลแต่ละประเภท เช่น การเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ตามประเภทของข้อมูล ความสำคัญของข้อมูล ความลับของข้อมูล และลำดับชั้นการเข้าถึงของข้อมูล โดยการเข้าถึงข้อมูลจะเข้าถึงได้เฉพาะผู้ที่ได้รับอนุญาต

(1) ต้องมีการกำหนดประเภทของข้อมูล ซึ่งมีการจัดแบ่งไว้เป็น 3 ประเภท คือ

(1.1) ข้อมูลสารสนเทศด้านการบริหารงาน เช่น ระบบบริหารทรัพยากรมหาวิทยาลัย ระบบคลังข้อมูลมหาวิทยาลัย ระบบภาระงานบุคลากรสายวิชาการ

(1.2) ข้อมูลสารสนเทศด้านการบริการอาจารย์ นิสิต และบุคลากร เช่น ระบบบริการการศึกษา ระบบทรัพยากรบุคคล

(1.3) ข้อมูลสารสนเทศด้านการบริการบุคคลทั่วไป เช่น ระบบรับนิสิตใหม่ ระบบประชาสัมพันธ์

(2) ต้องมีการจัดลำดับความสำคัญของข้อมูลโดยแบ่งออกเป็น 3 ลำดับคือ

(2.1) ข้อมูลที่มีระดับความสำคัญมากที่สุด

(2.2) ข้อมูลที่มีระดับความสำคัญปานกลาง

(2.3) ข้อมูลที่มีระดับความสำคัญน้อย

(3) ต้องมีการกำหนดระดับชั้นของการเข้าถึงข้อมูล โดยมีการพิสูจน์สิทธิในการเข้าถึงข้อมูลแต่ละระดับชั้นและต้องกำหนดรายชื่อผู้ใช้และรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นการเข้าถึงข้อมูล โดยแบ่งระดับชั้นออกเป็น 3 ระดับชั้น คือ

(3.1) ระดับชั้นสำหรับผู้บริหาร

(3.2) ระดับชั้นสำหรับผู้ใช้งานทั่วไป

(3.3) ระดับชั้นสำหรับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย

(4) ต้องกำหนดระยะเวลาในการเข้าถึง และวิธีการในการระงับการใช้งานเมื่อพ้นระยะเวลา

(5) ต้องกำหนดช่องทางในการเข้าถึงข้อมูลในแต่ละประเภท ว่ามีการเข้าถึงข้อมูลแต่ละประเภทได้โดยตรงหรือการเข้าถึงผ่านระบบงาน

(6) ต้องกำหนดให้มีการเข้ารหัส (encryption) และถอดรหัส (decryption) ในการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น ในกรณีการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ

(7) ผู้ใช้งานนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. 2554

(8) ต้องกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูล ในกรณีนำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของส่วนงาน เช่น ในการส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ต้องสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(9) ผู้ดูแลระบบต้องกำหนดให้มีระบบจัดเก็บประวัติการเข้าถึงข้อมูล

ส่วนที่ 4 รายละเอียดข้อกำหนดเกี่ยวกับการบริหารจัดการการเข้าถึงข้อมูล

	ระดับความสำคัญของข้อมูล		
	สำคัญมากที่สุด	**ปานกลาง**	**ต่ำ**
คำอธิบาย	ข้อมูลที่อยู่ในชั้นความสำคัญที่เป็นความลับหรือข้อมูลที่จะนำไปสู่ข้อมูลความเป็นส่วนบุคคลที่ต้องได้รับการป้องกันตามกฎหมาย	ข้อมูลที่ผู้รับผิดชอบข้อมูลกำหนด หรือระบุไว้ตามเงื่อนไขของสัญญามิให้เปิดเผยแพร่ หรือ เปิดสู่สาธารณะ	ข้อมูลซึ่งไม่ได้อยู่ในข้อกำหนดของการห้ามเผยแพร่หรือเปิดสู่สาธารณะ
ระดับชั้นการเข้าถึง	ป้องกันการเข้าถึงข้อมูลโดยกำหนดสิทธิ์ให้เฉพาะผู้ปฏิบัติงานซึ่งมีหน้าที่รับผิดชอบเท่านั้นและได้รับรองข้อตกลงการไม่เปิดเผยข้อมูล	เปิดให้เข้าถึงได้เฉพาะผู้ปฏิบัติ งานหรือผู้มีความจำเป็นต้องใช้ข้อมูล	ไม่มีข้อกำหนดหรือข้อห้ามการเข้าถึง ข้อมูลประเภทที่อนุญาตให้เปิดเผยสู่สาธารณะได้
ช่องทางการเข้าถึง	- การรับส่งข้อมูลผ่านเครือข่ายภายใน (Intranet) - หากจำเป็นต้องผ่านจากเครือข่ายสาธารณะให้ผ่านระบบ VPN ของมหาวิทยาลัย - หากจำเป็นต้องผ่านจากเครือข่ายสาธารณะกำหนดให้ต้องมีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN	-การรับส่งข้อมูลต้องหลีกเลี่ยงการส่งผ่านเครือข่ายสาธารณะ -หากจำเป็นต้องผ่านจากเครือข่ายสาธารณะให้ผ่านระบบ VPN ของมหาวิทยาลัย	-ไม่มีข้อกำหนดในการป้องกันแต่แนะนำให้ระมัดระวังในการนำไปใช้อย่างเหมาะสม -สามารถเข้าถึงได้ผ่านระบบอินเทอร์เน็ต
เวลาในการเข้าถึง	-เข้าถึงได้เฉพาะช่วงเวลาที่ได้รับอนุญาต	-เข้าถึงได้ตามช่วงเวลาที่เปิดให้บริการ	-เข้าถึงได้ทุกช่วงเวลา

	ระดับความสำคัญของข้อมูล		
	สำคัญมากที่สุด	ปานกลาง	ต่ำ
ประเภทของข้อมูล	ข้อมูลบุคลากร ได้แก่ -บัตรประจำตัว/พาสปอร์ต -เลขที่บัญชีธนาคาร -หลักฐานการจ่ายเงิน -ข้อมูลเงินเดือน เงินประจำตำแหน่ง -ข้อมูลการเลื่อนขั้นเงินเดือน -ข้อมูลการขอตำแหน่ง -ข้อมูลผลการประเมิน -คำสั่งสอบทางวินัย -คำสั่งพ้นราชการ -ทายาทบำเหน็จตกทอด -ข้อมูลสุขภาพ -เชื้อชาติ -ศาสนา ข้อมูลนิสิต ได้แก่ -บัตรประจำตัว/พาสปอร์ต -เลขที่บัญชีธนาคาร -หลักฐานการจ่ายเงิน -ผลการเรียน -เชื้อชาติ -ศาสนา	ข้อมูลบุคลากร ได้แก่ -สิทธิประโยชน์และสวัสดิการ - ประวัติครอบครัว - ประวัติการศึกษา - หมายเลขโทรศัพท์เคลื่อนที่ ข้อมูลนิสิต ได้แก่ -สิทธิประโยชน์และสวัสดิการ - ประวัติครอบครัว - ประวัติการศึกษา	ข้อมูลบุคลากร ได้แก่ -ชื่อ-นามสกุล -อีเมล์ -หมายเลขโทรศัพท์ภายใน -ตำแหน่ง -สาขาที่จบการศึกษา -รูปถ่ายที่ใช้ภายในมหาวิทยาลัย -ผลงานทางวิชาการ ข้อมูลนิสิต ได้แก่ -ชื่อ-นามสกุล -คณะ สาขาวิชา -ปีการศึกษา -ชั้นปี -สถานภาพ -ตารางสอน ข้อมูลทั่วไปของมหาวิทยาลัย -แผนที่มหาวิทยาลัย -ตำแหน่งงาน -ผลงานทางวิชาการ

ผู้รับผิดชอบ

ผู้บริหารส่วนงานที่เกี่ยวข้อง ผู้ดูแลระบบที่ได้รับมอบหมาย ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 5 แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

1. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (username) และรหัสผ่าน (password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของส่วนงาน

2. ผู้ใช้บริการต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และ รหัสผ่านของตน เพื่อการเข้าใช้งานเครื่องคอมพิวเตอร์ของส่วนงานร่วมกัน

3. ผู้ใช้บริการต้องตั้งค่าการพักจอภาพ เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานและต้องกรอกรหัสผ่านอีกครั้งเมื่อต้องการเข้าใช้งาน

4. ผู้ใช้ต้องทำการออกจากระบบปฏิบัติการทุกครั้งทันทีเมื่อเลิกใช้งาน

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 6 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

1. ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (access point) ให้อยู่ในพื้นที่ใช้งานระบบเครือข่ายไร้สายของมหาวิทยาลัย

2. ผู้ดูแลระบบต้องทำการตั้งค่าเอสเอสไอดี (SSID หรือ Service Set Identifier) ให้อยู่ในรูปแบบที่ระบบเครือข่ายมหาวิทยาลัยใช้งานทันทีที่นำอุปกรณ์กระจายสัญญาณมาติดตั้งใช้งาน

3. อุปกรณ์กระจายสัญญาณที่มีคุณสมบัติตามข้อกำหนดมาตรฐานของมหาวิทยาลัยจะต้องถูกติดตั้งระบบการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีของมหาวิทยาลัย

4.กรณีอุปกรณ์กระจายสัญญาณที่นำมาติดตั้งใช้งานไม่สามารถติดตั้งระบบการพิสูจน์ตัวตนการเข้าใช้งานเครือข่ายบัวศรีตามข้อ 3 ได้นั้น ผู้ดูแลระบบจะต้องดำเนินการตั้งค่าให้เป็นการกระจายสัญญาณแบบบริดจ์ (bridge)เท่านั้น เพื่อให้ผู้ใช้งานพิสูจน์ตัวตนผ่านรหัสบัวศรีไอดีของมหาวิทยาลัย

5. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งไฟร์วอลล์ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในส่วนงาน

6. ผู้ดูแลระบบต้องใช้ซอฟต์แวร์ หรือ ฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สาย เพื่อคอยติดตามและบันทึกเหตุการณ์น่าสงสัยในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจพบความผิดปกติในการใช้งาน ผู้ดูแลระบบต้องรายงานต่อหัวหน้าส่วนงานให้ทราบทันที

7. ผู้ดูแลระบบต้องควบคุมดูแลมิให้บุคคล หรือ หน่วยงานภายนอกที่มิได้รับอนุญาตเข้าใช้บริการระบบเครือข่ายไร้สายของมหาวิทยาลัยเพื่อผ่านเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในของมหาวิทยาลัย

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 7 แนวปฏิบัติในการติดตั้งสวิตช์และฮับ

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

2. การเดินสายยูทีพี (UTP) หรือดำเนินการติดตั้งจุดเชื่อมต่อสายยูทีพี บนอุปกรณ์สวิตช์ หรือ ฮับ ในตู้แร็คที่ดูแลโดยสำนักคอมพิวเตอร์ จะต้องแจ้งสำนักคอมพิวเตอร์ก่อนทุกครั้ง

3. หมายเลขไอพีที่ติดตั้งบนอุปกรณ์สวิตช์ จะต้องเป็นหมายเลขที่กำหนดให้โดยสำนักคอมพิวเตอร์เท่านั้น ห้ามดำเนินการโดยมิได้รับอนุญาต

4. อุปกรณ์สวิตช์ที่ติดตั้งใช้งานจะต้องเปิดใช้งานโปรโตคอลเอสเอ็นเอ็มพี (SNMP) เพื่อให้สำนักคอมพิวเตอร์สามารถตรวจสอบการทำงานของอุปกรณ์นั้นได้

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์ ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 8 แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย

1. สำนักคอมพิวเตอร์ และส่วนงานที่มีห้องคอมพิวเตอร์กลางให้กำหนดมาตรการควบคุมการเข้า-ออก ห้องคอมพิวเตอร์กลาง

2. ผู้ใช้บริการจะนำอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายของส่วนงานต้องได้รับอนุญาตจากหัวหน้าส่วนงานและต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

3. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งอุปกรณ์เพิ่มเติม เชื่อมต่อหรือกระทำการใด ๆ กับอุปกรณ์เครือข่ายส่วนกลาง ซึ่งได้แก่ อุปกรณ์จัดหาเส้นทาง (router) อุปกรณ์กระจายสัญญาณสวิตช์ (switch) โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

4. ผู้ดูแลระบบจะต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อให้การบริหารจัดการระบบเครือข่ายเป็นไปอย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) จำกัดช่องทางการเข้าใช้งานระบบเครือข่าย เพื่อควบคุมผู้ใช้บริการให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) จำกัดช่องทางการเข้าใช้งานระบบเครือข่ายจากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย

(3) ระบบเครือข่ายของมหาวิทยาลัยจะต้องเชื่อมต่อกับระบบรักษาความปลอดภัยของเครือข่ายคอมพิวเตอร์เพื่อเชื่อมต่อไปยังระบบเครือข่ายอื่นภายนอก

(4) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่อาจเข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติ

(5) การเข้าสู่ระบบเครือข่ายของมหาวิทยาลัย-เพื่อใช้งานอินเทอร์เน็ตต้องทำการพิสูจน์ตัวตนโดยการระบุชื่อผู้ใช้และรหัสผ่านบัวศรีไอดีของตน

(6) หมายเลขไอพี (IP Address) ของระบบเครือข่ายมหาวิทยาลัย จำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกสามารถเชื่อมต่อหรือมองเห็นได้

(7) จัดทำแผนผังระบบเครือข่าย (network diagram) โดยระบุรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและระบบเครือข่ายภายนอกพร้อมทั้งปรับปรุงให้เป็นปัจจุบัน

(8) การใช้เครื่องมือต่าง ๆ เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

5. ผู้ดูแลระบบต้องควบคุมดูแลระบบเครื่องคอมพิวเตอร์แม่ข่าย ให้อยู่ในสภาพพร้อมใช้งาน และต้องควบคุมการแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

6. มหาวิทยาลัยได้ดำเนินการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ เพื่อให้สามารถระบุถึงตัวบุคคลได้ตามแนวทาง ดังต่อไปนี้

(1) บันทึกข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ โดยข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึงข้อมูล และผู้ดูแลระบบมิได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ได้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของส่วนงาน (Internal IT Auditor) หรือบุคคลที่ส่วนงานมอบหมาย

(2) การบันทึกการทำงานของระบบการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งานคำสั่ง (command line) และ บันทึกการจราจรทาง เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องบันทึกข้อมูลดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(3) มีการตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ของผู้ใช้งานระบบอยู่เป็นประจำ

(4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกข้อมูลจราจรทางคอมพิวเตอร์ต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

7. มหาวิทยาลัยได้ควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายเพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งาน ระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสำนักคอมพิวเตอร์ ต้องทำบันทึกข้อความถึงผู้อำนวยการสำนักคอมพิวเตอร์เพื่อขออนุมัติการใช้งาน

(2) ผู้ดูแลระบบต้องควบคุมช่องทางการสื่อสาร ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องไม่เปิดช่องทางที่ใช้งานทิ้งไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อโดยอัตโนมัติเมื่อไม่ได้ใช้งาน และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

(3) การเชื่อมต่อเข้าสู่ข้อมูล หรือระบบข้อมูลได้จากระยะไกลต้องทำบันทึกข้อความถึงผู้อำนวยการสำนักคอมพิวเตอร์เพื่อขออนุมัติการใช้งาน

(4) การเข้าสู่ระบบจากระยะไกล (Remote Access) ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับส่วนงานอย่างเพียงพอ

(5) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนโดยใช้รหัสบัวศรีไอดีของมหาวิทยาลัย

(6) การเข้าสู่ระบบจากเครือข่ายสาธารณะต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น การใช้วีพีเอ็น เอสเอสแอล เป็นต้น

(7) ผู้ดูแลระบบจะต้องกำหนดช่องทางที่ใช้ในการเชื่อมต่อเข้าสู่ระบบเครือข่ายคอมพิวเตอร์และติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ 1 ครั้ง

8. ผู้ดูแลระบบต้องกำหนดวิธีการปกปิดหมายเลขไอพีภายในเครือข่ายของมหาวิทยาลัย เพื่อป้องกันมิให้บุคคลภายนอกสามารถทราบข้อมูลไอพีและโครงสร้างของระบบเครือข่าย โดยทำการแบ่งแยกเป็นหมายเลขไอพีสาธารณะ (public IP Address) และ หมายเลขไอพีภายใน (private IP Address) เพื่อแยกเครือข่ายย่อย และให้จัดทำระบบแปลงหมายเลขไอพีเครือข่าย (NAT หรือ Network Address Translation) เพื่อเชื่อมต่อไปยังภายนอกส่วนงาน

9. มหาวิทยาลัยกำหนดมาตรฐานการเชื่อมต่อระบบสารสนเทศของมหาวิทยาลัย โดยเชื่อมต่อผ่านระบบ OAuth2 เพื่อพิสูจน์ตัวตน

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์

ส่วนที่ 9 แนวปฏิบัติการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ

มาตรการควบคุมการเข้าถึงอุปกรณ์ในขณะที่ไม่มีผู้ใช้บริการ เพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของส่วนงานในขณะที่ไม่มีผู้ดูแล ดังต่อไปนี้

1. ผู้ใช้งานต้องออกจากระบบสารสนเทศทันทีเมื่อเสร็จสิ้นการปฏิบัติงาน เช่น ระบบสารสนเทศ ระบบปฏิบัติการคอมพิวเตอร์ เป็นต้น

2. ผู้ใช้งานต้องกำหนดชื่อผู้ใช้และรหัสผ่านก่อนเข้าใช้งานระบบปฏิบัติการคอมพิวเตอร์เพื่อป้องกันผู้อื่นเข้าใช้เครื่องคอมพิวเตอร์หรือระบบสารสนเทศของตน

3. ผู้ใช้บริการต้องควบคุมการเข้าใช้อุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งาน หรือปล่อยทิ้งไว้โดยไม่มีดูแล

4. ระบบสารสนเทศของมหาวิทยาลัยมีการจำกัดระยะเวลาการเชื่อมต่อเมื่อไม่มีการใช้งานตามระบบที่มีความสำคัญสูง โดยจะต้องไม่เกิน 30 นาที (Idle Timeout)

5. สำนักคอมพิวเตอร์ควรให้ความรู้ความเข้าใจแก่ผู้ใช้ในมาตรการป้องกันการเข้าถึงเครื่องคอมพิวเตอร์และอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน

ผู้รับผิดชอบ

ผู้ถือครองรหัสบัวศรีไอดี

ส่วนที่ 10 แนวปฏิบัติการควบคุมการใช้สินทรัพย์สารสนเทศ

1. ผู้ดูแลระบบและผู้ใช้งานจะต้องออกจากระบบทุกครั้งเมื่อเลิกการใช้งาน

2. ผู้ใช้งานจะต้องปิด เครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกปฏิบัติงาน ณ สิ้นวัน

3. เอกสารที่เป็นความลับทางราชการ จะต้องเก็บอยู่ในลิ้นชักที่ปลอดภัยสามารถล๊อคได้ และไม่วางเอกสารความลับทางราชการไว้ที่โต๊ะหลังเลิกงาน

4. กุญแจที่สามารถเปิดลิ้นชักเอกสารลับจะต้องมีผู้รับผิดชอบและอยู่ในที่ปลอดภัย

5. ผู้ใช้งานจะต้องไม่บันทึกรหัสผ่านเก็บไว้ที่โต๊ะหรือเครื่องคอมพิวเตอร์ที่ใช้งาน

6. เมื่อมีการพิมพ์เอกสารความลับทางราชการผ่านทางเครื่องพิมพ์จะต้องนำเอกสารออกจากเครื่องพิมพ์ทันที

7. เมื่อได้รับเอกสารความลับทางราชการผ่านเครื่องโทรสารจะต้องรีบนำออกจากเครื่องโทรสารทันที

8. กรณีที่มีการจำหน่ายพัสดุ อุปกรณ์คอมพิวเตอร์ หรือ อุปกรณ์จัดเก็บข้อมูลที่มีข้อมูลที่เป็นความลับทางราชการจะต้องดำเนินการทำลายข้อมูลนั้นก่อนทุกครั้ง วิธีการทำลายข้อมูลจะต้องดำเนินการดังตารางนี้

การทำลายข้อมูล			
อุปกรณ์	ขั้นตอนการดำเนินงาน		
	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
ฮาร์ดดิสก์ (Hard Disk)	ทำการเขียนข้อมูลทับข้อมูลเดิมและต้องได้รับอนุญาตจากผู้ที่มีสิทธิเท่านั้น	ทำการใช้เครื่องมือในการทำลายล้างข้อมูล เช่น โปรแกรม Secure Erase เป็นต้น	ทำการทุบเพื่อทำลาย
สื่อบันทึกข้อมูลแบบพกพา(USB Drives)	ทำการเขียนข้อมูลทับข้อมูลเดิมและต้องได้รับอนุญาตจากผู้ที่มีสิทธิเท่านั้น	ทำการใช้เครื่องมือในการทำลายล้างข้อมูล เช่น โปรแกรม Secure Erase เป็นต้น	ทำการทุบเพื่อทำลาย
ซีดีรอม หรือ ดีวีดีรอม	ย่อยเพื่อทำลาย	ย่อยเพื่อทำลาย	ย่อยเพื่อทำลาย

การทำลายข้อมูล			
อุปกรณ์	ขั้นตอนการดำเนินงาน		
	ระดับที่ 1 (Clear)	ระดับที่ 2 (Purge)	ระดับที่ 3 (Destroy)
อุปกรณ์พกพา (Cell, PDA)	ทำการล้างข้อมูลของผู้ใช้และข้อมูลการใช้งานทั้งหมดและรีเซตค่าไปยังค่าเริ่มต้นที่ออกจากโรงงาน	เหมือนระดับที่ 1	ทำการทุบเพื่อทำลาย
เครื่องถ่ายเอกสารหรือโทรสาร	รีเซตตามบริษัทผู้ผลิต	เหมือนระดับที่ 1	เหมือนระดับที่ 1
อุปกรณ์เครือข่าย (Network Devices)	ทำการรีเซตค่าไปยังค่าเริ่มต้นที่ออกจากโรงงาน	เหมือนระดับที่ 1	เหมือนระดับที่ 1

หมายเหตุ ระดับที่ 1 สำหรับผู้ดูแลระบบของส่วนงานระดับที่ 2 และ ระดับที่ 3 สำหรับผู้ดูแลระบบของมหาวิทยาลัย เช่น สำนักคอมพิวเตอร์ หรือ ส่วนงานที่ดูแลระบบของมหาวิทยาลัย

ผู้รับผิดชอบ

ผู้บริหารส่วนงานที่เกี่ยวข้อง

ส่วนที่ 11 แนวปฏิบัติการบริหารจัดการสิทธิและการจัดกลุ่มเครือข่าย

1. มีการจัดกลุ่มและควบคุมเครือข่ายด้วยอุปกรณ์ไฟร์วอลล์และทำงานร่วมกับอุปกรณ์เครือข่ายสวิตช์ (Switch) ที่สามารถกำหนดเครือข่ายเสมือน (VLAN) ได้

2. การจัดกลุ่มเครือข่ายผู้ใช้งานภายในให้ทำการจัดกลุ่มตามภารกิจ และหน้าที่ โดยจำกัดการเข้าถึงข้ามส่วนงาน หรือกลุ่มงาน เพื่อป้องกันข้อมูลรั่วไหล หรือการโจมตีในเครือข่าย

3. การใช้งานบนเครือข่ายหลักต้องมีการจัดกลุ่มพื้นที่การทำงานตามความเหมาะสม โดยแบ่งแยกเป็นส่วน ดังนี้

(1) กลุ่มเครือข่ายแบบใช้สาย (Wire)

(2) กลุ่มเครือข่ายแบบไร้สาย (Wireless)

(3) กลุ่มเจ้าหน้าที่ดูแลระบบ (Administrator)

(4) กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายให้บริการสาธารณะ (Public Server)

(5) กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายโปรแกรมประยุกต์ เฉพาะงาน (Application Server)

(6) กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายให้บริการเฉพาะภายในมหาวิทยาลัย (Internal Server)

(7) กลุ่มเครือข่ายส่วนขยายของมหาวิทยาลัย

(8) กลุ่มเครือข่ายภายนอกมหาวิทยาลัย

4. กลุ่มผู้ใช้งานมีสิทธิในการเข้าใช้งานระบบเครือข่ายดังนี้

(1) สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

(2) สามารถเข้าใช้งานระบบสารสนเทศภายในได้โดยไม่มีการจำกัดระยะเวลา

(3) สามารถใช้งานอินเทอร์เน็ตได้ต่อเมื่อมีการพิสูจน์ตัวตนโดยใช้รหัสบัวศรีไอดีเท่านั้น

5. กลุ่มผู้ใช้งานมีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย ดังนี้

(1) สามารถใช้งานอินเทอร์เน็ตที่เป็นประโยชน์ต่อมหาวิทยาลัยเท่านั้น

(2) สามารถใช้งานอินเทอร์เน็ตได้เมื่อมีการพิสูจน์ตัวตน โดยใช้รหัสบัวศรีไอดีเท่านั้น

6. กลุ่มเจ้าหน้าที่ภายนอกกำหนดให้เป็นกลุ่มของผู้รับจ้างพัฒนาระบบสารสนเทศของมหาวิทยาลัย โดยมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

(1) ไม่สามารถเชื่อมต่อไปยังภายนอกกลุ่มของตนเองเว้นแต่มีการขออนุญาตเป็นกรณีพิเศษ ซึ่งจะต้องได้รับความเห็นชอบจากสำนักคอมพิวเตอร์เป็นลายลักษณ์อักษร

7. กลุ่มเจ้าหน้าที่ดูแลระบบมีสิทธิในการเข้าใช้งานบนระบบเครือข่ายดังนี้

(1) สามารถเชื่อมต่อเข้าไปยังระบบเครือข่ายของมหาวิทยาลัยได้ทุกที่และตลอดเวลา

8. กลุ่มเครื่องคอมพิวเตอร์แม่ข่ายต้องมีการกำหนดระดับความสำคัญ ตามความต้องการเพื่อจัดกลุ่มเครื่องคอมพิวเตอร์แม่ข่ายไปยังตำแหน่งที่เหมาะสม ไม่ว่าจะเป็นกลุ่มของเครื่องแม่ข่ายที่ให้บริการสาธารณะ ระบบโปรแกรมประยุกต์ หรือเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการเฉพาะภายในเท่านั้น

(1) สามารถเชื่อมต่อจากกลุ่มต่างๆ ของมหาวิทยาลัยที่ได้กำหนดไว้ เพื่อเข้าใช้บริการบนเครื่องคอมพิวเตอร์แม่ข่าย

(2) เครื่องคอมพิวเตอร์ภายนอกระบบเครือข่ายของมหาวิทยาลัยต้องไม่สามารถเชื่อมต่อเข้ามายังเครื่องแม่ข่ายที่อยู่ในกลุ่ม เพื่อให้บริการภายในมหาวิทยาลัยเท่านั้น

(3) เครื่องคอมพิวเตอร์แม่ข่ายไม่สามารถเชื่อมต่อไปยังอินเทอร์เน็ตเว้นแต่มีเหตุจำเป็นที่จะต้องเชื่อมต่อ เช่น การใช้งานดีเอ็นเอส (DNS) การอัพเดตระบบ การปรับปรุงเรื่องไวรัส เป็นต้น

9. สำนักคอมพิวเตอร์สามารถระงับการใช้งาน หรือไม่อนุญาตให้มีการใช้งานเครื่องคอมพิวเตอร์ลูกข่าย หรือเครื่องคอมพิวเตอร์แม่ข่าย หากตรวจพบความผิดปกติที่อาจก่อให้เกิดความเสียหาย กับระบบเครือข่ายของมหาวิทยาลัย

10. มีการกำหนดการควบคุมการเข้าถึงในแต่ละกลุ่มพื้นที่การทำงาน โดยการเชื่อมต่อมายังส่วนกลางต้องได้รับการอนุญาตและต้องได้รับสิทธิในการเข้าถึงระบบเครือข่ายจากผู้อำนวยการสำนักคอมพิวเตอร์

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์

ส่วนที่ 12 แนวปฏิบัติการจัดการอุปกรณ์รักษาความปลอดภัย ไฟร์วอลล์ (firewall)

1. สำนักคอมพิวเตอร์มีหน้าที่ในการบริหารจัดการและกำหนดค่าการใช้งานของอุปกรณ์รักษาความปลอดภัยส่วนกลางบนระบบเครือข่ายของมหาวิทยาลัย

2. การใช้บริการต่าง ๆ จะไม่สามารถให้บริการได้แต่มีการขออนุญาตเป็นพิเศษ หรือบริการที่ทางสำนักคอมพิวเตอร์เปิดให้บริการเท่านั้น

3. ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนโดยใช้ชื่อผู้ใช้และรหัสผ่านบัวศรีไอดีทุกครั้ง ก่อนเข้าใช้งานอินเทอร์เน็ต

4. การเปลี่ยนแปลงการกำหนดค่าต่าง ๆ บนอุปกรณ์รักษาความปลอดภัยจะต้องดำเนินการโดยผู้ที่ได้รับมอบหมาย และทุกครั้งที่มีการเปลี่ยนแปลงต้องบันทึกข้อมูล และสำรองข้อมูลค่าต่าง ๆ เก็บไว้ก่อนทำการเปลี่ยนแปลง

5. การให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตที่เป็นการใช้งานพื้นฐาน หรือโปรแกรมทั่วไปเท่านั้น หากส่วนงานอื่นมีความจำเป็นต้องเชื่อมต่อผ่านพอร์ตนอกเหนือจากที่กำหนดไว้ ต้องได้รับอนุญาตเป็นกรณีพิเศษจากสำนักคอมพิวเตอร์

6. พอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบจะสามารถเข้าใช้งานได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

7. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายจะถูกกำหนดค่าตามแบบฟอร์มขอเปิดใช้บริการเครื่องคอมพิวเตอร์แม่ข่ายเท่านั้น

8. เส้นทางการเชื่อมต่อระบบเครือข่ายจะต้องมีการควบคุม เพื่อให้เกิดความปลอดภัยกับข้อมูลสารสนเทศที่มีความสำคัญสูง

9. ในกรณีตรวจพบว่าเครื่องคอมพิวเตอร์ลูกข่ายใดที่มีพฤติกรรมการใช้งานที่ขัดต่อนโยบาย หรือมีการใช้งานอันก่อให้เกิดปัญหาต่อเครือข่าย สำนักคอมพิวเตอร์ขอสงวนสิทธิ์ในการระงับ หรือบล็อกการใช้งานเครื่องคอมพิวเตอร์ลูกข่ายนั้นจนกว่าจะดำเนินการแก้ไขเสร็จสิ้น

10. ผู้ละเมิดนโยบายด้านความปลอดภัยของระบบเครือข่ายบัวศรีของมหาวิทยาลัยจะถูกระงับการใช้งานทันทีโดยมิต้องแจ้งให้ทราบล่วงหน้า

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์

ส่วนที่ 13 แนวปฏิบัติการควบคุมการให้บริการข้อมูล

1. มหาวิทยาลัยต้องกำหนดให้มีมาตรการควบคุมการให้บริการข้อมูลสารสนเทศเพื่อเป็นแนวปฏิบัติที่ดีในการรักษาความปลอดภัยของข้อมูลในกรณีที่ส่วนงานหรือหน่วยงานภายนอกขอข้อมูลสารสนเทศ

โดยกำหนดแนวปฏิบัติในการให้บริการข้อมูลอย่างเป็นทางการ ผู้ขอใช้ข้อมูลต้องขออนุญาตเป็นลายลักษณ์อักษรตามสายงานต่อถึงหัวหน้าส่วนงานของมหาวิทยาลัย

2. ผู้ดูแลข้อมูลจะต้องกำหนดรูปแบบการให้บริการข้อมูลสารสนเทศให้เหมาะสมกับการนำไปใช้

3. ผู้ดูแลข้อมูลต้องจัดให้มีการติดตั้งระบบบันทึกรายละเอียดการเข้าถึงข้อมูลและติดตามการใช้ข้อมูลสารสนเทศ

4. ผู้ดูแลข้อมูล หรือผู้ขอใช้ข้อมูลจะต้องไม่เปิดเผยข้อมูลหรือกระทำการใดให้ผู้อื่นทราบถึงข้อมูลของมหาวิทยาลัย

ผู้รับผิดชอบ

ผู้บริหารส่วนงานที่เกี่ยวข้อง

หมวดที่ 4
การจัดหาพัฒนา บำรุงรักษาและการส่งมอบระบบสารสนเทศ

ตามนโยบายในหมวดที่ว่าด้วยการจัดหา พัฒนาและบำรุงรักษาระบบสารสนเทศ ซึ่งกำหนดขึ้นเพื่อให้การพัฒนาและบำรุงระบบสารสนเทศสามารถดำเนินการได้โดยสอดคล้องกับนโยบายความมั่นคงปลอดภัย และเพื่อให้เกิดความถูกต้องสมบูรณ์ของข้อมูลในระบบสารสนเทศ มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติสำหรับการดำเนินการพัฒนาระบบขึ้นเพื่อให้ผู้ออกแบบ ผู้พัฒนา รวมทั้งผู้ดูแลระบบได้ตระหนักถึงความมั่นคงปลอดภัยของสารสนเทศ และปฏิบัติอย่างเคร่งครัด

ส่วนที่ 1 แนวปฏิบัติการพัฒนาระบบสารสนเทศ

1. การออกแบบระบบสารสนเทศต้องคำนึงถึงความต้องการในการใช้งานและความต้องการของผู้ใช้

2. การวิเคราะห์และออกแบบระบบสารสนเทศ ต้องคำนึงถึงความปลอดภัยในการเข้าถึงและจัดเก็บข้อมูล โดยระบบสารสนเทศหลักที่มีความสำคัญ ต้องมีการเข้ารหัสของการสื่อสารระหว่างเครื่องคอมพิวเตอร์แม่ข่ายและเครื่องคอมพิวเตอร์ลูกข่ายด้วยมาตรฐานใบรับรอง (SSL)

3. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องมีกระบวนการระบุและพิสูจน์ตัวตนตามนโยบายและแนวปฏิบัติการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

4. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องสามารถกำหนดกลุ่มของผู้ใช้งาน ได้แก่ ผู้ใช้งานทั่วไป เจ้าหน้าที่ดูแลระบบ ผู้เยี่ยมชม เป็นต้น

5. ระบบงานสารสนเทศที่พัฒนาขึ้นต้องสามารถกำหนดสิทธิให้แต่ละกลุ่มในการดำเนินการ ได้แก่ กลุ่มที่สามารถมองเห็นเมนู กลุ่มที่สามารถเพิ่ม แก้ไขข้อมูล กลุ่มที่สามารถลบข้อมูล เป็นต้น

6. ต้องมีการจัดเก็บข้อมูลการเข้าใช้ระบบงานโดยมีรายละเอียดอย่างน้อย คือ วัน เวลา และผู้ใช้งาน

7. ระบบสารสนเทศมีระยะเวลาในการเข้าใช้งานเป็นเวลา 3 ชั่วโมง ในกรณีที่ต้องการใช้งานต่อเนื่องจะต้องทำการกดปุ่ม Refresh เพื่อต่อเวลาในการเข้าใช้งานเพิ่มครั้งละ 3 ชั่วโมง (Session Timeout)

8. ในการพัฒนา และทดสอบระบบ ผู้พัฒนาจะต้องพัฒนาระบบบนเครื่องคอมพิวเตอร์ที่จัดเตรียมไว้สำหรับการพัฒนาเท่านั้น

9. ผู้พัฒนาระบบต้องตรวจสอบและควบคุมเวอร์ชั่นของซอร์สโค้ด และต้องมีระบบการสำรองซอร์สโค้ด ก่อนการแก้ไขทุกครั้ง

10. ผู้พัฒนาระบบต้องทำการทดสอบระบบตั้งแต่การนำข้อมูลเข้า กระบวนการประมวลผล และตรวจสอบผลลัพธ์จากการประมวลผลทุกครั้งก่อนนำระบบขึ้นใช้งานจริง

11. ระบบที่พัฒนาขึ้นต้องมีการควบคุมเวอร์ชั่นของโปรแกรม เพื่อควบคุมการเปลี่ยนแปลงหรือแก้ไข โดยต้องมีการทดสอบการทำงานของระบบกับเครื่องคอมพิวเตอร์ทดสอบทุกครั้ง เมื่อมีการเปลี่ยนแปลงก่อนที่จะดำเนินการใช้งานกับเครื่องคอมพิวเตอร์ใช้งานหลัก

12. ระบบสารสนเทศของมหาวิทยาลัยมีการควบคุมการเข้าถึงชุดคำสั่ง (Source code) ของระบบ โดยสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับสิทธิ์เท่านั้น

13. มีแผนในการบำรุงรักษาระบบ ได้แก่ การแนะนำและส่งเสริมการใช้งาน การบำรุงรักษาระบบ และการสำรวจความต้องการเพื่อนำมาปรับปรุงระบบ

14. ระบบสารสนเทศที่มีความสำคัญสูงและไวต่อการรบกวนจะต้องมีการแยกเครื่อง เพื่อใช้ในการพัฒนาและการทดสอบก่อนนำไปใช้งานจริง

ส่วนที่ 2 แนวปฏิบัติการส่งมอบข้อมูลส่วนบุคคลแก่หน่วยงานอื่น

การดำเนินการประเมินก่อนการส่งมอบข้อมูล

1. ผู้ร้องขอข้อมูลส่วนบุคคลต้องดำเนินการกรอกคำร้องขอข้อมูลส่วนบุคคล หรือบันทึกถึงผู้ควบคุมข้อมูลส่วนบุคคลถึงรายละเอียดและวัตถุประสงค์ในการนำข้อมูลไปใช้
2. ให้ผู้ควบคุมข้อมูลส่วนบุคคลดำเนินการตรวจสอบสิทธิ อำนาจหน้าที่ และฐานกฎหมายที่บุคคลหรือหน่วยงาน หรือนิติบุคคลนั้นร้องขอข้อมูลส่วนบุคคล
3. ตรวจสอบรายละเอียดวัตถุประสงค์ ว่าจะสามารถส่งมอบข้อมูลให้ตามคำร้องขอได้ในระดับใด ซึ่งในกรณีที่ต้องการข้อมูลที่ชี้จำเพาะถึงข้อมูลส่วนบุคคล สามารถทำการแปลงข้อมูลที่ชี้จำเพาะเป็นรหัสนิรนามเพื่อใช้ประโยชน์แทนได้หรือไม่

การส่งมอบข้อมูล

1. ดำเนินการจัดเตรียมข้อมูลให้เป็นไปตามผลการประเมิน โดยการส่งมอบข้อมูลส่วนบุคคลเท่าที่จำเป็นตามวัตถุประสงค์การใช้งาน
2. บันทึกชื่อของผู้ขอข้อมูล และข้อมูลการติดต่อ และฐานกฎหมายที่ใช้ ตลอดจนวัตถุประสงค์ในการใช้ข้อมูลส่วนบุคคล
3. แจ้งให้ผู้ร้องขอทราบ ว่าเมื่อได้รับข้อมูลแล้วต้องดำเนินการตามขอบเขตและวัตถุประสงค์ที่ร้องขอไปเท่านั้น

หลังส่งมอบข้อมูล

1. ติดตามทบทวนการใช้ข้อมูล ทุก 1 ปีว่ายังมีการใช้งานอยู่หรือมีการใช้งานตามวัตถุประสงค์หรือไม่ หากไม่ได้มีการใช้งานแล้ว ควรแจ้งให้ผู้ร้องขอทำการลบทำลายข้อมูลนั้น
2. กำหนดรูปแบบในการปรับปรุงข้อมูลให้มีความทันสมัยต่อการใช้งาน เช่น อาจจะใช้การส่งข้อมูลผ่านระบบ API เพื่อให้ข้อมูลที่ได้รับปลายทางเป็นข้อมูลที่ทันสมัยอัตโนมัติตลอดเวลา

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย และผู้ควบคุมข้อมูลส่วนบุคคล

หมวดที่ 5
การดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย

ตามนโยบายในหมวดที่ว่าด้วยการดำเนินการกับสถานการณ์ด้านความมั่นคงปลอดภัย ซึ่งกำหนดขึ้นเพื่อให้มีระบบการรายงานเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย และใช้เป็นเครื่องมือที่ช่วยในการตรวจสอบและปรับปรุงแก้ไขระบบให้มีประสิทธิภาพมากยิ่งขึ้น มหาวิทยาลัยจึงได้จัดทำแนวปฏิบัติเพื่อการตรวจสอบ และจัดการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยได้อย่างเหมาะสมและมีประสิทธิภาพ

ส่วนที่ 1 แนวปฏิบัติการจัดการแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัย

1. ผู้ดูแลระบบต้องดำเนินการตรวจสอบการใช้งานระบบเครือข่ายโดยใช้เครื่องมือในการตรวจสอบและจัดเก็บข้อมูลการให้บริการเครือข่าย
2. เมื่อมีการตรวจพบความผิดปกติซึ่งทำให้ระบบเครือข่ายไม่สามารถให้บริการได้ หรือการใช้งานไม่สะดวก ผู้ดูแลระบบจะต้องดำเนินการแจ้งให้ผู้ใช้ทราบและจัดเก็บลงระบบรายงานปัญหาระบบเครือข่าย
3. ผู้ดูแลระบบจะต้องเร่งดำเนินการแก้ไขปัญหาระบบเครือข่าย ให้สามารถกลับมาใช้งานได้ตามปกติ ในกรณีที่ไม่สามารถแก้ไขให้ใช้งานได้ภายใน 15 นาที ต้องดำเนินการแจ้งเจ้าหน้าที่ประชาสัมพันธ์ประกาศข่าวเครือข่ายและแจ้งหัวหน้าส่วนงานที่เกี่ยวข้องทราบ
4. เมื่อดำเนินการแก้ไขเสร็จสิ้น ต้องดำเนินการแจ้งเจ้าหน้าที่ประชาสัมพันธ์ประกาศข่าวเครือข่าย และจัดทำคู่มือวิธีการแก้ไขปัญหา รวมถึงรายงานสรุปผลการดำเนินงานต่อหัวหน้าส่วนงาน

ส่วนที่ 2 แนวปฏิบัติการแจ้งเหตุละเมิดข้อมูลส่วนบุคคล

1. มีการกำหนดให้ผู้รับผิดชอบในแต่ละระบบงานมีการแจ้งเหตุละเมิดให้กับเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคลของมหาวิทยาลัย
2. เจ้าหน้าที่คุ้มครองข้อมูลร่วมกับผู้ดูแลระบบรักษาความปลอดภัยปฏิบัติตามกระบวนการดำเนินการเมื่อทราบเหตุอุบัติการณ์ละเมิดข้อมูลส่วนบุคคล
3. กรณีที่มีเหตุละเมิดข้อมูลส่วนบุคคล ต้องกำหนดวิธีปฏิบัติหรือขั้นตอนการแจ้งต่อสำนักงานคณะกรรมการคุ้มครองข้อมูลส่วนบุคคลทราบถึงเหตุละเมิดข้อมูลส่วนบุคคลภายใน 72 ชั่วโมง (นับตั้งแต่ทราบเหตุ)
4. การแจ้งเหตุละเมิดอาจได้รับข้อยกเว้นไม่ต้องดำเนินการได้ หากมีการประเมินผลกระทบแล้วพบว่าไม่มีความเสี่ยงหรือกระทบต่อสิทธิและเสรีภาพของบุคคล เช่น กรณีข้อมูลถูกเข้ารหัสโดย Ransomware และไม่สามารถใช้งานได้ แต่ข้อมูลส่วนบุคคลไม่ได้มีการรั่วไหลออกไป เป็นต้น

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย และเจ้าหน้าที่คุ้มครองข้อมูลส่วนบุคคล

หมวด 6
การบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย

ตามนโยบายในหมวดที่ว่าด้วยการบริหารความต่อเนื่องของการดำเนินภารกิจของมหาวิทยาลัย ซึ่งกำหนดขึ้นเพื่อมิให้การดำเนินงานตามภารกิจของมหาวิทยาลัยเกิดการติดขัดหรือหยุดชะงัก และป้องกันมิให้การปฏิบัติงานตามภารกิจที่สำคัญของมหาวิทยาลัยต้องได้รับผลกระทบ หรือเกิดความเสียหายรุนแรง อันเนื่องจากความผิดพลาดของระบบสารสนเทศ และเพื่อให้มั่นใจได้ว่าสามารถกู้ระบบคืนได้ในระยะเวลาที่เหมาะสม มหาวิทยาลัยจึงได้กำหนดแนวปฏิบัติเพื่อการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยของสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงที่อาจเกิดขึ้นได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

ส่วนที่ 1 แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยง

1. ระบุความเสี่ยงและเหตุการณ์ความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของมหาวิทยาลัย เพื่อตรวจสอบและประเมินความเสี่ยง ดังต่อไปนี้

(1) ความเสี่ยงที่เกิดจากการลักลอบเข้าถึงระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet) และอินทราเน็ต (Intranet) โดยไม่ได้รับอนุญาต

(2) ความเสี่ยงที่เกิดจากการลักลอบเข้าถึงระบบเครือข่ายโดยไม่ได้รับอนุญาต

(3) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

(4) ความเสี่ยงที่เกิดจากการพิสูจน์ตัวตนกับระบบสารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้บัญชีเดียวกันมากกว่าหนึ่งจุด

(5) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่านของผู้อื่นโดยมิได้รับอนุญาต

(6) ความเสี่ยงที่เกิดจากมีเหตุละเมิดข้อมูลส่วนบุคคล

2. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดขึ้น โดยการประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

(1) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยง

(2) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์รวมถึงความเป็นไปได้ที่จะเกิดเหตุการณ์

(3) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์

3 กำหนดมาตรการจัดการความเสี่ยง

(1) ดำเนินการทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอนและภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศ (IT contingency plan)

(2) ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ 1 ครั้ง

(3) การตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบระบบสารสนเทศ (internal IT auditor) หรือผู้ตรวจสอบด้านความมั่นคงปลอดภัยจากภายนอก (external IT auditor)

ผู้รับผิดชอบ

สำนักคอมพิวเตอร์

ส่วนที่ 2 แนวปฏิบัติการสำรองข้อมูล

1. จัดทำสำเนาระบบซอฟต์แวร์และระบบฐานข้อมูล โดยจัดลำดับตามความสำคัญของระบบสารสนเทศของมหาวิทยาลัย

2. มีขั้นตอนในการดำเนินการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และระบบฐานข้อมูลมหาวิทยาลัย โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

4. จัดเก็บข้อมูลที่สำรองในสื่อเก็บข้อมูล โดยมีการจัดการระบบสำรองข้อมูลอย่างเป็นระบบ ซึ่งมีการจัดอันดับข้อมูลตามความสำคัญของระบบสารสนเทศ เพื่อให้สามารถตรวจสอบ ติดตาม และนำข้อมูลมาใช้งานได้ในภายหลัง

5. มีการทบทวนแผนในการตรวจสอบระบบสำรองข้อมูลของมหาวิทยาลัย อย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

ส่วนที่ 3 แนวปฏิบัติการจัดทำระบบสำรองข้อมูล

1. พิจารณาคัดเลือกระบบสำรองข้อมูลที่เหมาะสมกับมหาวิทยาลัยให้พร้อมใช้งาน

2. กำหนดกระบวนการในการวางแผนรับมือกับเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูง

3. กำหนดชนิดของภัยพิบัติที่มีผลต่อระบบที่มีความสำคัญสูง และจำเป็นต้องมีแผนรับมือ

4. กำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลแต่ละระบบสารสนเทศ และระบบสำรองข้อมูล

5. ทำการประเมินความเสี่ยงจากภัยพิบัติที่มีผลทำให้ระบบที่มีความสำคัญสูงติดขัด หรือไม่สามารถให้บริการได้ อันเป็นผลจากภัยพิบัติที่ได้กำหนดไว้

6. กำหนดขั้นตอนการแจ้งปัญหาต่อผู้ดูแลรับผิดชอบในแต่ละระดับชั้น เมื่อเกิดภัยพิบัติ

7. ทดสอบ ประเมิน และปรับปรุงแผนรับมือเหตุภัยพิบัติสำหรับระบบที่มีความสำคัญสูงอย่างน้อยปีละ 1 ครั้ง

ผู้รับผิดชอบ

ผู้ดูแลระบบที่ได้รับมอบหมาย

หมวด 7
การปฏิบัติตามข้อกำหนด

ตามนโยบายในหมวดที่ว่าด้วยการปฏิบัติตามข้อกำหนด ซึ่งกำหนดขึ้นเพื่อให้มั่นใจว่านิสิตและบุคลากรของมหาวิทยาลัยรับทราบ และปฏิบัติตามนโยบาย กฎ ระเบียบ ข้อบังคับ รวมทั้งกฎหมายที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสารสนเทศ มหาวิทยาลัยจึงได้กำหนดแนวปฏิบัติเพื่อให้มีการเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

ส่วนที่ 1 แนวปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของสารสนเทศ

1. จัดประชุมฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรม

2. จัดประชุมสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากร โดยการจัดสัมมนาอย่างน้อยปีละ 1 ครั้ง หรือจัดร่วมกับการสัมมนาอื่นและอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ เพื่อถ่ายทอดความรู้

3. ประชาสัมพันธ์ และเผยแพร่ให้ความรู้เกี่ยวกับแนวปฏิบัติ ในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ

4. ให้ทุกภาคส่วนมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

5. มหาวิทยาลัยต้องแต่งตั้งคณะกรรมการกำกับติดตามและประเมินผลความมั่นคงปลอดภัยของสารสนเทศ

ผู้รับผิดชอบ

มหาวิทยาลัยศรีนครินทรวิโรฒ