แนวนโยบายและแนวปฏิบัติ ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของคณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

จัดทำโดย คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

พ.ศ. 2566

คำนำ

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นสิ่งที่จำเป็นและต้องลงมือปฏิบัติอย่างต่อเนื่อง การกำหนดนโยบายและแนวปฏิบัติต้องมีความร่วมมือจากทุกส่วนงานที่เกี่ยวข้อง เพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างเหมาะสม และมีประสิทธิภาพ เพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานที่ไม่ถูกต้อง ซึ่งจะส่งผลให้เกิดความไม่มั่นคงและปลอดภัยในการใช้งานสารสนเทศ ด้วยเหตุผลดังคณะวิทยาการสารสนเทศจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2566 ขึ้น เพื่อเผยแพร่ให้ บุคลากร นักศึกษาในคณะวิทยาการสารสนเทศ และบุคคลภายนอกที่ปฏิบัติงานร่วมกับคณะวิทยาการสารสนเทศได้รับทราบ และให้ความร่วมมือปฏิบัติตามอย่างเคร่งครัดต่อไป

คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

ปี พ.ศ. 2566

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ คณะวิทยาการสารสนเทศ

หลักการและเหตุผล

คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม เป็นคณะที่เน้นการเรียนการสอน วิจัย บริการทางวิชาการ ทะนุบำรุงศิลปะวัฒนธรรม ถ่ายทอดและพัฒนาเทคโนโลยี โดยอาศัยเทคโนโลยีสารสนเทศเป็นตัวขับเคลื่อนหลัก เพื่อให้ทันต่อการเปลี่ยนแปลงและความเจริญทางสังคม การเมือง เศรษฐกิจ และสอดคล้องต่อความเจริญก้าวหน้าทางด้านเทคโนโลยีสารสนเทศ ระบบเทคโนโลยีสารสนเทศของคณะวิทยาการสารสนเทศประกอบไปด้วยฮาร์ดแวร์และซอฟต์แวร์ รวมทั้งการเชื่อมต่อกันทั้งภายในและภายนอกคณะวิทยาการสารสนเทศ จึงจำเป็นต้องมีการดูแลรักษาให้สามารถใช้งานได้อย่างต่อเนื่องและตลอดเวลา ซึ่งสถานะการณ์ในปัจจุบันปรากฏว่ามีความเสี่ยงเพิ่มมากขึ้นในการถูกโจมตี ไวรัสคอมพิวเตอร์ บุคลากร หรือจากปัจจัยทั้งภายในและภายนอกต่างๆ ซึ่งส่งผลเสียกับภาพรวมต่อระบบเทคโนโลยีสารสนเทศ และส่งผลกระทบต่อการดำเนินงานของคณะวิทยาการสารสนเทศ ดังนั้นคณะวิทยาการสารสนเทศจึงได้ดำเนินการจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของคณะวิทยาการสารสนเทศ เพื่อป้องกันและแก้ปัญหาที่อาจเกิดขึ้นในอนาคต

วัตถุประสงค์

1. เพื่อให้การใช้ระบบสารสนเทศสามารถดำเนินงานได้อย่างเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัย ใช้งานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อคณะวิทยาการสารสนเทศ
2. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของคณะวิทยาการสารสนเทศ
3. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ และขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของคณะวิทยาการสารสนเทศ
4. เพื่อเผยแพร่นโยบายและแนวปฏิบัตินี้ ให้บุคลากร นักศึกษา และบุคคลภายนอกที่ปฏิบัติงานร่วมกับคณะวิทยาการสารสนเทศได้รับทราบ และถือปฏิบัติตามอย่างเคร่งครัด
5. เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

6. เพื่อส่งเสริมให้บุคลากร และนักศึกษาของสถาบัน มีความรู้ ความเข้าใจ และสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของ คณะวิทยาการสารสนเทศ

หมวดที่ 1

ความหมายและคำจำกัดความ

วัตถุประสงค์

1. เพื่ออธิบายคำศัพท์ที่จำเป็นต้องทราบและคำศัพท์เกี่ยวกับเทคโนโลยีสารสนเทศ เพื่อให้บุคลากรในคณะวิทยาการสารสนเทศ ใช้เป็นแนวทางในการปฏิบัติงานได้อย่างมีประสิทธิภาพ

ผู้รับผิดชอบ

1. บุคลากร นิสิต นักศึกษา เจ้าหน้าที่ในคณะวิทยาการสารสนเทศทุกคน

คำศัพท์

1. **คณะวิทยาการสารสนเทศ** หมายความว่า คณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม
2. **หน่วยงานภายนอก** หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและการใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของคณะวิทยาการสารสนเทศ โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูล
3. **ห้องควบคุมระบบ** หมายถึง ห้องที่ติดตั้งและจัดวางระบบเซิร์ฟเวอร์ อุปกรณ์เชื่อมต่อ และอุปกรณ์เครือข่ายของคณะวิทยาการสารสนเทศ ภายใต้การดูแลของคณะวิทยาการสารสนเทศ
4. **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของคณะวิทยาการสารสนเทศเข้ากับเครือข่ายของสำนักคอมพิวเตอร์
5. **ระบบสารสนเทศ** หมายความว่า ระบบงานของคณะวิทยาการสารสนเทศที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่คณะวิทยาการสารสนเทศสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนให้การบริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ ฯลฯ

6. **ระบบคอมพิวเตอร์** หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ
7. **ระบบเครือข่ายคอมพิวเตอร์ (Computer Network System)** หมายความว่า ระบบที่เชื่อมต่อคอมพิวเตอร์ เซิร์ฟเวอร์อุปกรณ์เครือข่ายต่าง ๆ ของคณะวิทยาการสารสนเทศ
8. **สินทรัพย์คอมพิวเตอร์** หมายความว่า ข้อมูล คอมพิวเตอร์เซิร์ฟเวอร์ ระบบสารสนเทศ ระบบเครือข่าย อุปกรณ์เครือข่าย รวมถึงซอฟต์แวร์ที่มีลิขสิทธิ์
9. **ข้อมูลคอมพิวเตอร์** หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์
10. **ผู้บริหารเครือข่ายคอมพิวเตอร์** หมายถึง คณบดี รองคณบดี และผู้ช่วยคณบดีฝ่ายบริหารจัดการระบบเครือข่าย คณะวิทยาการสารสนเทศ
11. **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ซึ่งได้รับมอบหมายจากผู้บังคับบัญชาให้ทำหน้าที่ดูแลเซิร์ฟเวอร์ ระบบสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ให้บริการได้อย่างมีเสถียรภาพ ทั้งนี้ผู้ดูแลระบบมีสิทธิ์ในการดำเนินการดังต่อไปนี้
    - ผู้ดูแลระบบมีสิทธิ์ปรับตั้งระบบให้ทำงานได้อย่างมีประสิทธิภาพ และเสถียรภาพ
    - ผู้ดูแลระบบมีสิทธิ์ยุติการทำงานของกระบวนการที่สร้างภาระให้ระบบ หรืออาจทำให้เกิดปัญหากับการใช้งานต่อผู้ใช้ส่วนรวม
    - ผู้ดูและระบบมีสิทธิ์บีบอัดเพื่อลดขนาดแฟ้มข้อมูลของผู้ใช้ เพื่อบรรเทาปัญหาที่อาจเกิดจากเนื้อที่เก็บข้อมูลไม่พอเพียง
    - ผู้ดูแลระบบมีสิทธิ์กลั่นกรอง บริหารการใช้ช่องสัญญาณเครือข่าย จำกัดการเข้าถึงข้อมูล ทั้งข้อมูลที่อยู่ภายในเครือข่ายและภายนอกเครือข่าย เพื่อคงไว้ซึ่งประสิทธิภาพการใช้เครือข่ายและการใช้งานตามพันธกิจของคณะวิทยาการสารสนเทศ
12. **ผู้ใช้งาน (User)** หมายความว่า นิสิต บุคลากร คณะวิทยาการสารสนเทศหรือบุคคลภายนอกที่มีบัญชีรายชื่อที่ออกโดยคณะวิทยาการสารสนเทศ และ/หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์คอมพิวเตอร์ของคณะวิทยาการสารสนเทศ

13. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของคณะวิทยาการสารสนเทศ
14. **เจ้าหน้าที่** หมายถึง ข้าราชการ พนักงานราชการ ลูกจ้างชั่วคราว ลูกจ้างประจำ และเจ้าหน้าที่ประจำโครงการของคณะวิทยาการสารสนเทศ
15. **สื่อบันทึกพกพา (Portable media)** หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD , flash drive, external hard disk ฯลฯ
16. **ชื่อผู้ใช้ (Username)** หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่ายที่กำหนดสิทธิ์การใช้งานไว้
17. **รหัสผ่าน (Password)** หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคลเพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ
18. **การเข้ารหัสลับ (Encryption)** หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ
19. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบสารสนเทศและระบบเครือข่าย
20. **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การรักษาไว้ซึ่งความลับ (Confidentiality) ความครบถ้วนถูกต้อง (Integrity) และความพร้อมใช้ (Availability) ของสารสนเทศ
21. **เหตุการณ์ด้านความปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่งคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
22. **สถานการณ์ด้านความปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด หมายความว่า** สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของคณะวิทยาการสารสนเทศถูกบุกรุกโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
23. **การพิสูจน์ยืนยันตัวตน (Authentication)** หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบเป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้และรหัสผ่าน
24. **SSID (Service Set IDentifier)** หมายความว่า ชื่อระบุเครือข่ายไร้สาย

25. **MAC Address (Media Access Control address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ติดต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทาง (ชนิดจุดต่อจุด) ได้อย่างถูกต้อง
26. **VPN (Virtual Private Network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะ แล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
27. **แผนผังระบบเครือข่าย (Network diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของคณะวิทยาการสารสนเทศ
28. **ดีเอ็นเอส (Domain Name System: DNS)** หมายความว่า ระบบการตั้งชื่อโดเมนเพื่อใช้เก็บข้อมูลของชื่อโดเมน กับ IP address ที่ใช้งานอยู่
29. **ดีเอชซีพี (DHCP)** หมายความว่า ทำให้การจัดการและการกำหนดค่า IP Address ทั้งเครือข่ายเป็นไปโดยอัตโนมัติ

หมวดที่ 2

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีแนวทางการดำเนินงานการใช้ระบบเครือข่ายคอมพิวเตอร์และระบบสารสนเทศของคณะวิทยาการสารสนเทศ สำหรับการควบคุมการเข้าถึงข้อมูล เพื่อลดปัญหาในเรื่องความเสี่ยงต่างๆ ในการใช้ระบบสารสนเทศ
2. เพื่อให้บุคลากรในคณะวิทยาการสารสนเทศ ใช้เป็นแนวทางในการปฏิบัติงานให้เป็นไปอย่างมีประสิทธิภาพ

ผู้รับผิดชอบ

1. ฝ่ายบริหารจัดการระบบเครือข่าย คณะวิทยาการสารสนเทศ
2. หน่วยงานที่ให้บริการระบบเครือข่ายและคอมพิวเตอร์แม่ข่าย
3. ผู้ดูแลระบบที่ได้รับมอบหมาย
4. ผู้ใช้งาน

วิธีปฏิบัติ

1. ความมั่นคงทางกายภาพห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

ความมั่นคงทางกายภาพถือเป็นส่วนสำคัญของการรักษาความปลอดภัย เพื่อป้องกันสถานที่ที่ใช้ติดตั้งอุปกรณ์ระบบเครือข่ายและเครื่องแม่ข่ายต่างๆ ให้ปลอดภัยจากการปล้น การโจรกรรม อุบัติภัยทางธรรมชาติ เช่น แผ่นดินไหว น้ำท่วม กระแสไฟฟ้าลัดวงจร อุณหภูมิไม่เหมาะสมและการทำกระทำโดยประมาทของผู้ใช้งาน ดังนั้นจึงมีความจำเป็นต้องกำหนดนโยบายเพื่อควบคุมระบบคอมพิวเตอร์และเครือข่ายรวมถึงมาตรการในการใช้ห้องควบคุมระบบคอมพิวเตอร์และเครือข่าย

1.1 จำแนกและกำหนดพื้นที่ห้องควบคุมระบบ ดังนี้

1.1.1 ห้องควบคุมระบบแบ่งเป็นสองส่วน ได้แก่ พื้นที่ควบคุม (Control Area) และพื้นที่จำกัดการเข้าถึง (Restricted Area) โดยพื้นที่ควบคุม คือ พื้นที่ที่จัดไว้สำหรับการเยี่ยมชมหรือสังเกตการณ์ระบบ ส่วนพื้นที่จำกัดการเข้าถึง คือ ห้องที่มีเซิร์ฟเวอร์ และระบบเครือข่ายคอมพิวเตอร์ติดตั้งอยู่

1.2 การเข้าไปในพื้นที่ควบคุม

1.2.1 ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่ควบคุม ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบ ผู้บริหารหน่วยงานหรือบุคคลที่ผู้บริหารหน่วยงานนำเข้าเยี่ยมชม

1.2.2 ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

1.2.3 ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ควบคุมเว้นแต่ได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

1.2.4 ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

1.2.5 บุคคลอื่นที่มีความจำเป็นในการปฏิบัติงานหรือการเข้าเยี่ยมชมในพื้นที่ควบคุมต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมายและต้องมีเจ้าหน้าที่อยู่ด้วยตลอดเวลา

1.3 การเข้าไปในพื้นที่จำกัดการเข้าถึง

1.3.1 ไม่อนุญาตให้บุคคลใดเข้าไปในพื้นที่จำกัดการเข้าถึง ยกเว้นเจ้าหน้าที่ห้องควบคุมระบบหรือในกรณีที่บุคคลอื่นที่มีความจำเป็นเข้าไปปฏิบัติงานต้องได้รับอนุญาตจากผู้ดูแลระบบที่ได้รับมอบหมาย หรือได้รับมอบหมายจากผู้บังคับบัญชาตั้งแต่ระดับหัวหน้าภาควิชาขึ้นไป และต้องมีผู้ดูแลระบบที่ได้รับมอบหมายอย่างน้อย 1 คนเข้าไปร่วมปฏิบัติงานและประสานงานด้วยทุกครั้ง และให้บันทึกกิจกรรมการปฏิบัติงานทุกครั้ง

1.3.2 ไม่อนุญาตให้บุคคลที่มีอายุต่ำกว่า 15 ปี เข้าไปในพื้นที่จำกัดการเข้าถึง

1.3.3 ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในพื้นที่จำกัดการเข้าถึง

1.3.4 ไม่อนุญาตให้นำวัตถุไวไฟ วัตถุอันตราย และวัตถุติดไฟง่าย เช่น เศษกระดาษ เศษถุงพลาสติก เป็นต้น เข้าไปในเขตพื้นที่ เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

1.3.5 ไม่อนุญาตให้เข้าเยี่ยมชมในพื้นที่จำกัดการเข้าถึง

1.3.6 ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อ ทรัพย์สินจะอนุญาตให้เข้าไปในพื้นที่จำกัดการเข้าถึงได้ โดยได้รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย หรือได้รับมอบหมายจากผู้บังคับบัญชาตั้งแต่ระดับหัวหน้าภาควิชาขึ้นไป

1.4 ด้านกายภาพของห้องควบคุมระบบ

1.4.1 แยกอุปกรณ์ที่มีความสำคัญมากออกจากอุปกรณ์ที่ใช้งานทั่วไป เช่น router, switch, server, UPS เป็นต้น

1.4.2 จัดเก็บอุปกรณ์ต่างๆ ลงใน Rack อย่างเหมาะสมเพื่อสะดวกในการบำรุงรักษา

1.4.3 จัดวางอุปกรณ์ต่างๆ ให้ห่างจากประตู หน้าต่าง เพื่อป้องกันการโจรกรรม และงดการวางอุปกรณ์ให้ตรงกับเครื่องปรับอากาศโดยตรง เพื่อหลีกเลี่ยงความชื้นจากเครื่องปรับอากาศ

1.4.4 จัดวางสายเคเบิล สายไฟฟ้าให้เป็นระเบียบและไม่ควรทับกันเพื่อป้องกันสัญญาณรบกวน และควรมีการติดป้ายชื่อสายต้นทางและสายปลายทาง เพื่อให้ง่ายต่อการบำรุงรักษา

1.4.5 ติดประกาศบันทึกการบำรุงรักษา ชื่อ และหมายเลขโทรศัพท์ของผู้ดูแลรับผิดชอบอุปกรณ์แต่ละชนิด

1.4.6 มีระบบรักษาความปลอดภัยในห้องเช่น กล้อง CCTV ระบบการเข้าออกห้องโดยระบบ fingerprint scan หรือ RFID เป็นต้น

1.4.7 มีระบบสำรองไฟฟ้าเพื่อป้องกันไฟฟ้าดับ เช่น ติดตั้งระบบเครื่องกำเนิดไฟฟ้าอัตโนมัติและระบบสำรองไฟฟ้าอัตโนมัติ เป็นต้น

1.4.8 มีระบบป้องกันกระแสไฟฟ้าจากฟ้าผ่า

1.4.9 ระบบปรับอากาศแบบควบคุมอุณหภูมิ (20 - 25°C) และความชื้น (20 - 80%)

1.5 การบำรุงรักษาห้องควบคุมระบบและระบบเครือข่าย

1.5.1 ในกรณีที่ต้องการติดตั้งเซิร์ฟเวอร์หรืออุปกรณ์ต่างๆ ให้ประกอบให้แล้วเสร็จจากภายนอกพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึง ก่อนนำไปติดตั้ง เว้นแต่รับความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมาย

1.5.2 ในกรณีที่มีความจำเป็นต้องทำการก่อสร้าง ปรับปรุง และติดตั้ง ในพื้นที่ควบคุมและพื้นที่จำกัดการเข้าถึงต้องมีอุปกรณ์ควบคุม ฝุ่น ความร้อน เพื่อป้องกันความเสียหาย โดยผ่านความเห็นชอบจากผู้ดูแลระบบที่ได้รับมอบหมายก่อนการปฏิบัติงาน

1.5.3 ตรวจสอบความพร้อมของระบบรักษาความปลอดภัยทุก 3 เดือน

1.5.4 ร่างขั้นตอนแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน เช่น ไฟฟ้าลัดวงจร ไฟไหม้ แผ่นดินไหว น้ำท่วม หรือมีผู้บุกรุก เป็นต้น

1.5.5 ซ้อมการปฏิบัติงานตามแผนการดำเนินงานเมื่อเกิดกรณีฉุกเฉิน ทุก 6 เดือน

1.5.6 มีตารางการเข้าบำรุงรักษาอุปกรณ์ชัดเจน

2. การควบคุมการเข้าถึง (Access control)

สำหรับการควบคุมการเข้าถึงระบบสารสนเทศ หมายถึง การเข้าถึงระบบของผู้ใช้ และรวมความถึงการกำหนดหน้าที่ของผู้ใช้ การเข้าถึงเครือข่าย การใช้งานระบบที่ให้บริการและระบบสารสนเทศ การเฝ้าดูการใช้งานระบบ คอมพิวเตอร์ประเภทพกพาและการปฏิบัติงานนอกสถานที่ เป็นต้น

2.1 ผู้ดูแลระบบมีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิ์ในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้ ในการขออนุญาตเข้าระบบงานนั้นจะต้องทำเป็นเอกสารเพื่อขอสิทธิ์ในการเข้าสู่ระบบ และกำหนดให้ลงนามอนุมัติเอกสารดังกล่าวต้องจัดเก็บไว้เป็นหลักฐาน

2.2 เจ้าของข้อมูลและเจ้าของระบบงาน จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในหมวดที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น ดังนั้นการกำหนดสิทธิ์ในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็นขั้นต่ำเท่านั้น

2.3 ผู้ใช้งานจะต้องได้รับอนุญาตจากเจ้าหน้าที่ที่รับผิดชอบข้อมูลและระบบงานตามความจำเป็นต่อการใช้งานระบบสารสนเทศ

2.4 ผู้ใช้งานต้องไม่ดาวน์โหลดหรือติดตั้งโปรแกรม หรือให้ผู้อื่นผู้ใดติดตั้งโปรแกรม ที่ไม่ถูกต้องตามลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของหน่วยงาน หากฝ่าฝืนคณะวิทยาการสารสนเทศจะถือเป็นความรับผิดชอบของผู้ใช้งานเครื่องคอมพิวเตอร์เครื่องนั้น

2.5 ผู้ใช้งาน ต้องไม่นำทรัพย์สินของทางราชการไปใช้ในทางเสื่อมเสีย ผิดกฎหมาย หรือทำให้ผู้อื่นได้รับความเดือดร้อน

2.6 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์ชนิดพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

2.7 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านระบบเครือข่ายคอมพิวเตอร์จะต้องตรวจสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

2.8 ผู้ใช้งานต้องปฏิบัติตามการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์อย่างเคร่งครัด

3. การควบคุมการเข้าถึงเครือข่ายคอมพิวเตอร์ (Network access control)

เพื่อควบคุมการใช้บริการบนระบบเครือข่ายคอมพิวเตอร์

3.1 ผู้ดูแลระบบต้องจัดทำนโยบายเพื่อควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่าย โดยเฉพาะเพื่อป้องกันการเข้าถึงจากผู้ที่ไม่ได้รับอนุญาต

3.2 ผู้ดูแลระบบต้องจัดแบ่งเครือข่ายระหว่างการใช้งานภายในและผู้ใช้ภายนอก โดยพิจารณาจากบริการเครือข่าย ระบบสารสนเทศ กลุ่มของผู้ใช้งานของทั้งสองฝ่าย

3.3 การพิสูจน์ตัวตนสาหรับผู้ใช้ที่อยู่ภายนอกคณะวิทยาการสารสนเทศ ผู้ดูแลระบบต้องกำหนดให้พิสูจน์ตัวตน

3.4 การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการพิสูจน์ตัวตนในการเชื่อมต่อระหว่างเครือข่ายของคณะวิทยาการสารสนเทศและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

3.5 การควบคุมผู้ใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิ์การใช้งาน เพื่อควบคุมให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

3.6 ผู้ดูแลระบบต้องมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน

3.7 ผู้ดูแลระบบต้องจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องลูกข่ายไปยังเครื่องแม่ข่าย เพื่อไม่ให้ผู้ใช้สามารถใช้เส้นทางอื่น ๆ ได้

3.8 ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

3.9 ผู้ดูแลระบบ ต้องมีการออกแบบระบบเครือข่ายตามกลุ่มของผู้ใช้ เพื่อทำให้การควบคุม และป้องกันการบุกรุกได้อย่างเป็นระบบ

3.10 ต้องกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและควรมีการทบทวนการกำหนดค่า parameter ต่างๆ อย่างน้อยปีละครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

3.11 ระบบเครือข่ายทั้งหมดของคณะวิทยาการสารสนเทศที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ

3.12 ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย

3.13 ห้ามบุคคลใดกระทำการเคลื่อนย้ายหรือกระทำการใดๆ ต่ออุปกรณ์ของระบบเครือข่ายโดยพลการ เพราะอาจก่อให้เกิดความความเสียหายแก่ระบบเครือข่ายหลัก

3.14 ในกรณีที่ ตรวจสอบพบว่าเครือข่ายส่วนใดก่อให้เกิดความผิดปกติของระบบเครือข่ายหลักของอาจจะหยุดให้บริการจากระบบเครือข่ายกลางโดยไม่มีการแจ้งให้ทราบล่วงหน้าจนกว่าจะมีการแก้ไขให้ทำงานได้เป็นปกติก่อน

3.15 ห้ามทำการวางสายเครือข่ายเพิ่มเติมโดยไม่ได้รับอนุญาต ทั้งนี้รวมไปถึงการติดตั้งเครือข่ายแบบไร้สาย (Wireless Network) ด้วย

4. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

4.1 ต้องลงทะเบียนอุปกรณ์กระจายสัญญาณ (Access point) ทุกตัวก่อนเชื่อมต่อกับระบบเครือข่ายของคณะวิทยาการสารสนเทศ โดยแจ้งกับเจ้าหน้าที่ดูแลระบบเครือข่าย ถ้านำเอาอุปกรณ์กระจายสัญญาณ มาเชื่อมต่อโดยไม่ได้รับอนุญาต เจ้าหน้าที่สามารถตัดการเชื่อมต่อได้ทันที

4.2 ต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

4.3 เปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ มาใช้งาน

4.4 เปลี่ยนค่าชื่อบัญชีรายชื่อและรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สายและควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

4.5 ต้องกำหนดค่าใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสข้อมูลระหว่าง Wireless LAN client และอุปกรณ์กระจายสัญญาณ (Access point) เพื่อให้ยากต่อการดักจับข้อมูล

4.6 ใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อผู้บริหารระบบเครือข่ายทันที

5. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control)

5.1 ผู้ดูแลระบบต้องกำหนดให้มีการพิสูจน์ตัวตนสาหรับผู้ใช้เป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

5.2 ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด

5.3 ผู้ดูแลระบบต้องกำหนดกระบวนการในการเข้าสู่ระบบให้บริการเพื่อใช้งานเครื่องให้บริการที่มีความมั่นคงปลอดภัย เช่น กำหนดให้ระบบให้บริการปฏิเสธการใช้งาน หากผู้ใช้พิมพ์รหัสผ่านผิดพลาดเกิน 3 ครั้ง เป็นต้น

5.4 ผู้ดูแลระบบต้องมีวิธีการพิสูจน์ตัวตนสำหรับเครื่องคอมพิวเตอร์ ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบเครือข่ายคอมพิวเตอร์

5.5 ผู้ดูแลระบบต้องมีวิธีการกำหนดเวลาการใช้งานเครื่องคอมพิวเตอร์ เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง เช่น กลไกการล็อคหน้าจอ และต้องใช้รหัสผ่านในการเข้าสู่ระบบ เป็นต้น

5.6 ผู้ดูแลระบบต้องควบคุมการในการใช้โปรแกรมยูทิลิตี้ เพื่อป้องกันการเข้าถึงระบบโดยที่ไม่ได้รับอนุญาต โดยมีขั้นตอนดังนี้

5.6.1 ก่อนใช้ต้องพิสูจน์ตัวตนก่อน

5.6.2 ให้แยกโปรแกรมยูทิลิตี้ออกจากโปรแกรมระบบงาน

5.6.3 จำกัดการใช้งานโปรแกรมยูทิลิตี้ให้เฉพาะผู้ที่ได้รับมอบหมายแล้วเท่านั้น

5.6.4 ให้บันทึกรายละเอียดการเข้าใช้งานโปรแกรมยูทิลิตี้ เช่น ใครเป็นผู้ใช้งาน ใช้เมื่อไหร่ เป็นต้น

5.6.5 ติดตั้งระบบเตือนภัยสาหรับระบบที่มีความสำคัญสูง

6. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชันและสารสนเทศ (Application and information access control)

6.1 ต้องจัดให้มีการควบคุมการใช้งานสารสนเทศในระบบสารสนเทศ ได้แก่ กำหนดสิทธิ์ในการใช้งาน เช่น เขียน อ่าน ลบได้ เป็นต้น กำหนดกลุ่มของผู้ใช้ที่สามารถใช้งานได้ ตรวจสอบว่าสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

6.2 ต้องจำแนกระบบสารสนเทศที่มีความสำคัญหรือมีความเสี่ยงสูงไว้อีกบริเวณหนึ่ง เช่น การแบ่งระหว่างระบบที่เชื่อมต่ออินเทอร์เน็ตกับระบบอินทราเน็ต เป็นต้น

6.3 ต้องมีวิธีการพิสูจน์ตัวตนสาหรับผู้ใช้งาน ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศของคณะวิทยาการสารสนเทศ

6.4 ผู้ดูแลระบบสารสนเทศ ต้องตัดเวลาการใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานระบบสารสนเทศไม่ได้มีการใช้งานเป็นระยะเวลาเกิน 30 นาที หรือตามความเหมาะสม

7. ความมั่นคงปลอดภัยการใช้ระบบสารสนเทศและเครือข่าย

7.1 ผู้ดูแลระบบควรกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้นเช่น Proxy, Firewall, IPS-IDS เป็นต้น และห้ามผู้ใช้เชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและขออนุญาตจากคณะวิทยาการสารสนเทศ เป็นลายลักษณ์อักษร

7.2 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web browser) ต้องติดตั้งโปรแกรมป้องกันไวรัสและอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราเซอร์

7.3 ผู้ใช้ต้องปรับปรุง Patch และ HotFix อย่างสม่ำเสมอ โดยสามารถดาวน์โหลด Patch และ HotFix ต่างๆ จากเว็บไซต์เจ้าของผลิตภัณฑ์เพื่อแก้ปัญหาช่องโหว่ เป็นต้น

7.4 ในการรับส่งข้อมูลคอมพิวเตอร์ผ่านทางอินเทอร์เน็ตจะต้องทดสอบไวรัส (Virus Scanning) โดยโปรแกรมป้องกันไวรัสก่อนการรับส่งข้อมูลทุกครั้ง

7.5 ผู้ใช้ต้องไม่ใช้เครือข่ายของคณะวิทยาการสารสนเทศเพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัวและเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บการพนัน เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมเป็นต้น

7.6 ผู้ใช้จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่าย และความปลอดภัยทางข้อมูลของคณะวิทยาการสารสนเทศ

7.7 ผู้ใช้ต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวหรือข้อมูลที่ไม่เหมาะสมทางศีลธรรมหรือข้อมูลที่ละเมิดสิทธิ์ของผู้อื่นหรือข้อมูลที่อาจก่อความเสียหายให้กับคณะวิทยาการสารสนเทศ

7.8 ห้ามผู้ใช้เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของคณะวิทยาการสารสนเทศที่ยังไม่ได้ประกาศอย่างเป็นทางการ ผ่านอินเทอร์เน็ต

7.9 ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อ แก้ไขหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ที่จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

7.10 หลังจากใช้งานอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

8. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management)

8.1 ผู้ดูแลระบบต้องลงทะเบียนผู้ใช้งานใหม่เข้าเป็นสมาชิกของคณะวิทยาการสารสนเทศ เพื่อให้สามารถใช้งานระบบสารสนเทศ หรือโครงสร้างสนับสนุนระบบสารสนเทศอื่น ๆ ทั้งหมดได้ นอกจากนี้ต้องมีระเบียบปฏิบัติเพื่อยกเลิกการใช้งานของผู้ใช้งานทันที ในกรณีที่มีการลาออกจากงาน

8.2 ผู้ดูแลระบบต้องบริหารจัดการรหัสผ่านของผู้ใช้งานให้มีความมั่นคงปลอดภัย

8.3 กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ 8 ตัวอักษร (โดยผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวพิมพ์ใหญ่ ตัวเลข และสัญลักษณ์เข้าด้วยกัน แต่ไม่ควรกำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว หรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม ไม่ใช้รหัสผ่านส่วนบุคคลสาหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์)

8.4 ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ สาหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้ครอบครองอยู่ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

8.5 ผู้ดูแลระบบ ต้องกำหนดสิทธิ์ของผู้ใช้ในการเข้าถึงระบบสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบด้วย

8.6 ผู้ดูแลระบบต้องทบทวนสิทธิ์ในการเข้าถึงระบบสารสนเทศตามระยะเวลาที่กำหนดไว้ อย่างน้อย 1 ครั้งในรอบ 6 เดือน

9. หน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities)

9.1 ผู้ดูแลระบบต้องกำหนดวิธีปฏิบัติที่ดีในการเลือกใช้งานรหัสผ่าน การยกเลิก และการเปลี่ยนแปลงรหัสผ่าน

9.1.1 ผู้ดูแลระบบทำหน้าที่เฝ้าระวังการใช้งานผิดวัตถุประสงค์

9.1.2 ผู้ดูแลระบบมีหน้าที่รายงานเหตุการณ์ผิดปกติให้กับผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

9.1.3 ผู้ใช้งานต้องปฏิบัติตามคำแนะนำเมื่อผู้ดูแลระบบแจ้งให้เปลี่ยนรหัสผ่าน

9.1.4 ผู้ดูแลระบบจะมีรหัสผ่านสองชุดเพื่อจัดการระบบ ชุดแรกเป็นรหัสผ่านที่ใช้ปกติ ชุดที่สองเป็นรหัสผ่านสำรองสำหรับการใช้งานในกรณีฉุกเฉิน

9.1.5 ผู้ใช้งานต้องเขียนรหัสผ่านไว้ในรูปของเอกสารลับและส่งมอบให้ผู้ดูแลระบบเก็บรักษาไว้ หากมีการเปลี่ยนแปลงรหัสผ่านจะต้องแจ้งให้ผู้ดูแลระบบทราบทันที

9.1.6 เลือกรหัสผ่านที่ปลอดภัยและรักษารหัสนั้นให้เป็นความลับอยู่ตลอดเวลา การเปลี่ยนแปลงรหัสบัญชีควรเปลี่ยนทุก 6 เดือน

9.1.7 ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ

9.1.8 ไม่ปลอมแปลงชื่อภายใต้ระบบบัญชี หรือสร้างความเข้าใจให้ดูว่าเป็นบุคคลอื่น

9.1.9 ไม่ลักลอบใช้รหัสผ่าน หรือแกะรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

9.1.10 รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

9.2 การป้องกันอุปกรณ์ที่ไม่มีผู้ดูแล ผู้ใช้งานต้องมีวิธีการเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์เข้าถึงอุปกรณ์สำนักงานที่ไม่มีผู้ใช้ดูแล

9.2.1 ผู้ดูแลระบบมีอำนาจที่จะยุติหรือเพิกถอนสิทธิ์การใช้คอมพิวเตอร์และเครือข่ายโดยทันที หากตรวจพบผู้ใช้ที่ฝ่าฝืนระเบียบหรือกระทำการใดที่อาจสร้างความเสียหายให้กับระบบ

9.2.2 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องควรติดตั้งระบบ screen saver โดยกำหนดรหัสในการเข้าใช้

9.2.3 การรักษาความลับของข้อมูลในเครื่องคอมพิวเตอร์จะเป็นความรับผิดชอบของผู้ใช้งานประจำเครื่องคอมพิวเตอร์นั้น

9.3 การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ใน

ภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

9.3.1 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสาหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

9.3.2 ผู้ใช้งานควรล็อคอุปกรณ์ที่สำคัญเมื่อไม่ได้ใช้งานหรือปล่อยทิ้งไว้โดยไม่ได้ดูแลชั่วคราว

9.3.3 ผู้ใช้งานต้องมีวิธีการป้องกันข้อมูลและทรัพย์สินด้านสารสนเทศที่อยู่ในเครื่องคอมพิวเตอร์ประเภทพกพา, smart mobile device เช่น เมื่อปฏิบัติงานอยู่นอกสถานที่

9.3.3.1 ต้องใส่รหัสผ่านป้องกันหน้าจอทุกเครื่อง

9.3.3.2 ต้องใช้กุญแจล็อคเครื่องคอมพิวเตอร์พกพา

9.3.3.3 ต้องเข้ารหัสข้อมูลที่สำคัญไว้เป็นต้น

10. ข้อกำหนดการใช้งานเครือข่าย

10.1 สิทธิ์การใช้เครือข่าย

10.1.1 เครื่องคอมพิวเตอร์ส่วนบุคคลทุกเครื่องต้องมีรหัสผ่านประจำเครื่องสาหรับผู้ใช้งานและรหัสผ่านของผู้ดูแลระบบ

10.1.2 สิทธิ์การใช้เครือข่ายเป็นสิทธิพิเศษเฉพาะ (Privilege) ที่คณะวิทยาการสารสนเทศ มอบให้บุคคลหรือหน่วยงานที่ได้รับสิทธิ์ไม่สามารถโอนสิทธิ์ให้แก่บุคคลอื่นหรือหน่วยงานอื่นได้

10.1.3 ผู้ใช้ต้องเคารพในสิทธิส่วนบุคคลและไม่ละเมิดความเป็นส่วนตัวของผู้ใช้รายอื่น

10.1.4 ผู้ใช้ต้องใช้ระบบเครือข่ายคอมพิวเตอร์ตามมารยาทและจรรยาบรรณของการใช้เครือข่ายตามที่คณะวิทยาการสารสนเทศกำหนดและตามวิถีสากล

10.2 การใช้งานที่ไม่อนุญาตให้ปฏิบัติ

10.2.1 การใช้ระบบเครือข่ายคอมพิวเตอร์เพื่อกระทำสิ่งที่ผิดกฎหมาย

10.2.2 การเข้าใช้ระบบเครือข่ายคอมพิวเตอร์ด้วยบัญชีของผู้อื่นทั้งที่ได้รับอนุญาตและไม่ได้รับอนุญาตจากเจ้าของบัญชี

10.2.3 การเข้าถึงข้อมูลของผู้อื่นเพื่อคัดลอก แก้ไข ลบ หรือเพิ่มเติม โดยไม่ได้รับอนุญาต

10.2.4 การเผยแพร่ข้อมูลของผู้ใช้หรือของหน่วยงานโดยไม่ได้รับอนุญาต

10.2.5 การใช้งานที่เป็นสาเหตุให้ระบบคอมพิวเตอร์และระบบเครือข่ายคอมพิวเตอร์เสียหายหรือมีผลต่อประสิทธิภาพการทำงานของระบบ

10.2.6 การพยายามทำลายระบบรักษาความปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

10.2.7 การใช้หรือเผยแพร่ซอฟต์แวร์โดยไม่ได้รับอนุญาตจากเจ้าของลิขสิทธิ์

10.2.8 การลักลอบดักจับข้อมูลในระบบเครือข่ายคอมพิวเตอร์

10.2.9 การปลอมแปลงเป็นบุคคลอื่นเพื่อสร้างความเข้าใจผิดให้แก่ระบบคอมพิวเตอร์และผู้ใช้อื่น

10.2.10 การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อสร้างความเสียหายแก่ระบบคอมพิวเตอร์หรือเครือข่ายอื่น

10.2.11 การเผยแพร่และ/หรือการเข้าถึงสื่อลามกอนาจาร

10.2.12 การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อเปิดให้บริการใด ๆ โดยไม่ได้รับอนุญาต

10.2.13 การใช้ทรัพยากรและระบบเครือข่ายคอมพิวเตอร์เพื่อประกอบธุรกิจ

10.2.14 การนำไอพีแอดเดรสของคณะวิทยาการสารสนเทศไปจดทะเบียนชื่อโดเมนอื่นนอกเหนือจากชื่อโดเมน it.msu.ac.th, msu.ac.th โดยไม่ได้รับอนุญาต นอกเหนือจากมีหนังสือรับรองจากผู้บริหารคณะวิทยาการสารสนเทศ

10.2.15 การใช้ระบบเครือข่ายคอมพิวเตอร์อื่นใดที่ขัดต่อนโยบายและระเบียบของคณะวิทยาการสารสนเทศ

10.3 การฝ่าฝืนระเบียบและการพิจารณาโทษ

10.3.1 คณะวิทยาการสารสนเทศ จะไม่รับผิดชอบต่อผลของการกระทำที่เกิดขึ้นจากผู้ใช้และ/หรือบัญชีผู้ใช้

10.3.2 ผู้ใช้ที่ฝ่าฝืนระเบียบการใช้งานระบบเครือข่ายคอมพิวเตอร์จะถูกพิจารณาระงับและ/หรือยกเลิกบัญชีผู้ใช้

11. การใช้ไอพีแอดเดรสและชื่อโดเมนของระบบเครือข่ายคอมพิวเตอร์

11.1 การจัดสรรไอพีแอดเดรส

11.1.1 ไอพีแอดเดรส 202.28.34.192 - 202.28.34.255 (สำหรับไอพีเวอร์ชัน 4) และ 0:0:0:0:0:ffff:ca1c:22c0 - 0:0:0:0:0:ffff:ca1c:22ff ของระบบเครือข่ายคอมพิวเตอร์เป็นทรัพย์สินของคณะวิทยาการสารสนเทศ

11.1.2 ให้คณะวิทยาการสารสนเทศทำหน้าที่จัดสรรไอพีแอดเดรสให้กับหน่วยงานตามที่ร้องขอเพื่อให้ใช้งานได้อย่างเพียงพอและมีประสิทธิภาพ โดยคณะวิทยาการสารสนเทศสามารถ

ปรับเปลี่ยนไอพีแอดเดรสที่ได้จัดสรรให้กับหน่วยงานจากหมายเลขเดิมเป็นหมายเลขใหม่ได้ตามหลักวิชาการ เพื่อให้สามารถบริหารและจัดการได้อย่างมีประสิทธิภาพ

11.1.3 หมายเลขไอพีที่ได้รับการจัดสรรจะต้องมีการลงทะเบียนไว้กับผู้ดูแลระบบ หากมีการเปลี่ยนแปลงแก้ไขไอพีด้วยเหตุผลใดๆ ก็ตาม ต้องแจ้งต่อผู้ดูแลระบบเสมอ

11.1.4 หน่วยงานใดๆ ที่ต้องการขอรับหมายเลขไอพีเพื่อใช้งาน ต้องทำบันทึกข้อความชี้แจงถึงเหตุผลในการขอใช้งาน โดยต้องแสดงหลักฐานการเซ็นต์รับรองจากผู้บริหารต้นสังกัด (หัวหน้าภาควิชา) มายังผู้บริหารระบบเครือข่าย

11.1.5 ในกรณีที่ผู้ใช้งาน นำไอพีไปใช้งานที่ผิดวัตถุประสงค์ หรือมีความเสี่ยงที่จะเป็นอันตรายต่อความมั่นคงของระบบเครือข่าย ผู้ดูแลระบบสามารถยุติหรือยกเลิกไอพีดังกล่าวได้ทันที

11.1.6 เพื่อให้การใช้งานไอพีเป็นไปด้วยความยุติธรรมและเพียงพอต่อการใช้งานภายในคณะวิทยาการสารสนเทศ หมายเลขไอพีจะถูกจัดสรร (Assignment) ให้ 1 ไอพี ต่อ 1 หน่วยงาน/ภารกิจ ยกเว้นมีหนังสือรับรองจากผู้บริหารคณะวิทยาการสารสนเทศเพิ่มเติม

11.1.7 หมายเลขไอพีที่ถูกจัดสรรไปแล้ว ภายหลังทราบว่าไม่มีการใช้งานใดๆ ผู้ดูแลระบบสามารถขอคืนไอพีดังกล่าว มาเป็นไอพีส่วนกลางได้ทันที

11.2 การจัดการชื่อโดเมน

11.2.1 คณะวิทยาการสารสนเทศ ได้ขึ้นทะเบียนชื่อโดเมนของมหาวิทยาลัยมหาสารคามภายใต้ชื่อ “it.msu.ac.th” โดยสำนักคอมพิวเตอร์รับภาระชาระค่าธรรมเนียมการขึ้นทะเบียนและค่าบำรุงรักษาชื่อโดเมน

11.2.2 ให้ผู้ดูแลระบบทำหน้าที่จดทะเบียนชื่อโดเมนประจำหน่วยงาน และชื่อเครื่องภายใต้ชื่อโดเมนของคณะวิทยาการสารสนเทศ

11.2.3 หน่วยงานมีสิทธิ์ในการใช้ชื่อโดเมนภายใต้ it.msu.ac.th โดยยื่นเรื่องขออนุมัติต่อผู้บริหารระบบเครือข่าย คำขออนุมัติจะต้องลงนามรับรองโดยคณบดี หรือผู้อานวยการหรือหัวหน้าหน่วยงานเทียบเท่า

11.2.4 โครงการพิเศษหรือโครงการใด ๆ ที่ได้รับอนุมัติจากคณะวิทยาการสารสนเทศสามารถขอจดชื่อโดเมนประจำโครงการได้ โดยหากเป็นโครงการระดับหน่วยงานให้จดทะเบียนภายใต้ชื่อโดเมนย่อยประจำหน่วยงานนั้น หรือในกรณีที่เป็นโครงการระดับมหาวิทยาลัยจะสามารถยื่นขอจดชื่อโดเมนภายใต้ชื่อโดเมนของมหาวิทยามหาสารคามได้โดยตรงกับสำนักคอมพิวเตอร์

11.2.5 กลุ่มกิจกรรมมีสิทธิ์ในการขอใช้ชื่อโดเมนประจำกลุ่มกิจกรรมได้ โดยต้องมีหัวหน้ากลุ่มกิจกรรมและหัวหน้าหน่วยงานระดับภาควิชาหรือเทียบเท่าที่หัวหน้ากลุ่มกิจกรรมนั้นสังกัดอยู่ลงนามเห็นชอบ และยื่นเรื่องขออนุมัติต่อผู้บริหารคณะวิทยาการสารสนเทศ

11.2.6 การใช้ไอพีแอดเดรสของคณะวิทยาการสารสนเทศ เพื่อจดทะเบียนชื่อโดเมนภายนอกโดเมนของคณะวิทยาการสารสนเทศหรือมหาวิทยาลัยมหาสารคาม โดยมิได้รับอนุญาตเป็นสิ่งต้องห้าม ยกเว้นกรณีมีเหตุผลความจำเป็นอย่างยิ่ง ทั้งนี้ให้หัวหน้าหน่วยงานที่ดำรงตาแหน่งคณบดีหรือผู้อานวยการ หรือหัวหน้าหน่วยงานเทียบเท่า ดำเนินการยื่นคำร้องต่อผู้บริหารคณะวิทยาการสารสนเทศ โดยชี้แจงเหตุผลและความจำเป็นที่ต้องขอจดทะเบียนชื่อโดเมนนอกสารระบบ การอนุมัติจดทะเบียนให้อยู่ในดุลยพินิจของผู้บริหารคณะวิทยาการสารสนเทศ

12. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

การใช้บริการด้านไอซีทีจากหน่วยงานภายนอก บางครั้งหน่วยงานภายนอกอาจเข้าถึงระบบสารสนเทศ แก้ไข เปลี่ยนแปลง และประมวลผลระบบงานโดยไม่ได้รับอนุญาต ดังนั้น จึงต้องกำหนดแนวทางในการปฏิบัติงานของหน่วยงานภายนอกเพื่อความมั่นคง ปลอดภัย ของระบบสารสนเทศของคณะวิทยาการสารสนเทศ โดยนโยบายและแนวปฏิบัตินี้ต้องตรวจสอบ และประเมินตามระยะเวลา 1 ครั้งต่อปี

12.1 บุคคลภายนอก ที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของคณะวิทยาการสารสนเทศ จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารคณะวิทยาการสารสนเทศ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

12.2 คณะวิทยาการสารสนเทศ หรือหน่วยงานที่เกี่ยวข้องต้องจัดทำเอกสารแบบฟอร์มสาหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศ ดังนี้

12.2.1 เหตุผลในการขอใช้งาน

12.2.2 ระยะเวลาในการใช้งาน

12.2.3 การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

12.2.4 การตรวจสอบ Mac Address ของอุปกรณ์ที่เชื่อมต่อ

12.2.5 การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

12.3 หน่วยงานภายนอกที่ทำงานให้กับคณะวิทยาการสารสนเทศทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของคณะวิทยาการสารสนเทศ โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิ์ในการเข้าสู่ระบบสารสนเทศ

12.4 เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง 3 ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

12.5 คณะวิทยาการสารสนเทศมีสิทธิ์ในการตรวจสอบตามสัญญาการใช้บริการด้านไอซีทีเพื่อให้มั่นใจว่าสามารถควบคุมการใช้งานอย่างทั่วถึงตามข้อกำหนด

13. การดาเนินการตอบสนองเหตุการณ์มั่นคงปลอดภัยระบบสารสนเทศ

การรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ ก่อให้เกิดความเชื่อมั่นต่อระบบ ส่งผลถึงความเชื่อมั่นต่อองค์กร หากเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย จำเป็นต้องมีการตอบสนองต่อเหตุการณ์อย่างทันท่วงที ดังนั้น จึงต้องมีแนวปฏิบัติเมื่อเกิดเหตุการณ์ที่มีผลต่อความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ

13.1 ระบบไฟร์วอลล์

13.1.1 ดำเนินการตรวจสอบกฎ (Rule) ของระบบป้องกันการบุกรุก อย่างน้อยเดือนละครั้ง

13.1.2 ดำเนินการตรวจสอบบันทึกของไฟล์ล็อก (Log File) และรายงานของไฟล์วอลล์ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

13.1.2.1 กลุ่มข้อมูล (Packet) ที่ไฟล์วอลล์ได้ปิดกั้น

13.1.2.2 ลักษณะของกลุ่มข้อมูลที่ถูกปิดกั้น

13.1.2.3 หมายเลขไอพี ของเครือข่ายใดที่ถูกปิดกั้น

13.1.3 หากตรวจสอบพบการโจมตี หรือเหตุการณ์ละเมิดความมั่นคงปลอดภัยระบบสารสนเทศให้แจ้งผู้บริหารเครือข่ายคอมพิวเตอร์ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย เพื่อตัดสินใจดำเนินการแก้ไขปัญหา

13.1.4 กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

13.2 เครื่องคอมพิวเตอร์แม่ข่าย

13.2.1 ต้องตรวจสอบความปลอดภัยเครื่องคอมพิวเตอร์แม่ข่ายก่อนให้บริการ โดยอย่างน้อยต้องดำเนินการดังต่อไปนี้

13.2.1.1 ติดตั้งไฟล์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ เปิดเฉพาะ port ที่ใช้งาน

13.2.1.2 ปิด Service ที่ไม่ได้ใช้งาน

13.2.1.3 ติดตั้ง NTP เพื่อเทียบเวลาให้ถูกต้อง

13.2.1.4 จำกัดการเข้าถึงจาก root หรือ Administrator โดยตรง

13.2.2 หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแลและกำหนดผู้ดูแลรับผิดชอบหลัก และผู้รับผิดชอบสำรอง

13.2.3 หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบความมั่นคงปลอดภัย ต้องจดบันทึกตรวจสอบ แก้ไข และรายงาน เหตุการณ์ที่เกี่ยวกับความมั่นคงปลอดภัยต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

13.2.4 หน่วยงานที่ให้บริการระบบคอมพิวเตอร์ต้องตรวจสอบ แก้ไข และรายงานช่องโหว่ของเครื่องคอมพิวเตอร์แม่ข่ายต่อ หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

13.2.5 กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ต้องดำเนินการแจ้งไปยังผู้รับผิดชอบหน่วยงาน หรือผู้มีอำนาจที่ได้รับมอบหมาย ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

13.3 ภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ต ประกอบด้วย ไวรัส หนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์

13.3.1 คณะวิทยาการสารสนเทศต้องดำเนินการจัดหาซอฟต์แวร์เพื่อป้องกัน

13.3.2 หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายที่เชื่อมต่ออินเทอร์เน็ต ต้องดำเนินการติดตั้งโปรแกรมป้องกันภัยคุกคามทางอินเทอร์เน็ต และต้องตั้งให้มีการ Update อย่างน้อยสัปดาห์ละครั้ง

13.3.3 ดำเนินการตรวจสอบไฟล์ล็อก (Log File) และรายงานผลการตรวจสอบ สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้

13.3.3.1 การคุกคามทางอินเทอร์เน็ตใดที่มีเป็นจำนวนมากๆ

13.3.3.2 แพ็กเก็ตถูกส่งมาจากที่ใด และถูกส่งไปยังที่ใด

13.3.4 ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่มีภัยคุกคามทางอินเทอร์เน็ต โดยเฉพาะที่ตรวจพบว่ามีการกระจายภายในเครือข่ายคณะวิทยาการสารสนเทศ

13.3.5 กรณีที่ตรวจพบเหตุละเมิดความมั่นคงปลอดภัยที่มีผลกระทบค่อนข้างรุนแรง ที่อาจส่งผลต่อเครือข่ายโดยรวม ให้ระงับการเชื่อมต่อเครือข่าย และให้แก้ไขเครื่องนั้นทันที

ระดับความรุนแรงของเหตุการณ์

ระดับ	ความหมาย	คำอธิบายเพิ่มเติม
0	ไม่มีผลกระทบ	ไม่มีผลกระทบใด ๆ ต่อการดำเนินภารกิจ
1	กระทบเล็กน้อย	มีผลกระทบในระดับที่ยังไม่มีนัยสำคัญต่อการดำเนินงานขององค์กร
2	กระทบค่อนข้างน้อย	มีผลกระทบในระดับที่มีนัยสำคัญเล็กน้อย
3	กระทบค่อนข้างรุนแรง	มีผลกระทบอย่างมีนัยสำคัญต่อการดำเนินภารกิจ
4	กระทบรุนแรง	มีผลกระทบรุนแรงต่อความสามารถในการดำเนินงานต่อไปได้
5	ปิดให้บริการ	มีผลกระทบรุนแรงต่อการดำรงอยู่ขององค์กร

หมวดที่ 3

นโยบายการสำรองและกู้คืนสารสนเทศ

วัตถุประสงค์

1. เพื่อรักษาความถูกต้องสมบูรณ์และความพร้อมใช้ของสารสนเทศและระบบคอมพิวเตอร์
2. เพื่อให้มีการสำรองข้อมูลที่สำคัญ
3. เพื่อให้การสำรองข้อมูลและกู้คืนข้อมูลเป็นมาตรฐาน
4. เพื่อป้องกันและขจัดปัญหาข้อมูลสำคัญสูญหาย

ผู้รับผิดชอบ

1. ฝ่ายบริหารจัดการระบบเครือข่าย คณะวิทยาการสารสนเทศ
2. หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ข่าย
3. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติการสำรองข้อมูล

1. หน่วยงานที่มีเครื่องคอมพิวเตอร์แม่ข่ายให้บริการต้องดำเนินการสำรองข้อมูล ดังนี้
   1.1. ผู้ดูแลระบบต้องสำรวจเครื่องคอมพิวเตอร์ที่อยู่ในความดูแล และจัดระดับความสำคัญของข้อมูล
   1.2. ผู้ดูแลระบบต้องจัดให้มีระบบการสำรองข้อมูล
   1.3. ผู้ดูแลระบบต้องจัดทำผังหรือขั้นตอนการสำรองข้อมูล
   1.4. ผู้ดูแลระบบต้องทดสอบข้อมูลที่สำรองไว้อย่างสม่ำเสมอ
   1.5. ผู้ดูแลระบบต้องจัดทำบันทึกการสำรองข้อมูล และตรวจสอบว่าการสำรองข้อมูลสำเร็จหรือไม่ แก้ไข และรายงานต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย
   1.6. ผู้ดูแลระบบต้องจัดให้มีการเข้ารหัสข้อมูลที่มีระดับความสำคัญสูง (Encrypted backup) โดยการใช้เทคโนโลยีการเข้ารหัสที่เหมาะสม เพื่อป้องกันมิให้ข้อมูลสำรองเหล่านั้นถูกเปิดเผย

1.7. ผู้ดูแลระบบต้องดาเนินการแก้ไขปัญหาและสรุปผลการแก้ไขปัญหาและรายงานต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย ในกรณีที่พบปัญหาในการสำรองข้อมูลจนเป็นเหตุไม่สามารถดำเนินการอย่างสมบูรณ์ได้

1.8. ผู้ดูแลระบบเป็นผู้กำหนดชนิดและช่วงเวลาการสำรองข้อมูลตามความเหมาะสม พร้อมทั้งกำหนดสื่อที่ใช้เก็บข้อมูล โดยรูปแบบการสำรองข้อมูลมีสองชนิด คือ การสำรองข้อมูลแบบเต็ม (Full Backup) และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

1.9. ผู้ดูแลระบบทดสอบข้อมูลที่สำรองไว้อย่างน้อยปีละ 1 ครั้ง

1.10. ผู้ดูแลระบบสำรวจข้อมูล และ จัดระดับความสำคัญ กำหนดข้อมูลที่ต้องการสำรอง และความถี่ในการสำรองข้อมูล ดังนี้

ที่	รายการ	ระดับความสำคัญ	ข้อมูลที่ต้องสำรอง	ความถี่ในการสำรอง	ระยะเวลาในการสำรอง	ระยะเวลาในการกู้คืน
1	Web server	4	1. Configuration 2. ข้อมูลที่เผยแพร่บนเว็บ	1. ก่อนและหลังการปรับแต่ง 2. การสำรองข้อมูลแบบเต็ม 1 ครั้งต่อเดือน และนำสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	1. 1 เดือน 2. 1 เดือน	1. 4 ชม 2. 4 ชม
2	Database servers	4	1. Configuration 2. ข้อมูลในระบบฐานข้อมูล	1. ก่อนและหลังการปรับแต่ง 2. การสำรองข้อมูลแบบเต็ม ทุกวัน และนาสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	1. 1 เดือน 2. 1 เดือน	1. 4 ชม 2. 4 ชม
3	Servers อื่นๆ	N/A	1. Configuration 2. ข้อมูลในระบบที่สำคัญ	1. ก่อนและหลังการปรับแต่ง 2. การสำรองข้อมูลแบบเต็ม ทุกวัน และนาสื่อบันทึกข้อมูลนั้นไปไว้นอกสถานที่	1. 1 เดือน 2. 1 เดือน	1. 4 ชม 2. 4 ชม

2. แนวปฏิบัติการกู้คืนข้อมูล

2.1. ในกรณีที่พบปัญหาที่อาจสร้างความเสียหายต่อระบบคอมพิวเตอร์และ/หรือระบบเครือข่ายจนเป็นเหตุทำให้ต้องดำเนินการกู้คืนระบบ ให้ผู้ดูแลระบบคอมพิวเตอร์และ/หรือระบบเครือข่าย ดำเนินการแก้ไขรายงานผลการแก้ไขพร้อมทั้งบันทึกและรายงานสรุปผลการปฏิบัติงาน ต่อผู้บังคับบัญชา หรือ ผู้มีอำนาจตามที่ได้รับมอบหมาย

2.2. ให้ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

2.3. หากความเสียหายที่เกิดขึ้นกับระบบคอมพิวเตอร์ หรือระบบเครือข่ายกระทบต่อการให้บริการ หรือการใช้งานของผู้ใช้ระบบ ให้แจ้งผู้ใช้งานทราบทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

2.4. แผนการกู้คืน

สาเหตุ	วิธีการ
1. เกิดความเสียหายขึ้นกับโปรแกรมต้นฉบับ (Source code)	ดำเนินการติดตั้งโปรแกรมต้นฉบับ (Source code) ที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด
2. เกิดความเสียหายขึ้นกับฐานข้อมูล (Database)	ดำเนินการกู้คืนฐานข้อมูลที่เก็บไว้ล่าสุด เพื่อให้ใช้งานได้ต่อเนื่องโดยที่ข้อมูลสูญหายน้อยที่สุด
3. เกิดความเสียหายขึ้นกับระบบปฏิบัติการ (OS) โดยที่ฮาร์ดแวร์ยังคงทำงานปกติ	ดำเนินการติดตั้งระบบปฏิบัติการใหม่และติดตั้งระบบงานจากโปรแกรมต้นฉบับที่มีการใช้งานอยู่ ณ ปัจจุบัน หรือล่าสุด รวมถึงกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด
4. เกิดความเสียหายขึ้นกับฮาร์ดแวร์	ให้บริษัทผู้ดูแลแก้ไขเบื้องต้นให้ฮาร์ดแวร์สามารถทำงานได้ตามปกติ และหากเกิดความเสียหายกับระบบปฏิบัติการและระบบงาน ให้บริษัทหรือผู้ได้รับมอบหมายดำเนินการติดตั้งระบบปฏิบัติการและระบบงานนั้นใหม่ โดยใช้โปรแกรมต้นฉบับ ที่มีการใช้งานอยู่ ณ ปัจจุบันหรือล่าสุด และกู้คืนข้อมูลจากฐานข้อมูลที่เก็บไว้ล่าสุด

หมวดที่ 4

นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

1. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ
2. เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันเหตุการณ์ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

1. ฝ่ายบริหารจัดการระบบเครือข่าย คณะวิทยาการสารสนเทศ
2. หน่วยงานที่ให้บริการเครื่องคอมพิวเตอร์แม่ขาย
3. สำนักตรวจสอบภายใน
4. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการตรวจสอบและประเมินความเสี่ยงนั้น ดังต่อไปนี้
   1.1. ความเสี่ยงที่เกิดจากการลักลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต (Internet)
   1.2. ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต
   1.3. ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน
   1.4. ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่าน (Password) ของผู้อื่นโดยไม่ได้รับอนุญาต
2. การตรวจสอบและประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้
   2.1. ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ
   2.2. ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น
   2.3. จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ
3. ดำเนินการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ ปีละ 1 ครั้ง

4. ตรวจสอบและประเมินความเสี่ยงที่ดำเนินการโดยผู้ตรวจสอบภายในของสำนักตรวจสอบภายใน หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor)
5. กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น
6. มาตรการในการตรวจประเมินระบบสารสนเทศ อย่างน้อย ดังนี้
   6.1. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
   6.2. ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น สำหรับให้ผู้ตรวจสอบใช้งาน และควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้แหล่งจัดเก็บข้อมูลอื่นที่มีข้อกำหนดการเข้าถึงข้อมูล
   6.3. กำหนดให้ระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
   6.4. กำหนดให้เฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้ง บันทึกข้อมูลล็อก แสดงการเข้าถึงนั้นซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
   6.5. ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาตโดยมีการป้องกันเป็นอย่างดี
7. ในกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ผู้บริหารระดับสูง ซึ่งประกอบด้วย คณบดี รองคณบดีฝ่ายเทคโนโลยีสารสนเทศ ฝ่ายบริหารจัดการระบบเครือข่าย ซึ่งมีหน้าที่กำกับดูแลด้านสารสนเทศของคณะวิทยการสารสนเทศ เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงในกรณีที่มีการร้องเรียน และฟ้องร้องภายใต้กฎหมายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ 2560
8. ต้องสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันที่เหมาะสม
9. รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศปีละ 1 ครั้ง เสนอต่อคณะกรรมการยุทธศาสตร์เทคโนโลยีสารสนเทศ และแจ้งคณะกรรมการบริหารความเสี่ยงของมหาวิทยาลัยเพื่อดำเนินการต่อไป

10. แสดงผลการตรวจสอบตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศผ่านเว็บไซต์ ให้ประชาคมของคณะวิทยาการสารสนเทศทราบ ตามนโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

หมวดที่ 5

นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและเครือข่ายคอมพิวเตอร์

วัตถุประสงค์

1. เพื่อให้บุคลากรในสังกัดคณะวิทยาการสารสนเทศ ตลอดจนบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึงสารสนเทศ ตระหนักและเข้าใจถึงความรับผิดชอบถึงการใช้งานนั้นอย่างถูกต้องตามหลักจริยธรรมและหลักกฎหมาย
2. สร้างความมั่นใจว่าการใช้และการรักษาความมั่นคงปลอดภัยสารสนเทศภายในคณะวิทยาการสารสนเทศเป็นไปอย่างถูกต้องตามกฎหมายและข้อบังคับที่เกี่ยวข้อง
3. เพื่อป้องกันการใช้งานระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ผิดวัตถุประสงค์

ผู้รับผิดชอบ

1. ฝ่ายบริหารจัดการระบบเครือข่าย คณะวิทยาการสารสนเทศ
2. ผู้ดูแลระบบที่ได้รับมอบหมาย

แนวปฏิบัติ

1. จัดสัมมนาเพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับผู้ใช้งาน โดยจัดสัมมนาอย่างน้อยปีละ 1 ครั้ง
2. ติดประกาศประชาสัมพันธ์ ให้ความรู้เกี่ยวกับแนวปฏิบัติ หรือเผยแพร่เกร็ดความรู้ในการใช้งานอย่างสม่ำเสมอ
3. จัดทำคู่มือการใช้งานสารสนเทศ และเผยแพร่ทางเว็บไซต์ของคณะวิทยาการสารสนเทศ