ประกาศมหาวิทยาลัยสวนดุสิต
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของมหาวิทยาลัยสวนดุสิต
พ.ศ.๒๕๖๐

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐเพื่อให้การดำเนินการต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙

เพื่อให้การปฏิบัติงานและการบริหารงานมีความมั่นคงปลอดภัยเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล มหาวิทยาลัยสวนดุสิตจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยสวนดุสิต เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบสารสนเทศ ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศของมหาวิทยาลัย โดยความเห็นชอบของคณะอนุกรรมการธุรกรรมอิเล็กทรอนิกส์ จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศมหาวิทยาลัยสวนดุสิตเรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยสวนดุสิต พ.ศ.๒๕๖๐”

ข้อ ๒ ประกาศนี้ ให้ใช้บังคับเมื่อพ้นกำหนดเก้าสิบวัน นับแต่วันประกาศใช้ประกาศฉบับนี้ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“มหาวิทยาลัย” หมายถึง มหาวิทยาลัยสวนดุสิต

“หน่วยงาน” หมายถึง คณะ วิทยาเขต สำนัก สถาบัน ศูนย์การศึกษานอกที่ตั้ง ศูนย์การเรียน และส่วนงาน ที่เป็นหน่วยงานภายในมหาวิทยาลัยสวนดุสิต

“ผู้ใช้งาน” หมายถึง บุคลากร นักศึกษา ลูกจ้าง ผู้ดูแลระบบหรือผู้ที่มหาวิทยาลัยอนุญาตให้ใช้สินทรัพย์ของมหาวิทยาลัย

“สิทธิของผู้ใช้งาน” หมายถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใด ที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยสวนดุสิตหรือ เพื่อการเข้าถึงเข้าใช้สารสนเทศและทรัพย์สินสารสนเทศของมหาวิทยาลัยสวนดุสิต

“สินทรัพย์” หมายถึง เครื่องคอมพิวเตอร์ของมหาวิทยาลัย เครือข่ายย่อย และระบบสารสนเทศต่าง ๆ ที่มหาวิทยาลัยพัฒนาขึ้นหรือจัดหาเพื่อใช้ในการดำเนินการของมหาวิทยาลัย

“เครื่องคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่งซึ่งทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ห้องคอมพิวเตอร์แม่ข่าย” หมายถึง สถานที่ติดตั้งอุปกรณ์แม่ข่ายหรืออุปกรณ์เครือข่ายของมหาวิทยาลัยภายในมหาวิทยาลัย

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การเข้าถึงระบบสารสนเทศที่ได้รับการอนุญาต จากการกำหนดสิทธิหรือได้รับมอบอำนาจในการเข้าถึงระบบ ในการอ่าน สร้าง สำเนา และแก้ไขสารสนเทศ ทั้งโดยการเข้าถึงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการทางกายภาพ

“ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง ความมั่นคงและความปลอดภัยในบริบทของการรักษาความลับ ความเชื่อถือได้ และความพร้อมใช้งานของระบบสารสนเทศมหาวิทยาลัยสวนดุสิต โดยมีเป้าหมายเพื่อปกป้องสินทรัพย์ของมหาวิทยาลัยจากเหตุการณ์หรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์ ซึ่งอาจทำให้เกิดความเสียหายต่อสินทรัพย์ของมหาวิทยาลัย

“เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพใช้งานการให้บริการเครือข่ายสารสนเทศของมหาวิทยาลัยสวนดุสิตที่แสดงให้เห็นความเป็นไปได้ ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

“เครือข่ายสารสนเทศมหาวิทยาลัยสวนดุสิต” หมายถึง ระบบเครือข่ายเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยฯ โดยมีวัตถุประสงค์การเข้าใช้งานเพื่อการบริหารงาน การบริการวิชาการ การศึกษาและงานวิจัยที่เป็นพันธกิจของมหาวิทยาลัย

“ผู้ดูแลเครือข่ายสารสนเทศมหาวิทยาลัยสวนดุสิต” หมายถึง บุคลากรที่ได้รับมอบหมายจากมหาวิทยาลัยเพื่อปฏิบัติงานให้ดูแลบริหารจัดการระบบเครือข่ายสารสนเทศมหาวิทยาลัยสวนดุสิตให้พร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ปฏิบัติงานระบบสารสนเทศ” หมายถึง บุคลากรที่ได้รับมอบหมายจากหน่วยงาน เพื่อทำการป้อนข้อมูล และแก้ไขข้อมูลของระบบสารสนเทศของมหาวิทยาลัย

“เครือข่ายย่อย” หมายถึง อุปกรณ์ต่อพ่วงรวมถึงอุปกรณ์เครือข่ายที่เชื่อมโยงเครื่องคอมพิวเตอร์ภายในเครือข่ายสารสนเทศมหาวิทยาลัยสวนดุสิตตลอดจนถึงโปรแกรมและข้อมูล

“ผู้ดูแลระบบเครือข่ายย่อย” หมายถึง บุคลากรหรือลูกจ้างได้รับมอบหมายจากหัวหน้าหน่วยงานเพื่อปฏิบัติงานให้ระบบเครือข่ายของหน่วยงานพร้อมสำหรับการใช้งานของมหาวิทยาลัย

“ผู้ใช้บริการเครือข่าย” หมายถึง บุคคล หน่วยงานที่ต่อเชื่อมและรับบริการจากเครือข่ายสารสนเทศมหาวิทยาลัย

“ผู้บริหารระดับสูงสุด” หมายถึง อธิการบดีมหาวิทยาลัยสวนดุสิต

“ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง” หมายถึง ผู้ที่ได้รับการแต่งตั้งจากมหาวิทยาลัยสวนดุสิต ให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร” หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัยสวนดุสิตเพื่อทำหน้าที่ในการกำหนด ตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้ง ตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

“ผู้ตรวจสอบภายใน” หมายถึง บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัย เพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“ผู้ตรวจสอบจากภายนอก” หมายถึง เป็นบุคคลภายนอกที่มีความรู้ ความสามารถทางด้าน เทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

“บทลงโทษ” หมายถึง บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

“ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษา ความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

“บัญชีรายชื่อ (Account Internet)” หมายถึง รายการชื่อผู้ใช้และรหัสผ่านเพื่อนำไปใช้ในการ พิสูจน์ยืนยันตัวตนเพื่อเข้าใช้งานระบบสารสนเทศนั้นๆ

“การพิสูจน์ยืนยันตัวตน (Authentication)” หมายถึง ขั้นตอนการรักษาความปลอดภัยในการ เข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดย ใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password

“การยืนยันตัวบุคคล (Identification)” หมายถึง ข้อมูลที่สามารถใช้ระบุตัวตน ติดต่อหรือค้นหา บุคคลหนึ่งบุคคลใดโดยเฉพาะ หรือเป็นข้อมูลที่ใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวบุคคลหนึ่งบุคคลนั้น โดยบุคคล นั้นต้องได้รับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบ สารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

“การเข้ารหัสลับ (Encryption)” หมายถึง การนำข้อมูลเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามา ใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ ตามปกติ

“การถอดรหัส (Decryption)” หมายถึง วิธีการที่ทำการเปลี่ยนแปลงข้อมูลที่ได้จากการเข้ารหัส ข้อมูล เป็นข้อมูลก่อนที่จะถูกทำการเข้ารหัส

“การเข้าสู่ระบบจากระยะไกล (Remote Access)” หมายถึง การเข้าถึงคอมพิวเตอร์หรือ เครือข่ายจากระบบเครือข่ายอื่นระยะทางไกลผ่านระบบอินเทอร์เน็ต

“VPN (Virtual Private Network)” หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการ รับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถ อ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

ผู้ดูแลระบบ หรือ แอดมิน (System administrator)” หมายถึง ผู้ทำหน้าที่บริหารและจัดการ ระบบคอมพิวเตอร์ในองค์กร โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้ง และการปรับปรุงซอฟต์แวร์ สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้

“ตัวแทนผู้ดูแลระบบ (Delegate Administrator)” หมายถึง ตัวแทนผู้ดูแล ที่จะได้สิทธ์เฉพาะ ในการบริหารจัดการระบบสารสนเทศนั้น ซึ่งสิทธิ์ที่ได้จะไม่เทียบเท่า ผู้ดูแลระบบหลัก

“สื่อบันทึกข้อมูล” หมายถึง สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล เช่น CD , DVD, flash drive, external hard disk ฯลฯ

“อุปกรณ์จัดเส้นทาง (Router)” หมายถึง อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

“จดหมายอิเล็กทรอนิกส์ (E-mail)”หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว

“บัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail Address)” หมายถึง หมายเลขประจำตัวหรือรหัสประจำตัวที่กำหนดให้แก่สมาชิก ผู้ใช้หมายเลขนั้นๆ จะใช้สำหรับส่งจดหมายหรือเรียกดูข้อความที่ส่งมาทางจดหมายอิเล็กทรอนิกส์

“Web Browser” หมายถึง ซอฟต์แวร์หรือโปรแกรมคอมพิวเตอร์ที่ใช้ในการเข้าถึงข้อมูลและติดต่อสื่อสารกับระบบสารสนเทศที่อยู่ในรูปแบบของเว็บเพจ ซึ่งอยู่บนเครือข่ายคอมพิวเตอร์ที่ชื่อว่า World Wide Web (WWW) โปรแกรมที่ใช้สำหรับท่องอินเทอร์เน็ต ในการเปิด web page ได้แก่ Internet Explorer , Chrome , Firefox เป็นต้น

“เครือข่ายสังคมออนไลน์ (social network) ”หมายถึง การที่ผู้ใช้งานอินเตอร์เน็ตที่เชื่อมโยงกับเพื่อน รวมไปถึงเพื่อนของเพื่อนอีกนับร้อย ผ่านผู้ให้บริการด้านโซเชียลเน็ตเวิร์ค (Social Network) บนอินเตอร์เน็ต เช่น Facebook, Twitter ,Skype , Line การเชื่อมโยงดังกล่าว ทำให้เกิดเครือข่ายขึ้น เช่น เราสามารถรู้จักเพื่อนของเพื่อนเราได้ เป็นทอดๆ ต่อไปเรื่อย ทำให้เกิดสังคมเสมือนจริงขึ้นมา

“ผู้ใช้งานที่อยู่ภายนอกหน่วยงาน” (User Authentication for External Connections) หมายถึง บุคคล หรือหน่วยงานที่เชื่อมต่อและรับบริการจากระบบเครือข่ายอื่นๆ แล้วต้องการเชื่อมต่อระบบเข้ามาสู่ระบบเครือข่ายของมหาวิทยาลัยสวนดุสิตผ่านระบบอินเทอร์เน็ต

“การระบุอุปกรณ์ระบบเครือข่าย (Equipment Identification in Network)” หมายถึง การกำหนดให้อุปกรณ์คอมพิวเตอร์มีหมายเลขประจำเครื่องเพื่อใช้ในการพิสูจน์ตัวตนสำหรับการเชื่อมต่อกับระบบเครือข่าย

“ หมายเลข IP Address” หมายถึง หมายเลขประจำเครื่องคอมพิวเตอร์แต่ละเครื่องในระบบเครือข่ายที่ใช้โปรโตคอล TCP/IP

“แผนผังระบบเครือข่าย (Network Diagram)” หมายถึง แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของมหาวิทยาลัยสวนดุสิต

“พอร์ต (Port) ”หมายถึง ช่องทางสำหรับเข้าออกของข้อมูลใน Protocol TCP/IP โดยกำหนดเป็นเลข ๑๖ bit เริ่มตั้งแต่ ๐ ถึง ๖๕๕๓๕ ซึ่งแต่ละพอร์ตจะถูกกำหนดให้ Service ต่างๆใช้งานโดยมีหน่วยงาน Internet Assigned Numbers Authority (IANA) ทำหน้าที่ประสานการใช้งานในรูปแบบสากล

“การแบ่งแยกเครือข่าย (Segregation in Networks)” หมายถึง การแบ่งกลุ่มของระบบเครือข่ายภายในของมหาวิทยาลัยสวนดุสิตให้เป็นระบบเครือข่ายขนาดเล็กหลายๆระบบ เพื่อประโยชน์ในการบริหารจัดการ

“การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control)” หมายถึง การควบคุมการเชื่อมต่อให้สอดคล้องกับนโยบายและข้อกำหนดการใช้งานของระบบ

“ระบบตรวจจับการบุกรุก IPS (Intrusion Prevention System/ intrusion Detection System)” หมายถึง ระบบที่ใช้สำหรับตรวจจับการบุกรุก หรือการพยายามที่จะบุกรุก เข้าสู่ระบบเครือข่าย

การจัดเส้นทางบนเครือข่าย (Network Routing)” หมายถึง การกำหนดให้ระบบเครือข่ายใช้เส้นทางสำหรับสื่อสารจากต้นทางไปถึงปลายทาง

“ระบบเครือข่ายไร้สาย (Wireless LAN Access Control)” หมายถึง ระบบเครือข่ายที่ใช้คลื่นวิทยุ เพื่อเชื่อมโยงเครื่องคอมพิวเตอร์และอุปกรณ์ต่างๆ ภายในเครือข่ายสารสนเทศมหาวิทยาลัยสวนดุสิต

“อุปกรณ์กระจายสัญญาณ (Access Point)” หมายถึง อุปกรณ์ระบบเครือข่ายไร้สาย ที่เชื่อมต่อระบบเครือข่ายของมหาวิทยาลัยสวนดุสิต และให้บริการระบบเครือข่ายผ่านคลื่นวิทยุ ไปยังผู้ใช้งาน

“SSID (Service Set identifier)” หมายถึง ชื่อของระบบเครือข่ายไร้สายที่มหาวิทยาลัยสวนดุสิตตั้งขึ้น สำหรับรองรับการเชื่อมต่อระบบเครือข่ายจากผู้ใช้งาน

“ระบบอินเทอร์เน็ต (Internet)” หมายถึง ระบบเครือข่ายคอมพิวเตอร์หลายๆระบบที่เชื่อมต่อเข้าด้วยกันเป็นระบบเครือข่ายขนาดใหญ่

“Proxy Server” หมายถึง ระบบที่ทำหน้าที่ให้บริการระบบสารสนเทศต่างๆ ในระบบอินเตอร์เน็ตแทนเครื่องแม่ข่าย เพื่อรักษาความปลอดภัยให้กับเครื่องแม่ข่าย

“Firewall” หมายถึง ระบบที่ใช้สำหรับควบคุมการเข้าออกของข้อมูลที่สื่อสารระหว่างเครือข่ายคอมพิวเตอร์โดยพิจารณากฎ หรือ ตัวกรอง ที่กำหนดไว้

“การกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์” หมายถึง การกำหนดเส้นทางของการเข้าออกข้อมูลในระบบ ให้เป็นไปตามเส้นทางที่กำหนดไว้ให้เท่านั้น

“ช่องโหว่ระบบปฏิบัติการเว็บเบราเซอร์” หมายถึง จุดอ่อนอย่างหนึ่งของระบบเว็บเบราเซอร์ที่ทำให้ผู้โจมตีสามารถใช้จุดอ่อนนี้โจมตีเพื่อลดทอนการทำงานของระบบเว็บเบราเซอร์

“ผู้ดูแลระบบ (System Administrator) หมายถึง บุคลากรที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่ายคอมพิวเตอร์ เพื่อการจัดการฐานข้อมูลของเครือข่ายคอมพิวเตอร์ ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

“การเข้าใช้งานที่มั่นคงปลอดภัย หมายถึง การอนุญาต การกำหนดสิทธิ์ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทาง กายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการ เข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“โปรแกรมอรรถประโยชน์ หมายถึง โปรแกรมที่ติดมาพร้อมกับระบบปฏิบัติการวินโดว์ เรียกง่ายๆว่าเป็นโปรแกรมที่ช่วยดูแลระบบการทำงานของวินโดว์เพราะมีหลากหลายประเภท เช่น ประเภทการจัดไฟล์ ป้องกันไวรัส บีบอัดไฟล์ ฯลฯ

“การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time)” หมายถึง การกำหนดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง

“การควบคุมการเข้าถึงระบบปฏิบัติการ” หมายถึง การอนุญาต การกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

“การป้องกันจากโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ (Malware)” หมายถึง การป้องกันสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงาน ถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

“แนวปฏิบัติการสำรองข้อมูลและการกู้คืน” หมายถึง ขั้นตอนในการปฏิบัติเมื่อเกิดข้อผิดพลาดที่เกิดจากการทำงานของผู้ใช้งาน ความผิดพลาดที่เกิดจากการทำงานผิดพลาดในระบบและความผิดพลาดของฮาร์ดแวร์

“ระบบบริหารจัดการเครื่องคอมพิวเตอร์” หมายถึง ระบบ Desktop Management เป็นเครื่องมือที่จะช่วยแบ่งเบาภาระของเจ้าหน้าที่ IT ในการดูแลแก้ไขปัญหาคอมพิวเตอร์ ให้ทำได้อย่างรวดเร็ว ทำได้พร้อมกันหลายๆ เครื่องและทำได้จากศูนย์กลาง

“ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดย ได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

“ระบบปฏิบัติการ” หมายถึง ซอฟต์แวร์ระบบ (System Software) ที่ทำหน้าที่ควบคุมการทำงานของเครื่องและอุปกรณ์ ควบคุมและสั่งการให้ Hardware สามารถทำงานได้ และทำหน้าที่เป็นสื่อกลางในการเชื่อมการทำงานระหว่างผู้ใช้งานในการใช้โปรแกรมประยุกต์ (Application Software) ของผู้ใช้งานกับระบบเครื่องฯ อำนวยความสะดวกในการใช้งาน และเพิ่มประสิทธิภาพของระบบ

“ระบบสารสนเทศ (Information System)” หมายถึง ระบบที่มีการนำคอมพิวเตอร์มาช่วยในการรวบรวม จัดเก็บ หรือจัดการกับข้อมูลข่าวสารเพื่อให้ข้อมูลนั้นกลายเป็นสารสนเทศที่ดี สามารถนำไปใช้ในการประกอบการตัดสินใจได้ในเวลาอันรวดเร็วและถูกต้อง

“โปรแกรมประยุกต์ หรือ ซอฟต์แวร์แอปพลิเคชั่น” หมายถึง โปรแกรมที่มีความสามารถจัดการกับงานเฉพาะด้าน โดยตัวโปรแกรมจะเหมาะสมและใช้งานได้ดีกับงานเฉพาะนั้นๆ เท่านั้น

“ฟังก์ชั่น” หมายถึง โปรแกรมย่อย (subprogram) ชนิดหนึ่ง ที่มีหน้าที่ คำนวณหาค่า เมื่อได้ค่าแล้ว ต้องส่งค่านั้นกลับไปยัง โปรแกรม หลัก (main program) การส่งค่ามาคำนวณใน โปรแกรม ย่อยนั้นมี 2 แบบคือ แบบแรกเรียกว่า แบบฟังก์ชัน ซึ่งจะส่งค่ากลับไปยัง โปรแกรมหลักได้ทีละค่า (อีกแบบหนึ่งเรียกว่า แบบ procedures ซึ่งจะส่งค่าที่คำนวณ ได้กลับไปโปรแกรมหลักได้ทีละหลายค่า)

“ระบบสารสนเทศ (Information System)” หมายถึง ระบบที่มีการนำข้อมูลดิบไปประมวลผลให้อยู่ในรูปสารสนเทศที่พร้อมใช้งาน

“เทคโนโลยีสารสนเทศ (Information Technology)” หมายถึง เครื่องมือที่ทำให้สามารถพัฒนาข้อมูลต่างๆ ในระบบสารสนเทศให้อยู่ในรูปของ “สารสนเทศ” ที่สามารถนำไปใช้งานได้ทันที

“Outsource” หมายถึงการที่องค์กรมอบหมายงานบางส่วนของตนให้กับบุคคลหรือองค์กรภายนอกมาดำเนินการแทน โดยผู้ว่าจ้างจะเป็นผู้กำหนดและควบคุมกำกับทุกส่วนตั้งแต่นโยบายไปจนถึงการปฏิบัติงานในทุกๆขั้นตอนของผู้รับจ้าง

“รหัสต้นฉบับ (Source code)” หมายถึงแฟ้มข้อมูลที่เป็นตัวต้นฉบับของโปรแกรมใดโปรแกรมหนึ่ง พูดง่าย ๆ ก็คือเป็นโปรแกรมที่เครื่องแปลเป็นภาษาเครื่อง (Machine Language) เรียบร้อยแล้ว

“Log” หมายถึง การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ที่สามารถแสดงถึงแหล่งกำเนิดต้นทาง ปลายทาง เส้นทาง วันที่ เวลา ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์

“Audit Logging” หมายถึง ข้อมูลการเข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายที่สามารถตรวจสอบการเข้าใช้งาน หรือการบุกรุก รวมไปถึงข้อผิดพลาดของระบบปฏิบัติการของเครื่องคอมพิวเตอร์แม่ข่ายได้

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ตามประกาศนี้ มี ๒ ส่วน ดังนี้

(๑) นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๕

(๒) แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุม ตามข้อ ๖ – ๒๒

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

(๑) ส่วนที่ว่าด้วยการจัดทำนโยบาย

๑. ผู้บริหาร บุคลากรทางด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยสวนดุสิต

๒. นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของมหาวิทยาลัยสวนดุสิต

๓. กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

๔. ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

(๒) ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

๑. การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานและประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกและรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

๒. มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่มีระบบสำรองระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

๓. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีนโยบายในมีการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๔. การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

ข้อ ๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

(๔) มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อ ๗ บริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อย ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อย ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานภาพของผู้ใช้งาน

ข้อ ๘ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ อันได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๙ ควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างเครือข่ายให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๐ ควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) มีระบบบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน

(๒) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ต้องระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๑๑ ควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สาหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๑๒ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

(๑) ผู้ใช้งานระบบเครือข่ายไร้สายของหน่วยงาน ต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบเครือข่ายสารสนเทศมหาวิทยาลัย ที่ได้รับมอบหมาย

(๒) มีการกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access point) ให้เหมาะสม

(๓) มีแนวปฏิบัติในการตั้งค่าอุปกรณ์กระจายสัญญาณ (Access point) เพื่อการใช้งานมี ความปลอดภัย

ข้อ ๑๓ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

(๑) มีการกำหนด และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน พื้นที่ควบคุมให้ชัดเจน และประกาศให้รับทราบทั่วกัน

(๒) มีการกำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งาน

(๓) มีระบบควบคุมรักษาความปลอดภัยได้ครอบคลุมระบบงาน รวมถึงวิเคราะห์ความเสี่ยงที่อาจจะเกิดขึ้นในสถานการณ์ปัจจุบันนั้น ๆ อย่างน้อยปีละ 2 ครั้ง และนำเสนอรายงานผู้บริหารมหาวิทยาลัย

(๔) มหาวิทยาลัยมีการควบคุมการเข้าออกอาคารสถานที่

(๕) มีระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องทำงานผิดปกติหรือหยุดการทำงาน

(๖) ในการวางสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) ให้คำนึงถึงความปลอดภัยของระบบ มาตรฐานและเป็นระเบียบ

(๗) การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ให้มีการบำรุงรักษาตามมาตรฐานของอุปกรณ์นั้นๆ และคำนึงถึงความปลอดภัยของข้อมูลเป็นสำคัญ

(๘) การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property) ต้องได้รับอนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของทรัพย์สินนั้นๆ

(๙) มีการกำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ที่ใช้งานภายนอกหน่วยงาน (Security of Equipment off-premises)

(๑๐) มีมาตรการในการทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

(๑๑) มีระบบควบคุมและการรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ รวมถึงการเผยแพร่บนเครือข่ายอินเทอร์เน็ต

ข้อ ๑๔ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

(๑) ควบคุมการติดตั้งซอฟต์แวร์ในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

(๒) ทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

(๓) มีการกำหนดสิทธิ์เข้าถึงเครื่องคอมพิวเตอร์แม่ข่ายของผู้พัฒนาซอฟต์แวร์จากหน่วยงานภายนอก

(๔) มีมาตรการควบคุมและกระบวนการบริหารจัดการช่องโหว่ทางเทคนิคของระบบสารสนเทศ

(๕) บันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ

ข้อ ๑๕ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

(๑) มีการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

(๒) การสำรองข้อมูลและการกู้คืน อยู่ในความรับผิดชอบของผู้ใช้งาน

ข้อ ๑๖ การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

(๑) มีการกำหนดระดับชั้นความลับของข้อมูล วิธีการปฏิบัติ และการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ

(๒) มีการทบทวนสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง

(๔) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เป็นมาตรฐาน

ข้อ ๑๗ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

(๑) กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

(๒) มีการควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ตามสิทธิของผู้ใช้งาน

(๓) ผู้ใช้งานจะต้องรับผิดชอบผลกระทบที่เกิดจากการใช้งานไม่ถูกต้อง

(๔) มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับ เปลี่ยนแปลง หรือยกเลิก การใช้งาน ตามเหตุอันสมควร

ข้อ ๑๘ การใช้งานระบบอินเทอร์เน็ต (Internet)

(๑) กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้

(๒) การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีระบบรักษาความปลอดภัยเพื่อทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ของระบบปฏิบัติการ

(๓) ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ

(๔) การเผยแพร่ข้อมูลผ่านเครือข่ายอินเทอร์เน็ตจะเป็นไปตามแนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet) เท่านั้น

(๕) การกระทำใดๆ บนเครือข่ายอินเทอร์เน็ตที่ไม่ถูกต้องตาม พรบ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบ

ข้อ ๑๙ การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

(๑) ส่งเสริมให้ผู้ใช้งานเครือข่ายสังคมออนไลน์ มีความตระหนักถึงเรื่องความมั่นคงปลอดภัยในการใช้งาน

(๒) ผู้ใช้งานจะต้องรับผิดชอบในการเผยแพร่ข้อมูล หากเกิดความเสียหายที่มีผลกระทบต่อมหาวิทยาลัยและชื่อเสียงของบุคคลอื่นๆ

ข้อ ๒๐ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

(๑) กำหนดให้ระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และจัดเก็บไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

(๒) ข้อมูลจราจรทางคอมพิวเตอร์ (Log) จะต้องจัดเก็บไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน และถูกต้อง

(๓) มีการกำหนดชั้นความลับในการเข้าถึงข้อมูลที่จัดเก็บ และสามารถระบุตัวบุคคลที่เข้าถึงข้อมูลดังกล่าวได้

(๔) มีมาตรการในการป้องกันการแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log)

ข้อ ๒๑ จัดทำระบบสำรองสำหรับระบบสารสนเทศตามแนวทาง ต่อไปนี้

(๑) มหาวิทยาลัยจะต้องจัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูลที่หน่วยงานนั้นรับผิดชอบ เป็นประจำทุกปี

(๒) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

(๓) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๔) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๕) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๖) มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เป็นประจำทุกปี

ข้อ ๒๒ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาอย่างน้อย ดังนี้

(๑) มหาวิทยาลัยจะต้องจัดทำแนวปฏิบัติในการบริหารความเสี่ยงที่หน่วยงานนั้นรับผิดชอบ เป็นประจำทุกปี

(๒) มหาวิทยาลัยจะต้องวิเคราะห์ วางแผนบริหารความเสี่ยง และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

(๓) ต้องมีการกำหนดหน้าที่และผู้รับผิดชอบในการจัดการความเสี่ยง รวมถึงติดตาม ควบคุม และสรุปการดำเนินงานด้านบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อมหาวิทยาลัย โดยหน่วยงานตรวจสอบภายในของมหาวิทยาลัย

(๔) รายงานผลการดำเนินการต่อผู้บริหารของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

(๕) ต้องตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เป็นประจำทุกปี

ข้อ ๒๓ ต้องกำหนดความรับผิดชอบที่ชัดเจน กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ทั้งนี้ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงความเสียหาย หรืออันตรายที่เกิดขึ้น ดังนี้

(๑) ระดับนโยบาย

๑. ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบในการกำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยสวนดุสิต โดยมีหน้าที่กำกับ ดูแล รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้การสนับสนุนและส่งเสริมการดำเนินงานด้านสารสนเทศอย่างมีประสิทธิภาพ

๒. ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ ทำหน้าที่ติดตาม กำกับดูแล ควบคุม ตรวจสอบ และประเมินผลการดำเนินงานผู้รับผิดชอบระดับปฏิบัติงาน กำกับดูแลให้มีการปฏิบัติ และดำเนินการตามประกาศ ฉบับนี้

(๒) ระดับปฏิบัติงาน ได้แก่

๑. ผู้ดูแลรับผิดชอบเครือข่ายของมหาวิทยาลัยสวนดุสิตในตำแหน่ง เจ้าหน้าที่วิเคราะห์ระบบคอมพิวเตอร์รับผิดชอบงานพัฒนาระบบเครือข่ายและสารสนเทศ กำกับดูแลการฏิบัติงานของผู้ปฏิบัติอย่าง

ใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ความเสี่ยงของระบบฐานข้อมูลและสารสนเทศ วางแผนการปฏิบัติงาน ติดตาม การปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

๑.๑ ควบคุมการเข้า - ออก ห้องคอมพิวเตอร์แม่ข่าย (Server) ตามการกำหนดสิทธิการเข้าถึง คอมพิวเตอร์แม่ข่าย (Server)

๑.๒ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยสวนดุสิตให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๑.๓ กำกับดูแล การติดตั้ง รื้อถอน ตรวจสอบการเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Wi-Fi, Internet, Intranet ที่ให้บริการในมหาวิทยาลัยสวนดุสิต

๑.๔ กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของห้องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้

๑.๕ แก้ไขปัญหาที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสารสนเทศ

๑.๖ รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและ ระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาทราบทุกเดือน

๑.๗ กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึง ระบบการทำงานของ Server ตามสิทธิการเข้าถึงระบบ

๑.๘ กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้าระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาต

๑.๙ กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอก (Firewall) และโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ในเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของระบบฐานข้อมูลทั้งหมดที่ให้บริการให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง

๑.๑๐ กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่าต่าง ๆ ของระบบ

๑.๑๑ ประสานการปฏิบัติงานตามแผนป้องกันและแก้ไขปัญหาระบบความมั่นคงปลอดภัยของฐานข้อมูลและสารสนเทศจากสถานการณ์ความไม่แน่นอนและภัยพิบัติ

๑.๑๒ รายงานผลการปฏิบัติงานตามแผนการบริหารความเสี่ยงฯ ให้ผู้บังคับบัญชาทราบ

๑.๑๓ ทำการสำรองข้อมูลและเรียกคืนข้อมูล (Backup and Recovery) ตามรอบระยะเวลาที่กำหนด

๑.๑๔ บริหารจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Management) ระบบสารสนเทศแต่ละระบบของมหาวิทยาลัย เพื่อควบคุมการเข้าถึงระบบสารสนเทศ เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๒. ผู้ดูแลระบบ จากบริษัทที่จัดจ้างให้ดูแลระบบเครือข่ายและคอมพิวเตอร์ รับผิดชอบ ดังนี้

๒.๑ แก้ไขปัญหา อุปสรรค จากสถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบฐานข้อมูลและสารสนเทศที่เกิดจากการถูกเจาะระบบจากบุคคลภายนอก (Hack) และการถูกทำลายจากโปรแกรมไวรัส

๒.๒ กำหนด แก้ไข หรือเปลี่ยนแปลงค่า parameter ต่าง ๆ ของระบบ เครือข่ายและอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับระบบเครือข่าย

๒.๓ รายงานสภาพปัญหา และสถานการณ์ความเสียหายของระบบฐานข้อมูล และสารสนเทศที่ถูกทำลายจากบุคคลภายนอก (Hacker) และจากไวรัส (Virus)

๒.๔ บำรุงรักษาอุปกรณ์ และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดที่ให้บริการในมหาวิทยาลัยสวนดุสิตให้สามารถใช้งานได้ตามปกติตลอด ๒๔ ชั่วโมง (แก้ไขปัญหาขัดข้องของการเชื่อมโยงเครือข่ายในองค์กร)

ประกาศ ณ วันที่ ๒๗ กันยายน พ.ศ. ๒๕๖๐

(รองศาสตราจารย์ ดร.ศิโรจน์ ผลพันธิน)
อธิการบดีมหาวิทยาลัยสวนดุสิต

เอกสารแนบท้ายประกาศ

เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยทางสารสนเทศ

ของมหาวิทยาลัยสวนดุสิต พ.ศ. ๒๕๖๐

สารบัญ

ส่วนที่ ๑

นโยบายควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัยสำหรับการควบคุมการเข้าถึงและการใช้ระบบสารสนเทศของมหาวิทยาลัย

๒. เพื่อให้ผู้ใช้งานได้รับทราบแนวทางและสามารถปฏิบัติตามแนวทางที่กำหนด โดยตระหนักถึงความสำคัญของมาตรการรักษาความมั่นคงปลอดภัยให้ปฏิบัติตามอย่างเคร่งครัด

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. การควบคุมการเข้าถึงและใช้งานสารสนเทศ(Access control)

๑.๑ ควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๑.๒ กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

๑.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๔ มีข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๒.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้ รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๒.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศและปรับปรุงบัญชีผู้ใช้งาน อย่างน้อย ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสถานภาพของผู้ใช้งาน

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

๓.๑ การใช้งานรหัสผ่าน (Password Usage) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานเพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ อันได้แก่ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๓.๔ ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาตอย่างน้อยดังนี้

๔.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

๔.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างเครือข่ายให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๕. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access control)

๕.๑ มีระบบบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของหน่วยงานและกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ให้กับผู้ใช้งาน

๕.๒ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย ต้องระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๕.๓ การบริหารจัดการรหัสผ่าน (Password Management System) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (Interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๕.๔ การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๕.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๕.๖ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection Time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๖. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๖.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกหน่วยงาน

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สาหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

๗. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๗.๑ ผู้ใช้งานระบบเครือข่ายไร้สายของหน่วยงาน ต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับ การพิจารณาอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูงหรือผู้ดูแลระบบเครือข่ายสารสนเทศมหาวิทยาลัย ที่ได้รับมอบหมาย

๗.๒ มีการกำหนดตำแหน่งการวางอุปกรณ์กระจายสัญญาณ (Access point) ให้เหมาะสม

๗.๓ มีแนวปฏิบัติในการตั้งค่าอุปกรณ์กระจายสัญญาณ (Access point) เพื่อการใช้งานมีความปลอดภัย

๘. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๘.๑ มีการกำหนด และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน พื้นที่ควบคุมให้ชัดเจน และ ประกาศให้รับทราบทั่วกัน

๘.๒ มีการกำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งาน

๘.๓ มีระบบควบคุมรักษาความปลอดภัยได้ครอบคลุมระบบงาน รวมถึงวิเคราะห์ความเสี่ยงที่ อาจจะเกิดขึ้นในสถานการณ์ปัจจุบันนั้น ๆ อย่างน้อยปีละ ๒ ครั้ง และนำเสนอรายงานผู้บริหารมหาวิทยาลัย

๘.๔ มหาวิทยาลัยมีการควบคุมการเข้าออกอาคารสถานที่

๘.๕ มีระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องทำงานผิดปกติ หรือหยุดการทำงาน

๘.๖ ในการวางสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่นๆ (Cabling Security) ให้คำนึงถึงความ ปลอดภัยของระบบ มาตรฐานและเป็นระเบียบ

๘.๗ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance) ให้มีการบำรุงรักษาตามมาตรฐานของ อุปกรณ์นั้นๆ และคำนึงถึงความปลอดภัยของข้อมูลเป็นสำคัญ

๘.๘ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property) ต้องได้รับ อนุญาตจากหัวหน้าหน่วยงานที่เป็นเจ้าของทรัพย์สินนั้นๆ

๘.๙ มีการกำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์ที่ใช้งาน ภายนอกหน่วยงาน (Security of Equipment off-premises)

๘.๑๐ มีมาตรการในการทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Re-use of Equipment)

๘.๑๑ มีระบบควบคุมและการรักษาความมั่นคงปลอดภัยสำหรับเอกสารระบบสารสนเทศ รวมถึง การเผยแพร่บนเครือข่ายอินเทอร์เน็ต

๙. การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๙.๑ ควบคุมการติดตั้งซอฟต์แวร์ในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๙.๒ ทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๙.๓ มีการกำหนดสิทธิ์เข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย ของผู้พัฒนาซอฟต์แวร์จากหน่วยงาน ภายนอก

๙.๔ มีมาตรการควบคุมและกระบวนการบริหารจัดการช่องโหว่ทางเทคนิค ของระบบสารสนเทศ

๙.๕ บันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) และบันทึก พฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ

๑๐. การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๑ มีการควบคุมการใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๐.๒ การสำรองข้อมูลและการกู้คืน อยู่ในความรับผิดชอบของผู้ใช้งาน

๑๑. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๑.๑ มีการกำหนดระดับชั้นความลับของข้อมูล วิธีการปฏิบัติ และการควบคุมการเข้าถึงข้อมูลแต่ ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ

๑๑.๒ มีการทบทวนสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน

๑๑.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง

๑๑.๔ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลที่เป็นมาตรฐาน

๑๒. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

๑๒.๑ กำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

๑๒.๒ มีการควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ตามสิทธิของผู้ใช้งาน

๑๒.๓ ผู้ใช้งานจะต้องรับผิดชอบผลกระทบที่เกิดจากการใช้งานไม่ถูกต้อง

๑๒.๔ มหาวิทยาลัยขอสงวนสิทธิ์ในการระงับ เปลี่ยนแปลง หรือยกเลิก การใช้งาน ตามเหตุอัน สมควร

๑๓. การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่ เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่หน่วยงานจัดสรรไว้

๑๓.๒ การใช้งานเครื่องคอมพิวเตอร์ จะต้องมีระบบรักษาความปลอดภัยเพื่อทำการอุดช่องโหว่ ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์ของระบบปฏิบัติการ

๑๓.๓ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ

๑๓.๔ การเผยแพร่ข้อมูลผ่านเครือข่ายอินเทอร์เน็ตจะเป็นไปตามแนวปฏิบัติการใช้งานระบบ อินเทอร์เน็ต (Internet) เท่านั้น

๑๓.๕ การกระทำใดๆ บนเครือข่ายอินเทอร์เน็ตที่ไม่ถูกต้องตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ ผู้ใช้งานจะต้องเป็นผู้รับผิดชอบ

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔.๑ ส่งเสริมให้ผู้ใช้งานเครือข่ายสังคมออนไลน์ มีความตระหนักถึงเรื่องความมั่นคงปลอดภัยในการ ใช้งาน

๑๔.๒ ผู้ใช้งานจะต้องรับผิดชอบในการเผยแพร่ข้อมูล หากเกิดความเสียหายที่มีผลกระทบต่อ มหาวิทยาลัยและชื่อเสียงของบุคคลอื่นๆ

๑๕. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑๕.๑ กำหนดให้ระบบมีการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) และจัดเก็บไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้งานสิ้นสุดลง

๑๕.๒ ข้อมูลจราจรทางคอมพิวเตอร์ (Log) จะต้องจัดเก็บไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความ ครบถ้วน และถูกต้อง

๑๕.๓ มีการกำหนดชั้นความลับในการเข้าถึงข้อมูลที่จัดเก็บ และสามารถระบุตัวบุคคลที่เข้าถึงข้อมูลดังกล่าวได้

๑๕.๔ มีมาตรการในการป้องกันการแก้ไขข้อมูลจราจรทางคอมพิวเตอร์ (Log)

แนวปฏิบัติการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

แนวปฏิบัติ

๑.การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๑.๑ แต่ละหน่วยงานภายในมหาวิทยาลัยาจะต้องมีการระบุหมายเลขทรัพย์สินตามที่กองพัสดุกลางเป็นผู้กำหนด และจัดทำบัญชีทรัพย์สินของหน่วยงาน

๑.๒ การกำหนดหลักเกณฑ์ในการอนุญาตการเข้าถึง

๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์ หรือการมอบอำนาจแก่ผู้ใช้งานแต่ละกลุ่มดังนี้

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๒) กำหนดเกณฑ์ ระดับสิทธิ์ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการ การเข้าถึงผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๑.๓ การกำหนดหลักเกณฑ์เพื่อการจัดเก็บข้อมูล

การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.๒๕๔๔ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์ โดยได้กาหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑) จัดแบ่งประเภทของข้อมูล ออกเป็น

- ข้อมูลสารสนเทศด้านบุคลากร
- ข้อมูลสารสนเทศด้านนักศึกษา
- ข้อมูลสารสนเทศด้านการเงิน
- ข้อมูลสารสนเทศด้านการวิจัย
- ข้อมูลสารสนเทศด้านสิ่งอำนวยความสะดวก

๒) การแบ่งระดับความสำคัญของข้อมูล มี ๔ ระดับดังนี้

- ข้อมูลสำคัญมากที่สุด
- ข้อมูลสำคัญมาก
- ข้อมูลสำคัญปานกลาง
- ข้อมูลสำคัญน้อย

๓) การแบ่งระดับความลับของข้อมูล มี ๔ ระดับดังนี้

- ลับที่สุด
- ลับมาก
- ลับ
- ข้อมูลทั่วไป

(๑) ข้อมูลลับที่สุด คือ หากเปิดเผยทั้งหมดหรือเพียงบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด

(๒) ข้อมูลลับมาก คือ หากเปิดเผยทั้งหมด หรือบางส่วน จะก่อให้เกิดความเสียหายอย่างร้ายแรง

(๓) ข้อมูลลับ คือ หากเปิดเผยทั้งหมด หรือบางส่วน จะก่อให้เกิดความเสียหาย

(๔) ข้อมูลทั่วไป คือ ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๓) การจัดระดับชั้นการเข้าถึง

- ระดับผู้บริหาร
- ระดับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย
- ระดับผู้ปฏิบัติงาน
- ระดับผู้ใช้งานทั่วไป

๔) การกำหนดเวลาที่เข้าถึงได้

- ผู้ใช้งานเข้าถึงสารสนเทศได้ตลอดเวลา โดยผ่านระบบพิสูจน์ตัวตนก่อนเข้าใช้งาน
- การใช้งานสารสนเทศในแต่ละครั้ง กำหนดระยะเวลาใช้งาน ๘ ชั่วโมงต่อครั้ง

๕) การกำหนดช่องทางที่สามารถเข้าถึงได้

- ช่องทางการใช้งานแบบมีสาย (Wired LAN)
- ช่องทางการใช้งานแบบไร้สาย (Wireless LAN)

๑.๔ ข้อกำหนดการใช้งานตามภารกิจ (Business requirements for access control) แบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ แนวทางการควบคุมการเข้าถึง โดยมีการแบ่งระดับชั้นและสิทธิการเข้าถึงดังนี้

- ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรง และเข้าถึงผ่านระบบงาน รวมไปถึงวิธีการทำลายข้อมูล
- ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

- ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูลและรายงานข้อมูลตามต้องการของมหาวิทยาลัย

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มหาวิทยาลัยมอบให้เท่านั้น

๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

- ตรวจสอบและประเมินผลการใช้งานระบบสารสนเทศ

- มีรายงานปัญหาและข้อเสนอแนะการใช้งานระบบสารสนเทศต่อมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง

- ทบทวนและปรับปรุงการใช้งานให้เหมาะสมกับภาระงานในปัจจุบัน

๒ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (User access management)

๒.๑ จัดให้มีการอบรมหลักสูตรเกี่ยวกับการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศด้านระบบเครือข่าย ด้านสารสนเทศ เพื่อให้ตระหนักถึงผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์เป็นประจำทุกปี

๒.๒ กำหนดขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งาน (User registration) ผู้ใช้งานระบบสารสนเทศมีทั้งแบบสร้างให้อัตโนมัติ และแบบต้องส่งคำร้องผ่านผู้ดูแลระบบเป็นรายกรณี ทั้งนี้ขึ้นอยู่กับบริการ โดยแบ่งการลงทะเบียน เป็น ๒ ประเภทดังนี้

๑) การลงทะเบียนขอใช้บริการระบบสารสนเทศพื้นฐานของมหาวิทยาลัย การลงทะเบียนขอใช้บริการระบบสารสนเทศพื้นฐานของมหาวิทยาลัย ซึ่งได้แก่ (การขอใช้เครือข่ายอินเทอร์เน็ต / Wi-Fi / ระบบทะเบียนนักศึกษา/ ระบบเมล์ โดยมีระบบบริหารจัดการผู้ใช้จากส่วนกลาง จะเป็นผู้ลงทะเบียนการใช้งานระบบสารสนเทศ ผ่านระบบการสร้างบัญชีรายชื่อ (Account Internet) ให้อัตโนมัติ โดยระบบจะกำหนดสิทธิ์การใช้งานระบบสารสนเทศนั้นๆ ตามประเภทผู้ใช้งาน(End User) ซึ่งจะมีทั้งบุคลากร นักศึกษาของมหาวิทยาลัย ซึ่งแต่ละประเภทจะได้รับสิทธิ์การใช้งานที่แตกต่างกันไป ทั้งนี้ข้อมูลที่จะนำมาลงทะเบียน กำหนดสิทธิ์ และการทบทวนสิทธิ์ สำหรับผู้ใช้งานทั่วไปจะมาจากหน่วยงานกลางที่กำกับดูแลข้อมูลบุคลากรนั้นๆ มีแนวทางการดำเนินงานดังนี้

- นักศึกษาของมหาวิทยาลัย ยึดตามสถานะที่ได้จากฐานข้อมูลระบบบริหารการศึกษาซึ่งอยู่ภายใต้การดูแลของสำนักส่งเสริมวิชาการและงานทะเบียน

- บุคลากรของมหาวิทยาลัย ยึดตามสถานะที่ได้จากฐานข้อมูลระบบบริหารงานบุคคล ซึ่งอยู่ภายใต้การดูแลของกองบริหารงานบุคคล

- บุคลากรสำนักกิจการพิเศษ ยึดตามสถานะที่ได้จากฐานข้อมูลระบบงานบุคลากรซึ่งอยู่ภายใต้การดูแลของสำนักกิจการพิเศษ

- บุคคลภายนอก ยึดตามสถานะเจ้าของโครงการ ได้แจ้งความประสงค์มา แต่ทั้งนี้อายุการใช้งานต้องไม่เกิน ๑๘๐ วัน /ครั้ง

๒) การลงทะเบียนขอใช้บริการระบบสารสนเทศตามภารกิจ

(๑) การลงทะเบียนขอใช้บริการระบบสารสนเทศตามภารกิจ สำหรับผู้ใช้งานทั่วไป (ได้แก่ การให้บริการ webhosting / Cloud Computing /บุคคลภายนอกที่ขอใช้เครือข่ายอินเทอร์เน็ต) ต้องมีการลงทะเบียน ส่งคำร้องขอใช้บริการผ่านผู้ดูแลระบบ พร้อมรับทราบข้อพึงปฏิบัติ เป็นรายกรณี

(๒) การลงทะเบียนขอใช้บริการระบบสารสนเทศตามภารกิจสำหรับผู้ดูแลระบบ (Administrator) และตัวแทนผู้ดูแลระบบ (Delegate Administrator) ต้องมีการลงทะเบียน และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาจากต้นสังกัด และจากผู้อำนวยการสำนักวิทยบริการฯ / รองผู้อำนวยการฯ โดยมีหลักเกณฑ์ในการอนุญาต เพื่อให้การเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดได้ตามความเหมาะสมตามหน้าที่ความรับผิดชอบของแต่ละบุคคล

๓) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

๔) การกำหนดชื่อผู้ใช้งาน (Username)

(๑) บุคลากร กำหนดจากชื่อภาษาอังกฤษและตามด้วย อักษรสามตัวแรกของนามสกุล หากซ้ำให้ใช้อักษรตัวที่สี่ขึ้นมาแทน หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๒) นักศึกษา การกำหนดจากรหัสนักศึกษา โดยมีอักษรนำดังนี้

- ระดับปริญญาตรี จะได้อักษร u นำหน้า เช่น u๕๙๕๖๙๙๐๐๐๓๕
- ระดับปริญญาโท จะได้อักษร g นำหน้า เช่น g๕๙๕๖๙๙๐๐๐๓๕
- ระดับปริญญาเอก จะได้อักษร d นำหน้า เช่น d๕๙๕๖๙๙๐๐๐๓๕

(๓) บุคคลภายนอก (ผู้มางานอบรม /สัมมนา) มหาวิทยาลัยจะมีระบบในการสร้างบัญชีผู้ใช้งานแบบสุ่ม โดยมีรูปแบบดังนี้

- Username = อักษรนำ (tp)
- ตามด้วยปีพุทธศักราช
- ตามด้วยเดือนที่ใช้งาน
- ตามด้วยลำดับเลขที่ ๔ หลัก

เช่น มาขอใช้เครือข่ายอินเทอร์เน็ตมหาวิทยาลัย เดือน พฤษภาคม ๒๕๕๙ จะได้ username ดังนี้ tp๒๕๕๙๐๕๐๐๐๑

๒.๓ การบริการจัดการสิทธิของผู้ใช้งาน (User Management) ต้องตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือความต้องการทางการศึกษา

๑) ต้องมีกระบวนการในการมอบหมาย/กำหนดสิทธิ ทั้งสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ เพื่อให้การเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดได้ตามความเหมาะสมของแต่ละกลุ่มบุคคลผู้ใช้งาน

๒) ต้องกำหนดระดับสิทธิในการเข้าถึงสารสนเทศที่เหมาะสมตามประเภทของผู้ใช้งาน โดยมีการแบ่งสิทธิผู้ใช้งานดังนี้ คือ อ่านอย่างเดียว/สร้างข้อมูล/ป้อนข้อมูล/แก้ไข/อนุมัติ/ไม่มีสิทธิ

๓) ต้องจัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน ซึ่งต้องลงนามรับทราบด้วย

๔) ต้องกำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาต จากผู้อำนวยสำนักฯหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๕) ต้องทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management) โดยจัดทำกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม ดังนี้

๑) มีขั้นตอนปฏิบัติสำหรับการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย

(๑) ความยาวของรหัสผ่านต้องไม่น้อยกว่า ๘ ตัวอักษร

(๒) รหัสผ่านจะต้องประกอบไปด้วย อักษรละตินตัวพิมพ์ใหญ่ (A ถึง Z) อักษรละตินตัวพิมพ์ เล็ก (a ถึง z) และต้องมีตัวเลข (๐ ถึง ๙) ร่วมด้วย

(๓) ต้องไม่นำรหัสผ่านเดิมที่เคยใช้งาน มาตั้งใหม่

๒) ต้องมีช่องทางสำหรับผู้ใช้งานสามารถเปลี่ยนรหัสผ่านได้ด้วยตนเอง ทั้งนี้ต้องมีการใช้งานร่วมกับคำถามกันลืมหรืออาจจะใช้เทคนิคอื่นใดในการพิสูจน์ตัวตน ก่อนที่จะอนุญาตให้เปลี่ยนรหัสผ่านได้ เพื่อป้องกันการเจาะระบบจากบุคคลอื่นที่จะเข้ามา Reset Password ได้

๓) ต้องมีรอบระยะเวลาในการเปลี่ยนรหัสผ่านใหม่ ทุกๆ ๖ เดือน

๒.๕ มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัด ออกจากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น โดยมีหลักเกณฑ์ การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (review of user access rights) ดังนี้

๑) การทบทวนสิทธิ์สำหรับผู้ใช้งานทั่วไป มหาวิทยาลัยมีระบบบริหารจัดการผู้ใช้จากส่วนกลาง ที่จะตรวจสอบสถานะนักศึกษา/บุคลากร /บุคคลภายนอก โดยระบบบริหารจัดการผู้ใช้จากส่วนกลาง จะระงับการใช้งานระบบอัตโนมัติ โดยยึดตามสถานะที่ได้จากหน่วยงานกลางที่เป็นเจ้าของข้อมูล

๒) การทบทวนสิทธิ์สำหรับผู้ดูแลระบบ (Administrator) และตัวแทนผู้ดูแลระบบ (Delegate Administrator) และปรับปรุงบัญชีชื่อผู้ดูแลระบบ ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง อันเนื่องจากจากโอนย้ายหน่วยงานหรือลาออก

๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เปิดเผย ล่วงรู้ หรือลักลอบทำสำเนาข้อมูลสารสนเทศ และลักขโมยอุปกรณ์ประมวลผลสารสนเทศ จึงได้กำหนดข้อปฏิบัติดังนี้

๓.๑ ข้อกำหนดวิธีการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน ดังนี้

๑) ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๒) ผู้ใช้งานไม่เปิดเผยรหัสผ่านของตนเองและไม่ใช้รหัสผ่านของตนร่วมกับผู้อื่น

๓) ผู้ใช้งานต้องจัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย

๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือมีผู้อื่นล่วงรู้

๕) การตั้งรหัสผ่านต้องเป็นไปตามข้อกำหนดการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User password management)

๖) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตามรอบระยะเวลาที่กำหนด

๗) ผู้ใช้งานต้องไม่บันทึกรหัสผ่านหรือจดจำรหัสผ่านของตนเองไว้ในระบบ เนื่องจากมีความเสี่ยงต่อความไม่ปลอดภัย

๓.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

๑) มีบัญชีควบคุมอุปกรณ์คอมพิวเตอร์ที่ใช้งานเพื่อป้องกันการสูญหาย หรือการเข้าถึงโดยไม่ได้รับอนุญาต

๒) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการการป้องกัน

๓) กำหนดให้เครื่องคอมพิวเตอร์มีการปิดหน้าจอหลังจากที่ไม่มีผู้ใช้งานตามระยะเวลาที่กำหนดและต้องใส่รหัสผ่านทุกครั้งเมื่อต้องเปิดหน้าจอ

๔) ต้องปิดอุปกรณ์และเครื่องคอมพิวเตอร์ทุกครั้ง เมื่อไม่ได้ถูกใช้งาน หรือต้องปล่อยทิ้ง โดยไม่มีผู้ดูแลชั่วคราว

๓.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy)

๑) มีมาตรการป้องกันทรัพย์สินของมหาวิทยาลัย และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานะการที่ปลอดภัย

(๑) มีการควบคลุมพื้นที่ห้อง Data Center บริเวณล้อมรอบ/การควบคุมการเข้า-ออก/การจัดบริเวณการเข้าถึงการส่งผลิตภัณฑ์โดยบุคคลภายนอก

(๒) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับอนุญาต

(๓) จัดเก็บบันทึกการเข้า-ออก สำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๔) ผู้มาเยือนต้องติดบัตรให้เห็นชัดตลอดระยะเวลาที่อยู่บริเวณพื้นที่ใช้งานระบบ

(๕) ลงทะเบียนและตรวจนับผลิตภัณฑ์ที่ส่งมอบโดยผู้ขายหรือผู้ให้บริการภายนอกให้ สอดคล้องกับระเบียบพัสดุ หรือขั้นตอนปฏิบัติสำหรับการบริหารจัดการทรัพย์สินของมหาวิทยาลัย

(๖) จัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม เพื่อหลีกเลี่ยงการเข้าถึงพื้นที่ในห้อง ที่มีความสำคัญให้น้อยที่สุด

๒) การป้องกันต้องมีความสอดคล้องกับเรื่องต่างๆ ดังนี้

(๑) แนวทางการจัดหมวดหมู่สารสนเทศและการจัดการกับสารสนเทศ

(๒) กฎหมาย ระเบียบ ข้อบังคับ หรือข้อกำหนดอื่น ๆ

(๓) วัฒนธรรมองค์กร

๓) มีการป้องกันเครื่องคอมพิวเตอร์ โดยใช้กลไกการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน

๔) มีการกำหนดขอบเขตของการป้องกัน ดังนี้

(๑) ทุกคนต้องตระหนัก และปฏิบัติการใดๆ ให้ต้องตระหนักถึงความมั่นคงปลอดภัย รวมถึงการทะนุบำรุง เพื่อป้องกันทรัพย์สินของมหาวิทยาลัย

(๒) ลงชื่อออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล

(๓) จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

(๔) ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน

(๕) ป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน

(๖) ป้องกันตู้หรือบริเวณที่ใช้ในการรับส่งเอกสารทางไปรษณีย์

(๗) ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ เครื่องพิมพ์ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

(๘) นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๕) กำหนดมาตรการทำลายสื่อบันทึกข้อมูล/ข้อมูลอิเล็กทรอนิกส์ หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง มีข้อปฏิบัติดังนี้

(๑) ต้องทำลายข้อมูลสำคัญภายในอุปกรณ์บันทึกข้อมูลหรือสื่อที่ใช้บันทึกข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) สื่อบันทึกข้อมูลที่เป็นประเภทจานแม่เหล็กให้ทำการ Format อุปกรณ์ดังกล่าว โดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD ๕๒๒๐.๐๐ M หรือวิธีบดขยี้ตามมาตรฐาน ISO/IEC ๒๗๐๐๒ : ๒๐๐๕

(๓) สื่อบันทึกข้อมูลประเภท Optical Disk ทำลาย โดยวิธีบดขยี้ การหัก หรือ เจาะรูโดยไม่สามารถเรียกข้อมูลกลับมาได้ตามมาตรฐาน ISO/IEC ๒๗๐๐๒ : ๒๐๐๕

(๔) สื่อบันทึกข้อมูลขนาดเล็กแบบพกพา (flash drive) ให้ทำการ Format อุปกรณ์ดังกล่าว โดยไม่สามารถเรียกคืนกลับมาได้ตามมาตรฐาน DOD ๕๒๒๐.๐๐ M

(๕) มีกระบวนการในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มี การเข้าถึงข้อมูลสำคัญนั้นได้ตามมาตรฐาน NSA

๓.๔ ผู้ใช้งานอาจมีการหัสข้อมูล กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ.๒๕๔๔ ตามแนวปฏิบัติข้อ ๕(๓)

๔. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๔.๑ การใช้งานบริการเครือข่ายต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑) ระบบสารสนเทศต้องมีการควบคุมการเข้าถึงโดยระบุเป็น กลุ่มของบุคคล กลุ่มของระบบเครือข่ายหรือบริการที่อนุญาตให้ใช้งานได้

๒) ให้ผู้ใช้งานแต่ละกลุ่มให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๓) การใช้งานระบบสารสนเทศต้องกำหนดสิทธิเฉพาะการปฏิบัติงานในหน้าที่ที่รับผิดชอบและต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างน้อยปีละ ๑ ครั้ง

๔) การใช้งานระบบเครือข่ายจะต้องมีการลงทะเบียนการใช้งาน โดยชื่อผู้ใช้รหัสผ่านและสิทธิการใช้งาน ตามแนวปฏิบัติการเข้าถึงของผู้ใช้งานโดยมหาวิทยาลัย

๔.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกมหาวิทยาลัย สามารถเข้าถึงบริการใช้งานเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ ดังนี้

๑) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ทุกครั้ง

๒) ต้องตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง

๓) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงาน

๕) การเข้าสู่ระบบเครือข่ายภายในและระบบสารสนเทศในหน่วยงานจากระยะไกลต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยแสดงตัวตนด้วยชื่อผู้ใช้งาน และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการใช้รหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๔.๓ มีบัญชีอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ที่ใช้งานและมีการยืนยันการเข้าถึงอุปกรณ์ดังกล่าว ดังนี้

๑) การระบุอุปกรณ์และการจัดเก็บข้อมูล

(๑)ใช้หมายเลข IP Address ในการระบุอุปกรณ์ โดยกำหนดเป็นช่วงของหมายเลข IP แยกตามประเภทของอุปกรณ์

(๒)จัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๓)จัดเก็บข้อมูล อุปกรณ์บนเครือข่ายโดยระบุชนิดของอุปกรณ์การใช้งานและเก็บบันทึกในรูปแบบสื่ออิเล็กทรอนิกส์ และเอกสารแล้วนำไปเก็บไว้ในตู้นิรภัย

๒) มีการพิสูจน์ตัวตนทุกครั้งที่ใช้อุปกรณ์ ดังนี้

(๑) กำหนดบัญชีผู้ใช้และสิทธิการเข้าถึงอุปกรณ์บนอุปกรณ์เครือข่าย

(๒) ให้ใช้โปรแกรมประเภท terminal ในการเข้าถึงอุปกรณ์

(๓) ตั้งค่าความเร็วของการเข้าถึงตามคุณลักษณะของอุปกรณ์นั้น(สามารถดูได้จาก คู่มือของอุปกรณ์)

(๔) เมื่อเข้าสู่อุปกรณ์แล้วระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่าน

(๕) เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ถูกต้องระบบจะยอมให้ใช้งานอุปกรณ์ตามสิทธิ์ที่ได้กำหนดไว้

(๖) เมื่อกรอกชื่อผู้ใช้และรหัสผ่านที่ไม่ถูกต้องระบบจะไม่ยอมให้เข้าใช้งานอุปกรณ์

(๗) ระบบจะให้กรอกชื่อผู้ใช้และรหัสผ่านไม่เกิน ๓ ครั้ง มิฉะนั้นระบบจะล็อคการเข้าใช้งานอุปกรณ์ เป็นเวลา ๓๐ นาที

๓) ควบคุมการติดตั้งอุปกรณ์เครือข่ายและการใช้งานอย่างเหมาะสม

๔) จำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

๔.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่ง ระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑) การปรับเปลี่ยนหรือควบการเข้าถึงพอร์ตต้องการทำหนังสือขออนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๒) บันทึกและควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบสำหรับการเข้าถึงทางกายภาพและการเข้าถึงทางเครือข่าย

๓) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

๔.๕ การแบ่งแยกเครือข่าย (Segregation in Networks) ต้องทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอกและมีการแบ่งแยกเครือข่ายตามแต่ละหน่วยงานและการใช้งาน (VLAN)

๔.๖ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างเครือข่ายให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง ดังนี้

๑) ต้องจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

๒) ต้องจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน

๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่น ๆ ได้

๔) ระบบเครือข่ายทั้งหมดของหน่วยงานที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ภายนอกหน่วยงานต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมี ความสามารถในการตรวจจับโปรแกรมประสงค์ร้าย (Malware) ด้วย

๕) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ

๖) การเข้าสู่ระบบเครือข่ายภายในหน่วยงาน โดยผ่านทางระบบอินเตอร์เน็ต จำเป็นต้องมีการลงบันทึกเข้าใช้งาน (Login) โดยต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ด้วยชื่อผู้ใช้และรหัสผ่าน เพื่อตรวจสอบความถูกต้องของผู้ใช้งานก่อนทุกครั้ง

๗) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของหน่วยงาน

๔.๗ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address)

๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่ายสามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

๔.๘ การควบคุมการเข้าใช้งานระบบจากภายนอก

๑) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบสารสนเทศและเครือข่ายของหน่วยงาน ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๒) การเข้าสู่ระบบจากระยะไกล (Remote Access) สู่ระบบเครือข่ายของมหาวิทยาลัย ต้องควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยกำหนดมาตรการการรักษาความปลอดภัยที่ เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกลต้องได้รับ การอนุมัติจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศหรือบุคคลที่ได้รับมอบหมายจากมหาวิทยาลัยก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตาม ข้อกำหนดของมหาวิทยาลัยในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๔) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัย และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๕) มีการควบคุมพอร์ต(Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวให้ตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว

๕ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๕.๑) ผู้ดูแลระบบ (System Administrator) ต้องติดตั้งโปรแกรมช่วยบริหารจัดการ (Domain Control) เพื่อบริหารจัดการเครื่องคอมพิวเตอร์ทุกเครื่องของมหาวิทยาลัยและกำหนดชื่อผู้ใช้งานและรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

๕.๒) กำหนดขั้นตอนปฏิบัติการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวทางปฏิบัติ ดังนี้

๑) ต้องจัดไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

๓) จำกัดระยะเวลาสำหรับใช้ในการป้องกันรหัสผ่าน

๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง command line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๕.๓) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้มีผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวทางปฏิบัติ ดังนี้

๑) มหาวิทยาลัยจัดให้ผู้ใช้งานทุกคนที่เป็นบุคลากร นักศึกษา บุคคลภายนอกที่มาอบรมสัมมนา ต้องมีบัญชีรายชื่อผู้ใช้งานอันประกอบด้วย username และ password เป็นของตนเองทุกคน

๒) ผู้ใช้งานจะต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหา หรือเกิดความผิดพลาด ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทำการแก้ไขทันที

๓) บางระบบงานอนุญาตให้ใช้ชื่อผู้ใช้งาน และรหัสผ่านร่วมกัน โดยต้องขึ้นอยู่กับความจำเป็นทางด้านการศึกษาหรืองานที่ต้องทำ

๔) ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕) ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอนจำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๖) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๗) การระบุและยืนยันตัวตนของผู้ใช้งาน สามารถใช้อุปกรณ์ควบคุมความปลอดภัยเพิ่มเติม ได้แก่ สมาร์ทการ์ด RFID หรือ เครื่องอ่านลายพิมพ์นิ้วมือ ฯลฯ

๕.๔) การบริหารจัดการรหัสผ่าน (password management system) มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

๑) มีระบบบริหารจัดการรหัสผ่าน ผ่านระบบเครือข่ายสารสนเทศของมหาวิทยาลัย ต้องอนุญาตให้ผู้ใช้งานเลือกหรือเปลี่ยนรหัสผ่านได้ด้วยตนเองและมีขั้นตอนปฏิบัติ เพื่อยืนยันรหัสผ่านใหม่

๒) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้มีการใช้งานบัญชีผู้ใช้งานและรหัสผ่านแยกเป็นรายบุคคล เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๓) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเลือกรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น

๔) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านใหม่ ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุกๆ ๖ เดือน เป็นต้น

๕) ระบบบริหารจัดการรหัสผ่าน ต้องกำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันทีที่ได้รับบัญชีผู้ใช้งานและทำการล็อกอินเข้าใช้งานระบบงานเป็นครั้งแรก

๖) ระบบบริหารจัดการรหัสผ่าน ต้องไม่แสดงข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลล็อกอิน ได้แก่ ให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอเป็นต้น

๗) ระบบบริหารจัดการรหัสผ่าน ควรป้องกันรหัสผ่านที่ได้มีการจัดเก็บไว้ หรือที่จำเป็นต้องมีการส่งไปในเครือข่าย เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

๕.๕) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยทางระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการดังนี้

๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๔) มีการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๕.๖) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time-out)

๑) การยุติการใช้งานระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๓๐ นาที เป็นอย่างน้อย เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๒) ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติหลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๕.๗) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of Connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๑) มีการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น โดยมีการกำหนดให้ใช้งานได้ไม่เกิน ๘ ชั่วโมงต่อการเชื่อมต่อหนึ่งครั้ง

๒) กำหนดให้ใช้งานได้เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

๓) การกำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทาง จะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

๖.การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control)

๖.๑ การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและผู้สนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและ ฟังก์ชัน (Functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น โดยสอดคล้องตามนโยบายควบคุม การเข้าถึงสารสนเทศที่ได้กำหนดไว้ โดยมีแนวปฏิบัติดังนี้

๑) ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนผู้ใช้งานใหม่ โดยปฏิบัติตามข้อ ๒ เรื่องการควบคุมการเข้าถึงใช้งานสารสนเทศ หัวข้อ ๒.๒ ส่วนการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน ตามข้อ ๒.๕

๒) ผู้ดูแลระบบ ต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยปฏิบัติตามข้อ ๒.๓

๓) ข้อกำหนดการใช้งานตามภารกิจ แบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ

๓.๑) การควบคุมการเข้าถึงสารสนเทศ โดยกำหนดแนวทางการควบคุมการเข้าถึงระบบสารสนเทศและสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ แนวทางการควบคุมการเข้าถึง โดยมีการแบ่งระดับชั้นและสิทธิการเข้าถึงดังนี้

- ระดับผู้ดูแลระบบ มีหน้าที่ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภททั้งการเข้าถึงโดยตรง และเข้าถึงผ่านระบบงาน รวมไปถึงวิธีการทำลายข้อมูล

- ระดับเจ้าของข้อมูล มีหน้าที่ตรวจสอบความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน อย่างน้อยปีละ ๑ ครั้ง

- ระดับผู้ปฏิบัติงาน มีหน้าที่ในการบันทึกข้อมูล ตรวจสอบข้อมูล ปรับปรุงข้อมูล และรายงานข้อมูลตามต้องการของมหาวิทยาลัย

- ระดับชั้นสำหรับผู้ใช้งานทั่วไป มีสิทธิในการใช้ข้อมูลตามสิทธิที่มหาวิทยาลัยมอบให้เท่านั้น

๓.๒) ข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

- ต้องตรวจสอบและประเมินผลการใช้งานระบบสารสนเทศ

- มีรายงานปัญหาและข้อเสนอแนะการใช้งานระบบสารสนเทศต่อมหาวิทยาลัย อย่างน้อยปีละ ๑ ครั้ง

- ทบทวนและปรับปรุงการใช้งานให้เหมาะสมกับภาระงานในปัจจุบัน

๔) ผู้ดูแลระบบ ต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศ ที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่าง ๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๒๐ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องลงบันทึกการเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

๕) ผู้ดูแลระบบ ต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากรดังต่อไปนี้

๕.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๕.๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๕.๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

๕.๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าหน่วยงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๖) ผู้ดูแลระบบ ต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลาย ข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

๖.๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

๖.๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูล ในแต่ละชั้นความลับของข้อมูล

๖.๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลา

๖.๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

๖.๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

๖.๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๗) การควบคุมผู้ให้บริการภายนอกด้านเทคโนโลยีสารสนเทศ (Outsourcing)

(๗.๑) การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑)จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์ จากผู้ให้บริการภายนอก

(๒)พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้ให้บริการภายนอก

(๓)พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔)ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕)หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

(๖)ผู้ให้บริการภายนอก ต้องไม่นำข้อมูลที่เป็นความลับขององค์กร ไปเปิดเผยต่อบุคคลที่ไม่มีส่วนเกี่ยวข้องต้องได้ทราบ โดยไม่ได้รับอนุญาตจากองค์การ

(๗.๒) การรักษาความปลอดภัยและและความลับของระบบงานข้อมูล

๗.๒.๑ ผู้ให้บริการภายนอกต้องมีกระบวนการขั้นตอน การประเมิน และการควบคุมความเสี่ยง อย่างน้อยตามกรอบหลักการด้านเทคโนโลยีสารสนเทศที่สำคัญ ๓ ประการคือ

(๑) การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security)

(๒) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity)

(๓) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการ (Availability)

๗.๒.๒.ผู้ให้บริการภายนอกต้องจัดให้มีการประเมิน ทดสอบ และตรวจสอบผู้ให้บริการภายนอก เพื่อให้มั่นใจว่า จะไม่ก่อให้เกิดความเสี่ยง ด้านเทคโนโลยีสารสนเทศ จนนำมาสู่ช่องโหว่ และหรือภัยคุกคามด้านเทคโนโลยีสารสนเทศทั้งจากภายในและภายนอก ซึ่งอาจส่งผลกระทบการการดำเนินงาน / ภาพลักษณ์ของมหาวิทยาลัย ที่สำคัญ ๓ ประการคือ

๑) การรักษาความปลอดภัยและความลับของระบบงานและข้อมูล (Security)

๒) ความถูกต้องเชื่อถือได้ของระบบงานและข้อมูล (integrity)

๓) ความพร้อมใช้ของงานเทคโนโลยีสารสนเทศที่ให้บริการ (Availability)

๖.๒ ระบบซึ่งไวต่อการรบกวน ที่มีผลกระทบและมีความสำคัญสูงต่อหน่วยงานจะต้องดำเนินการดังนี้

๑) แยกระบบที่ไวตอการรบกวนออกจากระบบงานอื่น ๆ

๒) มีการควบคุมสภาพแวดลอมของตนเอง โดยมีหองปฏิบัติงานแยกเปนสัดสวน

๓) มีการกำหนดสิทธิ์ใหเฉพาะผู้ที่มีสิทธิ์ใชระบบเทานั้น

๖.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

ลงทะเบียนอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ มีแนวทางปฏิบัติในการใช้งาน โดยแบ่งออกเป็น ๒ กลุ่ม ดังนี้

๑) อุปกรณ์คอมพิวเตอร์

๑) เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้จึงต้องใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ต้องเป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกกฎหมาย ดังนั้นห้ามผู้ใช้คัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๓) ไม่อนุญาตให้ผู้ใช้ ทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของมหาวิทยาลัย

๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่สำนักวิทยบริการฯ หรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

๖) ผู้ใช้มีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

๗) ปิดเครื่องคอมพิวเตอร์ส่วนบุคคลที่ตนเองครอบครองใช้งานอยู่เมื่อใช้งานประจำวันเสร็จสิ้น หรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

๘) ทำการล็อกหน้าจอเครื่องคอมพิวเตอร์หลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

๙) การนำเครื่องคอมพิวเตอร์มาใช้กับระบบเครือข่ายของมหาวิทยาลัยต้องยืนยันตัวตน ผ่านระบบก่อนเข้าใช้งานทุกครั้ง

๒) อุปกรณ์สื่อสารเคลื่อนที่

๑) เครื่องคอมพิวเตอร์แบบพกพาและอุปกรณ์สื่อสารเคลื่อนที่ จะต้องยืนยันตัวตนก่อนเข้าใช้งานระบบเครือข่ายอินเทอร์เน็ต

๒) อนุญาตให้เข้าใช้งานระบบได้ไม่เกิน ๕ ชั่วโมง หลังจากนั้นระบบจะบังคับให้ ต้องมีการยืนยันตัวตนใหม่

๓) ไม่อนุญาตให้เข้าใช้งานเว็บไซต์ที่ไม่เหมะสม หากผู้ดูแลระบบตรวจพบจะระงับสิทธิ์การเข้าถึงระบบ

๔) ไม่อนุญาตให้ผู้ใช้งานผ่านอุปกรณ์สื่อสารกระทำผิด พ.ร.บ.ว่าด้วยการกระทำความ ผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายเทคโนโลยีสารสนเทศ

๖.๔ การปฏิบัติงานจากภายนอกหน่วยงาน ต้องกำหนดให้มีการควบคุมการใช้งานระบบที่ผู้ดูแลระบบได้ติดตั้งไว้ในมหาวิทยาลัย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอก โดยมีแนวทางปฏิบัติ ดังนี้

๑) ผู้ใช้ระบบทุกคน เมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของมหาวิทยาลัย

๒) การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายของมหาวิทยาลัย ต้องควบคุมบุคคลจะเข้าสู่ระบบของมหาวิทยาลัยจากระยะไกล โดยกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าถึงข้อมูลหรือระบบข้อมูลจากระยะไกล ต้องได้รับการอนุมัติจากผู้อำนวยการสำนักวิทยบริการฯ ก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของมหาวิทยาลัยสวนดุสิต ในการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

๔) การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับมหาวิทยาลัยอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้มีอำนาจอย่างเป็นทางการ

๕) มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม

๖) การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น และไม่ควรเปิดพอร์ตทิ้งไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗ การควบคุมเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๗.๑ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคล

๑) เครื่องคอมพิวเตอร์ที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศอนุญาตให้ผู้ใช้งานเป็นทรัพย์สินของมหาวิทยาลัย ดังนั้นผู้ใช้งานควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

๒) ผู้ใช้งานต้องยอมรับกฎระเบียบหรือนโยบายต่าง ๆ ที่มหาวิทยาลัยกำหนดขึ้น โดยอ้างว่าไม่ว่าทราบกฎระเบียบหรือนโยบายมิได้

๓) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ ต้องเป็นโปรแกรมที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศติดตั้งมาให้หรือหน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานอย่างผิดกฎหมาย หากตรวจพบว่ามีการติดตั้งชุดโปรแกรม เปลี่ยนแปลงโปรแกรมหรืออุปกรณ์เครื่องคอมพิวเตอร์อื่นใดเพิ่มเติมและก่อให้เกิดความเสียหายหรือละเมิดลิขสิทธิ์ ผู้ใช้งานต้องเป็นผู้รับผิดชอบแต่เพียงฝ่ายเดียว

๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ส่วนบุคคลไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักวิทยบริการและเทคโนโลยีสารสนเทศหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

๕) การเคลื่อนย้ายเครื่องคอมพิวเตอร์ส่วนบุคคลไปยังจุดติดตั้งอื่น ผู้ใช้งานควรโทรแจ้งสำนักวิทยบริการและเทคโนโลยีสารสนเทศให้รับทราบตำแหน่งการติดตั้งตำแหน่งใหม่ทุกครั้งเพื่อให้ข้อมูลเป็นปัจจุบัน

๖) การเคลื่อนย้ายคอมพิวเตอร์แบบพกพาให้ใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพา เพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงาน หรือหลุดมือ ฯลฯ

๗) การเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพา ขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามเคลื่อนย้ายโดยการดึงหน้าจอภาพขึ้น

๘) ไม่วางสื่อแม่เหล็กไว้ใกล้หน้าจอเครื่องคอมพิวเตอร์ Disk Driveหรือสื่อบันทึกที่อาจก่อให้เกิดความเสียหายได้

๙) ไม่ควรเก็บข้อมูลสำคัญขององค์กรไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคลที่ท่านใช้งานอยู่

๑๐)ไม่ควรสร้าง Short–cut หรือปุ่มกดง่ายบน Desktop ที่เชื่อมต่อไปยังข้อมูลสำคัญของหน่วยงาน

๑๑)ไม่ควรวางอาหารและเครื่องดื่มใกล้บริเวณเครื่องคอมพิวเตอร์

๑๒)ไม่วางของทับบนหน้าจอและแป้นพิมพ์

๑๓)การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไป ในสภาพที่มีอากาศร้อนจัดให้ปิดเครื่องคอมพิวเตอร์ เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

๑๔)หลีกเลี่ยงการใช้นิ้วหรือของแข็งกดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วน หรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้

๑๕)ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อคเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องคอมพิวเตอร์ทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

๑๖)ห้ามมิให้ผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (Sub Component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

๑๗)ผู้ใช้งานต้องให้ความร่วมมือและอำนวยความสะดวกแก่ผู้ดูแลระบบคอมพิวเตอร์ในการตรวจสอบระบบความปลอดภัยของเครื่องคอมพิวเตอร์และเครือข่าย รวมทั้งปฏิบัติตามคำแนะนำของผู้ดูแล

๑๘)ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น กล่าวคือผู้ใช้งานจะต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต เช่น การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่นหรือเข้าใช้เครื่องคอมพิวเตอร์ที่อยู่ในความรับผิดชอบของผู้อื่น

๑๙)หากผู้ใช้งานกระทำการล่วงละเมิด หรือไม่ปฏิบัติตามกฎระเบียบหรือนโยบายต่าง ๆ ที่มหาวิทยาลัยกำหนดขึ้น สำนักวิทยบริการและเทคโนโลยีสารสนเทศในฐานะผู้ดูแลคอมพิวเตอร์และเครือข่ายของมหาวิทยาลัยขอสงวนสิทธิ์ที่จะยกเลิกการใช้งาน หรือระงับการเชื่อมต่อ หรือการใช้งานใด ๆ ตามความเหมาะสม

๗.๒ การควบคุมการเข้าถึงระบบปฏิบัติการ

๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการ

๒) ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของตนในการเข้าใช้เครื่องคอมพิวเตอร์ร่วมกัน

๓) ในระหว่างเวลาพักกลางวันหรือเมื่อไม่ใช้งานผู้ใช้งานควรล็อคหน้าจอด้วยโปรแกรม Screen Saver

๔) ผู้ใช้งานควรทำการบันทึกออก (Logout) ออกจากเครื่องคอมพิวเตอร์ทุกครั้งเมื่อเลิกใช้งาน

๕) ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer – to – Peer หรือโปรแกรมที่มีความเสี่ยง เว้นแต่ได้รับอนุญาตจากผู้บังคับบัญชาหรือสำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๖) มีการกำหนดระยะเวลาการเชื่อมต่อระบบสารสนเทศ เมื่อไม่มีการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session Time - out)

๗.๓ แนวปฏิบัติการป้องกันจากโปรแกรมชุดคำสั่งที่ไม่พึงประสงค์ (Malware)

๑) ผู้ใช้งานต้องทำการ Update ระบบปฏิบัติการ เว็บบราวเซอร์และโปรแกรมใช้งานต่าง ๆ อย่างสม่ำเสมอ เพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจาก Software เป็นการป้องกันการโจมตีจากภัยคุกคามต่าง ๆ หรือแจ้งเจ้าหน้าที่ผู้ดูแลให้ดำเนินการให้

๒) ผู้ใช้งานหรือเจ้าหน้าที่ผู้ดูแลควรติดตั้งโปรแกรมป้องกันไวรัส (Antivirus) ให้กับเครื่องคอมพิวเตอร์

๓) ผู้ใช้งานควรตรวจสอบหาไวรัสจากสื่อต่าง ๆ เช่น Thumb Drive Data Storage หรืออุปกรณ์บันทึกข้อมูลต่าง ๆ ก่อนนำมาใช้กับเครื่องคอมพิวเตอร์

๔) ผู้ใช้งานควรตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์หรือไฟล์ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งานทุกครั้ง

๗.๔ แนวปฏิบัติการสำรองข้อมูลและการกู้คืน

๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่น ๆ เช่น CD DVD External Hard Disk เป็นต้น

๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลสำรองไว้อย่างสม่ำเสมอ

๘. การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

๑) ต้องใช้จดหมายอิเล็กทรอนิกส์ ของมหาวิทยาลัยเพื่อติดต่องานของราชการเท่านั้น

๒) ผู้ใช้งานมีหน้าที่ต้องรักษาชื่อผู้ใช้งาน รหัสผ่าน ไว้เป็นความลับส่วนบุคคล ไม่ควรเปิดเผยแก่บุคคลอื่น

๓) การควบคุมการเข้าถึงระบบ ต้องปฏิบัติตามข้อปฏิบัติการบริหารจัดการเข้าถึงผู้ใช้งาน (user access management) ที่ได้กำหนดไว้อย่างเคร่งครัด

๔) ต้องกำหนดให้มีการออกจากระบบอัตโนมัติ (Auto Log Out) เมื่อไม่มีผู้ใช้งานระบบตามระยะเวลาที่ได้กำหนดไว้ เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๕) ควรออกจากระบบ (Log Out) ทุกครั้ง หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๖) ต้องไม่ตั้งค่าการใช้โปรแกรมช่วยจำรหัสผ่านส่วนบุคคลอัตโนมัติ (Save Password) ของระบบจดหมายอิเล็กทรอนิกส์

๗) ผู้ใช้งานต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อมหาวิทยาลัยสวนดุสิต หรืออาจเป็นการละเมิดสิทธิสร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย ละเมิดศีลธรรม และไม่แสวงหาประโยชน์ หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยสวนดุสิต

๘) ห้ามไม่ให้ผู้ใช้งาน ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail Address) ของผู้อื่น เพื่ออ่านรับ-ส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

๙) ผู้ใช้งานต้องใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยสวนดุสิต เพื่อการทำงานของมหาวิทยาลัยสวนดุสิตเท่านั้น ไม่นำไปใช้เพื่อแสวงหาผลประโยชน์ในเชิงธุรกิจ จากการใช้จดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของมหาวิทยาลัยสวนดุสิต

๑๐) ผู้ใช้งานไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

๑๑) ผู้ใช้งานต้องลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้พื้นที่จัดเก็บข้อมูลเครื่องแม่ข่ายระบบจดหมายอิเล็กทรอนิกส์

๙. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (LOG)

เพื่อให้เป็นไปตาม พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และเพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้อง ได้กำหนดแนวทางปฏิบัติไว้ดังนี้

(๑)ต้องจัดเก็บข้อมูลการจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่มั่นคงปลอดภัยที่สามารถรักษาข้อมูลให้มีความครบถ้วน ถูกต้อง แท้จริง สามารถระบุรายละเอียดเป็นรายบุคคลได้ตามข้อกำหนดของ พรบ. ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

(๒)ให้มีการบันทึกข้อมูลการจราจรทางคอมพิวเตอร์ อย่างน้อย ๙๐ วันนับตั้งแต่การใช้งานสิ้นสุดลง เพื่อประโยชน์ในการใช้ตรวจสอบย้อนหลัง

(๓)ต้องกำหนดวิธีการป้องกันการแก้ไข เปลี่ยนแปลงข้อมูล และจำกัดสิทธิ์เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น ในการเข้าถึงข้อมูลสารสนเทศที่ได้บันทึกไว้

(๔)มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูล เพื่อรักษาความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ผู้มีหน้าที่เกี่ยวข้องที่เจ้าของหรือผู้บริหารองค์การกำหนดให้เข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศขององค์กร (IT Auditor) เป็นต้น

๑๐. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and environment security)

๑๐.๑ ผู้ดูแลระบบเครือข่ายมหาวิทยาลัย

๑) ภายในมหาวิทยาลัยสวนดุสิต มีการจำแนกและกำหนดพื้นที่ของเครื่องแม่ข่าย อุปกรณ์เครื่องแม่ข่ายระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม โดยกำหนดพื้นที่รักษาความมั่นคงปลอดภัย ของระบบสารสนเทศและเครือข่ายมหาวิทยาลัยสวนดุสิต มีจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร ให้ชัดเจนรวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน และประกาศให้ทราบทั่วกัน โดยแบ่งออกเป็นพื้นที่ทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Network Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๓) กำหนดสิทธิให้กับเจ้าหน้าที่ ที่มีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายอย่างครบถ้วน

๔) จัดทำ “ทะเบียนผู้ที่มีสิทธิเข้า-ออกพื้นที่” เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับมอบหมาย

๕) กำหนดผู้ที่มีหน้าที่รับผิดชอบการบันทึกการเข้า-ออกพื้นที่ โดยจัดทำเป็นเอกสาร “บันทึกการเข้า-ออกพื้นที่

๖) จัดให้มีเจ้าหน้าที่ทำหน้าที่ ตรวจสอบประวัติการเข้า-ออกพื้นที่เป็นประจำทุกวัน และให้มีการปรับปรุงรายการผู้มีสิทธิเข้า-ออกพื้นที่ ปีละ ๑ ครั้งเป็นอย่างน้อย

๗) บุคคลภายนอกเข้าติดต่อต้องลงชื่อขออนุญาตการเข้า-ออก ในแบบฟอร์มการเข้า-ออกให้ถูกต้อง และจะต้องมีเจ้าหน้าที่อยู่กับบุคคลที่มาติดต่อตลอดเวลา

๘) บุคคลอื่นที่ไม่มีหน้าที่เกี่ยวข้องขอเข้าพื้นที่ ต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่อนุญาต

๙) ประกาศห้ามผู้ไม่มีส่วนเกี่ยวข้องเข้าพื้นที่ เว้นแต่ได้รับอนุญาตให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (General Working Area) พื้นที่

ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) และพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area)

๑๐.๒ กระบวนการควบคุมการเข้าออกห้องควบคุมระบบเครือข่าย

ผู้ดูแลห้องควบคุมระบบเครือข่ายและเจ้าหน้าที่มหาวิทยาลัยสวนดุสิต มีแนวทางปฏิบัติดังนี้

๑) ผู้ดูแลห้องควบคุมระบบเครือข่าย ต้องทำการกำหนดสิทธิส่วนบุคคลในการเข้าออกห้องควบคุม ระบบเครือข่าย โดยเฉพาะบุคลากรภายในที่ปฏิบัติหน้าที่ที่เกี่ยวข้อง และมีการบันทึก “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เช่น เจ้าหน้าที่ปฏิบัติงานคอมพิวเตอร์ (Computer Operator) เจ้าหน้าที่ผู้ดูแลระบบ (System Administrator) เป็นต้น

๒) สิทธิในการเข้าออกห้องต่างๆ ภายในห้องควบคุมระบบเครือข่ายของเจ้าหน้าที่แต่ละคนต้องได้รับอนุมัติจากผู้อำนวยสำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมายเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมระบบเครือข่าย

๓) ต้องจัดทำระบบเก็บบันทึกการเข้าออก ห้องควบคุมระบบเครือข่าย

๔) กรณีเจ้าหน้าที่ที่ไม่มีหน้าที่เกี่ยวข้องประจำ มีความจำเป็นต้องเข้าออกห้องควบคุมระบบเครือข่ายก็ต้องมีการควบคุมอย่างรัดกุม

๕) การเข้าถึงห้องควบคุมระบบเครือข่ายต้องมีการลงบันทึกตามแบบฟอร์มที่ระบุไว้ในเอกสาร “บันทึกการเข้าออกพื้นที่”

๑๐.๓ แนวปฏิบัติการจัดทำเอกสารระบุสิทธิในการเข้าถึงพื้นที่

การจัดทำเอกสารระบุสิทธิของผู้ใช้ และ “หน่วยงานภายนอก” ในการเข้าถึงพื้นที่มีดังนี้

๑) กำหนดสิทธิผู้ใช้ที่มีสิทธิผ่านเข้าออกและช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

๒) การเข้าถึงอาคารของหน่วยงาน บุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องมีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประชาชนใบอนุญาติขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๓) บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในมหาวิทยาลัยสวนดุสิต

๔) เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๕) ผู้ใช้จะได้รับสิทธิให้เข้าออกพื้นที่ทำงานได้เฉพาะบริเวณที่ที่ถูกกำหนด เพื่อใช้ในการทำงานเท่านั้น

๖) หากมีบุคคลอื่นที่ไม่ใช่ผู้ใช้ขอเข้าพื้นที่ โดยมิได้ขอรับสิทธิการเข้าพื้นที่นั้นเป็นการล่วงหน้าหน่วยงานเจ้าของพื้นที่ต้องตรวจสอบเหตุผล และความจำเป็นก่อนที่จะอนุญาต ทั้งนี้

จะต้องแสดงบัตรประจำตัวที่หน่วยราชการออกให้ โดยหน่วยงานเจ้าของพื้นที่ต้องจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานทั้งเป็นกรณีที่อนุญาตและไม่อนุญาตให้เข้าพื้นที่

๑๐.๔ การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ใน การตรวจสอบหรือประเมินในภายหลัง

๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและ ปรับปรุงอุปกรณ์ดังกล่าว

๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุง รักษาอุปกรณ์ภายในหน่วยงาน

๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการ จาก ภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๑๐.๕ การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

๒) กำหนดผู้มีอำนาจในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

๔) เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงานเพื่อเอาไว้เป็น หลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๑๐.๖ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off premises)

๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน

๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๑๐.๗ การทำลายอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or Reuse of Equipment)

๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะทำลายอุปกรณ์ดังกล่าว

๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึง ข้อมูลสำคัญนั้นได้

๑๑. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๑) ผู้ใช้งาน ที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัยสวนดุสิต จะต้องทำการ ลงทะเบียนกับผู้ดูแลระบบ และต้องได้รับพิจารณาอนุญาตจากผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

๒) ต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้จะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

๓) จะต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๔) ต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสมเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์ รั่วไหลออกนอกบริเวณที่ใช้งาน เพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

๕) เลือกใช้กำลังส่งให้เหมาะสมกับพื้นที่ใช้งาน และควรสำรวจว่าสัญญาณรั่วไหลออกไปภายนอกหรือไม่ นอกจากนี้การใช้เสาอากาศพิเศษที่สามารถกำหนดทิศทางการแพร่กระจายของสัญญาณอาจช่วยลดการรั่วไหลของสัญญาณได้ดีขึ้น

๖) ต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าเริ่มต้น (Default) มาจากผู้ผลิตทันทีที่นำมาใช้งาน

๗) ผู้ดูแลระบบ ควรเปลี่ยนค่า ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบควรเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความ คาดเดาได้ยาก เพื่อป้องกันการโจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

๘) ผู้ดูแลระบบต้องกำหนดค่าความปลอดภัยของระบบเครือข่ายไร้สาย ด้วยการเข้ารหัสข้อมูลแบบ WEB หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และ AP เพื่อให้ยากต่อการดักจับจะช่วยให้ปลอดภัยมากยิ่งขึ้น

๙) เลือกใช้วิธีการควบคุม MAC Address หรือ ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มี สิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC Address หรือชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

๑๐)ควรจะมีการติดตั้งไฟร์วอล (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัยสวนดุสิต

๑๑)ผู้ดูแลระบบ ควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย

๑๒. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย

๑๒.๑ ควบคุมการติดตั้งซอฟต์แวร์ในระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑) กำหนดบุคคลที่รับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่าย (Server) ในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของโปรแกรมระบบ (System Software) อย่างชัดเจน

๒) มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบมาว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติ จะต้องนำเนินการแก้ไขรวมทั้งการมีการรายงานโดยทันที

๓) เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet FTP หรือ Ping เป็นต้น ทั้งนี้หากบริการที่จำเป็นต้องมีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๔) ติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่างๆ ของโปรแกรมระบบ (System Software) อย่างสม่ำเสมอ เช่น webserver เป็นต้น

๕) มีการทดสอบโปรแกรมระบบ (System Software) เกี่ยวกับการรักษาความปลอดภัย และ ประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

๖) การติดตั้งและเชื่อมต่อระบบคอมพิวเตอร์แม่ข่าย จะต้องดำเนินการโดยเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ หรือต้องได้รับอนุญาตจากเจ้าหน้าที่สำนักวิทยบริการและเทคโนโลยีสารสนเทศ ให้มีสิทธ์ติดตั้งระบบ

๗) ไม่ควรติดตั้งซอร์สโค้ด(Source Code), คอมไพเลอร์ (Complier) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้นๆ

๘) กำหนดให้มีการจัดเก็บซอร์สโค้ดและไลบรารี่สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๙) กำหนดให้ผู้ใช้งานหรือผู้ที่เกี่ยวข้องต้องทำการทดสอบระบบสารสนเทศตามจุดประสงค์ที่กำหนดไว้อย่างครบถ้วน เพียงพอ ก่อนดำเนินการติดตั้งบนเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ

๑๐)ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

๑๒.๒ ให้มีการทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ

๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการเพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบและทบทวนก่อนที่จะดำเนินการ เปลี่ยนแปลงระบบปฏิบัติการ

๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่หน่วยงานต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

๑๒.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอก

๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ใน การพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอก นั้น

๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

๑๒.๔ มาตรการควบคุมช่องโหว่ทางเทคนิค

๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการช่องโหว่ของระบบเหล่านั้น ให้มีการบันทึกดังต่อไปนี้

- ชื่อซอฟต์แวร์และเวอร์ชันที่ใช้งาน
- สถานที่ที่ติดตั้ง
- เครื่องที่ติดตั้ง
- ผู้ผลิตซอฟต์แวร์
- ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟแวร์นั้นๆ

๒) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสม โดย ทันที

๓) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบการดำเนินการ ดังนี้

- มีการเฝ้าระวังและติดตามประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม
- ให้กำหนดแหล่งข้อมูลข่าวสารเพื่อใช้ในการติดตามช่องโหว่ของระบบสารสนเทศของหน่วยงาน
- กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้งหรือทราบเกี่ยวกับช่องโหว่นั้น

๔) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์ อักษร

๑๒.๕ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (Audit Logging) มี การบันทึกพฤติกรรมการใช้งาน (Log) การเข้าถึงระบบสารสนเทศ ดังนี้

๑) ข้อมูลชื่อบัญชีผู้ใช้งาน
๒) ข้อมูลวันเวลาที่เข้าถึงระบบ
๓) ข้อมูลวันเวลาที่ออกจากระบบ
๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น
๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ
๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ
๗) ข้อมูลการเปลี่ยนคอนฟิกกูเรชั่น(Configuration) ของระบบ
๘) ข้อมูลแสดงการใช้งานแอพพลิเคชัน
๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์
๑๐) ข้อมูลไอพีแอดเดรส (IP Address)ที่เข้าถึง
๑๑) ข้อมูลโปรโตคอล (Protocol)เครือข่ายที่ใช้
๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์
๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

๑๓. การใช้งานระบบอินเทอร์เน็ต

๑๓.๑ กำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์ เพื่อการเข้าใช้งานอินเทอร์เน็ตที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยสวนดุสิต จัดสรรไว้เท่านั้น เช่น Proxy, Firewall, IPS-IDS เป็นต้น ห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นเช่น Dial Up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและทำการขออนุญาตจากผู้อำนวยสำนักวิทยบริการและเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร

๑๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราเซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสและทำการอุดช่องโหว่ของระบบปฏิบัติการเว็บเบราเซอร์

๑๓.๓ ผู้ใช้งาน ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยสวนดุสิต เพื่อหาประโยชน์ในเชิงธุรกิจส่วนตัว และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาที่ขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๑๓.๔ ผู้ใช้งาน จะถูกกำหนดสิทธิ์ในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัยสวนดุสิต

๑๓.๕ ผู้ใช้งานต้องไม่เผยแพร่ข้อมูลที่เป็นการหาประโยชน์ส่วนตัวข้อมูลที่ไม่เหมาะสมทางศีลธรรมข้อมูลที่ละเมิดสิทธิของผู้อื่นและข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัยสวนดุสิต

๑๓.๖ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยสวนดุสิตที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านอินเทอร์เน็ต

๑๓.๗ ผู้ใช้งานต้องไม่นำข้อมูลคอมพิวเตอร์ใดๆที่มีลักษณะอันเป็นเท็จอันเป็นความผิดที่เกี่ยวกับความมั่นคงแห่งราชอาณาจักรอันเป็นความผิดเกี่ยวกับการก่อการร้ายหรือภาพลักษณ์ที่มีลักษณะอันลามกและไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวทางอินเทอร์เน็ต

๑๓.๘ ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและนำภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใดทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๓.๙ ผู้ใช้ไม่นำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่นและนำภาพนั้นซึ่งเป็นภาพที่เกิดจากการสร้างขึ้นตัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้จะทำให้ผู้อื่นนั้นเสียชื่อเสียงถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๓.๑๐ ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

๑๓.๑๑ ผู้ใช้งานต้องระมัดระวังการดาวโหลดโปรแกรมใช้งานจากอินเทอร์เน็ตซึ่งรวมถึง Patch หรือ Fixes ต่างๆ การดาวน์โหลดทุกประเภทต้องเป็นไปโดยไม่ละเมิดทรัพย์สินทางปัญญา

๑๓.๑๒ ในการเสนอความคิดเห็นผู้ใช้ต้องไม่ใช้ข้อความที่ยั่วยุให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัยสวนดุสิต รวมถึงการทำลายความสัมพันธ์กับเจ้าหน้าที่ของหน่วยงานอื่นๆ

๑๓.๑๓ หลังจากใช้งานอินเทอร์เน็ตแล้วให้ทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๑๔. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๔.๑ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้ เท่านั้น

๑๔.๒ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ต้องมีความตระหนักเรื่องความมั่นคงปลอดภัย อยู่เสมอ และต้องรับผิดชอบหากเกิดความเสียหายใดๆ ที่มีผลกระทบกับมหาวิทยาลัยจากการใช้งาน เครือข่ายสังคมออนไลน์

๑๔.๓ ไม่อนุญาตให้ใช้เครือข่ายสังคมออนไลน์เพื่อเผยแพร่ข้อมูลที่เป็นความลับ และมีผลกระทบด้านชื่อเสียงต่อบุคคลอื่น

๑๔.๔ ใช้งานเครือข่ายสังคมออนไลน์เท่าที่จำเป็นเท่านั้น และไม่มีผลกระทบต่องานประจำที่ ทำอยู่

๑๔.๕ หากเกิดปัญหาจากการใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานต้องแจ้งต่อสำนักวิทยบริการและเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๑๕. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๕.๑ ผู้ดูแลระบบ ต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

๑๕.๒ เจ้าของข้อมูล จะต้องมีการสอบทานความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่างๆ ที่ให้ไว้ยังคงมีความเหมาะสม

๑๕.๓ วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรง และการเข้าถึงรหัสผ่านระบบงานผู้ดูแลระบบ ต้องมีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๑๕.๔ การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑๕.๕ มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของมหาวิทยาลัย เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๑๖. ต้องทบทวนปรับปรุงแนวนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง โดยให้ครอบคุมเนื้อหา ดังนี้

๑๖.๑. มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑) การเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)

๒) การการเข้าถึงของผู้ใช้งาน (User Access Management)

๓) หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๔) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๕) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๖) การควบคุมการเข้าถึงโปรแกรมประยุกต์ หรือแอพพลิเคชั่น และสารสนเทศ (Application and Information Access Control)

๗) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๘) การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๙) การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย

๑๐) การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

๑๑) การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ

๑๒) การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (e-mail)

๑๓) การใช้งานระบบอินเทอร์เน็ต (Internet)

๑๔) การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๑๕) การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Log)

๑๖.๒ ระบบสารสนเทศและระบบสำรองของสารสนเทศ และแผนเตรียมความพร้อมกรณีฉุกเฉิน

๑๖.๓ แผนประเมินความเสี่ยงด้านสารสนเทศ

ส่วนที่ ๒
นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยให้บริการได้อย่างต่อเนื่อง

๒. เพื่อเป็นมาตรฐาน แนวทางปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับหน่วยงาน เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิต

๒. ผู้ดูแลระบบที่ได้รับมอบหมายจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. มหาวิทยาลัยจะต้องจัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูลที่หน่วยงานนั้นรับผิดชอบ เป็นประจำทุกปี

๒. ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๓. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๔. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๕. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๖. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เป็นประจำทุกปี

แนวปฏิบัติ

๑. ผู้รับผิดชอบระบบสารสนเทศทุกระบบภายในมหาวิทยาลัย ต้องจัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล โดยจัดระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๑.๑ มีการจัดทำบัญชีระบบสารสนเทศที่สำคัญของหน่วยงาน ได้แก่ ระบบบริหารการศึกษา ระบบบริหารบุคลากร ระบบบริหารการเงิน ระบบบริหารงานวิจัย ระบบสำนักงานอิเล็กทรอนิกส์ พร้อมจัดทำระบบสำรอง โดยมีวิธีดำเนินการดังนี้

ระบบ	ข้อมูลที่จัดเก็บ	ความถี่ : ข้อมูลที่มีส่วนต่าง Incremental backup	ความถี่: สำรองแบบเต็ม Full Backup
๑.ระบบบริหารการศึกษา	-File system -data	รายวัน	ทุกวันอาทิตย์
๒.ระบบบริหารงานบุคคล	-File system -data	รายวัน	ทุกวันอาทิตย์
๓.ระบบบริหารการเงิน	-File system -data	รายวัน	ทุกวันอาทิตย์
๔.ระบบบริหารงานวิจัย	-File system -data	รายวัน	ทุกวันอาทิตย์
๕.ระบบสำนักงานอิเล็กทรอนิกส์	-File system -data	รายวัน	ทุกวันอาทิตย์

๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) สัปดาห์ละครั้ง และการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup) แบบรายวัน
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน ได้แก่ ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลการตั้งค่า (Configuration) ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน

- ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่
- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ
- กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

๒. มีแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอัตโนมัติ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามแนวทางต่อไปนี้

๒.๑ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอัตโนมัติ โดยมีรายละเอียดอย่างน้อย ดังนี้

- มีการกำหนดหน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด
- มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการ เพื่อลดความเสี่ยงเหล่านั้น
- มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ
- มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลที่สำรองไว้
- มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ
- การสร้างความตระหนัก หรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติ หรือ สิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

๒.๒ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง ด้านเทคโนโลยีสารสนเทศ

บุคลากรหลัก		บุคลากรสำรอง		บทบาท
ชื่อ	เบอร์โทรศัพท์	ชื่อ	เบอร์โทรศัพท์	
ดร.สวงค์ บุญปลูก (รองอธิการบดีฝ่ายเทคโนโลยีสารสนเทศ) **นายวีระพันธ์ ชมภูแดง** (ผู้อำนวยการสำนักวิทยบริการและเทคโนโลยีสารสนเทศ)	๐๙๖-๔๕๔-๕๙๙๑	**นางสาวทิพสุดา คิดเลิศ** (รองผู้อำนวยการสำนักวิทยบริการฯ) **นายธีรบุญ เดชอุดม** (ผู้ช่วยผู้อำนวยการสำนักวิทยบริการฯ)	๐๘๑-๖๓๓-๑๔๘๕ ๐๘๑-๓๒๗-๔๕๗๔	หัวหน้าคณะบริหารความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ
นางจำนรรจา พลอยมุกดา	๐๘๖-๔๐๓-๑๙๕๙	นายไพฑูรย์ นามเสนา นายณัฐกานต์ พงธิพันธ์	๐๘๑-๒๘๕-๗๒๖๒ ๐๘๔-๐๐๔-๒๕๕๔	หัวหน้าทีมงานบริหารความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ(ระบบเครือข่ายอินเทอร์เน็ต)
นายสถิตย์ เชิดฉันท์	๐๘๔-๐๗๔-๗๑๙๔	นายวิทวัส ทองยศ	๐๘๗-๓๘๔-๓๒๑๑	หัวหน้าทีมงานบริหารความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ (ระบบสารสนเทศ)
นายสนธยา แย้มเดช นายชัชวาลย์ ลาภเกิน	๐๘๗-๘๗๘-๐๗๔๕ ๐๘๙-๔๕๓-๗๑๔๐	นายกษินันท์ ก.ศรีสุวรรณ นายปภาวิน ปัญญาใส	๐๘๑-๒๐๗-๓๒๓๗ ๐๙๕-๗๐๙-๖๓๖๙	หัวหน้าทีมงานบริหารความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ (ศูนย์ข้อมูลกลาง)
นายจักร ชมภูนุช	๐๘๑-๙๒๒-๖๙๒๖	นายสุทัศน์ รุ่งเรือง	๐๘๙-๙๑๖-๔๔๘๙	หัวหน้าทีมงานบริหารความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ (งานช่างเทคนิค)
นส.ธันยมัย กลุ่นเขียว	๐๘๑-๓๔๔-๗๔๕๘	นส.ชัยญามล เลิศสงคราม นส.มลธิรา โพธิ์น้อย	๐๘๔-๘๙๙-๐๙๘๙ ๐๘๑-๗๕๒-๔๗๑๙	ผู้ประสานงานคณะกรรมการดำเนินงานเตรียมความพร้อมฉุกเฉินและแผนสำรองด้านเทคโนโลยีสารสนเทศ

๒.๓ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๒.๔ มีการทบทวนเพื่อปรับปรุงแผน ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔
นโยบายการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้กับผู้ใช้งานของมหาวิทยาลัย

๒. เพื่อเป็นการป้องกันการกระทำผิดที่เกิดจากการรู้เท่าไม่ถึงการณ์ของผู้ใช้

๓. เพื่อให้การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. กลุ่มงานระบบสารสนเทศและระบบเครือข่าย สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิต

๒. ผู้ดูแลระบบที่ได้รับมอบหมายจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. จัดทำแผนการฝึกอบรมทางด้านการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ สำหรับผู้ใช้งาน

๒. จัดทำคู่มือการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ของมหาวิทยาลัยทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์

๓. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของมหาวิทยาลัย เมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๔. มีการประเมินระดับความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ใช้งาน

๕. รายงานผลการประเมินระดับความรู้ความเข้าใจในการใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ของผู้ใช้งานต่อผู้บริหารระดับสูง

๖. นำผลการประเมินไปปรับปรุงแผนการการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ สาหรับผู้ใช้งานต่อไป

แนวปฏิบัติ

๑. จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของแต่ละหน่วยงาน เมื่อมีการปรับปรุงและเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๒. จัดให้มีการทบทวนการใช้งานระบบสารสนเทศของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๓. จัดทำคู่มือและแนวปฏิบัติงานระบบสารสนเทศของแต่ละหน่วยงานทั้งในรูปแบบเอกสารและรูปแบบอิเล็กทรอนิกส์

๔. มีการเผยแพร่นโยบายและแนวปฏิบัติในการใช้ระบบสารสนเทศ ระบบคอมพิวเตอร์ และนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ

หน่วยงาน: สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิต

โครงการ: การส่งเสริมและความเข้าใจในการรักษาความปลอดภัยบนโลกอินเทอร์เน็ต สำหรับอาจารย์ เจ้าหน้าที่ นักศึกษา มหาวิทยาลัยสวนดุสิต

หลักการและเหตุผล:

ปัจจุบันเทคโนโลยีสารสนเทศและการสื่อสารมีการพัฒนาก้าวหน้าอย่างรวดเร็ว และได้เข้ามาเป็นส่วนหนึ่งในชีวิตประจำวันของทุกคนรวมถึงอาจารย์ เจ้าหน้าที่ มหาวิทยาลัยสวนดุสิต โดยไม่สามารถหลีกเลี่ยงได้ เพราะต้องใช้เทคโนโลยีเหล่านั้นเป็นส่วนหนึ่งในการทำงาน สำหรับการสื่อสารทั้งภาพ เสียง สื่อมัลติมีเดียต่างๆ และการทำธุรกรรมสามารถดำเนินการรับส่งผ่านระบบเครือข่ายได้อย่างรวดเร็ว แต่ถึงอย่างไรก็ตามการใช้เทคโนโลยีนั้นมีคุณอนันต์แต่ก็มีโทษมหันต์เช่นเดียวกัน หากผู้ใช้รู้ไม่เท่าทันอันตรายที่กิดจากการใช้งานงานผ่านอุปกรณ์ต่างๆ โดยเฉพาะอุปกรณ์ประเภทโมบาย

ด้วยเหตุนี้ทางสำนักวิทยบริการและเทคโนโลยีสารสนเทศได้ตระหนักถึงความสำคัญและเล็งเห็นประโยชน์ที่จะจัดอบรมเพื่อให้ความรู้ อาจารย์ เจ้าหน้าที่ มหาวิทยาลัยสวนดุสิต ได้รู้เท่าทันเพื่อป้องกันอันตรายที่จะเกิดขึ้นแก่ชื่อเสียง หรือทรัพย์สิน

วัตถุประสงค์โครงการ:

๑. เพื่อให้อาจารย์ เจ้าหน้าที่ นักศึกษาได้ทราบถึงเทคโนโลยีที่เป็นปัจจุบันพร้อมสามารถนำไปใช้ในชีวิตประจำวันวันทั้งการทำงานและการเรียนให้ได้มากที่สุด
๒. เพื่อให้อาจารย์ เจ้าหน้าที่ นักศึกษาได้ตระหนักถึงความปลอดภัยในการใช้งานเทคโนโลยี ที่เกี่ยวข้องกับชีวิตประจำวันจากการใช้งานอุปกรณ์ประเภทโมบายให้มากขึ้น

ตัวชี้วัดความสำเร็จของโครงการ:

๑. ผู้เข้ารับการอบรมมีความเข้าใจในเทคโนโลยีที่สามารถนำไปใช้ในชีวิตประจำวันวันทั้งการทำงานและการเรียนไม่น้อยกว่าร้อยละ ๗๐
๒. ผู้เข้ารับการอบรมต้องมีความเข้าใจในความปลอดภัยในการใช้งานเทคโนโลยี และสามารถนำไปใช้งานได้จริงไม่น้อยกว่าร้อยละ ๕๐

ผู้รับผิดชอบโครงการ:

ผู้สนับสนุน/แหล่งเงินทุน	มหาวิทยาลัยสวนดุสิต
ผู้รับผิดชอบโครงการ	สำนักวิทยบริการและเทคโนโลยีสารสนเทศ
คณะทำงานโครงการ	๑. ฝ่ายเทคโนโลยีสารสนเทศและคอมพิวเตอร์ ๒. ฝ่ายสำนักงานผู้อำนวยการฯ ๓. ฝ่ายพัฒนาระบบการเรียนรู้ ๔. ฝ่ายศูนย์ข้อมูลกลาง

กลุ่มเป้าหมาย:

๑. บุคลากรมหาวิทยาลัยสวนดุสิต จำนวน ๑๐๐ คน
๒. นักศึกษาทุกหลักสูตร จำนวน ๑๐๐ คน

กิจกรรมดำเนินการ: ระหว่างเดือนกรกฎาคมถึงกันยายน

กิจกรรมสำคัญในการดำเนินการ	ตัวชี้วัดความสำเร็จของกิจกรรม	ระยะเวลาสถานที่ดำเนินการ	ผู้รับผิดชอบ/บทบาทความรับผิดชอบ
๑. อบรมการใช้อินเทอร์เน็ตผ่านสมาร์ทโฟนหรือแท็บเล็ตให้ปลอดภัย	๑. ร้อยละความพึงพอใจของนักศึกษาที่มีต่อการอบรมการใช้อินเทอร์เน็ตผ่านสมาร์ทโฟนหรือแท็บเล็ตให้ปลอดภัยไม่ต่ำกว่า ๗๐ ๒. ร้อยละความพึงพอใจของบุคลากรที่มีต่อการอบรมการใช้อินเทอร์เน็ตผ่านสมาร์ทโฟนหรือแท็บเล็ตให้ปลอดภัยไม่ต่ำกว่า ๗๐	สิงหาคม-กันยายน ห้องปฏิบัติการคอมพิวเตอร์ ๑๑๒๐๑	สำนักวิทยบริการฯ
๒. อบรมการระวังอันตรายเรื่องข้อมูลส่วนตัวในการใช้งานอินเทอร์เน็ต	๑. ร้อยละความพึงพอใจของนักศึกษาที่มีต่อการอบรมการระวังอันตรายเรื่องข้อมูลส่วนตัวในการใช้งานอินเทอร์เน็ตไม่ต่ำกว่า ๗๐	สิงหาคม-กันยายน ห้องประชุมปิ่นน้อย อาคารวิทยบริการ ชั้น ๔	สำนักวิทยบริการฯ

กิจกรรมสำคัญในการดำเนินการ	ตัวชี้วัดความสำเร็จของกิจกรรม	ระยะเวลาสถานที่ดำเนินการ	ผู้รับผิดชอบ/บทบาทความรับผิดชอบ
	๒.ร้อยละความพึงพอใจของบุคลากรที่มีต่อการอบรมการระวังอันตรายเรื่องข้อมูลส่วนตัวในการใช้งานอินเทอร์เน็ตไม่ต่ำกว่า ๗๐		
๓. อบรมการรู้เท่าทันและระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ จากการใช้งานอินเทอร์เน็ต	๑.ร้อยละความพึงพอใจของนักศึกษาที่มีต่อการอบรมการรู้เท่าทันและระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ จากการใช้งานอินเทอร์เน็ตไม่ต่ำกว่า ๗๐ ๒.ร้อยละความพึงพอใจของบุคลากรที่มีต่อการอบรมการรู้เท่าทันและระวังอันตรายจากการหลอกลวงรูปแบบต่างๆ จากการใช้งานอินเทอร์เน็ตไม่ต่ำกว่า ๗๐	สิงหาคม-กันยายน ห้องประชุมปิ่นน้อย อาคารวิทยบริการ ชั้น ๔	สำนักวิทยบริการฯ

งบประมาณ: ๑๐๐,๐๐๐ บาท (หนึ่งแสนบาทถ้วน)

ความสอดคล้องกับแผนต่างๆ ของมหาวิทยาลัย

๑. ยุทธศาสตร์ที่ ๔ แผนกลยุทธ์มหาวิทยาลัยปี ๒๕๕๗-๒๕๖๐ ฉบับปรับปรุง ๒๕๕๘
๒. การปรับยุทธศาสตร์ มหาวิทยาลัยสวนดุสิต Suan Dusit University Reprofiling Update ๒๓ มกราคม ๒๕๖๐

ความสอดคล้องกับตัวชี้วัด/ตัวบ่งชี้กับเกณฑ์มาตราฐาน

๑. ตัวบ่งชี้ ๖.๑ สิ่งสนับสนุนการเรียนรู้ (สำนักงานคณะกรรมการการอุดมศึกษา)

ผลที่คาดว่าจะได้รับ

๑. อาจารย์ เจ้าหน้าที่ นักศึกษา มหาวิทยาลัยสวนดุสิต มีความรู้ความเข้าใจในเทคโนโลยีสารสนเทศและสามารถถ่ายทอดไปยังบุคคลอื่นได้

๒. อาจารย์ เจ้าหน้าที่ นักศึกษา มหาวิทยาลัยสวนดุสิต สามารถป้องการอันตรายอาจจะเกิดขึ้นจากการใช้เทคโนโลยีจากอุปกรณ์ประเภทโมบายได้เบื้องต้น

๓. อาจารย์ เจ้าหน้าที่ นักศึกษา มหาวิทยาลัยสวนดุสิต มีความระมัดระวังในข้อมูลส่วนตัวจากการใช้งานอินเทอร์เน็ต

๔. อาจารย์ เจ้าหน้าที่ นักศึกษา มหาวิทยาลัยสวนดุสิต รู้เท่าทันการหลอกลวงในรูปแบบต่างๆ ที่เป็นภัยอันตรายจากการใช้งานอินเทอร์เน็ต

ความเสี่ยงที่สำคัญ

ความเสี่ยงที่สำคัญ	แนวทางบริหารความเสี่ยง
๑. ผู้เข้ารับการอบรมไม่สามารถเข้าร่วมตามเป้าหมายที่ตั้งไว้	๑.๑ ประชาสัมพันธ์ผ่านช่องทางที่กลุ่มเป้าหมายสามารถเข้าถึงได้ง่าย ได้แก่ วิทยุกระจายเสียง จดหมายข่าว โทรศัพท์สายตรง เป็นต้น ๑.๒ ให้หน่วยงานแจ้งรายชื่อผู้เข้ารับการอบรมผ่านทางใบตอบรับพร้อมระบุหมายเลขโทรศัพท์เพื่อยืนยันในการเข้าร่วมโครงการ
๒. กลุ่มเป้าหมายได้รับความรู้ไม่ครบถ้วนหลังจากที่เข้ารับการอบรม	๒.๑ แจกเอกสารประกอบการอบรมหรือแจ้งลิงค์ให้ดาวโหลดเอกสาร เพื่อให้ผู้เข้าร่วมอบรมสามารถจัดเก็บและอ่านย้อนหลังได้

ความคุ้มค่าในการดำเนินโครงการ

๑. มหาวิทยาลัยมีบุคลกรที่มีความรู้ความเข้าใจในเทคโนโลยีสารสนเทศและการสื่อสารอย่างดีเยี่ยมและสามารถนำความรู้ที่ได้รับไปต่อยอดเพื่อสนับสนุนในการเรียนการสอนและการปฏิบัติงานได้

๒. มหาวิทยาลัยสามารถให้บริการอินเทอร์เน็ตได้อย่างมีประสิทธิภาพเนื่องจากอุปกรณ์ที่ใช้งานภายใต้เครือข่ายของมหาวิทยาลัยมีความปลอดภัยจากอันตรายที่เกิดขึ้นจากการใช้อินเทอร์เน็ต เช่น อุปกรณ์ไม่ติดไวรัสและป้องกันการติดไวรัสทั้งระบบเครือข่ายของมหาวิทยาลัยได้

วิธีการสื่อสารกับผู้มีส่วนได้ส่วนเสีย

<u>การสื่อสารกับกลุ่มเป้าหมาย</u>

๑. ประชาสัมพันธ์การอบรมสัมมนาผ่านทางช่องทางวิทยุกระจายเสียง จดหมายข่าว โทรศัพท์สายตรง งานสารบรรณอิเล็กทรอนิกส์ ตู้ให้บริการอัตโนมัติ (ตู้ KIOSK) โปสเตอร์โครงการเกี่ยวกับกำหนดการอบรมสัมมนา

๒. จัดบริการตอบคำถามสายตรงเกี่ยวกับการใช้ฐานข้อมูลและ ICT ของมหาวิทยาลัย

<u>การสื่อสารกับกลุ่มผู้ดำเนินงาน</u>

๑. จัดประชุมชี้แจงคณะกรรมการดำเนินงานเกี่ยวกับรูปแบบการจัดอบรมสัมมนา

๒. ประสานงานระหว่างการดำเนินงานด้วยโทรศัพท์ ประชุมกลุ่ม และสื่อสังคมออนไลน์

ส่วนที่ ๔
นโยบายแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร(IT Contingency Plan)

วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ขององค์กร

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๔. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๕. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ขององค์กร

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์

นโยบาย

๑. มหาวิทยาลัยจะต้องจัดทำแนวปฏิบัติสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร(IT Contingency Plan)

๒. มหาวิทยาลัยจะต้องวิเคราะห์ วางแผนสถานการณ์ฉุกเฉินจากภัยพิบัติ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓. ต้องมีการกำหนดหน้าที่และผู้รับผิดชอบในการจัดการสถานการณ์ฉุกเฉิน และสรุปการดำเนินงานต่อมหาวิทยาลัย

๔. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๕. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากร ซึ่งทำหน้าที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๖. ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๗. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เป็นประจำทุกปี

แผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ อันอาจมีผลกระทบต่อ ระบบเทคโนโลยีสารสนเทศและการสื่อสาร (IT Contingency Plan)

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศ ถือเป็นทรัพย์สินทางการบริหารที่มีความสำคัญต่อทางราชการ จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนพัฒนาองค์กร การบริหารจัดการองค์กร และการปฏิบัติงานของบุคลากรในหน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิตได้ตระหนักถึงความสำคัญของระบบเทคโนโลยีสารสนเทศขององค์กร ซึ่งอาจมีปัจจัยจากภายนอกและปัจจัยภายในมากระทบทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งระบบอุปกรณ์ต่างๆ เสียหายได้

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิต จึงได้จัดทำแผนรับสถานการณ์ฉุกเฉินจากภัยพิบัติ อันอาจมีผลกระทบต่อระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัยสวนดุสิต เพื่อเป็นกรอบแนวทางในการดูแลรักษาระบบ และแก้ไขปัญหาที่อาจจะส่งผลกระทบต่อระบบเทคโนโลยีสารสนเทศรวมถึงระบบอุปกรณ์ต่างๆ

๒. วัตถุประสงค์

๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติ ในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ขององค์กร

๒. เพื่อลดความเสียหายที่อาจจะเกิดแก่ระบบเทคโนโลยีสารสนเทศ

๓. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศขององค์กร ให้มีเสถียรภาพและมีความพร้อมสำหรับการใช้งาน

๔. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่องและมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๕. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ ขององค์กร

๓. ภัยพิบัติ

ภัยพิบัติที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศมหาวิทยาลัยสวนดุสิต สามารถจำแนกได้เป็นสองกลุ่มหลักๆ ได้แก่

๓.๑ ภัยพิบัติจากภายนอก

๑) ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย ได้แก่ ภัยพิบัติ อัคคีภัย อุทกภัย ความชื้น อุณหภูมิ แมลงกัดแทะ เป็นต้น

๒) การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓) ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง

๔) ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

๕) การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหาย หรือทำลายระบบข้อมูล

๖) ไวรัสคอมพิวเตอร์

๓.๒ ภัยพิบัติจากภายใน

๑) ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

๒) ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

๓) เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้ หรือหยุดการทำงาน

๔. แนวทางการจัดการภัยพิบัติ

๔.๑ ภัยพิบัติจากภายนอก

๔.๑.๑ ภัยธรรมชาติและการเกิดสถานการณ์ความไม่สงบที่กระทำต่ออาคารสถานที่ตั้งของเครื่องประมวลผลหลัก หรือเครื่องแม่ข่าย

๔.๑.๑.๑ การป้องกันอัคคีภัย การดำเนินการ ดังนี้

๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนต่างๆ

๒) อบรมขั้นต้นสำหรับพนักงานทุกคนในแผนป้องกันและระงับอัคคีภัย และมีการซ้อมดับเพลิงการหนีไฟ

๓) ติดตั้งเครื่องดับเพลิงสำหรับอุปกรณ์อิเล็กทรอนิกส์สำหรับห้องคอมพิวเตอร์แม่ข่าย

๔) จัดทำเครื่องหมายระบุความสำคัญตามลำดับของอุปกรณ์คอมพิวเตอร์แม่ข่าย เพื่อประสิทธิภาพในการเคลื่อนย้ายเมื่อเกิดเหตุฉุกเฉิน

๔.๑.๑.๒ การป้องกันอุทกภัยและการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม การดำเนินการ ดังนี้

๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น สำหรับเครื่องแม่ข่ายตลอด ๒๔ ชั่วโมง และตรวจสอบการทำงานให้ใช้งานได้อย่างสม่ำเสมอ

๒) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๓) เครื่องคอมพิวเตอร์แม่ข่ายต้องไม่อยู่ในบริเวณที่น้ำท่วมถึง

๔.๑.๒ การโจรกรรมอุปกรณ์คอมพิวเตอร์แม่ข่ายที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

การดำเนินการ

๑) ควบคุมการเข้าออกห้องคอมพิวเตอร์แม่ข่ายและการป้องกันความเสียหาย โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในห้องคอมพิวเตอร์แม่ข่าย หากจำเป็นให้มีเจ้าหน้าที่ของฝ่ายเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำเข้าไป

๒) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น เครื่องตรวจสอบลายนิ้วมือ (Finger Scan) และมีการตรวจสอบการทางานของระบบให้ใช้งานได้อยู่เสมอ

๓) ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๑.๓ ระบบการสื่อสารของเครื่องแม่ข่ายที่เชื่อมต่อระบบอินเทอร์เน็ตเกิดความขัดข้อง

การดำเนินการ

๑) การตรวจสอบระบบเครือข่ายทั้งภายในและภายนอกอาคารให้สามารถใช้งานได้ตลอดเวลา

๒) ต้องจัดให้มีเครือข่ายสำรอง สำหรับใช้ในกรณีที่เครื่องแม่ข่ายหลักไม่สามารถใช้งานได้

๔.๑.๔ ระบบกระแสไฟฟ้าขัดข้อง / ไฟฟ้าดับ

การดำเนินการ

๑) แยกไฟระบบคอมพิวเตอร์แม่ข่ายออกจากสายไฟหลักที่ผ่านสะพานไฟเข้าสู่หน่วยงาน

๒) ติดตั้งเครื่องสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ (UPS) เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์หรือการประมวลผลของระบบคอมพิวเตอร์ ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย (Server) และเครื่องคอมพิวเตอร์ส่วนบุคคล (PC) ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

๓) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานเสมอ ตรวจสอบระบบสำรองไฟฟ้าทุกวันศุกร์

๔) เมื่อเกิดกระแสไฟฟ้าดับ ให้ผู้ใช้บันทึกข้อมูลที่ยังค้างอยู่ทันที และปิดเครื่องคอมพิวเตอร์รวมทั้งอุปกรณ์ต่างๆ

๔.๑.๕ การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศรวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

การดำเนินการ

๑) สแกนหาจุดอ่อนและอัพเดท Patch เพื่อปิดกั้นช่องโหว่และจุดอ่อน โดยใช้ซอฟต์แวร์เพื่อเป็นเครื่องมือในการค้นหาช่องโหว่

๒) ติดตั้ง Firewall เพื่อป้องกันผู้ที่มิได้รับอนุญาตจากระบบเครือข่ายอินเทอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบเทคโนโลยีสารสนเทศ และเครือข่ายคอมพิวเตอร์ขององค์กรได้ โดยจะต้องเปิดใช้งาน Firewall ตลอดเวลา

๓) ติดตั้ง Proxy Server เพื่อเพิ่มประสิทธิภาพในการให้บริการอินเทอร์เน็ตขององค์กรและกลั่นกรองข้อมูลที่มาทาง website ซึ่งจะมีการกำหนดค่า Configuration ให้มีความปลอดภัยต่อระบบเทคโนโลยีสารสนเทศและเครือข่ายคอมพิวเตอร์

๔) จัดเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือการเรียกใช้ ระบบเทคโนโลยีสารสนเทศ มีความถี่ในการเรียกใช้ผิดปกติ เพื่อจะได้สรุปหาสาเหตุ และป้องกันต่อไป

๕) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และอัพเดทอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่มีการใช้งาน

๖) กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติดังนี้

- ตั้งรหัสผ่านที่ยากต่อการเดาโดยผู้อื่น
- ไม่เปิดเผยรหัสผ่านของตนเองแก่ผู้อื่น
- จัดเก็บรหัสผ่านไว้ในสถานที่ที่มีความปลอดภัย
- เปลี่ยนรหัสผ่านโดยทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น
- ตั้งรหัสผ่านที่มีความยาวขั้นต่ำอย่างน้อย ๘ อักขระ
- ตั้งรหัสผ่านโดยใช้เทคนิคส่วนตัวที่ง่ายต่อการจำรหัสผ่านที่ได้กำหนดไว้
- ไม่ตั้งรหัสผ่านจากคำที่ปรากฏในพจนานุกรม
- ไม่ตั้งรหัสผ่านที่ประกอบด้วยอักขระที่เรียงกัน เช่น ๑๒๓, abcd เป็นต้น หรือเป็นกลุ่มของตัวอักขระที่เหมือนกัน เช่น ๑๑๑๑๑, aaa, bbb เป็นต้น
- เปลี่ยนรหัสผ่านใหม่ตามรอบระยะเวลาที่กำหนดไว้ เช่น ทุก ๆ ๖ เดือน ส่วนในกรณีของผู้ดูแลระบบ ให้เปลี่ยนรหัสผ่านใหม่ด้วยความถี่ที่มากกว่าผู้ใช้งานทั่วไป เช่น ทุก ๆ ๓ เดือน เป็นต้น
- เปลี่ยนรหัสผ่านโดยหลีกเลี่ยงการใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว
- เปลี่ยนรหัสผ่านชั่วคราวที่ได้รับโดยทันทีครั้งแรกที่ทำการล็อกอินเข้าสู่ระบบงาน

- ไม่ให้ระบบงานทำการบันทึกหรือจดจำรหัสผ่านของตนเองไว้ เช่น บันทึกไว้ในหน้าจอล็อกอิน (ทั้งนี้เพื่อความสะดวกของตนเองเมื่อทำการล็อกอินในภายหลังจะได้ไม่ต้องใส่รหัสผ่านอีกครั้ง)
- ไม่ใช้รหัสผ่านของตนเองร่วมกับผู้อื่น
- หลีกเลี่ยงการใช้รหัสผ่านเดียวกันสำหรับระบบงานต่าง ๆ ที่ตนใช้งาน
- ป้องกันการปลอมแปลง IP address โดยการกรอง packet ที่มาจากภายนอกโดยการนำระบบ DMZ มากรอง IP ที่จะเข้ามายังระบบเครือข่าย
- ติดตั้งระบบให้อุปกรณ์เครือข่ายสามารถป้องกันการโจมตีแบบ DOS และ DDOS

๔.๑.๖ ไวรัสคอมพิวเตอร์

การดำเนินการ

๑) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละหนึ่งครั้ง

๒) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

- สแกนหาไวรัสจากสื่อบันทึกข้อมูลก่อนใช้งานทุกครั้ง
- ไม่ควรเปิดไฟล์ที่มีนามสกุลแปลกปลอม หรือน่าสงสัย
- ไม่ใช้สื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มา

๓) ใช้ความระมัดระวังในการเปิด e-Mail

- ไม่เปิดไฟล์ e-Mail ถ้าไม่ทราบแหล่งที่มา
- ลบ e-Mail ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

๔) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

- ไม่ควรเปิดไฟล์ที่ไม่รู้จัก ที่แนบมากับโปรแกรมสนทนาต่างๆ
- ไม่ควรเปิด website ที่แนะนำมาทาง e-Mail
- ไม่ดาวน์โหลดไฟล์จาก website ที่ไม่น่าเชื่อถือ
- ติดตามข้อมูลการแจ้งเตือนการโจมตีของไวรัสต่างๆ อย่างสม่ำเสมอ
- หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔.๒ ภัยพิบัติจากภายใน

๔.๒.๑ ระบบแม่ข่ายหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

การดำเนินการ

๑) การสำรองข้อมูลอัตโนมัติ โดยระบบเครื่องประมวลผลแม่ข่ายจะสำรองข้อมูลไว้ในสื่อบันทึกข้อมูลทุกวัน

๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กาหนดทุกสัปดาห์ โดยจะสำรองข้อมูล โครงสร้างข้อมูล Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๓) ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึก ทุกสัปดาห์

๔) ทดสอบ Recovery ฐานข้อมูลและโปรแกรมปฏิบัติการฐานข้อมูล และระบบปฏิบัติการของเครื่องแม่ข่ายสำรองที่ได้สำรองไว้ เพื่อทดสอบระบบการทำงานเมื่อเครื่องแม่ข่ายหลักเสียหาย

๕) จัดเจ้าหน้าที่ในการบำรุงรักษาสื่อบันทึกข้อมูลของเครื่องคอมพิวเตอร์แม่ข่าย เพื่อลดความเสียหายของข้อมูล

๔.๒.๒ ไวรัสคอมพิวเตอร์จากผู้ใช้งานภายในองค์กร

การดำเนินการ

๑) ติดตั้งโปรแกรมป้องกันไวรัสที่เครื่องแม่ข่ายและลูกข่ายเพื่อให้สามารถตรวจสอบได้

๒) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ

๓) หลีกเลี่ยงการแชร์ไฟล์โดยไม่จำเป็น

๔.๒.๓ เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในการใช้เครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้านฮาร์ดแวร์ และซอฟต์แวร์ อันอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหาย ใช้งานไม่ได้หรือหยุดการทำงานการดำเนินการ

๑) ให้ความรู้แก่บุคลากรและหน่วยงานผ่านช่องทางต่างๆ เช่น website, หนังสือเวียน เป็นต้น

๒) ใส่กุญแจตู้อุปกรณ์เครือข่าย เพื่อป้องกันการเชื่อมต่อโดยเจ้าหน้าที่ หรือบุคลากรที่ไม่มีหน้าที่โดยตรง (Unauthorized Personals)

๕. ขั้นตอนปฏิบัติในมาตรการที่สำคัญ

๕.๑ การสำรองข้อมูล (Back Up)

๑) การสำรองข้อมูลอัตโนมัติโดยระบบเครื่องประมวลผลแม่ข่ายโดยสำรองข้อมูลไว้ในสื่อบันทึก ๑ ชุด

๒) การสำรองข้อมูลด้วยระบบ Manual โดยกำหนดให้เจ้าหน้าที่สำรองข้อมูลตามระยะเวลาที่กำหนดเป็นประจำทุกสัปดาห์ โดยสำรองข้อมูล โครงสร้างข้อมูล และ Source Code และบันทึกข้อมูลลงในสื่อบันทึก

๕.๒ การกู้ข้อมูล (Recovery)

๑) ทดสอบ Recovery ข้อมูล โครงสร้าง และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึกข้อมูล

๒) ทดสอบ Recovery ฐานข้อมูล และโปรแกรมปฏิบัติการฐานข้อมูล ที่ได้สำรองไว้ในสื่อบันทึกข้อมูล

๖. ข้อปฏิบัติในการแก้ไขปัญหาจากภัยพิบัติ

๖.๑กรณีเครื่องลูกข่าย

๑) ในกรณีที่มีเหตุทำให้เครื่องคอมพิวเตอร์ไม่สามารถดำเนินการให้งานระบบเทคโนโลยีสารสนเทศได้ตามปกติ ให้เจ้าหน้าที่ผู้นั้นแจ้งเหตุให้เจ้าหน้าที่ผู้เกี่ยวข้อง หรือผู้ดูแลทราบ หรือกรณีมีเหตุอันทำให้เจ้าหน้าที่ผู้เกี่ยวข้องไม่สามารถดำเนินการให้บริการด้านเครือข่ายได้ จะต้องประกาศให้ทุกหน่วยงานในสังกัดทราบ

๒) กรณีเกิดการขัดข้องเนื่องจากติดไวรัสคอมพิวเตอร์เพื่อป้องกันความเสียหายที่จะแพร่กระจายไปยังเครื่องคอมพิวเตอร์อื่นๆ ในระบบเครือข่าย ให้ปลดสายเชื่อมโยงระบบเครือข่าย (LAN) ออกจากเครื่องโดยทันที

๓) ในกรณีที่เกรงว่าเหตุที่เกิดขึ้น จะเป็นอันตรายต่อหน่วยงานภายในอาคารที่ตั้งของเครื่องคอมพิวเตอร์ที่พบการขัดข้อง ให้ปลดสาย LAN ออกจากจุดชุมสายในชั้นนั้นออก

๔) ให้เจ้าหน้าที่ที่เกี่ยวข้องแจ้งเหตุขัดข้องนั้นให้หัวหน้า หรือผู้บังคับบัญชาทราบโดยเร็ว

๖.๒ กรณีเครื่องแม่ข่ายและอุปกรณ์เครือข่าย

๑) ตัดการเชื่อมต่อระบบเครือข่ายโดยเร็ว แล้วปิดอุปกรณ์เครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ตามสำดับความสำคัญของการให้บริการ

๒) ถ้าไฟฟ้าดับ/ไฟฟ้าตก ให้ปิดเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยพิจารณาตามความสำคัญของการให้บริการ ระยะเวลาที่เกิดปัญหาทางไฟฟ้า และประสิทธิภาพของเครื่องสำรองไฟฟ้า

๓) ปิดระบบจ่ายไฟ ในกรณีไฟไหม้ ให้ใช้น้ำยาดับเพลิงฉีดควบคุมเพลิงโดยเร็ว

๔) ขนย้ายอุปกรณ์ไปไว้ในที่ที่ปลอดภัย

๕) ประสานขอความช่วยเหลือกับผู้เชี่ยวชาญที่รับผิดชอบดูแลเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายโดยเร็ว

๖) ในกรณีที่อุปกรณ์ด้านฮาร์ดแวร์เสีย ให้รีบจัดหาอุปกรณ์สำรองหรือแจ้งบริษัทที่รับผิดชอบนำอุปกรณ์มาเปลี่ยนให้โดยเร็ว

๗) ผู้ดูแลระบบต้องแจ้งให้ผู้บังคับบัญชาทราบโดยเร็ว ตามลำดับชั้น

๖.๓ กรณีเครื่องคอมพิวเตอร์ลูกข่ายติดไวรัส

๑) เจ้าหน้าที่ผู้ใช้เครื่องคอมพิวเตอร์นั้นๆ ปลดสาย LAN ออกจากเครื่องคอมพิวเตอร์เพื่อตัดการเชื่อมต่อกับระบบเครือข่าย

๒) สแกนและกำจัดไวรัสด้วยโปรแกรมป้องกันไวรัส

๓) แจ้งเจ้าหน้าที่ที่เกี่ยวข้องเพื่อทำการตรวจสอบ

๖.๔ หลักปฏิบัติของบุคลากรในการป้องกันอัคคีภัย หรือเมื่อเกิดอัคคีภัย

๑) ไม่กระทำการใดๆ อันจะนำไปสู่การเกิดอัคคีภัยในอาคาร

๒) ควรศึกษาเรื่องตำแหน่งการหนีไฟ เส้นทางหนีไฟ ทางออกจากตัวอาคาร การติดตั้งอุปกรณ์ที่เกี่ยวกับความปลอดภัยจากเพลิงไหม้และการหนีไฟอย่างละเอียด

๓) ควรหาทางออกฉุกเฉินสองทางที่ใกล้กับห้องทำงาน ตรวจสอบทางออกฉุกเฉินมิให้ปิดตาย หรือมีสิ่งกีดขวาง และสามารถใช้เป็นเส้นทางจากภายในอาคารได้อย่างปลอดภัย ให้นับจำนวนประตูห้องโดยเริ่มจากห้องทำงานตนเองไปยังทางออกฉุกเฉิน เพื่อให้สามารถไปได้แม้ว่าไฟดับหรือปกคลุมไปด้วยควัน

๔) เมื่อเกิดเพลิงไหม้ ให้หาตำแหน่งสัญญานเตือนเพลิงไหม้ เปิดสัญญานเตือน จากนั้นออกจากอาคารแล้วแจ้งหน่วยดับเพลิงทันที

๕) เมื่อได้ยินสัญญานเตือนเพลิงไหม้ ให้รีบหาทางหนีออกจากอาคารทันที

๖) หากเพลิงไหม้ในห้องทำงาน ให้ออกจากประตู ปิดประตู แล้วแจ้งหน่วยดับเพลิงทันที

๗) หากเกิดเพลิงไหม้นอกห้องทำงาน ก่อนออกจากอาคารให้วางมือบนประตู หากประตูมีความเย็น ค่อยๆ เปิดประตู แล้วไปยังทางหนีไฟฉุกเฉินที่ใกล้ที่สุด

๘) หากเพลิงไหม้อยู่บริเวณใกล้ประตูจะมีความร้อนห้ามเปิดประตูโดยเด็ดขาด ให้รีบแจ้งหน่วยดับเพลิงและแจ้งให้ทราบว่าท่านอยู่ที่ใดของอาคารซึ่งเกิดเพลิงไหม้ หาผ้าเปียก ปิดทางเข้าของควัน ปิดพัดลมและเครื่องปรับอากาศ ส่งสัญญานขอความช่วยเหลือที่หน้าต่าง

๙) เมื่อต้องเผชิญกับควันไฟ ให้คลานไปยังทางออกฉุกเฉิน

๑๐)ห้ามใช้ลิฟท์ขณะเกิดเพลิงไหม้

๖.๕ ระบบป้องกันและแก้ปัญหาที่เกิดจากกระแสไฟฟ้า

เนื่องจากเครื่องคอมพิวเตอร์และอุปกรณ์เครือข่ายส่วนใหญ่ มีความไวต่อความผิดปกติของกระแสไฟฟ้ามาก ดังนั้นสิ่งที่มักจะเกิดขึ้นและยากต่อการหลีกเลี่ยงคือ ผลกระทบต่างๆ ที่เกิดจากปัญหาทางไฟฟ้า เช่น การชำรุดและเสียหายของอุปกรณ์คอมพิวเตอร์ หรือการสูญหายของข้อมูลที่สำคัญ รวมถึงการเสียเวลาจากผลกระทบที่เกิดจากปัญหาทางไฟฟ้า แนวทางในการปฏิบัติเพื่อป้องกันเหตุดังกล่าวประกอบด้วย

๑) เปิดใช้งานเครื่องสำรองไฟฟ้าและปรับแรงดันไฟฟ้าอัตโนมัติ (UPS) ตลอดระยะเวลาในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล

๒) เมื่อกระแสไฟฟ้าดับ ให้รีบทำการบันทึกข้อมูลทันที และปิดเครื่องคอมพิวเตอร์และอุปกรณ์ในภายหลัง

๗. แผนกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติเดิม

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย โดยปกติเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย ต้องอยู่ในสภาพที่พร้อมรองรับการให้บริการกับเครื่องลูกข่ายต่างๆ ได้ตลอดเวลา หากไม่สามารถให้บริการได้ ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเสียหายหรือหยุดทำงาน ให้ดำเนินการ ดังนี้

๑) จัดหาอุปกรณ์/ชิ้นส่วน เพื่อทดแทน

๒) เปลี่ยนอุปกรณ์/ชิ้นส่วนที่เสียหาย

๓) ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๔) จัดหาอุปกรณ์คอมพิวเตอร์จากแหล่งอื่นมาใช้งานเป็นการชั่วคราว

๕) นำสื่อบันทึกข้อมูลที่ได้สำรองข้อมูลไว้กลับมา Recovery โดยเร็ว

๖) ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

๘. ผู้รับผิดชอบ

๘.๑ ระดับนโยบาย

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วยงาน (CIO) รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ

๘.๒ ระดับปฏิบัติ

เจ้าหน้าที่ผู้ดูแลระบบของหน่วยงาน รับผิดชอบ กำกับดูแล ปฏิบัติ ศึกษาทบทวน วางแผน ติดตาม บริหารความเสี่ยงและรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศ

๙. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการหรือการตรวจสอบให้ผู้บังคับบัญชาทราบเป็นประจำทุกเดือน และให้รายงานการเกิดปัญหาและผลการแก้ไขให้ทราบในทันทีที่สามารถดำเนินการได้ ในทุกกรณีตามที่ได้ระบุไว้

ส่วนที่ ๕

นโยบายแผนบริหารความเสี่ยง
สำนักวิทยบริการและเทคโนโลยีสารสนเทศ มหาวิทยาลัยสวนดุสิต

๑.วัตถุประสงค์

๑.๑ เพื่อลดมูลเหตุของโอกาสที่องค์กรจะเกิดความเสียหาย ทั้งในรูปแบบของตัวเงินและไม่ใช้ตัวเงิน

๑.๒ เพื่อให้ระดับความเสี่ยงและขนาดของความเสียหายที่เกิดขึ้นอยู่ในระดับที่องค์กรยอมรับได้ ควบคุมได้ และตรวจสอบได้อย่างมีระบบโดยคำนึงถึงการบรรลุเป้าหมายขององค์กรหรือยุทธศาสตร์เป็นสำคัญ

ผู้รับผิดชอบ

๑. สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

-

นโยบาย

๑. มหาวิทยาลัยจะต้องจัดทำแนวปฏิบัติในการบริหารความเสี่ยงที่หน่วยงานนั้นรับผิดชอบ เป็นประจำทุกปี

๒. มหาวิทยาลัยจะต้องวิเคราะห์ วางแผนบริหารความเสี่ยง และจัดทำแผนบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

๓. ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๔. ในการตรวจสอบและประเมินความเสี่ยง จะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๕ การกำหนดหน้าที่และผู้รับผิดชอบในการจัดการความเสี่ยง รวมถึงติดตาม ควบคุม และสรุปการดำเนินงานด้านบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศต่อมหาวิทยาลัย โดยหน่วยงานตรวจสอบภายในของมหาวิทยาลัย

๖. รายงานผลการดำเนินการต่อผู้บริหารของหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

๗. มีการทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน เป็นประจำทุกปี

SDU_RM ๑

ตารางที่ ๑ การกำหนดวัตถุประสงค์ของงานตามพันธกิจของหน่วยงาน และวัตถุประสงค์ของขั้นตอนหลัก

งาน	วัตถุประสงค์ของงาน	ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอนหลัก
ความเสี่ยงด้านสวัสดิการในชีวิตและทรัพย์สิน			
โครงการจัดหาทรัพยากรสารสนเทศ	วัตถุประสงค์ ๑.บริการทรัพยากรสารสนเทศแก่นักศึกษา อาจารย์ บุคลากรและบุคคลภายนอก ๒.เป็นแหล่งศึกษา ค้นคว้าข้อมูลให้กับนักศึกษา อาจารย์บุคลากรและบุคคลภายนอก	จัดหาทรัพยากรสารสนเทศที่สอดคล้องกับการจัดการเรียนการสอนของมหาวิทยาลัย	วัตถุประสงค์ : เพื่อสนับสนุนการจัดการเรียนการสอนของแต่ละคณะและหลักสูตร
การให้บริการสืบค้น ค้นคว้า ผ่านอินเทอร์เน็ตด้วยเครื่องคอมพิวเตอร์	วัตถุประสงค์: เพื่อบริการสืบค้น และค้นคว้า ออนไลน์	ให้บริการใช้เครื่องคอมพิวเตอร์ PC	วัตถุประสงค์ : เพื่อสนับสนุนการศึกษาค้นคว้าของนักศึกษาบุคลากร และบุคคลภายนอก
ความเสี่ยงด้านการเงิน			
การบริหารจัดการแผนและงบประมาณ	วัตถุประสงค์ : เพื่อให้การบริหารจัดการด้านแผนและงบประมาณมีประสิทธิภาพ	การดำเนินงานตามปฏิทิน (Gantt Chart)	วัตถุประสงค์ : เพื่อให้การดำเนินงานเป็นไปตามแผนที่กำหนดไว้
ความเสี่ยงด้านยุทธศาสตร์ กลยุทธ์			
การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมความเป็นพลวัต	วัตถุประสงค์ : เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศสอดรับกับการดำเนินงานของมหาวิทยาลัย	การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมการเป็นพลวัต	วัตถุประสงค์ : เพื่อให้มีระบบเทคโนโลยีสารสนเทศที่ทันสมัยและสามารถใช้ในการบริหารงานได้อย่างคล่องตัว
ความเสี่ยงด้านการปฏิบัติตามและไม่ปฏิบัติตามกฎหมายหรือกฎระเบียบ			
ให้ความรู้ในเรื่องการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐	วัตถุประสงค์ : เพื่อให้นักศึกษาและบุคลากรของมหาวิทยาลัยมีความรู้ความ	เผยแพร่และให้ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐	วัตถุประสงค์ : เพื่อสร้างสื่อประชาสัมพันธ์และรณรงค์การใช้คอมพิวเตอร์ให้ถูกต้องตามระเบียบข้อปฏิบัติ

งาน	วัตถุประสงค์ของงาน	ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอนหลัก
	เข้าใจเกี่ยวกับกฎหมายทางด้านคอมพิวเตอร์		
ความเสี่ยงด้านบุคลากรและหลักธรรมาภิบาล			
การถ่ายโอนอัตรากำลังจากภาครัฐสู่ภาคเอกชน	วัตถุประสงค์ : เพื่อสร้างแรงจูงใจให้กับบุคลากรในการปฏิบัติงาน	การปฏิบัติงานเชี่ยวชาญเฉพาะด้านทางเทคโนโลยีสารสนเทศ	วัตถุประสงค์ : เพื่อรองรับบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน
ความสี่ยงด้านเทคโนโลยีสารสนเทศ			
พัฒนาเว็บไซต์ต้นแบบของหน่วยงานภายในมหาวิทยาลัย	วัตถุประสงค์ : เพื่อพัฒนาเว็บไซต์ที่สามารถเป็นมาตรฐานเดียวกันทุกหน่วยงานในมหาวิทยาลัย	รวบรวมและตรวจสอบข้อมูลความต้องการพื้นฐานร่วมกันด้านต่างๆ จากหน่วยงานในมหาวิทยาลัย	วัตถุประสงค์ : เพื่อให้ได้ข้อมูลที่ถูกต้องและมีรูปแบบเว็บไซต์ที่เป็นมาตรฐานสำหรับหน่วยงานต่างๆ ของมหาวิทยาลัย
ความปลอดภัยในการใช้เครื่องคอมพิวเตอร์ของมหาวิทยาลัย	วัตถุประสงค์ : เพื่อดูแลอุปกรณ์คอมพิวเตอร์และความปลอดภัยจากการโจมตีโดยไวรัสคอมพิวเตอร์	๑.๑.๑ เพิ่มความเข้มงวดในการใช้อุปกรณ์ต่อพ่วงประเภทจัดเก็บข้อมูลแบบพกพา ๑.๑.๒ เพิ่มความเข้มงวดในการเข้าถึงระบบเว็ปไซต์ภายนอกต่างๆ	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง
ความพร้อมของเทคโนโลยีสารสนเทศ	วัตถุประสงค์ : เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยมีความพร้อมและเกิดประโยชน์สูงสุดในการให้บริการแก่นักศึกษา	๑.๑.๑ สำรวจความพร้อมของระบบสารสนเทศ ๑.๑.๒ ดำเนินการงานตามวัตถุประสงค์ ๑.๑.๓ ติดตามและประเมินผลการให้บริการแก่นักศึกษา	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง

ตารางที่ ๒ การระบุความเสี่ยง และปัจจัยเสี่ยง SDU_RM ๒

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง
ความเสี่ยงด้านสวัสดิการในชีวิตและทรัพย์สิน			
จัดหาทรัพยากรสารสนเทศที่สอดคล้องกับการจัดการเรียนการสอนของมหาวิทยาลัย	วัตถุประสงค์ : เพื่อสนับสนุนการจัดการเรียนการสอนของแต่ละคณะและหลักสูตร	ฉีกและทำลายทรัพยากรสารสนเทศจนหนังสือเกิดความเสียหาย	๑.๑.๑ ผู้ใช้บริการขาดความตระหนักเกี่ยวกับการยืม-คืนหนังสือ ๑.๑.๒ ผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้ห้องสมุดอย่างเคร่งครัด
ให้บริการใช้เครื่องคอมพิวเตอร์ PC	วัตถุประสงค์ : เพื่อสนับสนุนการศึกษาค้นคว้าของนักศึกษาบุคลากร และบุคคลภายนอก	อุปกรณ์ภายในเครื่องคอมพิวเตอร์ถูกโจรกรรม	๑.๑.๑ ผู้ใช้บริการขาดจิตสำนึกในการใช้บริการคอมพิวเตอร์ของมหาวิทยาลัย ๑.๑.๒ มูลค่าของอุปกรณ์มีราคาสูง
ความเสี่ยงด้านการเงิน			
การดำเนินงานตามปฏิทิน (Gantt Chart)	วัตถุประสงค์ : เพื่อให้การดำเนินงานเป็นไปตามแผนที่กำหนดไว้	การดำเนินโครงการไม่เป็นไปตามแผนทำให้งบประมาณที่เตรียมไว้ไม่เพียงพอ	นโยบายการดำเนินงานเปลี่ยนแปลงเพื่อให้สอดคล้องกับเหตุการณ์ปัจจุบัน
ความเสี่ยงด้านยุทธศาสตร์ กลยุทธ์			
การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมการเป็นพลวัต	วัตถุประสงค์ : เพื่อให้มีระบบเทคโนโลยีสารสนเทศที่ทันสมัยและสามารถใช้ในการบริหารงานได้อย่างคล่องตัว	การดึงข้อมูลพื้นฐานจากฐานข้อมูลต่างๆ ของมหาวิทยาลัยไม่ทันกับความต้องการของผู้บริหารหรือคณะกรรมการประเมินคุณภาพต่างๆ	ฐานข้อมูลในแต่ละหน่วยงานมีรูปแบบโครงสร้างที่แตกต่างกัน
ความเสี่ยงด้านการปฏิบัติตามและไม่ปฏิบัติตามกฎหมายหรือกฎระเบียบ			
เผยแพร่และให้ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐	วัตถุประสงค์ : เพื่อสร้างสื่อประชาสัมพันธ์และรณรงค์การใช้คอมพิวเตอร์ให้ถูกต้องตามระเบียบข้อปฏิบัติ	นักศึกษา อาจารย์และบุคลากรละเลยการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ โดยไม่มีเจตนา	๑.๑.๑ บุคลากร นักศึกษา บางส่วนยังขาดความใส่ใจตระหนักถึงโทษที่ได้รับเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่า

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง
			ด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ ผู้โจรกรรมข้อมูลทางคอมพิวเตอร์ใช้พื้นที่ในการกระทำผิดต่อความมั่นคงของประเทศ หรือหมิ่นประมาทผู้อื่นทำให้ได้รับความเสียหาย
ความเสี่ยงด้านบุคลากรและหลักธรรมาภิบาล			
การปฏิบัติงานเชี่ยวชาญเฉพาะด้านทางเทคโนโลยีสารสนเทศ	วัตถุประสงค์ : เพื่อรองรับบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน	บุคลากรที่มีความเชี่ยวชาญเฉพาะด้านมีการเปลี่ยนย้ายงานตามแรงจูงใจจากภายนอก	๑.๑.๑ ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน ๑.๑.๒ สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ			
รวบรวมและตรวจสอบข้อมูลความต้องการพื้นฐานด้านต่างๆ จากหน่วยงานในมหาวิทยาลัย	วัตถุประสงค์ : เพื่อให้ได้ข้อมูลที่ถูกต้องและเป็นปัจจุบันตรงกับความต้องการของหน่วยงานต่างๆ	ความต้องการหรือข้อมูลที่แตกต่างกันมากของแต่ละหน่วยงาน	เว็บไซต์ต้นแบบไม่สามารถตอบสนองความต้องการของทุกหน่วยงานได้
๑.๑ เพิ่มความเข้มงวดในการใช้อุปกรณ์ต่อพ่วงประเภทจัดเก็บข้อมูลแบบพกพา ๑.๒ เพิ่มความเข้มงวดในการเข้าถึงระบบเว็ปไซต์ภายนอกต่างๆ	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง	เครื่องคอมพิวเตอร์ติดไวรัสโดยไม่ทราบสาเหตุ	คอมพิวเตอร์ไม่ติดตั้งหรือ update โปรแกรมป้องกันไวรัส
๑.๑ สำรวจความพร้อมของระบบสารสนเทศ ๑.๒ ดำเนินการงานตามวัตถุประสงค์ ๑.๓ ติดตามและประเมินผลการให้บริการแก่นักศึกษา	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง	เครื่องคอมพิวเตอร์มีไม่เพียงพอต่อการให้บริการกับนักศึกษา	๑.๑.๑ การหมดสัญญาเช่าเครื่องคอมพิวเตอร์ของมหาวิทยาลัยและยังไม่มีการจัดเครื่องใหม่มาทดแทน สัญญาณ wireless มีปัญหา

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง
			๑.๑.๒ บุคลากรผู้ดูแลการบริการด้านคอมพิวเตอร์ไม่เพียงพอ

SDU_RM ๓

ตารางที่ ๓ การประเมินความเสี่ยง

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง			
				โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
จัดหาทรัพยากรสารสนเทศที่สอดคล้องกับการจัดการเรียนการสอนของมหาวิทยาลัย	วัตถุประสงค์ : เพื่อสนับสนุนการจัดการเรียนการสอนของแต่ละคณะและหลักสูตร	ฉีกและทำลายทรัพยากรสารสนเทศจนหนังสือเกิดความเสียหาย	๑.๑.๑ ผู้ใช้บริการขาดความตระหนักเกี่ยวกับการยืม-คืนหนังสือ ๑.๑.๒ ผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้ห้องสมุดอย่างเคร่งครัด	๕	๕	สูงมาก	๒
ให้บริการใช้เครื่องคอมพิวเตอร์ PC	วัตถุประสงค์ : เพื่อสนับสนุนการศึกษาค้นคว้าของนักศึกษาบุคลากร และบุคคลภายนอก	อุปกรณ์ภายในเครื่องคอมพิวเตอร์ถูกโจรกรรม	๑.๑.๑ ผู้ใช้บริการขาดจิตสำนึกในการใช้บริการคอมพิวเตอร์ของมหาวิทยาลัย ๑.๑.๒ มูลค่าของอุปกรณ์มีราคาสูง	๕	๕	สูงมาก	๑
การดำเนินงานตามปฏิทิน (Gantt Chart)	วัตถุประสงค์ : เพื่อให้การดำเนินงานเป็นไปตามแผนที่กำหนดไว้	การดำเนินโครงการไม่เป็นไปตามแผนทำให้งบประมาณที่เตรียมไว้ไม่เพียงพอ	นโยบายการดำเนินงานเปลี่ยนแปลงเพื่อให้สอดคล้องกับเหตุการณ์ปัจจุบัน	๔	๓	สูง	๔
การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมการเป็นพลวัต	วัตถุประสงค์ : เพื่อให้มีระบบเทคโนโลยีสารสนเทศที่ทันสมัยและสามารถใช้ในการบริหารงานได้อย่างคล่องตัว	การดึงข้อมูลพื้นฐานจากฐานข้อมูลต่างๆ ของมหาวิทยาลัยไม่ทันกับความต้องการของผู้บริหารหรือคณะกรรมการประเมินคุณภาพต่างๆ	ฐานข้อมูลในแต่ละหน่วยงานมีรูปแบบโครงสร้างที่แตกต่างกัน	๔	๓	สูง	๓

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง			
				โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
เผยแพร่และให้ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐	วัตถุประสงค์ : เพื่อสร้างสื่อประชาสัมพันธ์และรณรงค์การใช้คอมพิวเตอร์ให้ถูกต้องตามระเบียบข้อปฏิบัติ	นักศึกษา อาจารย์และบุคลากรละเลยการปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ โดยไม่มีเจตนา	๑.๑.๑ บุคลากร นักศึกษา บางส่วนยังขาดความใส่ใจตระหนักถึงโทษที่ได้รับเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ ผู้โจรกรรมข้อมูลทางคอมพิวเตอร์ใช้พื้นที่ในการกระทำผิดต่อความมั่นคงของประเทศ หรือหมิ่นประมาทผู้อื่นทำให้ได้รับความเสียหาย	๔	๓	สูง	๕
การปฏิบัติงานเชี่ยวชาญเฉพาะด้านทางเทคโนโลยีสารสนเทศ	วัตถุประสงค์ : เพื่อรองรับบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน	บุคลากรที่มีความเชี่ยวชาญเฉพาะด้านมีการเปลี่ยนย้ายงานตามแรงจูงใจจากภายนอก	๑.๑.๑ ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน ๑.๑.๒ สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน	๓	๓	สูง	๖
รวบรวมและตรวจสอบข้อมูลความต้องการพื้นฐานร่วมกันด้านต่างๆ จากหน่วยงานในมหาวิทยาลัย	วัตถุประสงค์ : เพื่อให้ได้ข้อมูลที่ถูกต้องและเป็นปัจจุบันตรงกับความต้องการของหน่วยงานต่างๆ	ความต้องการหรือข้อมูลที่แตกต่างกันมากของแต่ละหน่วยงาน	เว็บไซต์ต้นแบบไม่สามารถตอบสนองความต้องการของทุกหน่วยงานได้	๓	๓	สูง	๘

ขั้นตอนหลัก	วัตถุประสงค์ของขั้นตอน	ความเสี่ยง	ปัจจัยเสี่ยง	การประเมินความเสี่ยง			
				โอกาส	ผลกระทบ	ระดับความเสี่ยง	ลำดับความเสี่ยง
๑.๑ เพิ่มความเข้มงวดในการใช้อุปกรณ์ต่อพ่วงประเภทจัดเก็บข้อมูลแบบพกพา ๑.๒ เพิ่มความเข้มงวดในการเข้าถึงระบบเว็ปไซต์ภายนอกต่างๆ	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง	เครื่องคอมพิวเตอร์ติดไวรัสโดยไม่ทราบสาเหตุ	คอมพิวเตอร์ไม่ติดตั้งหรือ update โปรแกรมป้องกันไวรัส	๓	๓	สูง	๙
๑.๑ สำรวจความพร้อมของระบบสารสนเทศ ๑.๒ ดำเนินการงานตามวัตถุประสงค์ ๑.๓ ติดตามและประเมินผลการให้บริการแก่นักศึกษา	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง	เครื่องคอมพิวเตอร์มีไม่เพียงพอต่อการให้บริการกับนักศึกษา	๑.๑.๑ การหมดสัญญาเช่าเครื่องคอมพิวเตอร์ของมหาวิทยาลัยและยังไม่มีการจัดเครื่องใหม่มาทดแทน ๑.๑.๒ สัญญาณ wireless มีปัญหา ๑.๑.๓ บุคลากรผู้ดูแลการบริการด้านคอมพิวเตอร์ไม่เพียงพอในกรณีมีงานซ้ำซ้อน	๓	๓	สูง	๗

ตารางที่ ๔ การประเมินมาตรการควบคุม

ขั้นตอนหลัก / ปัจจัยเสี่ยง (๑)	การควบคุมที่ควรจะมี (๒)	การควบคุมที่มีอยู่แล้ว (๓)	ผลการประเมินการควบคุมที่มีอยู่แล้วว่าได้ผลหรือไม่ (๔)
๑. จัดหาทรัพยากรสารสนเทศที่สอดคล้องกับการจัดการเรียนการสอนของมหาวิทยาลัย - ผู้ใช้บริการขาดความตระหนักเกี่ยวกับการยืม-คืนหนังสือ - ผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้ห้องสมุดอย่างเคร่งครัด	๑.๑ ตรวจสอบการเข้า-ออกเพื่อตรวจจับการขโมยหนังสือ ๑.๒ ประชาสัมพันธ์ภายในอาคารวิทยบริการเรื่องการใช้ห้องสมุดอย่างต่อเนื่อง	?	✕
๒. ให้บริการใช้เครื่องคอมพิวเตอร์ PC - ผู้ใช้บริการขาดจิตสำนึกในการใช้บริการคอมพิวเตอร์ของมหาวิทยาลัย - มูลค่าของอุปกรณ์มีราคาสูง	๑.๑ รณรงค์การใช้บริการเครื่องคอมพิวเตอร์ PC ๑.๒ ควบคุมการให้บริการโดยกล้องวงจรปิด หากมีเหตุการณ์ผิดปกติ	?	✕
๓. การดำเนินงานตามปฏิทิน (Gantt Chart) - นโยบายการดำเนินงานเปลี่ยนแปลงเพื่อให้สอดคล้องกับเหตุการณ์ปัจจุบัน	มีการคาดการณ์ล่วงหน้าและมีการปรับแผนการดำเนินงานให้สอดคล้องกับนโยบาย	?	✕
๔. การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมการเป็นพลวัต - ฐานข้อมูลในแต่ละหน่วยงานมีรูปแบบโครงสร้างที่แตกต่างกัน	๑.๑.๑ ปรับปรุงข้อมูลพื้นฐานและบูรณาการความเชื่อมโยงระบบฐานข้อมูลจากทุกหน่วยงานของมหาวิทยาลัยเพื่อในการบริหารและประกันคุณภาพ ๑.๑.๒ พัฒนาระบบฐานข้อมูลของแต่ละหน่วยงานให้มีโครงสร้างเดียวกัน	✓	?

ขั้นตอนหลัก / ปัจจัยเสี่ยง (๑)	การควบคุมที่ควรจะมี (๒)	การควบคุมที่มีอยู่แล้ว (๓)	ผลการประเมินการควบคุมที่มีอยู่แล้วว่าได้ผลหรือไม่ (๔)
๕. เผยแพร่และให้ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ - บุคลากร นักศึกษา บางส่วนยังขาดความใส่ใจตระหนักถึงโทษที่ได้รับเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ - ผู้โจรกรรมข้อมูลทางคอมพิวเตอร์ใช้พื้นที่ในการกระทำผิดต่อความมั่นคงของประเทศ หรือหมิ่นประมาทผู้อื่นทำให้ได้รับความเสียหาย	๑.๑.๑ เผยแพร่ประชาสัมพันธ์บทลงโทษของการกระทำความผิดเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ๑.๑.๒ เพิ่มระบบรักษาความปลอดภัย ในการเข้าถึงหรือโจรกรรมข้อมูลให้รัดกุม	✓	?
๖. การปฏิบัติงานเชี่ยวชาญเฉพาะด้านทางเทคโนโลยีสารสนเทศ - ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน - สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน	๑.๑.๑ ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน ๑.๑.๒ สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน	✓	?
๗. รวบรวมและตรวจสอบข้อมูลความต้องการพื้นฐานร่วมกันด้านต่างๆ จากหน่วยงานในมหาวิทยาลัย - เว็บไซต์ต้นแบบไม่สามารถตอบสนองความต้องการของทุกหน่วยงานได้	ประสานความร่วมมือกับหน่วยงานต่างๆ เพื่อปรับรูปแบบของข้อมูลในเว็บไซต์ให้สอดคล้องกัน	✓	?
๘.๑ เพิ่มความเข้มงวดในการใช้อุปกรณ์ต่อพ่วงประเภทจัดเก็บข้อมูลแบบพกพา	ดูแลตรวจสอบโปรแกรมป้องกันไวรัสให้เป็นปัจจุบันและพร้อมใช้งานได้	✓	?

ขั้นตอนหลัก / ปัจจัยเสี่ยง (๑)	การควบคุมที่ควรจะมี (๒)	การควบคุมที่มีอยู่แล้ว (๓)	ผลการประเมินการควบคุมที่มีอยู่แล้วว่าได้ผลหรือไม่ (๔)
๘.๒ เพิ่มความเข้มงวดในการเข้าถึงระบบเว็ปไซต์ภายนอกต่างๆ - คอมพิวเตอร์ไม่ติดตั้งหรือ update โปรแกรมป้องกันไวรัส			
๙.๑ สำรวจความพร้อมของระบบสารสนเทศ ๙.๒ ดำเนินการงานตามวัตถุประสงค์ ๙.๓ ติดตามและประเมินผลการให้บริการแก่นักศึกษา - การหมดสัญญาเช่าเครื่องคอมพิวเตอร์ของมหาวิทยาลัยและยังไม่มีการจัดเครื่องใหม่มาทดแทน - สัญญาณ wireless มีปัญหา - บุคลากรผู้ดูแลการบริการด้านคอมพิวเตอร์ไม่เพียงพอในกรณีมีงานซ้ำซ้อน	๑.๑.๑ ให้นักศึกษานำ Note Book ส่วนตัวที่ได้รับจากมหาวิทยาลัยมาใช้งานทดแทนเครื่องที่หมดสัญญาเช่า ๑.๑.๒ ตรวจสอบจุดอับสัญญาณและปรับปรุงแก้ไข ๑.๑.๓ มอบหมายให้นักศึกษาช่วยงานในโครงการของศูนย์สนเทศและแนะแนวการศึกษาและอาชีพมาช่วยให้บริการ	✓	?

<u>เครื่องหมายที่ระบุในช่อง (๓)</u>
✓ = มี ✕ = ไม่มี ? = มีแต่ไม่สมบูรณ์
<u>เครื่องหมายที่ระบุในช่อง (๔)</u>
✓ = ได้ผลตามที่คาดหมาย ✕ = ไม่ได้ผลตามที่คาดหมาย ? = ได้ผลบ้างแต่ไม่สมบูรณ์

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านสวัสดิการในชีวิตและทรัพย์สิน

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
โครงการจัดหาทรัพยากรสารสนเทศ วัตถุประสงค์ ๑.บริการทรัพยากรสารสนเทศแก่นักศึกษา อาจารย์ บุคลากร และบุคคลภายนอก ๒.เป็นแหล่งศึกษา ค้นคว้าข้อมูลให้กับนักศึกษา อาจารย์ บุคลากรและบุคคลภายนอก	จัดหาทรัพยากรสารสนเทศที่สอดคล้องกับการจัดการเรียนการสอนของมหาวิทยาลัย วัตถุประสงค์ : เพื่อสนับสนุนการจัดการเรียนการสอนของแต่ละคณะและหลักสูตร	๑.๑ หนังสือสูญหาย ๑.๒ ผู้ใช้บริการฉีกหนังสือหรือวารสารที่ตนเองต้องการ	๑.๑.๑ ผู้ใช้บริการขาดความตระหนักเกี่ยวกับการยืม-คืนหนังสือ ๑.๑.๒ ผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้ห้องสมุดอย่างเคร่งครัด	๑.๑ ตรวจสอบการเข้า-ออกเพื่อตรวจจับการขโมยหนังสือ ๑.๒ ประชาสัมพันธ์ภายในอาคารวิทยบริการเรื่องการใช้ห้องสมุดอย่างต่อเนื่อง	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	
การให้บริการสืบค้น ค้นคว้าผ่านอินเทอร์เน็ตด้วยเครื่องคอมพิวเตอร์ วัตถุประสงค์: เพื่อบริการสืบค้น และค้นคว้า ออนไลน์	ให้บริการใช้เครื่องคอมพิวเตอร์ PC วัตถุประสงค์ : เพื่อสนับสนุนการศึกษา ค้นคว้าของนักศึกษาบุคลากร และบุคคลภายนอก	๑.๑ อุปกรณ์ประกอบของเครื่องคอมพิวเตอร์ PC สูญหาย เช่น Mouse RAM	๑.๑.๑ ผู้ใช้บริการขาดจิตสำนึกในการใช้บริการคอมพิวเตอร์ของมหาวิทยาลัย ๑.๑.๒ มูลค่าของอุปกรณ์มีราคาสูง	๑.๑ รณรงค์การใช้บริการเครื่องคอมพิวเตอร์ PC ๑.๒ ควบคุมการให้บริการโดยกล้องวงจรปิด หากมีเหตุการณ์ผิดปกติ	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

SDU_RM ๕

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการเงิน

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
การบริหารจัดการแผนและงบประมาณ วัตถุประสงค์ : เพื่อให้การบริหารจัดการด้านแผนและงบประมาณมีประสิทธิภาพ	การดำเนินงานตามปฏิทิน (Gantt Chart) วัตถุประสงค์ : เพื่อให้การดำเนินงานเป็นไปตามแผนที่กำหนดไว้	การใช้งบประมาณไม่เป็นไปตามแผนที่กำหนดไว้	นโยบายการดำเนินงานเปลี่ยนแปลงเพื่อให้สอดคล้องกับเหตุการณ์ปัจจุบัน	มีการคาดการณ์ล่วงหน้าและมีการปรับแผนการดำเนินงานให้สอดคล้องกับนโยบาย	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

SDU_RM ๕

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านยุทธศาสตร์ กลยุทธ์

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมความเป็นพลวัต วัตถุประสงค์ : เพื่อให้การบริหารจัดการด้านเทคโนโลยีสารสนเทศสอดรับกับการดำเนินงานของมหาวิทยาลัย	การพัฒนาระบบเทคโนโลยีสารสนเทศเพื่อส่งเสริมการเป็นพลวัต วัตถุประสงค์ : เพื่อให้มีระบบเทคโนโลยีสารสนเทศที่ทันสมัยและสามารถใช้ในการบริหารงานได้อย่างคล่องตัว	๑.๑ ขาดการบูรณาการการใช้ข้อมูลเทคโนโลยีสารสนเทศระหว่างหน่วยงาน	๑.๑.๑ ฐานข้อมูลในแต่ละหน่วยงานมีรูปแบบโครงสร้างที่แตกต่างกัน	๑.๑.๑ ปรับปรุงข้อมูลพื้นฐานและบูรณาการความเชื่อมโยงระบบฐานข้อมูลจากทุกหน่วยงานของมหาวิทยาลัยเพื่อในการบริหารและประกันคุณภาพ ๑.๑.๒ พัฒนาระบบฐานข้อมูลของแต่ละหน่วยงานให้มีโครงสร้างเดียวกัน	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

SDU_RM ๕

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านการปฏิบัติตามและไม่ปฏิบัติตามกฎหมายหรือกฎระเบียบ

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
ให้ความรู้ในเรื่องการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ วัตถุประสงค์ : เพื่อให้นักศึกษาและบุคลากรของมหาวิทยาลัยมีความรู้ความเข้าใจเกี่ยวกับกฎหมายทางด้านคอมพิวเตอร์	เผยแพร่และให้ความรู้เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ วัตถุประสงค์ : เพื่อสร้างสื่อประชาสัมพันธ์และรณรงค์การใช้คอมพิวเตอร์ให้ถูกต้องตามระเบียบข้อปฏิบัติ	๑.๑ บุคลากร นักศึกษา บางส่วนยังฝ่าฝืนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐	๑.๑.๑ บุคลากร นักศึกษา บางส่วนยังขาดความใส่ใจตระหนักถึงโทษที่ได้รับเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ ผู้โจรกรรมข้อมูลทางคอมพิวเตอร์ใช้พื้นที่ในการกระทำผิดต่อความมั่นคงของประเทศ หรือหมิ่นประมาทผู้อื่นทำให้ได้รับความเสียหาย	๑.๑.๑ เผยแพร่ประชาสัมพันธ์บทลงโทษของการกระทำความผิดเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ เพิ่มระบบรักษาความปลอดภัย ในการเข้าถึงหรือโจรกรรมข้อมูลให้รัดกุม	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

SDU_RM ๕

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านบุคลากรและหลักธรรมาภิบาล

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
การถ่ายโอนอัตรากำลังจากภาครัฐสู่ภาคเอกชน วัตถุประสงค์ : เพื่อสร้างแรงจูงใจให้กับบุคลากรในการปฏิบัติงาน	การปฏิบัติงานเชี่ยวชาญเฉพาะด้านทางเทคโนโลยีสารสนเทศ วัตถุประสงค์ : เพื่อรองรับบุคลากรที่มีความเชี่ยวชาญเฉพาะด้าน	ข้อเปรียบเทียบอัตราค่าตอบแทนของบุคลากรภาครัฐและเอกชน	๑.๑ อัตราค่าตอบแทนของภาคเอกชนสูงกว่าภาครัฐ ๑.๒ ค่าครองชีพในสถานการณ์ปัจจุบันที่มีอัตราสูง	๑.๑.๑ ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน ๑.๑.๒ สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน	กองบริหารงานบุคคล	

SDU_RM ๕

แผนบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ.๒๕๖๐

สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยงด้านเทคโนโลยีสารสนเทศ

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
๑. พัฒนาเว็บไซต์ต้นแบบของหน่วยงานภายในมหาวิทยาลัย	รวบรวมและตรวจสอบข้อมูลความต้องการพื้นฐานร่วมกันด้านต่างๆ จากหน่วยงานในมหาวิทยาลัย วัตถุประสงค์ : เพื่อให้ได้ข้อมูลที่ถูกต้องและเป็นปัจจุบันตรงกับความต้องการของหน่วยงานต่างๆ	ความต้องการหรือข้อมูลที่แตกต่างกันมากของแต่ละหน่วยงาน	เว็บไซต์ต้นแบบไม่สามารถตอบสนองความต้องการของทุกหน่วยงานได้	ประสานความร่วมมือกับหน่วยงานต่างๆ เพื่อปรับรูปแบบของข้อมูลในเว็บไซต์ให้สอดคล้องกัน	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	
๒. ความปลอดภัยในการใช้เครื่องคอมพิวเตอร์ของมหาวิทยาลัย วัตถุประสงค์: เพื่อดูแลอุปกรณ์คอมพิวเตอร์และความปลอดภัยจาก	๑. เพิ่มความเข้มงวดในการใช้อุปกรณ์ต่อพ่วงประเภทจัดเก็บข้อมูลแบบพกพา ๒. เพิ่มความเข้มงวดในการเข้าถึงระบบเว็ปไซต์ภายนอกต่างๆ	การโจมตีโดยไวรัสคอมพิวเตอร์มีการพัฒนาอย่างต่อเนื่อง	คอมพิวเตอร์ไม่ติดตั้งหรือ update โปรแกรมป้องกันไวรัส	ดูแลตรวจสอบโปรแกรมป้องกันไวรัสให้เป็นปัจจุบันและพร้มใช้งานได้	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

โครงการ/กิจกรรม วัตถุประสงค์ (๑)	ขั้นตอนหลักและ วัตถุประสงค์ (๒)	ความเสี่ยงที่ยังเหลืออยู่ (๓)	ปัจจัยเสี่ยง (๔)	การจัดการความเสี่ยง (๕)	กำหนดเสร็จ/ ผู้รับผิดชอบ (๖)	หมายเหตุ (๗)
การโจมตีโดยไวรัสคอมพิวเตอร์	วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง					
๓. ความพร้อมของเทคโนโลยีสารสนเทศ วัตถุประสงค์: เพื่อให้ระบบสารสนเทศของศูนย์การเรียนรางน้ำมีความพร้อมและเกิดประโยชน์สูงสุดในการให้บริการแก่นักศึกษา	๑. สำรวจความพร้อมของระบบสารสนเทศ ๒. ดำเนินการงานตามวัตถุประสงค์ ๓. ติดตามและประเมินผลการให้บริการแก่นักศึกษา วัตถุประสงค์ : เพื่อให้การดำเนินงานด้านคอมพิวเตอร์เป็นไปอย่างต่อเนื่อง	๑. จำนวนเครื่องคอมพิวเตอร์ยังไม่เพียงพอต่อการใช้งานเมื่อเทียบกับจำนวนนักศึกษา ๒. คอมพิวเตอร์และระบบการใช้งานเกิดความล่าช้าอยู่เสมอ ๓. ขาดประสิทธิภาพในการดูแล	๑.๑ การหมดสัญญาเช่าเครื่องคอมพิวเตอร์ของมหาวิทยาลัยและยังไม่มีการจัดเครื่องใหม่มาทดแทน ๑.๒ สัญญาณ wireless มีปัญหา ๑.๓ บุคลากรผู้ดูแลการบริการด้านคอมพิวเตอร์ไม่เพียงพอในกรณีมีงานซ้ำซ้อน	๑.๑.๑ ให้นักศึกษานำ Note Book ส่วนตัวที่ได้รับจากมหาวิทยาลัยมาใช้งานทดแทนเครื่องที่หมดสัญญาเช่า ๑.๑.๒ ตรวจสอบจุดอับสัญญาณและปรับปรุงแก้ไข ๑.๑.๓ มอบหมายให้นักศึกษาช่วยงานในโครงการของศูนย์สนเทศและแนะแนวการศึกษาและอาชีพมาช่วยให้บริการ	กันยายน ๒๕๖๐ สำนักวิทยบริการและเทคโนโลยีสารสนเทศ	

รายงานผลการบริหารความเสี่ยง ประจำปีงบประมาณ พ.ศ. ๒๕๖๐

หน่วยงาน สำนักวิทยบริการและเทคโนโลยีสารสนเทศ

ความเสี่ยง	ผลกระทบ	มาตรการ	สถานะการดำเนินงาน	การจัดการความเสี่ยง	ปัญหาและอุปสรรค
ความเสี่ยงด้านสวัสดิการในชีวิตและทรัพย์สิน					
๑.๑ หนังสือสูญหาย ๑.๒ ผู้ใช้บริการฉีกหนังสือหรือวารสารที่ตนเองต้องการ	๑.๑.๑ ผู้ใช้บริการขาดความตระหนักเกี่ยวกับการยืม-คืนหนังสือ ๑.๑.๒ ผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้ห้องสมุดอย่างเคร่งครัด	๑.๑ ตรวจสอบการเข้า-ออกเพื่อตรวจจับการขโมยหนังสือ ๑.๒ ประชาสัมพันธ์ภายในอาคารวิทยบริการเรื่องการใช้ห้องสมุดอย่างต่อเนื่อง	★ ★	๑.๑ ตรวจสอบการเข้า-ออกบรีเวณประตูทางเข้า-ออก ๒ ด้านคือ ด้านห้องสมุด และด้าน Virtual Library ๑.๒ จัดทำเอกสารและสื่อประชาสัมพันธ์อย่างทั่วถึงในบริเวณห้องสมุด	
๑.๑ อุปกรณ์ประกอบของเครื่องคอมพิวเตอร์ PC สูญหาย เช่น Mouse RAM	๑.๑.๑ ผู้ใช้บริการขาดจิตสำนึกในการใช้บริการคอมพิวเตอร์ของมหาวิทยาลัย ๑.๑.๒ มูลค่าของอุปกรณ์มีราคาสูง	๑.๑ รณรงค์การใช้บริการเครื่องคอมพิวเตอร์ PC ๑.๒ ควบคุมการให้บริการโดยกล้องวงจรปิด หากมีเหตุการณ์ผิดปกติ	★ ★	๑.๑ รณรงค์ด้วยการมีเจ้าหน้าที่ให้คำปรึกษาในการใช้งานเครื่องคอมพิวเตอร์ ๑.๒ เจ้าหน้าที่รักษาความปลอดภัยเพิ่มความเข้มงวดในการเดินตรวจเช็ค	
ความเสี่ยงด้านการเงิน					
การใช้งบประมาณไม่เป็นไปตามแผนที่กำหนดไว้	นโยบายการดำเนินงานเปลี่ยนแปลงเพื่อให้สอดคล้องกับเหตุการณ์ปัจจุบัน	มีการคาดการณ์ล่วงหน้าและมีการปรับแผนการดำเนินงานให้สอดคล้องกับนโยบาย	★	เจ้าหน้าที่จัดซื้อจัดจ้างของสำนักได้ดำเนินการโครงการและเบิกจ่ายตามแผนประจำปีงบประมาณ ๒๕๕๔	มีโครงการและกิจกรรมที่นอกเหนือจากแผนปฏิบัติราชการ

ความเสี่ยง	ผลกระทบ	มาตรการ	สถานะการดำเนินงาน	การจัดการความเสี่ยง	ปัญหาและอุปสรรค
ความเสี่ยงด้านยุทธศาสตร์ กลยุทธ์					
๑.๑ ขาดการบูรณาการการใช้ข้อมูลเทคโนโลยีสารสนเทศระหว่างหน่วยงาน	๑.๑.๑ ฐานข้อมูลในแต่ละหน่วยงานมีรูปแบบโครงสร้างที่แตกต่างกัน	๑.๑.๑ ปรับปรุงข้อมูลพื้นฐานและบูรณาการความเชื่อมโยงระบบฐานข้อมูลจากทุกหน่วยงานของมหาวิทยาลัยเพื่อในการบริหารและประกันคุณภาพ ๑.๑.๒ พัฒนาระบบฐานข้อมูลของแต่ละหน่วยงานให้มีโครงสร้างเดียวกัน	★	๑.๑ มีการจัดทำความเชื่อมโยงของฐานข้อมูลที่ช่วยในการตัดสินใจ คือ ข้อมูลนักศึกษา ข้อมูลบุคลากร ข้อมูลด้านการเงิน และข้อมูลด้านการวิจัย โดยแต่ละรายการสามารถหาความเชื่อมโยงของข้อมูลได้	ข้อมูลด้านการวิจัยและการเงินอยู่ระหว่างการจัดทำเนื่องจากรอข้อมูลมา Process ในการปรับปรุงฐานข้อมูล
ความเสี่ยงด้านปฏิบัติและไม่ปฏิบัติตามกฎหมายและกฎระเบียบ					
๑.๑ บุคลากร นักศึกษา บางส่วนยังฝ่าฝืนพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐	๑.๑.๑ บุคลากร นักศึกษา บางส่วนยังขาดความใส่ใจตระหนักถึงโทษที่ได้รับเกี่ยวกับการกระทำความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ ผู้โจรกรรมข้อมูลทางคอมพิวเตอร์ใช้พื้นที่ในการกระทำผิดต่อความมั่นคงของประเทศ หรือหมิ่นประมาทผู้อื่นทำให้ได้รับความเสียหาย	๑.๑.๑ เผยแพร่ประชาสัมพันธ์บทลงโทษของการกระทำความผิดเกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ ๑.๑.๒ เพิ่มระบบรักษาความปลอดภัย ในการเข้าถึงหรือโจรกรรมข้อมูลให้รัดกุม	★ ★	๑.๑ เผยแพร่ข้อบังคับเกี่ยวกับการกระทำความผิดทางประกาศสำหรับนักศึกษา และคู่มือการใช้ ICT ของสำนัก ๑.๒ .๑ มีการติดตั้ง proxy server เพื่อแสดงตัวตนของผู้เข้าใช้งานทุกครั้ง รวมถึงการติดตั้ง firewall เพื่อป้องกันการโจรกรรมข้อมูลจากภายในและภายนอกมหาวิทยาลัย	บุคลากรเพิกเฉยต่อการกระทำผิด

ความเสี่ยง	ผลกระทบ	มาตรการ	สถานะการดำเนินงาน	การจัดการความเสี่ยง	ปัญหาและอุปสรรค
				๑.๒.๒ มีการติดตั้งโปรแกรม antivirus ให้กับเครื่องคอมพิวเตอร์ทุกเครื่องภายในมหาวิทยาลัย	
ความเสี่ยงด้านบุคลากรและหลักธรรมาภิบาล					
ข้อเปรียบเทียบอัตราค่าตอบแทนของบุคลากรภาครัฐและเอกชน	๑.๑ อัตราค่าตอบแทนของภาคเอกชนสูงกว่าภาครัฐ ๑.๒ ค่าครองชีพในสถานการณ์ปัจจุบันที่มีอัตราสูง	๑.๑.๑ ส่งเสริมการได้รับค่าตอบแทนเชี่ยวชาญเฉพาะด้าน ๑.๑.๒ สนับสนุนการพัฒนาบุคลากรให้มีความก้าวหน้าในสายงาน	★ ★	๑.๑ บุคลากรของสำนักได้เข้าทดสอบ certificate เฉพาะด้าน เช่น ITIL, cisco และ oracle เป็นต้น ๑.๒ จัดให้บุคลากรเข้าร่วมการอบรมตามความเชี่ยวชาญของแต่ละบุคคลอย่างน้อย ๑ ด้าน	การสอบ certificate มีราคาค่อนข้างสูง
ความเสี่ยงด้านเทคโนโลยีสารสนเทศ					
ความต้องการหรือข้อมูลที่แตกต่างกันมากของแต่ละหน่วยงาน	เว็บไซต์ต้นแบบไม่สามารถตอบสนองความต้องการของทุกหน่วยงานได้	ประสานความร่วมมือกับหน่วยงานต่างๆ เพื่อปรับรูปแบบของข้อมูลในเว็บไซต์ให้สอดคล้องกัน	★	มอบผู้รับผิดชอบโดยตรงเพื่อประสานงานกับหน่วยงานต่างๆ ในการปรับปรุงข้อมูลให้เหมาะสม	
การโจมตีโดยไวรัสคอมพิวเตอร์มีการพัฒนาอย่างต่อเนื่อง	คอมพิวเตอร์ไม่ติดตั้งหรือ update โปรแกรมป้องกันไวรัส	ดูแลตรวจสอบโปรแกรมป้องกันไวรัสให้เป็นปัจจุบันและพร้มใช้งานได้	★	จัดกิจกรรม big cleaning เครื่องคอมพิวเตอร์ภายในมหาวิทยาลัย	ลักษณะการใช้งานของแต่ละหน่วยงานมีความแตกต่างกันทำให้จำเป็นต้องอธิบายวิธีการใช้งานของแต่ละบุคคล

ความเสี่ยง	ผลกระทบ	มาตรการ	สถานะการดำเนินงาน	การจัดการความเสี่ยง	ปัญหาและอุปสรรค
๑. จำนวนเครื่องคอมพิวเตอร์ยังไม่เพียงพอต่อการใช้งานเมื่อเทียบกับจำนวนนักศึกษา ๒. คอมพิวเตอร์และระบบการใช้งานเกิดความล่าช้าอยู่เสมอ ๓. ขาดประสิทธิภาพในการดูแล	๑.๑ การหมดสัญญาเช่าเครื่องคอมพิวเตอร์ของมหาวิทยาลัยและยังไม่มีการจัดเครื่องใหม่มาทดแทน ๑.๒ สัญญาณ wireless มีปัญหา ๑.๓ บุคลากรผู้ดูแลการบริการด้านคอมพิวเตอร์ไม่เพียงพอในกรณีมีงานซ้ำซ้อน	๑.๑.๑ ให้นักศึกษานำ Note Book ส่วนตัวที่ได้รับจากมหาวิทยาลัยมาใช้งานทดแทนเครื่องที่หมดสัญญาเช่า ๑.๑.๒ ตรวจสอบจุดอับสัญญาณและปรับปรุงแก้ไข ๑.๑.๓ มอบหมายให้นักศึกษาช่วยงานในโครงการของศูนย์สนเทศและแนะแนวการศึกษาและอาชีพมาช่วยให้บริการ	★ ★ ★	๑.๑ มีการจัดหาเครื่องคอมพิวเตอร์มาทดแทน ๑.๒ มีการติดตั้ง wireless เพิ่มเติม ๑.๓ รับนักศึกษามาช่วยงานช่างเทคนิคและระบบเครือข่าย	

สถานะการดำเนินงาน

★ = ดำเนินการแล้ว เสร็จตามกำหนดการ

√ = ดำเนินการแล้ว เสร็จล่าช้ากว่ากำหนดการ

X = ยังไม่ได้เริ่มดำเนินการ

○ = อยู่ระหว่างดำเนินการ