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 ผู้ที่ได้รับการแต่งตั้งจากมหาวิทยาลัยสวนดุสิตให้รับผิดชอบด้านเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

"คณะกรรมการนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร" หมายถึง คณะกรรมการที่ได้รับการแต่งตั้งจากมหาวิทยาลัยสวนดุสิตเพื่อทำหน้าที่ในการกำหนด ตรวจสอบ ทบทวน ปรับปรุงนโยบายการรักษาความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศและการสื่อสาร รวมทั้งตรวจสอบและประเมินความเสี่ยงของระบบเทคโนโลยีสารสนเทศและการสื่อสารของมหาวิทยาลัย

"ผู้ตรวจสอบภายใน" หมายถึง บุคลากรภายในมหาวิทยาลัยที่ได้รับการแต่งตั้งจากมหาวิทยาลัยเพื่อทำหน้าที่ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

"ผู้ตรวจสอบจากภายนอก" หมายถึง เป็นบุคคลภายนอกที่มีความรู้ ความสามารถทางด้านเทคโนโลยีสารสนเทศที่ได้รับเชิญเป็นผู้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของมหาวิทยาลัย

"บทลงโทษ" หมายถึง บทลงโทษที่มหาวิทยาลัยเป็นผู้กำหนดหรือบทลงโทษตามกฎหมาย

"ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลขที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"บัญชีรายชื่อ (Account Internet)" หมายถึง รายการชื่อผู้ใช้และรหัสผ่านเพื่อนำไปใช้ในการพิสูจน์ยืนยันตัวตนเพื่อเข้าใช้งานระบบสารสนเทศนั้นๆ

"การพิสูจน์ยืนยันตัวตน (Authentication)" หมายถึง ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้บริการระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดย ใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password

"การยืนยันตัวบุคคล (Identification)" หมายถึง ข้อมูลที่สามารถใช้ระบุตัวตน ติดต่อหรือค้นหาบุคคลหนึ่งบุคคลใดโดยเฉพาะ หรือเป็นข้อมูลที่ใช้ร่วมกับข้อมูลอื่นเพื่อระบุตัวบุคคลหนึ่งบุคคลนั้น โดยบุคคลนั้นต้องได้รับการอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

"การเข้ารหัสลับ (Encryption)" หมายถึง การนำข้อมูลเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องมีโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"การถอดรหัส (Decryption)" หมายถึง วิธีการที่ทำการเปลี่ยนแปลงข้อมูลที่ได้จากการเข้ารหัสข้อมูล เป็นข้อมูลก่อนที่จะถูกทำการเข้ารหัส

"การเข้าสู่ระบบจากระยะไกล (Remote Access)" หมายถึง การเข้าถึงคอมพิวเตอร์หรือเครือข่ายจากระบบเครือข่ายอื่นระยะทางไกลผ่านระบบอินเทอร์เน็ต

"VPN (Virtual Private Network)" หมายถึง เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะแล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

ผู้ดูแลระบบ หรือ แอดมิน (System administrator)" หมายถึง ผู้ทำหน้าที่บริหารและจัดการระบบคอมพิวเตอร์ในองค์กร โดยดูแลการติดตั้งและบำรุงรักษาระบบปฏิบัติการ การติดตั้งฮาร์ดแวร์ การติดตั้งและการปรับปรุงซอฟต์แวร์ สร้าง ออกแบบและบำรุงรักษาบัญชีผู้ใช้

"ตัวแทนผู้ดูแลระบบ (Delegate Administrator)" หมายถึง ตัวแทนผู้ดูแล ที่จะได้สิทธิ์เฉพาะในการบริหารจัดการระบบสารสนเทศนั้น 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