(สำเนา)

ประกาศมหาวิทยาลัยบูรพา
ที่ ๐๗๙๙ /๒๕๖๐
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยบูรพา มีความมั่นคง ปลอดภัย สามารถดำเนินงานได้อย่างมีประสิทธิภาพ และมิให้มีผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งหรือผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อการเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยบูรพา และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม หรือไม่สอดคล้องตามมาตรา ๗ ในพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

อาศัยอำนาจตามความในมาตรา ๒๖ และมาตรา ๓๒ (๓) แห่งพระราชบัญญัติมหาวิทยาลัยบูรพา พ.ศ. ๒๕๕๐ จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศมหาวิทยาลัยบูรพา เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐"

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ บรรดาประกาศ ระเบียบ คำสั่งหรือแนวปฏิบัติอื่นใดที่ได้กำหนดไว้แล้ว ซึ่งขัดหรือแย้งกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ข้อ ๔ ในประกาศนี้

๔.๑ "มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยบูรพา

๔.๒ "ส่วนงาน" หมายความว่า ส่วนงานตามมาตรา ๙ ของพระราชบัญญัติมหาวิทยาลัยบูรพา พ.ศ. ๒๕๕๐

๔.๓ "สำนักคอมพิวเตอร์" หมายความว่า สำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

๔.๔ "ผู้บริหารระดับสูงสุด" หมายความว่า อธิการบดี มหาวิทยาลัยบูรพา

๔.๕ "ผู้บริหารระดับสูง" หมายความว่า รองอธิการบดี และหัวหน้าส่วนงาน

๔.๖ "ผู้อำนวยการสำนักคอมพิวเตอร์" หมายความว่า ผู้อำนวยการสำนักคอมพิวเตอร์มหาวิทยาลัยบูรพา

๔.๗ "ผู้ใช้งาน" หมายความว่า ผู้ปฏิบัติงานในมหาวิทยาลัยบูรพา และให้หมายความรวมถึงนิสิตมหาวิทยาลัยบูรพา นักเรียนโรงเรียนสาธิตอาชีวศึกษา มหาวิทยาลัยบูรพา นักเรียนโรงเรียนสาธิต "พิบูลบำเพ็ญ" มหาวิทยาลัยบูรพา บุคคลอื่นที่มหาวิทยาลัยบูรพามอบหมายให้ปฏิบัติงานตามสัญญา และผู้ใช้งานทั่วไป

๔.๘ "ผู้ดูแลระบบ" หมายความว่า ผู้ที่ได้รับมอบหมายจากหัวหน้าส่วนงาน ให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบคอมพิวเตอร์ และระบบเครือข่ายให้ทำงานได้อย่างมีประสิทธิภาพ

๔.๙ "สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของมหาวิทยาลัยบูรพา

๔.๑๐ "สินทรัพย์" หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูลและสารสนเทศของมหาวิทยาลัยบูรพา

๔.๑๑ "ระบบเครือข่าย" หมายความว่า เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยบูรพา

๔.๑๒ "การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานระบบเครือข่าย ระบบสารสนเทศและอุปกรณ์ในการประมวลผลข้อมูล ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบ

๔.๑๓ "ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความเชื่อถือ (reliability)

๔.๑๔ "เหตุการณ์ด้านความมั่นคงปลอดภัย (information security incident)" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือระบบเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๔.๑๕ "สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของมหาวิทยาลัยถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่มหาวิทยาลัย หรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๖ ให้อธิการบดีรักษาการให้เป็นไปตามประกาศนี้

ส่วนที่ ๑
นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐

ข้อ ๗ นโยบายหลักในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัย (information security event) กำหนดประเด็นสำคัญ ดังนี้

<u>หมวดที่ ๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ</u>

(ส่วนที่ ๒ แนวปฏิบัติฯ หมวดที่ ๑)

(๑) การเข้าถึงระบบสารสนเทศและระบบเครือข่าย เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล ให้คำนึงถึงความมั่นคงปลอดภัยในการใช้งาน โดยกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึง กำหนดสิทธิ และการปรับปรุงสิทธิ เพื่อให้ผู้ใช้งานทุกระดับได้เข้าถึงข้อมูลและใช้งานได้ตามสิทธิที่กำหนดให้

(๒) การบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

(๓) การควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

(๔) การควบคุมการเข้าถึงโปรแกรมประยุกต์ และสารสนเทศ เพื่อป้องกันการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานระบบสารสนเทศของมหาวิทยาลัย และป้องกันความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

<u>หมวดที่ ๒ การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ</u>

(ส่วนที่ ๒ แนวปฏิบัติฯ หมวดที่ ๒)

ระบบสารสนเทศต้องจัดทำระบบสำรองของสารสนเทศให้อยู่ในสภาพพร้อมใช้งาน พร้อมทั้งจัดทำแผนเตรียมความพร้อมฉุกเฉิน เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

<u>หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ</u>

(ส่วนที่ ๒ แนวปฏิบัติฯ หมวดที่ ๓)

กำหนดให้ผู้ดูแลระบบตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในส่วนงานของแต่ละส่วนงาน (internal auditor) หรือผู้ตรวจสอบด้านความมั่นคงปลอดภัยจากหน่วยงานภายนอกมหาวิทยาลัย (external auditor)

<u>หมวดที่ ๔ การทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ</u>

ให้ทำการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นปัจจุบัน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๒
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐

หมวดที่ ๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

ตอนที่ ๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ (access control)

ข้อ ๘ ผู้ดูแลระบบกำหนดสิทธิการเข้าถึงหรือควบคุม (๑) การใช้งานระบบเครือข่าย ระบบสารสนเทศ และอุปกรณ์ในการประมวลผลข้อมูล โดยแบ่งกลุ่มผู้ใช้งานและกำหนดสิทธิของผู้ใช้งานให้เหมาะสมกับบทบาทและหน้าที่ของผู้ใช้งานแต่ละกลุ่ม (๒) กรณีของผู้รับเหมาดำเนินการ (outsource) ในเรื่องต่าง ๆ ให้ขออนุญาตเป็นลายลักษณ์อักษร ระบุระยะเวลาการใช้งาน ลงนามรักษาความลับ และได้รับการพิจารณาอนุญาตจากหัวหน้าส่วนงาน (๓) นอกจากนี้ให้ผู้ดูแลระบบตรวจสอบและปรับปรุงความถูกต้องของการให้สิทธิ ระงับสิทธิและยกเลิกสิทธิอย่างสม่ำเสมอ

ข้อ ๙ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร ให้เชื่อมต่อเข้าใช้งานระบบเครือข่ายโดยใช้บัญชีผู้ใช้งานที่ได้รับจากสำนักคอมพิวเตอร์ ผ่านระบบ VPN (Virtual Private Network) ของมหาวิทยาลัย

ข้อ ๑๐ ผู้ดูแลระบบจัดแบ่งประเภทของข้อมูล ลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล เวลาและช่องทางการเข้าถึงข้อมูล ดังนี้

(๑) ประเภทของข้อมูล จัดเรียงตามลำดับความสำคัญ ดังนี้

(ก) ข้อมูลด้านการบริหาร

(ข) ข้อมูลด้านการเรียนการสอน

(ค) ข้อมูลด้านการวิจัย

(ง) ข้อมูลสำหรับประชาชนทั่วไป

(๒) ระดับชั้นการเข้าถึง

(ก) ระดับผู้บริหารระดับสูง เข้าถึงข้อมูลภาพรวมด้านการบริหาร ด้านการเรียนการสอน และด้านการวิจัย ตามอำนาจหน้าที่และลำดับชั้นการบังคับบัญชาในส่วนงาน

(ข) ระดับผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมาย มีสิทธิในการบริหารจัดการระบบและเข้าถึงข้อมูลตามที่ได้รับมอบหมาย

(ค) ระดับผู้ใช้งานภายในส่วนงาน เข้าถึงข้อมูลได้ตามอำนาจหน้าที่ที่ได้รับมอบหมาย

(ง) ประชาชนทั่วไป เข้าถึงข้อมูลได้เฉพาะข้อมูลสาธารณะ ข้อมูลสำหรับประชาชนทั่วไป

(๓) ช่องทางการเข้าถึงข้อมูล

เข้าถึงได้โดยตรงหรือผ่านระบบงานได้ตลอดเวลา ตามสิทธิของผู้ใช้งาน

ข้อ ๑๑ ผู้ดูแลระบบ ทำการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

ข้อ ๑๒ ผู้ดูแลระบบ ทำการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิของผู้ใช้งาน เพื่อเป็นหลักฐานในการตรวจสอบ

ข้อ ๑๓ ผู้ดูแลระบบ ทำการบันทึกการผ่านเข้าออกสถานที่ตั้งของระบบสารสนเทศ

ตอนที่ ๒ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management)

ข้อ ๑๔ ผู้ดูแลระบบ ดำเนินการดังนี้

(๑) จัดทำแบบฟอร์มการลงทะเบียนของผู้ใช้งานประเภทบุคลากร เพื่อเข้าใช้งานสารสนเทศ กรณีนิสิต ระบบจะสร้างบัญชีผู้ใช้งานให้อัตโนมัติเมื่อรายงานตัวเข้าเป็นนิสิต

(๒) ตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๓) ตรวจสอบ ให้สิทธิของผู้ใช้งานและยกเลิกสิทธิที่เหมาะสมต่อหน้าที่ความรับผิดชอบ

(๔) กำหนดให้มีการแจกเอกสารหรือสิ่งที่แสดงเป็นลายลักษณ์อักษรให้แก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิของผู้ใช้งานและหน้าที่ความรับผิดชอบในการเข้าถึงระบบสารสนเทศ

ข้อ ๑๕ สิทธิของผู้ใช้งาน มีการบริหารจัดการในแต่ละระดับดังนี้

(๑) ผู้บริหาร และผู้ดูแลระบบ มีสิทธิเข้าถึงข้อมูลทั้งหมด

(๒) ผู้ใช้งานภายในส่วนงาน มีสิทธิเข้าถึงข้อมูลตามหน้าที่ความรับผิดชอบ

ข้อ ๑๖ ผู้ดูแลระบบ ทบทวนบัญชีผู้ใช้งาน สิทธิการใช้งาน อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยปฏิบัติตามแนวทาง ดังนี้

(๑) พิมพ์รายชื่อของผู้ที่ยังมีสิทธิในระบบแยกตามส่วนงาน

(๒) จัดส่งรายชื่อให้แก่หัวหน้าส่วนงานเพื่อทบทวนรายชื่อและสิทธิการใช้งานว่าถูกต้องหรือไม่

(๓) ดำเนินการแก้ไขข้อมูลสิทธิต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งกลับจากส่วนงาน

(๔) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เมื่อลาออกต้องดำเนินการภายใน ๓ วัน หรือเมื่อเปลี่ยนตำแหน่งงานภายในต้องดำเนินการภายใน ๗ วัน สำหรับประเภทบุคลากร และยกเลิกสิทธิโดยระบบสำหรับนิสิตเมื่อสำเร็จการศึกษา

ข้อ ๑๗ ผู้ดูแลระบบ บริหารจัดการรหัสผ่าน ดังนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๓) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการให้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าส่วนงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิพิเศษที่ได้รับ ว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ข้อ ๑๘ ผู้ดูแลระบบ บริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังนี้

(๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) กำหนดรายชื่อผู้ใช้งาน (username) และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) ในการรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ให้ใช้วิธีการเข้ารหัส (encryption) ที่เป็นมาตรฐานสากล

(๕) กำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกส่วนงาน เช่น บำรุงรักษา ตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ข้อ ๑๙ หัวหน้าส่วนงานพิจารณาประเด็นต่าง ๆ ทางด้านความมั่นคงปลอดภัย และจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงานสารสนเทศทางธุรกิจที่เชื่อมโยงกัน (business information systems) หรือระบบสารสนเทศที่จะเชื่อมโยง ดังนี้

(๑) กำหนดนโยบายและมาตรการเพื่อควบคุม ป้องกัน และบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิหรือได้รับอนุญาตให้เข้าใช้งาน

(๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกัน ในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

ตอนที่ ๓ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities)

ข้อ ๒๐ การใช้งานรหัสผ่าน กำหนดให้ผู้ใช้งานปฏิบัติ ดังนี้

(๑) ป้องกัน ดูแล รักษาข้อมูลบัญชีชื่อผู้ใช้งาน และรหัสผ่าน ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่ แจกจ่าย ทำให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) กำหนดรหัสผ่านด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ประกอบด้วย ตัวเลข (numerical character) ตัวอักษร (alphabet) และตัวอักษรพิเศษ (special character)

(๓) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๔) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๕) เปลี่ยนรหัสผ่านภายใน ๑๘๐ วันหรือเมื่อมีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

ข้อ ๒๑ การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานต้องใช้ใบรับรองอิเล็กทรอนิกส์สำหรับบุคคลธรรมดาหรือนิติบุคคล (digital signature) มาใช้สำหรับการเข้ารหัสข้อมูล

ข้อ ๒๒ การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน อันมีกฎหมายกำหนดให้เป็นความผิด ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตาม ให้ถือว่าเป็นความรับผิดชอบส่วนบุคคล ซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ข้อ ๒๓ ผู้ใช้งานทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของส่วนงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากรหัสผ่านหมดอายุ หรือเกิดจากความผิดพลาดใด ๆ ผู้ใช้งานจะต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ ๒๔ ผู้ใช้งานต้องตั้งเวลาล๊อคหน้าจอคอมพิวเตอร์ เมื่อไม่มีการใช้งานนานเกิน ๑๕ นาที

ข้อ ๒๕ ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครองหรือดูแลของส่วนงาน ห้ามเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนงาน

ข้อ ๒๖ ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัย และข้อมูลของผู้รับบริการ หากเกิดการสูญหาย การนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาต ผู้ใช้งานจะต้องร่วมรับผิดชอบต่อความเสียหายนั้นด้วย

ข้อ ๒๗ ผู้ใช้งานต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล ตลอดจนเอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์ หรือสารสนเทศต่าง ๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อ ๒๘ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บรักษา ใช้งาน และป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร มหาวิทยาลัยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่มหาวิทยาลัยต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับมหาวิทยาลัย ซึ่งมหาวิทยาลัยอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

ข้อ ๒๙ ห้ามผู้ใช้งานเปิดหรือใช้งานโปรแกรมประเภท peer-to-peer (วิธีการจัดระบบเครือข่ายคอมพิวเตอร์แบบหนึ่ง ที่กำหนดให้คอมพิวเตอร์ในระบบเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกัน หมายความว่า แต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เอง การจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของคอมพิวเตอร์เครื่องใดก็ได้ แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (file server) เท่านั้น)

ข้อ ๓๐ ห้ามผู้ใช้งานใช้สินทรัพย์ของส่วนงาน ที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพหรือสิ่งอื่นใด ที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๓๑ ห้ามผู้ใช้งานใช้สินทรัพย์ของส่วนงาน เพื่อการรบกวน ก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๓๒ ห้ามผู้ใช้งานใช้สินทรัพย์ของมหาวิทยาลัยเพื่อประโยชน์ทางการค้า

ข้อ ๓๓ ห้ามผู้ใช้งานกระทำการใด ๆ เพื่อการดักข้อมูล ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดในระบบเครือข่าย ระบบสารสนเทศของมหาวิทยาลัยโดยเด็ดขาด ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม

ข้อ ๓๔ ห้ามผู้ใช้งานกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของส่วนงานต้องหยุดชะงัก

ข้อ ๓๕ ห้ามผู้ใช้งานใช้ระบบสารสนเทศของมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนงานหรือผู้ดูแลระบบที่ได้รับมอบหมาย

ข้อ ๓๖ ห้ามผู้ใช้งานกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสผ่านส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใด ๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรก็ตาม

ข้อ ๓๗ ห้ามผู้ใช้งานติดตั้งอุปกรณ์หรือกระทำการใด ๆ เพื่อเข้าถึงระบบสารสนเทศของมหาวิทยาลัย โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนงานหรือผู้ดูแลระบบ

ตอนที่ ๔ การควบคุมการเข้าถึงระบบเครือข่าย (network access control)

ข้อ ๓๘ ในการใช้บริการระบบเครือข่าย ผู้ดูแลระบบกำหนดสิทธิการใช้งานโดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาของส่วนงานเจ้าของระบบเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวปีละ ๑ ครั้ง

ข้อ ๓๙ ผู้ดูแลระบบกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัยได้ โดยให้ผู้ใช้งานที่จะเข้าใช้งานระบบ แสดงตัวตน (identification) ด้วยชื่อผู้ใช้งานทุกครั้ง

ข้อ ๔๐ การควบคุมอุปกรณ์บนเครือข่าย (equipment control in network) ดำเนินการดังนี้

(๑) ผู้ดูแลระบบใช้ซอฟต์แวร์ควบคุมสำหรับการบริหารจัดการอุปกรณ์บนระบบเครือข่ายและอุปกรณ์สื่อสารเคลื่อนที่ ซึ่งสามารถตรวจสอบสถานะของการทำงานของอุปกรณ์ โดยระบุจุดเชื่อมต่อ และ mac address ของอุปกรณ์บนเครือข่ายที่ต่อพ่วงกับระบบเครือข่ายได้

(๒) ผู้ใช้งานที่ต้องการนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์โมบายมาใช้ภายในมหาวิทยาลัย จะต้องนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์โมบาย มาลงทะเบียน mac address ผ่านระบบให้บริการ ก่อนการใช้งานในมหาวิทยาลัย

(๓) ผู้ใช้งานภายในมหาวิทยาลัยแสดงตัวตน ด้วยชื่อผู้ใช้งานทุกครั้งผ่านซอฟต์แวร์ควบคุม เพื่อระบุตัวตน จุดเชื่อมต่อ ของอุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย

(๔) ผู้ดูแลระบบมีสิทธิในการจำกัดอุปกรณ์ต่อพ่วงที่ไม่ได้รับอนุญาตได้

ข้อ ๔๑ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ให้ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่าย ดังนี้

(๑) ผู้ดูแลระบบปิดพอร์ตที่ไม่จำเป็นทุกพอร์ตเพื่อจำกัดและควบคุมการเข้าถึงพอร์ตโดยไม่ได้รับอนุญาต

(๒) ผู้ดูแลระบบกำหนดพอร์ตสำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางระบบเครือข่าย และแจ้งให้ผู้ดูแลระบบที่มีสิทธิในการตรวจสอบและปรับแต่งระบบทราบ

(๓) หากผู้ดูแลระบบตรวจสอบพบการใช้งานพอร์ตโดยผู้ใช้ที่ไม่ได้รับอนุญาต ผู้ดูแลระบบสามารถปิดการใช้งานพอร์ตที่ไม่ได้รับอนุญาตได้ทันที

ข้อ ๔๒ การแบ่งแยกเครือข่าย (segregation in networks) ผู้ดูแลระบบจะทำการแบ่งแยกเครือข่ายสำหรับกลุ่มผู้ใช้งาน โดยแบ่งออกเป็น ๒ เครือข่าย คือ เครือข่ายสำหรับผู้ใช้งานภายใน และเครือข่ายสำหรับผู้ใช้งานภายนอก

ข้อ ๔๓ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ผู้ดูแลระบบจะควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อ ดังนี้

(๑) มีการตรวจสอบการเชื่อมต่อเครือข่าย

(๒) จำกัดสิทธิ ความสามารถของผู้ใช้งานในการเชื่อมต่อเข้าสู่เครือข่าย

(๓) ใช้อุปกรณ์ Firewall สำหรับควบคุมการเชื่อมต่อ

(๔) มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ควบคุมไม่ให้มีการเปิดให้บริการบนเครือข่าย โดยไม่ได้รับอนุญาต

ข้อ ๔๔ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ผู้ดูแลระบบจะควบคุมการจัดเส้นทางบนเครือข่าย เพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ ดังนี้

(๑) ควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (ip address plan)

(๒) กำหนดให้มีการแปลงหมายเลขเครือข่าย เพื่อแยกเครือข่ายย่อย

(๓) กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย กล่าวคือ สามารถเชื่อมเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการใช้บริการเครือข่าย

ข้อ ๔๕ การควบคุมการเข้าใช้งานระบบจากภายนอก ให้ปฏิบัติดังนี้

(๑) การเข้าสู่ระบบจากระยะไกล (remote access) ผู้ดูแลระบบต้องมีการตรวจสอบเพื่อพิสูจน์ตัวตนของผู้ใช้งาน

(๒) การเข้าสู่ระบบจากระยะไกลสู่ระบบสารสนเทศและเครือข่ายของมหาวิทยาลัย ต้องมีการกำหนดมาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

(๓) วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักคอมพิวเตอร์ก่อนและมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

ตอนที่ ๕ การควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ ๔๖ ติดตั้งโปรแกรมช่วยบริหารจัดการและกำหนดชื่อผู้ใช้งาน และรหัสผ่าน ให้กับผู้ใช้งาน

ข้อ ๔๗ กำหนดขั้นตอนปฏิบัติการเข้าถึงระบบปฏิบัติการมีแนวปฏิบัติ ดังนี้

(๑) ไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่าง ๆ ของระบบ ก่อนที่การเข้าสู่ระบบจะเสร็จสมบรูณ์

(๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

ข้อ ๔๘ การยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ให้นำชื่อผู้ใช้งาน และรหัสผ่าน มาตรวจสอบสิทธิของผู้ใช้งานบนระบบ AD (Active Directory) เพื่อเข้าสู่ระบบ

ข้อ ๔๙ ส่วนงานต้องมีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ โดยมีแนวปฏิบัติดังนี้

(๑) มีระบบบริหารจัดการรหัสผ่าน ผ่านระบบเครือข่ายสารสนเทศของมหาวิทยาลัย

(๒) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านของตนเองในครั้งแรกที่มีการเข้าสู่ระบบ

(๓) มีระบบแจ้งระดับความปลอดภัยของรหัสผ่าน

ข้อ ๕๐ การใช้งานโปรแกรมอรรถประโยชน์ ให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานหลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว ให้ผู้ดูแลระบบดำเนินการดังนี้

(๑) จำกัดสิทธิการเข้าถึง และกำหนดสิทธิอย่างรัดกุมในการอนุญาตให้ใช้โปรแกรมอรรถประโยชน์

(๒) กำหนดให้อนุญาตใช้งานโปรแกรมอรรถประโยชน์เป็นรายครั้งไป

(๓) จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

(๔) การเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

(๕) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

(๖) ตรวจสอบการละเมิดลิขสิทธิ์และจัดเก็บหลักฐานการใช้งาน

ตอนที่ ๖ การควบคุมการเข้าถึงโปรแกรมประยุกต์และสารสนเทศ (application and information access control)

ข้อ ๕๑ ผู้ดูแลระบบกำหนดการลงทะเบียนผู้ใช้งานใหม่ ในการใช้งานตามความจำเป็น รวมทั้งขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในส่วนงาน เป็นต้น

ข้อ ๕๒ ผู้ดูแลระบบกำหนดสิทธิการใช้งานระบบสารสนเทศที่สำคัญ ได้แก่ ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ จดหมายอิเล็กทรอนิกส์ ระบบเครือข่ายไร้สาย ระบบอินเทอร์เน็ต เป็นต้น โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากหัวหน้าส่วนงานเป็นลายลักษณ์อักษร รวมทั้งทำการทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

ข้อ ๕๓ การกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศและแอพพลิเคชั่น

(๑) เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศ เกิน ๑๕ นาที (session/idle time out) ให้ตัดการเชื่อมต่อ

(๒) ระบบสารสนเทศหรือแอพพลิเคชั่นที่มีความเสี่ยงหรือมีความสำคัญสูง ให้ใช้งานต่อเนื่องได้ไม่เกิน ๖๐ นาที (limitation of connection time) แล้วตัดการเชื่อมต่อ

ข้อ ๕๔ ผู้ดูแลระบบบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากรสำหรับเข้าใช้โปรแกรมประยุกต์ดังนี้

(๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๓) กำหนดชื่อผู้ใช้งาน หรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๔) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากหัวหน้าส่วนงาน โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันที เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

ตอนที่ ๗ การเข้าถึงเครื่องคอมพิวเตอร์แม่ข่าย (server access control)

ข้อ ๕๕ ผู้ดูแลระบบควบคุมการติดตั้งซอฟต์แวร์ลงไปยังระบบเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการ ให้ปฏิบัติดังนี้

(๑) การติดตั้งหรือปรับปรุงซอฟต์แวร์ของระบบสารสนเทศ ต้องได้รับอนุมัติจากหัวหน้าส่วนงานก่อนดำเนินการ

(๒) ให้ผู้ดูแลระบบเป็นผู้ทำหน้าที่ดำเนินการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย

(๓) ควบคุมการเปลี่ยนแปลงและบันทึกการปฏิบัติงานสำหรับการเปลี่ยนแปลงต่อระบบสารสนเทศของมหาวิทยาลัย

(๔) ไม่ควรติดตั้งรหัสต้นฉบับ (source code) ของระบบสารสนเทศในเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการนั้น ๆ

(๕) ให้จัดเก็บรหัสต้นฉบับและคลังโปรแกรม (library) สำหรับซอฟต์แวร์ของระบบสารสนเทศไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

(๖) ให้ผู้ที่เกี่ยวข้องต้องทำการทดสอบด้านความมั่นคงปลอดภัยของระบบสารสนเทศอย่างครบถ้วน ก่อนดำเนินการติดตั้งบนเครื่องให้บริการระบบสารสนเทศ

(๗) ให้จัดเก็บซอฟต์แวร์เวอร์ชั่นเก่า ข้อมูลที่เกี่ยวข้องกับระบบสารสนเทศเดิมและขั้นตอนปฏิบัติที่เกี่ยวข้องของระบบสารสนเทศในกรณีที่จำเป็นต้องกลับไปใช้เวอร์ชั่นเก่าเหล่านั้น ตามระยะเวลาที่เหมาะสม

ข้อ ๕๖ ให้ทบทวนการทำงานของระบบสารสนเทศภายหลังจากที่เปลี่ยนแปลงระบบปฏิบัติการ ดังนี้

(๑) แจ้งให้ผู้ที่เกี่ยวข้องกับระบบสารสนเทศได้รับทราบเกี่ยวกับการเปลี่ยนแปลงระบบปฏิบัติการ เพื่อให้บุคคลเหล่านั้นมีเวลาเพียงพอในการดำเนินการทดสอบ และทบทวนก่อนที่จะดำเนินการเปลี่ยนแปลงระบบปฏิบัติการ

(๒) พิจารณาวางแผนดำเนินการเปลี่ยนแปลงระบบปฏิบัติการของระบบสารสนเทศ รวมทั้งวางแผนด้านงบประมาณที่จำเป็นต้องใช้ ในกรณีที่มหาวิทยาลัยต้องเปลี่ยนไปใช้ระบบปฏิบัติการใหม่

ข้อ ๕๗ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก

(๑) ควรจัดให้มีการควบคุมการพัฒนาซอฟต์แวร์ที่จัดจ้างจากบุคคลหรือหน่วยงานภายนอก

(๒) ให้ระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับรหัสต้นฉบับในการพัฒนาซอฟต์แวร์ โดยผู้รับจ้างให้บริการจากภายนอก

(๓) ให้กำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี (malware) ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

ข้อ ๕๘ ส่วนงานต้องปฏิบัติตามมาตรการควบคุมช่องโหว่ทางเทคนิค ประกอบด้วย

(๑) กำหนดให้มีการจัดทำบัญชีของระบบสารสนเทศเพื่อใช้สำหรับกระบวนการบริหารจัดการ

(๒) ช่องโหว่ของระบบเหล่านั้น ควรมีการบันทึกดังนี้

(ก) ชื่อซอฟต์แวร์และเวอร์ชั่นที่ใช้งาน

(ข) สถานที่ที่ติดตั้ง

(ค) เครื่องที่ติดตั้ง

(ง) ผู้ผลิตซอฟต์แวร์

(จ) ข้อมูลสำหรับติดต่อผู้ผลิตหรือผู้พัฒนาซอฟต์แวร์นั้น ๆ

(๓) กำหนดให้มีการจัดการกับช่องโหว่สำคัญของระบบสารสนเทศอย่างเหมาะสม โดยทันที

(๔) กระบวนการบริหารจัดการช่องโหว่ของระบบสารสนเทศให้ผู้ดูแลระบบ ดำเนินการดังนี้

(ก) มีการเฝ้าระวังและติดตาม ประเมินความเสี่ยงสำหรับช่องโหว่ของระบบสารสนเทศรวมทั้งการประสานงานเพื่อให้ผู้ที่เกี่ยวข้องดำเนินการแก้ไขช่องโหว่ตามความเหมาะสม

(ข) กำหนดให้ผู้ที่เกี่ยวข้องดำเนินการประเมินความเสี่ยงเมื่อได้รับแจ้ง หรือทราบเกี่ยวกับช่องโหว่นั้น

(๕) ปิดการใช้งานหรือควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบ และปรับแต่งระบบให้ใช้งานได้อย่างจำกัดระยะเวลาเท่าที่จำเป็น โดยต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร

ข้อ ๕๙ การบันทึกเหตุการณ์ที่เกี่ยวข้องกับการใช้งานระบบสารสนเทศ (audit logging) ให้ทำการบันทึกพฤติกรรมการใช้งาน (log) การเข้าถึงระบบสารสนเทศ ดังนี้

(๑) ข้อมูลชื่อบัญชีผู้ใช้งาน

(๒) ข้อมูลวันเวลาที่เข้าถึงระบบ

(๓) ข้อมูลวันเวลาที่ออกจากระบบ

(๔) ข้อมูลเหตุการณ์สำคัญที่เกิดขึ้น

(๕) ข้อมูลการล็อกอิน ทั้งที่สำเร็จและไม่สำเร็จ

(๖) ข้อมูลความพยายามในการเข้าถึงทรัพยากรทั้งที่สำเร็จและไม่สำเร็จ

(๗) ข้อมูลการเปลี่ยนแปลงการตั้งค่า (configuration) ของระบบ

(๘) ข้อมูลแสดงการใช้งานซอฟต์แวร์

(๙) ข้อมูลแสดงการเข้าถึงไฟล์และการกระทำกับไฟล์ เช่น เปิด ปิด เขียน หรืออ่านไฟล์ ฯลฯ

(๑๐) ข้อมูลเลขที่อยู่ไอพีที่เข้าถึง

(๑๑) ข้อมูลโพรโทคอลเครือข่ายที่ใช้

(๑๒) ข้อมูลแสดงการหยุดการทำงานของระบบป้องกันไวรัสคอมพิวเตอร์

(๑๓) ข้อมูลแสดงการสำรองข้อมูลไม่สำเร็จ

ตอนที่ ๘ การใช้งานเครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา

ข้อ ๖๐ ในการใช้งานทั่วไป ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) เครื่องคอมพิวเตอร์ที่มหาวิทยาลัยอนุญาตให้ผู้ใช้งานใช้งานเป็นสินทรัพย์ของมหาวิทยาลัย ดังนั้น ผู้ใช้งานจึงควรใช้งานเครื่องคอมพิวเตอร์อย่างมีประสิทธิภาพเพื่องานของมหาวิทยาลัย

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของมหาวิทยาลัย ที่เป็นโปรแกรมที่มหาวิทยาลัยได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ของมหาวิทยาลัย

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของส่วนงานหรือผู้รับจ้างในการบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับมหาวิทยาลัยเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่าง ๆ ต้องมีการตรวจสอบเพื่อหาไวรัสคอมพิวเตอร์โดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย ฯลฯ

(๗) ห้ามผู้ใช้งานทำการเปลี่ยนแปลงแก้ไขส่วนประกอบย่อย (sub component) ที่ติดตั้งอยู่ภายในรวมถึงแบตเตอรี่

ตอนที่ ๙ การบริหารจัดการสินทรัพย์ (ip, webhost, storage, network equipment, data)

ข้อ ๖๑ ผู้ใช้งานต้องไม่เข้าไปในห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖๒ ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์ เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ ๖๓ ผู้ใช้งานต้องไม่นำเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

ข้อ ๖๔ ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

ข้อ ๖๕ ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะทำลายหรือจำหน่ายอุปกรณ์ดังกล่าว เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ข้อ ๖๖ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่ส่วนงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่ส่วนงานมอบหมาย กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของส่วนงานที่ได้รับมอบหมาย

ข้อ ๖๗ ผู้ใช้งานต้องจัดเก็บเอกสาร สื่อบันทึกข้อมูล และเครื่องคอมพิวเตอร์ ภายหลังจากการใช้งานแล้ว ในสถานที่ที่มีการป้องกันการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ

ข้อ ๖๘ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าสินทรัพย์นั้นจะชำรุด หรือสูญหายตามมูลค่าสินทรัพย์ หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๖๙ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์พกพา ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าส่วนงาน

ข้อ ๗๐ ผู้ใช้งานมีสิทธิใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่ส่วนงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของส่วนงานเท่านั้น ห้ามผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่ส่วนงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัย

ข้อ ๗๑ ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อปฏิบัติข้างต้น ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ตอนที่ ๑๐ การควบคุมการใช้อินเทอร์เน็ต

ข้อ ๗๒ ผู้ดูแลระบบกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ตที่เชื่อมต่อผ่านระบบรักษาความปลอดภัยที่มหาวิทยาลัยจัดสรรไว้เท่านั้น ห้ามผู้ใช้งานทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่นที่ไม่ได้รับการอนุมัติจากผู้อำนวยการสำนักคอมพิวเตอร์

ข้อ ๗๓ การใช้งานเครื่องคอมพิวเตอร์จะต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์และทำการอุดช่องโหว่ก่อนที่จะทำการเชื่อมต่อระบบอินเทอร์เน็ตผ่านเว็บบราวเซอร์

ข้อ ๗๔ ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของมหาวิทยาลัย และต้องไม่ใช้ระบบอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือน หรือเป็นภัยต่อความมั่นคงแห่งชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคมหรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับมหาวิทยาลัย

ข้อ ๗๕ ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของมหาวิทยาลัยที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

ข้อ ๗๖ ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือสินทรัพย์ทางปัญญา

ข้อ ๗๗ ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของมหาวิทยาลัย ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของมหาวิทยาลัย การทำลายความสัมพันธ์กับบุคลากรของส่วนงานอื่น ๆ

ข้อ ๗๘ หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ผู้ใช้งานทำการปิดเว็บบราวเซอร์ เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ตอนที่ ๑๑ การใช้งานเครือข่ายสังคมออนไลน์ (social network)

ข้อ ๗๙ อนุญาตให้ใช้งานเครือข่ายสังคมออนไลน์ในรูปแบบและลักษณะตามที่มหาวิทยาลัยได้กำหนดไว้เท่านั้น

ข้อ ๘๐ ผู้ใช้งานที่ใช้งานเครือข่ายสังคมออนไลน์ ที่อาจมีผลกระทบกับมหาวิทยาลัย ผู้ใช้งานจะต้องแจ้งต่อผู้ดูแลระบบโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

ตอนที่ ๑๒ การควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์

ข้อ ๘๑ การใช้งานจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย ให้ผู้ใช้งานปฏิบัติดังนี้

(๑) ใช้จดหมายอิเล็กทรอนิกส์ ของมหาวิทยาลัยเพื่อติดต่องานของมหาวิทยาลัยเท่านั้น

(๒) ไม่ควรใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นจะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(๓) หลังจากการใช้งาน ควรลงชื่อออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานระบบ

(๔) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(๕) ควรตรวจสอบและลบจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน เพื่อลดปริมาณการใช้พื้นที่ของระบบจดหมายอิเล็กทรอนิกส์ให้เหลือจำนวนน้อยที่สุด

(๖) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้งาน และรหัสผ่าน เป็นความลับไม่ให้รั่วไหลไปถึงบุคคลที่ไม่เกี่ยวข้อง

(๗) ปฏิบัติตามวิธีการใช้งานรหัสผ่านที่ได้กำหนดไว้อย่างเคร่งครัด

ข้อ ๘๒ แนวทางการควบคุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์สำหรับผู้ดูแลระบบ มีดังนี้

(๑) กำหนดสิทธิเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งาน

(๒) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน ผิดพลาดได้ไม่เกิน ๕ ครั้ง

(๓) ทบทวนสิทธิการเข้าใช้งานและปรับปรุงบัญชีผู้ใช้งาน ปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลง เช่น มีการลาออกหรือเปลี่ยนแปลงตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง ฯลฯ

(๔) ควบคุมการเข้าถึงระบบตามแนวทางการบริหารจัดการเข้าถึงผู้ใช้งานที่ได้กำหนดไว้อย่างเคร่งครัด

ตอนที่ ๑๓ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์ และการป้องกันโปรแกรมไม่ประสงค์ดี (software licensing and intellectual property and preventing malware)

ข้อ ๘๓ มหาวิทยาลัยให้ความสำคัญต่อเรื่องสินทรัพย์ทางปัญญา ดังนั้นซอฟต์แวร์ที่ส่วนงานอนุญาตให้ใช้งานหรือที่ส่วนงานมีลิขสิทธิ์ ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็น และห้ามผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ ให้ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

ข้อ ๘๔ ซอฟต์แวร์ที่ส่วนงานได้จัดเตรียมไว้ให้ผู้ใช้งาน ถือเป็นสิ่งจำเป็นต่อการทำงาน ห้ามผู้ใช้งานทำการถอดถอน เปลี่ยนแปลง แก้ไข หรือทำสำเนาเพื่อนำไปใช้งานที่อื่น ๆ ยกเว้นได้รับการอนุญาตจากหัวหน้าส่วนงานหรือผู้ที่ได้รับมอบหมายที่มีสิทธิในลิขสิทธิ์

ข้อ ๘๕ เครื่องคอมพิวเตอร์ของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษา โดยต้องได้รับอนุญาตจากหัวหน้าส่วนงาน

ข้อ ๘๖ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๘๗ ผู้ใช้งานต้องทำการปรับปรุงข้อมูล สำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (update patch) ให้ใหม่เสมอ เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๘๘ ผู้ใช้งานต้องพึงระวังไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

ข้อ ๘๙ เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัส ผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่าย และต้องแจ้งแก่ผู้ดูแลระบบ

ข้อ ๙๐ ห้ามลักลอบทำสำเนา เปลี่ยนแปลง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใด ๆ ที่เป็นสินทรัพย์ทางปัญญาของมหาวิทยาลัย เว้นแต่จะได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้มีอำนาจลงนาม

ข้อ ๙๑ การบริหารจัดการซอฟต์แวร์ที่พัฒนาโดยส่วนงานภายนอก (outsourced software development) ส่วนงานต้องปฏิบัติดังนี้

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิในสินทรัพย์ทางปัญญาสำหรับรหัสต้นฉบับในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอก โดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดี ในซอฟต์แวร์ต่าง ๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟต์แวร์จากส่วนงานภายนอก ส่วนงานต้องดำเนินการเปลี่ยนรหัสผ่านต่าง ๆ

ตอนที่ ๑๔ การตรวจจับการบุกรุกและการป้องกันโปรแกรมไม่ประสงค์ดี (intrusion detection system / intrusion prevention system policy : ids/ips)

ข้อ ๙๒ ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ ids/ips (คือระบบตรวจสอบการบุกรุก และตรวจสอบความปลอดภัยของเครือข่าย เพื่อป้องกันทรัพยากร ระบบสารสนเทศ และข้อมูลบนเครือข่ายภายในส่วนงานให้มีความมั่นคงปลอดภัย เป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่าย พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง)

ข้อ ๙๓ ผู้ดูแลระบบกำหนด policy ของ ids/ips ให้ครอบคลุมทุกโฮสต์ (host) ในเครือข่ายของส่วนงานและเครือข่ายข้อมูลทั้งหมด รวมถึงเส้นทางที่ข้อมูลอาจเดินทาง ซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง และบันทึกข้อมูลจราจร (log) ของการส่งผ่านข้อมูล

ข้อ ๙๔ ผู้ดูแลระบบตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการระบบทั้งหมดใน dmz (demilitarized zone) โดยแยกระบบที่ไวต่อการรบกวน คือ Video Conference ไว้ในโซน dmz และไม่อนุญาตให้ใช้งานจากภายนอกองค์กร

ข้อ ๙๕ ผู้ดูแลระบบทำการ update patch/signature ของระบบ ids/ips เป็นประจำ

ข้อ ๙๖ ผู้ดูแลระบบตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวัน

ข้อ ๙๗ ผู้ดูแลระบบตรวจสอบข้อมูลประจำวันของเครื่องแม่ข่ายที่มีการติดตั้ง host-based ids หากพบพฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด ที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบ พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ให้ผู้ดูแลระบบรายงานให้หัวหน้าส่วนงานทราบ และเก็บบันทึกข้อมูลจราจรไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๙๘ ส่วนงานมีสิทธิในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบ โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูล และทรัพยากรระบบของส่วนงาน จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

ตอนที่ ๑๕ การจัดเก็บข้อมูลจราจรคอมพิวเตอร์

ข้อ ๙๙ จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง และจะต้องระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

ข้อ ๑๐๐ ห้ามผู้ดูแลระบบแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของมหาวิทยาลัย (it auditor) หรือบุคคลที่มหาวิทยาลัยมอบหมาย

ข้อ ๑๐๑ บันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ ฯลฯ เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้ ๙๐ วันนับตั้งแต่การใช้งานสิ้นสุดลง

ตอนที่ ๑๖ การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (wireless lan access control)

ข้อ ๑๐๒ ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของมหาวิทยาลัย จะต้องทำการลงทะเบียนกับผู้ดูแลระบบ โดยจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักคอมพิวเตอร์

ข้อ ๑๐๓ ผู้ดูแลระบบจัดการควบคุมการเข้าถึงระบบเครือข่ายไร้สายโดย

(๑) ทำการลงทะเบียนกำหนดสิทธิของผู้ใช้งานการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ระบบจะต้องได้รับอนุญาตจากผู้ดูแลและระบบตามความจำเป็นในการใช้งาน

(๒) ทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

(๓) ควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ เพื่อป้องกันไม่ให้สัญญาณของอุปกรณ์รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย และป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคารหรือบริเวณขอบเขตที่ควบคุมได้

(๔) ทำการเปลี่ยนค่า ssid ที่ถูกกำหนดเป็นค่าโดยปริยายมาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

(๕) เปลี่ยนค่าชื่อบัญชีรายชื่อ และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และควรจะเลือกใช้ชื่อบัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

(๖) เข้ารหัสข้อมูลระหว่าง wireless lan client และอุปกรณ์กระจายสัญญาณเพื่อให้ยากต่อการดักจับและทำให้ปลอดภัยมากขึ้น

(๗) ติดตั้งอุปกรณ์ป้องกันการบุกรุก (firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในมหาวิทยาลัย

(๘) ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยที่เกิดขึ้นในระบบเครือข่ายไร้สาย และเมื่อพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้รายงานต่อหัวหน้าส่วนงาน และ/หรือ ผู้อำนวยการสำนักคอมพิวเตอร์ทราบโดยทันที

หมวดที่ ๒ การจัดทำระบบสำรองของสารสนเทศ

ข้อ ๑๐๔ ผู้ดูแลระบบจัดทำแนวทางปฏิบัติในการสำรองและกู้คืนข้อมูล โดยจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

(๑) จัดทำบัญชีระบบสารสนเทศทั้งหมดของส่วนงาน พร้อมจัดทำระบบสำรองและจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

(๒) สำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูลดังนี้

(ก) กำหนดประเภทของข้อมูลที่ต้องทำการสำรองและความถี่ในการสำรอง

(ข) กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง

(ค) บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการวัน/เวลาชื่อข้อมูลที่สำรองสำเร็จ/ไม่สำเร็จ เป็นต้น

(ง) ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน

(จ) จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

(ฉ) จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับส่วนงานควรห่างกันเพียงพอ เพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติ

(ช) ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

(ซ) ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

(ฌ) จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

(ญ) ตรวจสอบและทดสอบขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

(ฎ) กำหนดให้มีการเข้ารหัสข้อมูลกับข้อมูลที่ได้สำรองเก็บไว้

ข้อ ๑๐๕ ให้ส่วนงานจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง ตามแนวทางต่อไปนี้

(๑) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยมีรายละเอียดอย่างน้อยดังนี้

(ก) กำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(ข) ประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น

(ค) กำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(ง) กำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

(จ) กำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอกเมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

(ฉ) สร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วน

(๒) ทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐๖ ส่วนงานกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ข้อ ๑๐๗ ส่วนงานทำการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๐๘ ส่วนงานทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละส่วนงาน อย่างน้อยปีละ ๑ ครั้ง

หมวดที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ข้อ ๑๐๙ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ให้ผู้ดูแลระบบดำเนินการดังนี้

(๑) แต่งตั้งคณะกรรมการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศจากผู้เชี่ยวชาญทั้งภายในและภายนอกมหาวิทยาลัย

(๒) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๑๐ แนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องดำเนินการ มีอย่างน้อยดังนี้

(๑) ระบุความเสี่ยงและผลกระทบให้สอดคล้องตามแผนบริหารความเสี่ยงของส่วนงาน

(๒) ทบทวนแผนแก้ไขปัญหาจากสถานการณ์ความไม่แน่นอน และภัยพิบัติที่อาจจะเกิดขึ้นกับระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๓) ประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังนี้

(ก) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(ข) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุ รวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(ค) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

(๔) กำหนดมาตรการจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อยดังนี้

(ก) กำหนดให้ผู้ตรวจสอบเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบแบบอ่านได้อย่างเดียว

(ข) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่น ๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้คณะกรรมการตรวจสอบฯ ใช้งาน รวมทั้งทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

(ค) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

(ง) กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญ ๆ

(จ) กำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๕) ผู้ดูแลระบบจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยระบุผู้รับผิดชอบและหน้าที่ความรับผิดชอบอย่างชัดเจน

(๖) ผู้ดูแลระบบทดสอบและปรับปรุงแผนเตรียมความพร้อมฉุกเฉินอยู่เสมอ เพื่อให้แผนมีความทันสมัยและสามารถใช้งานได้หากเกิดเหตุการณ์ขึ้นจริง

หมวดที่ ๔ การรักษาความปลอดภัยด้านกายภาพ สถานที่และสิ่งแวดล้อม

ข้อ ๑๑๑ ห้องควบคุมระบบเครือข่ายคอมพิวเตอร์ ส่วนงานต้องกำหนดให้ห้องมีลักษณะดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาด หรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้าออกของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อกห้อง หรือใส่กุญแจประตูหน้าต่างเสมอ เมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสาร ให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าว เป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์ โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

ข้อ ๑๑๒ การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย ส่วนงานต้องดำเนินการดังนี้

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบสารสนเทศต่าง ๆ อย่างเหมาะสม เพื่อเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้น

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบสารสนเทศให้ชัดเจน รวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็นพื้นที่ทำงานทั่วไป (general working area) พื้นที่ทำงานของผู้ดูแลระบบ (system administrator area) พื้นที่ติดตั้งอุปกรณ์ระบบสารสนเทศ (it equipment area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (data storage area) และพื้นที่ใช้งานเครือข่ายไร้สาย (wireless lan coverage area) เป็นต้น

ข้อ ๑๑๓ การควบคุมการเข้าออก อาคารสถานที่ ส่วนงานต้องดำเนินการดังนี้

(๑) กำหนดสิทธิของผู้ใช้งาน ที่มีสิทธิผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละพื้นที่ใช้งานระบบอย่างชัดเจน

(๒) การเข้าถึงอาคารของส่วนงาน ของบุคคลภายนอกหรือผู้มาติดต่อ เจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้น ๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในส่วนงาน

(๕) บริษัทผู้ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น data center เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของสินทรัพย์หรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอก และต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่าง ๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้าออกในพื้นที่หรือบริเวณที่มีความสำคัญ ได้แก่ data center

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวน หรือยกเลิกสิทธิการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๑๔ ระบบและอุปกรณ์สนับสนุนการทำงาน (supporting utilities) ส่วนงานต้องดำเนินการดังนี้

(๑) มีระบบสนับสนุนการทำงานของระบบสารสนเทศของส่วนงานที่เพียงพอต่อความต้องการใช้งาน ประกอบด้วย

(ก) ระบบสำรองกระแสไฟฟ้า (ups)

(ข) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (generator)

(ค) ระบบระบายอากาศ

(ง) ระบบปรับอากาศ และควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติ และลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือน เพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

ข้อ ๑๑๕ การเดินสายไฟ สายสื่อสาร และสายเคเบิ้ลอื่น ๆ (cabling security) ส่วนงานต้องดำเนินการดังนี้

(๑) หลีกเลี่ยงการเดินสายสัญญาณเครือข่ายของส่วนงานในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่าง ๆ เพื่อป้องกันการดักจับสัญญาณ หรือการตัดสายสัญญาณ

(๓) ให้เดินสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกัน เพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์ เพื่อป้องกันการตัดต่อสายสัญญาณผิดเส้น

(๕) จัดทำผังสายสัญญาณสื่อสารต่าง ๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่าง ๆ ให้ปิดใส่สลักให้สนิท เพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานสายใยแก้วนำแสงแทนสายสัญญาณสื่อสารแบบเดิม เช่น สายสัญญาณแบบ coaxial cable เป็นต้น สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมด เพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

ข้อ ๑๑๖ การบำรุงรักษาอุปกรณ์ (equipment maintenance) ส่วนงานต้องดำเนินการดังนี้

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้ง เพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบ เพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในส่วนงาน

(๖) จัดให้มีการอนุมัติสิทธิการเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

ข้อ ๑๑๗ การนำสินทรัพย์ของส่วนงานออกนอกส่วนงาน (removal of property) ส่วนงานต้องดำเนินการดังนี้

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือสินทรัพย์นั้นออกไปใช้งานนอกส่วนงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกส่วนงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกส่วนงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืน ให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาต และตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของส่วนงานออกไปใช้งานนอกส่วนงาน เพื่อเก็บไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

ข้อ ๑๑๘ การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกส่วนงาน (security of equipment off-premises) ส่วนงานต้องดำเนินการดังนี้

(๑) กำหนดมาตรการความปลอดภัย เพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือสินทรัพย์ของส่วนงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ไม่ทิ้งอุปกรณ์หรือสินทรัพย์ของส่วนงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือสินทรัพย์เสมือนเป็นสินทรัพย์ของตนเอง

ข้อ ๑๑๙ การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (secure disposal or re-use of equipment) ส่วนงานต้องดำเนินการดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญ

ในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

หมวดที่ ๕ การดำเนินการตอบสนองเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑๒๐ การวิเคราะห์รูปแบบการโจมตีของระบบตรวจหาการบุกรุก ผู้ดูแลระบบปฏิบัติดังนี้

(๑) ตรวจติดตามข้อมูลการใช้งานเครือข่าย เพื่อตรวจสอบความผิดปกติเป็นประจำทุกวัน และตอบสนองต่อการถูกบุกรุก

(๒) ติดตามข่าวสารใหม่ ๆ เรื่องการรูปแบบการโจมตีและภัยคุกคามของสารสนเทศ

ข้อ ๑๒๑ การตรวจหาช่องโหว่ของระบบเครือข่ายและระบบสารสนเทศ ผู้ดูแลระบบปฏิบัติดังนี้

(๑) ตรวจหาช่องโหว่ของระบบปฏิบัติการ และซอฟต์แวร์ประยุกต์ที่ให้บริการ

(๒) อุดช่องโหว่ (patch) ระบบปฏิบัติการ และซอฟต์แวร์ประยุกต์จากผู้พัฒนาผลิตภัณฑ์

ข้อ ๑๒๒ การกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตี ผู้ดูแลระบบปฏิบัติดังนี้

(๑) ป้องกันทางด้านกายภาพ โดยกำหนดให้ห้องที่ใช้เป็นศูนย์ข้อมูลเป็นบริเวณที่ต้องรักษาความปลอดภัย โดยจัดให้มีการควบคุมและการเข้า-ออกสามารถทำได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น

(๒) ปรับปรุงแนวทางในการตอบสนองต่อภัยคุกคามให้เป็นปัจจุบัน

(๓) ปรับปรุงนโยบายและกฎ (policy and rules) ของอุปกรณ์หรือซอฟต์แวร์ที่เกี่ยวข้องกับการตรวจจับและป้องกันภัยคุกคามให้เป็นปัจจุบันอยู่เสมอ

(๔) ประชาสัมพันธ์ผ่านสื่อทุกช่องทาง เช่น หนังสือเวียนแจ้ง จดหมายอิเล็กทรอนิกส์ เว็บไซต์ และสื่อทางสังคม (social media) เป็นต้น เพื่อให้ผู้ใช้งานทราบและตระหนักถึงภัยคุกคามด้านสารสนเทศใหม่ ๆ และปฏิบัติตามนโยบายฯ อย่างเคร่งครัด

หมวดที่ ๖ การสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๒๓ ผู้อำนวยการสำนักคอมพิวเตอร์นำเสนอ "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" ในวาระการประชุมกรรมการบริหารมหาวิทยาลัย เพื่อสร้างความรู้ความเข้าใจและความตระหนักให้แก่ผู้บริหารระดับสูงถึงความสำคัญของความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๒๔ การสร้างความรู้ ความเข้าใจและความตระหนัก ดำเนินการดังนี้

(๑) จัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายฯ ให้แก่ผู้ใช้งานสารสนเทศของมหาวิทยาลัยอย่างสม่ำเสมอ

(๒) จัดทำสื่อสำหรับฝึกอบรมในรูปแบบอิเล็กทรอนิกส์ (e-training) เรื่อง "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" และเผยแพร่ผ่านทางเว็บไซต์

(๓) ประชาสัมพันธ์ให้ความรู้เรื่อง "นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ" โดยผ่านสื่อต่าง ๆ เช่น ป้ายประกาศ เว็บไซต์ และสื่อทางสังคม เป็นต้น เพื่อให้ผู้ใช้งานตระหนักและปฏิบัติตามกฎหมายใด ๆ ที่ได้ประกาศใช้และนโยบายฯของมหาวิทยาลัยอย่างเคร่งครัด

หมวดที่ ๗ หน้าที่และความรับผิดชอบ

ข้อ ๑๒๕ ผู้บริหารระดับสูงสุด มีหน้าที่และความรับผิดชอบเชิงนโยบาย ดังนี้

(๑) กำหนดนโยบายด้านความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) ให้ข้อเสนอแนะ คำปรึกษา กำกับ และติดตามให้ผู้ปฏิบัติงานดำเนินงานตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย หรืออันตรายใด ๆ ที่เกิดขึ้นกับองค์กรใดหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๒๖ ผู้ดูแลระบบ มีหน้าที่และความรับผิดชอบดังนี้

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) แก้ปัญหาและประสานงานกับผู้ที่เกี่ยวข้อง เพื่อให้สารสนเทศมีความมั่นคงปลอดภัย

(๓) รับผิดชอบระบบสารสนเทศ ระบบสำรองข้อมูล และจัดทำแผนเตรียมความพร้อมฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ตรวจสอบและทดสอบสภาพความพร้อมในการใช้งานของระบบสารสนเทศ

(๕) ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศ

(๖) รับผิดชอบในการควบคุม ดูแล รักษาความปลอดภัย และบำรุงรักษาระบบสารสนเทศและการสื่อสารของมหาวิทยาลัย

(๗) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย หรืออันตรายใด ๆ ที่เกิดขึ้นกับองค์กรใดหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๒๗ ผู้พัฒนาระบบ มีหน้าที่และความรับผิดชอบดังนี้

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๒) พัฒนาระบบสารสนเทศโดยให้มีความปลอดภัย และไม่เปิดเผยข้อมูลของมหาวิทยาลัย

(๓) ตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศอย่างสม่ำเสมอ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติและอย่างต่อเนื่อง

(๔) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย หรืออันตรายใด ๆ ที่เกิดขึ้นกับองค์กรใดหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๒๘ ผู้ใช้งาน มีหน้าที่และความรับผิดชอบดังนี้

(๑) ปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของมหาวิทยาลัยบูรพา

(๒) รับผิดชอบต่อความเสี่ยง ความเสียหาย หรือ อันตรายที่เกิดขึ้นกับระบบสารสนเทศของมหาวิทยาลัย หรืออันตรายใด ๆ ที่เกิดขึ้นกับองค์กรใดหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ปฏิบัติตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

ประกาศ ณ วันที่ ๒ พฤศจิกายน พ.ศ. ๒๕๖๐

(ลงชื่อ) สมนึก ธีระกุลพิศุทธิ์
(รองศาสตราจารย์สมนึก ธีระกุลพิศุทธิ์)
ผู้ปฏิบัติหน้าที่อธิการบดีมหาวิทยาลัยบูรพา

สำเนาถูกต้อง

(นายสยาม ศรีพั่ว)
นักวิชาการคอมพิวเตอร์