ประกาศมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ
เรื่อง นโยบายด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ
(KMUTNB Information Technology Security Policy)

.....

โดยที่เป็นการสมควรกำหนดนโยบายด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ หรือ Information Technology Security Policy ของมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ โดยมีวัตถุประสงค์เพื่อให้เกิดความมั่นคงและปลอดภัย ในกิจการด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัย เพื่อให้สอดคล้อง และรองรับกับมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

อาศัยอำนาจตามความในมาตรา ๓๑(๓) แห่งพระราชบัญญัติมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พ.ศ. ๒๕๕๐ มาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบกับมติคณะกรรมการนโยบายและแผน ในคราวประชุมครั้งที่ ๑๔/๒๕๕๖ เมื่อวันที่ ๑ กรกฎาคม ๒๕๕๖ จึงกำหนดนโยบายด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ (Information Technology Security Policy) มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ไว้ดังนี้

ข้อ ๑ ในประกาศนี้

"มหาวิทยาลัย" หมายความว่า มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ

"สำนักคอมพิวเตอร์" หมายความว่า สำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ

"ส่วนงาน" หมายความว่า ส่วนงานตามประกาศมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ว่าด้วย การจัดตั้งส่วนงานในมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ พ.ศ. ๒๕๕๑ และที่แก้ไขเพิ่มเติม

"ผู้ดูแลระบบหรือเครือข่าย (System or Network Administrator)" หมายความว่า ผู้ที่มีหน้าที่รับผิดชอบในการดูแลระบบหรือเครือข่ายให้เป็นไปตามนโยบายฉบับนี้ โดยได้รับการแต่งตั้งจากผู้บังคับบัญชา

"ผู้ใช้งาน (User)" หมายความว่า บุคลากรและนักศึกษาของมหาวิทยาลัย รวมถึงผู้ที่มาขอใช้บริการชั่วคราว

"ผู้ใช้ข้อมูล" หมายความว่า ผู้ใช้งานหรือผู้อื่นใด ที่ได้รับข้อมูลจากระบบสารสนเทศมหาวิทยาลัย เพื่อนำไปใช้งานเพื่อการใดๆ ก็ตาม ที่มีส่วนเกี่ยวข้องกับภารกิจของมหาวิทยาลัย

"สิทธิการใช้งาน" หมายความว่า สิทธิในการเข้าถึงข้อมูลที่ได้รับอนุญาตหรือที่ได้รับมอบหมาย

"เครือข่ายหลัก (Core Network)" หมายความว่า เครือข่ายที่อยู่ในความรับผิดชอบของสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศซึ่งทำหน้าที่ในการเชื่อมต่อเครือข่ายของส่วนงานกับเครือข่ายอินเตอร์เน็ต

"เครือข่ายของส่วนงาน" หมายความว่า เครือข่ายที่อยู่ในความรับผิดชอบของส่วนงานที่ได้รับอนุญาตให้จัดตั้งขึ้นอย่างเป็นลายลักษณ์อักษรจากสำนักคอมพิวเตอร์และเทคโนโลยีสารสนเทศ เพื่อเชื่อมต่อกับเครือข่ายหลัก และส่วนงานต้องปฏิบัติตามข้อตกลงการใช้งานเครือข่ายร่วมกันระหว่างสำนักคอมพิวเตอร์และส่วนงานต่างๆ

"เครือข่ายไร้สาย" หมายความว่า เครือข่ายการสื่อสารแบบไร้สายแบบ Wi-Fi ที่มีการให้บริการในเขตพื้นที่ของมหาวิทยาลัยที่เชื่อมต่อกับเครือข่ายหลัก หรือเครือข่ายของส่วนงาน

"เครือข่ายอินเทอร์เน็ต" หมายความว่า เครือข่ายของส่วนงานหรือองค์กรภายนอกความรับผิดชอบของมหาวิทยาลัย หรือเครือข่ายที่เป็นสาธารณะที่จำเป็นต้องมีการปฏิบัติตามพระราชบัญญัติ ว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

"เครือข่ายสังคมออนไลน์ (Social Network)" หมายความว่า ระบบหรือซอฟต์แวร์ที่สามารถแลกเปลี่ยนข้อมูลกันได้อย่างกว้างขวางผ่านสื่อสังคมออนไลน์ต่างๆ เช่น Facebook, Twitter, Hi5, Windows Live Messenger, Skype, Yahoo! Messenger, Camfrog เป็นต้น รวมถึง ระบบอื่นๆ ที่เป็นโปรแกรมประเภทส่งข้อความทันที หรือมีลักษณะการสื่อสารข้อมูลแบบโปรแกรมประเภทมีบทบาทเท่าเทียมกัน (Peer-to-Peer)

"ทรัพยากรสารสนเทศ" หมายความว่า ทรัพย์สินของมหาวิทยาลัยหรือส่วนงานที่เกี่ยวข้องกับเทคโนโลยีสารสนเทศ เช่น เครือข่ายหลัก เครือข่ายส่วนงาน เครือข่ายไร้สาย ระบบฐานข้อมูล ระบบความปลอดภัยข้อมูล โปรแกรมประยุกต์ (Application) คอมพิวเตอร์ คอมพิวเตอร์แม่ข่าย เป็นต้น รวมถึงเครือข่ายอื่น ที่มีส่วนเกี่ยวข้องกับกิจการของมหาวิทยาลัย หรือของส่วนงาน

"ระบบเทคโนโลยีสารสนเทศที่สำคัญ" หมายความว่า ระบบสารสนเทศที่ใช้งานของมหาวิทยาลัยหรือของส่วนงานที่มีความสำคัญต่อการดำเนินงานของมหาวิทยาลัย หรือของส่วนงาน

"ระเบียบการขอใช้บริการ" หมายความว่า ระเบียบที่จัดทำขึ้นเพื่อกำหนด กฎ ระเบียบ และขั้นตอนการขอใช้บริการสารสนเทศต่างๆ ของมหาวิทยาลัย หรือหมายถึงที่จัดทำขึ้นโดยส่วนงานสำหรับการให้บริการสารสนเทศของส่วนงาน และให้หมายความรวมถึงระเบียบที่ออกโดยส่วนงานสำหรับการให้บริการสารสนเทศของส่วนงานด้วย

"ชื่อผู้ใช้งาน (Username)" หมายความว่า ชื่อเรียกของผู้ใช้งานสำหรับการควบคุมการเข้าถึงทรัพยากรสารสนเทศของมหาวิทยาลัยหรือของส่วนงาน

"รหัสผ่าน (Password)" หมายความว่า รหัสที่เป็นความลับที่เฉพาะผู้ใช้งานนั้นทราบแต่เพียงผู้เดียว

"ชั้นความลับข้อมูล" หมายความว่า ระดับการเข้าถึงของข้อมูลที่มีความลับที่แตกต่างกันที่ต้องมีการกำหนดการเข้าถึงข้อมูลได้ต่างกันตามอำนาจหน้าที่ โดยให้กำหนดชั้นความลับข้อมูลและการกำหนดการเข้าถึงข้อมูลตามระเบียบ ว่าด้วย การรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

"คอมพิวเตอร์แม่ข่าย (Host Computer หรือ Server)" หมายความว่า คอมพิวเตอร์ที่มีการเชื่อมต่อกับเครือข่ายหลัก หรือเครือข่ายของส่วนงาน และมีการอนุญาตให้เข้าถึงข้อมูลจากเครือข่ายหลัก หรือเครือข่ายส่วนงาน ที่มีโปรแกรมบริการติดตั้งอยู่ ที่เป็นเครื่องบริการข้อมูลสารสนเทศ หรือที่มีลักษณะการให้บริการข้อมูล

"คอมพิวเตอร์" หมายความว่า คอมพิวเตอร์และอุปกรณ์ รวมถึงคอมพิวเตอร์ส่วนบุคคล (Personal Computer) คอมพิวเตอร์แบบพกพา (Portable Computer หรือ Notebook Computer) แท็บเล็ตพีซี (Tablet Personal Computer) แท็บเล็ต (Tablet Computer) และโทรศัพท์เคลื่อนที่ที่สามารถเชื่อมต่อกับเครือข่ายไร้สาย เครือข่ายหลัก หรือเครือข่ายส่วนงาน

ข้อ ๒ กรณีมีปัญหาในการวินิจฉัยหรือการตีความเพื่อปฏิบัติตามประกาศนี้ ให้อธิการบดีเป็นผู้มีอำนาจในการวินิจฉัยชี้ขาด และให้ถือเป็นที่สุด

ข้อ ๓ นโยบายด้านเทคโนโลยีสารสนเทศของมหาวิทยาลัยมีผลใช้บังคับกับทุกส่วนงาน ประกอบด้วยนโยบาย ๑๑ ด้าน ดังต่อไปนี้

(๑) นโยบายด้านการควบคุมการเข้าถึงทรัพยากรสารสนเทศ

(๒) นโยบายด้านการใช้งานเครือข่ายอินเทอร์เน็ต

(๓) นโยบายด้านการใช้งานเครือข่ายไร้สาย

(๔) นโยบายด้านการพิสูจน์ตัวบุคคล (Authentication Policy)

(๕) นโยบายด้านการใช้งานคอมพิวเตอร์แม่ข่าย (Host Computer or Server Usage Policy)

(๖) นโยบายด้านการใช้งานจดหมายอิเล็กทรอนิกส์

(๗) นโยบายด้านการควบคุมการจราจรข้อมูล

(๘) นโยบายด้านการตรวจจับและการป้องกันการบุกรุก

(๙) นโยบายด้านการใช้งานคอมพิวเตอร์และซอฟต์แวร์ที่จำเป็น (Computer and Software Usage Policy)

(๑๐) นโยบายด้านการบริหารจัดการข้อมูล ฐานข้อมูล และการพัฒนาระบบสารสนเทศเพื่อการใช้งาน

(๑๑) นโยบายด้านการสำรองข้อมูลและการกู้คืนระบบจากเหตุให้เกิดการสูญเสียข้อมูลอย่างถาวรและฉับพลัน

หมวด ๑
นโยบายด้านการควบคุมการเข้าถึงทรัพยากรสารสนเทศ
(Access Control Policy)

ข้อ ๔ นโยบายนี้ครอบคลุมการควบคุมการเข้าถึงทรัพยากรสารสนเทศที่เป็นของมหาวิทยาลัย เพื่อความมั่นคงปลอดภัยของข้อมูลและเครือข่ายของมหาวิทยาลัย

(๖) บริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับข้อมูล ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ ดังต่อไปนี้

ก. ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบสารสนเทศ

ข. กำหนดชื่อผู้ใช้งานและรหัสผ่านเพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

ค. ควรกำหนดระยะเวลาการเข้าใช้ข้อมูลและระงับการเข้าใช้ข้อมูลทันทีเมื่อพ้นระยะเวลาดังกล่าว

ง. การรับส่งข้อมูลสำคัญผ่านเครือข่ายหน่วยงาน หรือเครือข่ายหลัก ควรได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

จ. การรับส่งข้อมูลสำคัญผ่านเครือข่ายอินเทอร์เน็ต ต้องได้รับการเข้ารหัสลับ (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

ฉ. ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดของชั้นความลับข้อมูล

ช. ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำคอมพิวเตอร์ของมหาวิทยาลัย หรือส่วนงานที่มีข้อมูลที่เป็นความลับออกนอกพื้นที่ของมหาวิทยาลัย เช่น ส่งคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เป็นความลับที่เก็บอยู่ในสื่อบันทึกก่อน หรือให้มีการเข้ารหัสลับข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

(๗) ควบคุมการเชื่อมต่อเครือข่ายของส่วนงานกับเครือข่ายหลักสำหรับผู้ดูแลส่วนงาน และควบคุมการเชื่อมต่อเครือข่ายหลักกับเครือข่ายอินเตอร์เน็ตสำหรับมหาวิทยาลัยโดยสำนักคอมพิวเตอร์ เพื่อให้การบริหารจัดการเครือข่ายของมหาวิทยาลัยเป็นไปอย่างมีประสิทธิภาพและมีความปลอดภัย ดังต่อไปนี้

ก. กำหนดวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายของส่วนงานและเครือข่ายหลักด้วยอุปกรณ์จัดเส้นทางที่มีการป้องกันการเข้าถึงอย่างปลอดภัย

ข. กำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายของส่วนงานและเครือข่ายหลักเพื่อให้คอมพิวเตอร์ของผู้ใช้งานใช้เส้นทางที่กำหนดให้ และไม่ให้สามารถใช้เส้นทางอื่นได้

ค. เครือข่ายหลักและเครือข่ายของส่วนงานต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานเครือข่ายหลักและเครือข่ายของส่วนงานในลักษณะที่ผิดปกติ

ง. การเข้าสู่ระบบเครือข่ายของส่วนงาน โดยผ่านทางระบบอินเทอร์เน็ตต้องมีการลงบันทึกเข้าใช้งาน (Login Logging) และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) ของผู้ใช้งาน

จ. เลขที่อยู่ไอพี (IP Address) ภายในของเครือข่ายของส่วนงานต้องมีการป้องกันมิให้ส่วนงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

ฉ. จัดทำแผนผังระบบเครือข่าย (Network System Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในของส่วนงานและเครือข่ายภายนอกของส่วนงาน และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ และให้ถือว่าแผนผังระบบเครือข่ายนี้เป็นความลับ ไม่สามารถเปิดเผยกับผู้ที่ไม่ได้รับผิดชอบระบบเครือข่าย

ช. การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(๘) ในกรณีที่หน่วยงานมีการเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตด้วยการเช่าวงจรเพื่อใช้งานเอง ต้องกำหนดให้อุปกรณ์จัดเส้นทางทำการจำกัดเส้นทางผ่านทางอุปกรณ์จัดเส้นทางหลักของมหาวิทยาลัยโดยการดูแลของสำนักคอมพิวเตอร์ ทั้งนี้ เพื่อให้การเชื่อมต่อดังกล่าวมีความปลอดภัย

(๙) ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของส่วนงาน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ ๗ ให้มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ กำหนดมาตรการควบคุมการจัดเก็บและการบันทึกข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) และบันทึกข้อมูลการเข้าปฏิบัติงาน (Login Log) ที่สามารถระบุถึงเหตุการณ์ทางคอมพิวเตอร์และระบุถึงตัวบุคคลผู้กระทำการดังกล่าวได้ และให้ข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการเข้าปฏิบัติงานมีความถูกต้อง ปลอดภัย และตรวจสอบย้อนหลังได้ ตามแนวทางดังต่อไปนี้

(๑) กำหนดประเภทและความหมายของข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการเข้าปฏิบัติงานที่ต้องจัดเก็บและบันทึก วิธีการป้องกันการแก้ไขบันทึกข้อมูลจราจรทางคอมพิวเตอร์ ข้อมูลการเข้าปฏิบัติงาน และข้อมูลอื่นๆ ที่เกี่ยวข้อง และระดับสิทธิการเข้าถึงบันทึกข้อมูลเหล่านั้น

(๒) ควรจัดเก็บบันทึกข้อมูลจราจรทางคอมพิวเตอร์และข้อมูลการเข้าปฏิบัติงานไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบบที่ใช้ในการจัดเก็บสามารถระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ สามารถกำหนดชั้นความลับในการเข้าถึงบันทึกข้อมูลได้ตามระดับสิทธิการเข้าถึง และสามารถกำหนดให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

(๓) ผู้ใช้งานต้องไม่ได้รับอนุญาตในการแก้ไขบันทึกข้อมูลดังกล่าวที่เก็บรักษาไว้ ยกเว้นผู้ดูแลระบบ ผู้ตรวจสอบระบบสารสนเทศของส่วนงาน (IT Auditor) หรือบุคคลที่ส่วนงานมอบหมาย

(๔) ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศที่สำคัญ และควรกำหนดให้ระบบสารสนเทศอื่นๆ มีการบันทึกการเข้าปฏิบัติงานของผู้ใช้งาน และมีการบันทึกรายละเอียดของระบบป้องกันการบุกรุกหรือโจมตี เช่น บันทึกการเข้า-ออกระบบ บันทึกความพยายามหรือความผิดพลาดในการเข้าสู่ระบบ บันทึกการแก้ไขข้อมูลที่สำคัญ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและเก็บบันทึกดังกล่าวไว้อย่างน้อย ๙๐ วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(๕) ควรตรวจสอบบันทึกข้อมูลจราจรทางคอมพิวเตอร์และบันทึกข้อมูลการเข้าปฏิบัติงานของผู้ใช้งานระบบสารสนเทศต่างๆ อย่างสม่ำเสมอ

ข้อ ๘ ห้ามผู้ใดที่ไม่ได้รับอนุญาตจากผู้ดูแลระบบ กระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม แก้ไขค่าการติดตั้ง หรือทำการใดๆ ต่ออุปกรณ์ส่วนกลางของมหาวิทยาลัย ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลักที่มีผลให้เกิดการเปลี่ยนแปลงเส้นทางข้อมูลหรือการจราจรข้อมูล การดักข้อมูล (Interception) การสร้างข้อมูลเท็จ (Fabrication) การปลอมแปลงข้อมูล (Spoofing) หรือเหตุการณ์ใดๆ อันมีผลกระทบต่อเครือข่ายหลักของมหาวิทยาลัย

ข้อ ๙ ห้ามผู้ใดหรือส่วนงานใดใช้ทรัพยากรสารสนเทศและระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยที่จัดเตรียมให้ เพื่อการเผยแพร่ ข้อมูล ข้อความ รูปภาพ หรือสิ่งอื่นใด ที่เป็นข้อมูลส่วนบุคคล ข้อมูลของมหาวิทยาลัย หรือข้อมูลอื่นๆ ที่มีลักษณะขัดต่อ กฎหมาย ศีลธรรม และความมั่นคงของประเทศ หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๑๐ ห้ามผู้ใดหรือส่วนงานใดใช้ทรัพยากรสารสนเทศและระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัยเพื่อการรบกวน ก่อให้เกิดความเสียหายต่อบุคคลหรือมหาวิทยาลัย หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของมหาวิทยาลัย

ข้อ ๑๑ ห้ามผู้ใดหรือส่วนงานใดใช้ทรัพยากรสารสนเทศและระบบสื่อสารทุกประเภท รวมถึงอุปกรณ์อื่นใดของมหาวิทยาลัย เพื่อประโยชน์ทางการค้า

ข้อ ๑๒ ห้ามผู้ใดหรือส่วนงานใดกระทำการใดๆ เพื่อการดักข้อมูลหรือการโจรกรรมข้อมูล (Sabotage) ไม่ว่าจะเป็นข้อความ ภาพ เสียง หรือสิ่งอื่นใดไม่ว่าจะด้วยวิธีการใดๆ ก็ตามด้วยทรัพยากรสารสนเทศของมหาวิทยาลัยโดยไม่ได้รับอนุญาต

ข้อ ๑๓ ห้ามผู้ใดหรือส่วนงานใดกระทำการรบกวน ทำลาย หรือทำให้เครือข่ายหลัก เครือข่ายของส่วนงาน เครือข่ายไร้สาย ระบบเทคโนโลยีสารสนเทศที่สำคัญ และระบบเทคโนโลยีสารสนเทศอื่นๆ ของมหาวิทยาลัยหรือส่วนงานต้องหยุดชะงัก

ข้อ ๑๔ ห้ามผู้ใดหรือส่วนงานใดใช้ทรัพยากรสารสนเทศของมหาวิทยาลัย เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอก โดยไม่ได้รับอนุญาตจากผู้มีอำนาจ

ข้อ ๑๕ ห้ามผู้ใดหรือส่วนงานใดกระทำการใดๆ อันมีลักษณะเป็นการลักลอบใช้งานหรือรับรู้รหัสส่วนบุคคลหรือข้อมูลส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูล หรือเพื่อการใช้ทรัพยากรสารสนเทศก็ตาม

ข้อ ๑๖ ห้ามผู้ใดหรือส่วนงานใดติดตั้งอุปกรณ์หรือกระทำการใด เพื่อให้สามารถเข้าถึงทรัพยากรสารสนเทศของมหาวิทยาลัยโดยไม่ได้รับอนุญาต

หมวด ๒
นโยบายด้านการใช้งานเครือข่ายอินเทอร์เน็ต
(Internet Usage Policy)

ข้อ ๑๗ การใช้งานเครือข่ายอินเทอร์เน็ตต้องเป็นไปตามพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

ข้อ ๑๘ ในการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) บันทึกส่วนตัวออนไลน์ (Blog) กระดานสนทนาอิเล็กทรอนิกส์ (Web Board) ต้องไม่เปิดเผยข้อมูลส่วนบุคคลของผู้อื่น หรือข้อมูลที่สำคัญและเป็นความลับทางราชการของมหาวิทยาลัยหรือส่วนงาน

ข้อ ๑๙ ในการใช้งานเครือข่ายสังคมออนไลน์ (Social Network) บันทึกส่วนตัวออนไลน์ (Blog) กระดานสนทนาอิเล็กทรอนิกส์ (Web Board) ต้องไม่เสนอความคิดเห็นที่ขัดแย้งกับข้อเท็จจริง หรือใช้ข้อความที่ยั่วยุปั่นป่วน ให้ร้ายที่จะก่อให้เกิดการทะเลาะวิวาทหรือการทำลายความสัมพันธ์กับบุคลากรระหว่างส่วนงาน ความเสื่อมเสียต่อชื่อเสียงของส่วนงาน และความเสื่อมเสียอื่นๆ

ข้อ ๒๐ ผู้ใช้งานต้องรับผิดชอบหากมีการเข้าใช้งานเครือข่ายอินเทอร์เน็ตโดยบุคคลอื่นโดยใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ของผู้ใช้งานและมีการกระทำความผิดใดๆ เกิดขึ้นโดยให้ความผิดนั้นเสมือนเป็นความผิดของผู้ใช้งาน

ข้อ ๒๑ ห้ามผู้ใดหรือส่วนงานใดใช้เครือข่ายอินเทอร์เน็ตของมหาวิทยาลัยเพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับมหาวิทยาลัยหรือส่วนงาน

ข้อ ๒๒ ห้ามผู้ใดหรือส่วนงานใดเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของส่วนงานที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ตหรือเครือข่ายสังคมออนไลน์

ข้อ ๒๓ ห้ามผู้ใดหรือส่วนงานใดดาวน์โหลด (Download) อัพโหลด (Upload) หรือการอัพเดท (Update) โปรแกรมใช้งานต่างๆ ผ่านเครือข่ายอินเทอร์เน็ตที่เป็นการละเมิดลิขสิทธิ์

หมวด ๓
นโยบายด้านการใช้งานเครือข่ายไร้สาย
(Wireless Network Usage Policy)

ข้อ ๒๔ การติดตั้งเครือข่ายไร้สายต้องได้รับอนุญาตจากหน่วยงานอย่างเป็นลายลักษณ์อักษร

ข้อ ๒๕ การติดตั้งเครือข่ายไร้สายต้องกำหนดให้มีผู้ดูแลระบบ

ข้อ ๒๖ การติดตั้งเครือข่ายไร้สายต้องไม่ให้เกิดสัญญาณรบกวนกับเครือข่ายไร้สายของมหาวิทยาลัย

ข้อ ๒๗ การใช้งานเครือข่ายไร้สายต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) และค่ารหัสผ่านสำหรับผู้ดูแลระบบ (Administrator Password) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีก่อนนำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

ข้อ ๒๘ การตั้งค่าเครือข่ายไร้สายต้องกำหนดระดับความปลอดภัยแบบ WPA (Wi-Fi Protected Access) หรือที่มีระดับความปลอดภัยมากกว่า และควรกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย และห้ามใช้มาตรฐาน WEP ในการใช้งานเครือข่ายไร้สายเนื่องจากมีความไม่ปลอดภัย

ข้อ ๒๙ การใช้งานเครือข่ายไร้สายผู้ดูแลระบบต้องควบคุมไม่ให้บุคคลหรือส่วนงานภายนอกที่ไม่ได้รับอนุญาตใช้งานเครือข่ายไร้สายด้วยกระบวนการการป้องกันต่างๆ เพื่อป้องกันการโจมตีรูปแบบต่างๆ

ข้อ ๓๐ การเลือกใช้วิธีการควบคุมการใช้งานควรใช้การควบคุมด้วย MAC Address และชื่อผู้ใช้งานกับรหัสผ่านของผู้ใช้งาน โดยให้อนุญาตเฉพาะคอมพิวเตอร์ที่มี MAC Address และชื่อผู้ใช้งานกับรหัสผ่านตามที่ได้กำหนดไว้ล่วงหน้าโดยวิธีการที่สามารถพิสูจน์ผู้ใช้งานได้

ข้อ ๓๑ การติดตั้งเครือข่ายไร้สายควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายของส่วนงานเพื่อใช้ในการควบคุมการใช้งานและป้องกันการโจมตี

ข้อ ๓๒ ผู้ใช้งานในเครือข่ายไร้สายที่ต้องการสื่อสารข้อมูลกับคอมพิวเตอร์แม่ข่ายในเครือข่ายหลักหรือเครือข่ายส่วนงานให้ติดต่อกันผ่านทางเครือข่ายส่วนบุคคลเสมือน (Virtual Private Network) หรือทางอุโมงค์ข้อมูลแบบปลอดภัย (Secure Tunnel) เท่านั้น

ข้อ ๓๓ ผู้ดูแลระบบควรใช้ซอฟต์แวร์ หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของเครือข่ายไร้สายเพื่อคอยตรวจจับและบันทึกเหตุการณ์ และในกรณีที่ตรวจพบการใช้งานเครือข่ายไร้สายที่ผิดปกติหรือที่ไม่ปลอดภัยให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบทันที

หมวด ๔
นโยบายด้านการพิสูจน์ตัวบุคคล
(Authentication Policy)

ข้อ ๓๔ ผู้ใช้งานมีหน้าที่เกี่ยวกับนโยบายด้านการพิสูจน์ตัวบุคคล ดังต่อไปนี้

(๑) ป้องกัน ดูแล รักษาข้อมูล ชื่อผู้ใช้งานและรหัสผ่าน โดยผู้ใช้งานแต่ละคนต้องมีชื่อผู้ใช้งานของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่หรือแจกจ่ายเป็นเหตุให้ผู้อื่นล่วงรู้รหัสผ่าน

(๒) รับผิดชอบต่อการกระทำใดๆ ที่เกิดจากการใช้ชื่อผู้ใช้งานของผู้ใช้งาน ไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานจริงหรือไม่ก็ตาม

(๓) ตั้งรหัสผ่านให้เกิดความปลอดภัย โดยรหัสผ่านต้องประกอบด้วยตัวอักษรไม่น้อยกว่า ๘ ตัวอักษร ซึ่งต้องประกอบด้วยตัวอักษร (Alphabet) และตัวเลข (Number) และ/หรือตัวอักษรพิเศษ (Special Character)

(๔) ไม่ใช้รหัสผ่านชุดเดียวกันกับรหัสผ่านของระบบสารสนเทศอื่นๆ ที่ไม่ใช่ระบบสารสนเทศของมหาวิทยาลัย

(๕) เปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓ - ๖ เดือน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

(๖) ทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ทรัพยากร หรือระบบสารสนเทศของมหาวิทยาลัย และหากการพิสูจน์ตัวตนนั้นมีปัญหา ไม่ว่าจะเกิดจากการลืมรหัสผ่าน หรือชื่อผู้ใช้งานถูกห้ามใช้ หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันที

ข้อ ๓๕ นโยบายนี้กำหนดให้การพิสูจน์ตัวตนต้องกระทำในกรณีต่างๆ ดังต่อไปนี้

(๑) คอมพิวเตอร์แบบพกพาให้ทำการพิสูจน์ตัวตนในระดับไบออส (BIOS) ก่อนการใช้งาน

(๒) คอมพิวเตอร์ทุกประเภท ก่อนการเข้าถึงระบบปฏิบัติการให้ทำการพิสูจน์ตัวตนทุกครั้ง

(๓) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายให้ทำการพิสูจน์ตัวตนทุกครั้ง

(๔) การใช้งานอินเทอร์เน็ต ให้ทำการพิสูจน์ตัวตนและมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนของผู้ใช้งานได้ และบ่งบอกถึงคอมพิวเตอร์ที่ใช้งานอยู่ และอาจบ่งบอกถึงตำแหน่งที่ตั้งของคอมพิวเตอร์เครื่องนั้น

(๕) เมื่อผู้ใช้งานไม่อยู่ที่คอมพิวเตอร์อย่างน้อย ๑๕ นาที คอมพิวเตอร์ทุกเครื่องต้องทำการปิดกั้นจอภาพ (Screen Lock) ทุกครั้ง และให้ทำการพิสูจน์ตัวตนก่อนการเริ่มใช้งานทุกครั้ง

(๖) คอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักจอภาพ (Screen Saver) และต้องตั้งให้ทำการปิดกั้นจอภาพทำงานแบบอัตโนมัติในเวลาไม่เกิน ๑๕ นาที

ข้อ ๓๖ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ ต้องติดตั้งและบำรุงรักษาระบบคอมพิวเตอร์แม่ข่ายการพิสูจน์ตัวตนกลาง (Central Authentication Server) เพื่อเป็นศูนย์กลางสำหรับการพิสูจน์ตัวตนสำหรับการใช้งานร่วมกับทรัพยากรสารสนเทศ ระบบเทคโนโลยีสารสนเทศที่สำคัญของมหาวิทยาลัย และให้สามารถใช้งานได้ตลอดเวลาและให้มีความปลอดภัยของข้อมูลในระดับสูง

ข้อ ๓๗ สำหรับผู้ใช้งานแบบชั่วคราว ให้กำหนดให้มีผู้รับผิดชอบชื่อผู้ใช้งานและรหัสผ่านชั่วคราวแทนผู้ใช้งานตัวจริงได้ในกรณีการจัดสัมมนาหรืออบรม โดยให้หัวหน้าโครงการการจัดสัมมนาหรืออบรมเป็นผู้รับผิดชอบการพิสูจน์ตัวตนของผู้ใช้งานที่เข้าสัมมนาหรืออบรม และหากมีการกระทำผิดอันใดของผู้ใช้งานแบบชั่วคราว ให้ผู้รับผิดชอบเป็นผู้รับผิดต่อการกระทำดังกล่าวหรือเป็นผู้หาพยานหลักฐานการกระทำผิดของผู้ใช้งานแบบชั่วคราวเพื่อหาผู้กระทำผิดที่แท้จริง

หมวด ๕
นโยบายด้านการใช้งานคอมพิวเตอร์แม่ข่าย
(Host Computer or Server Usage Policy)

ข้อ ๓๘ ให้มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ กำหนดมาตรการควบคุมการใช้งานและการติดตั้งคอมพิวเตอร์แม่ข่ายเพื่อดูแลรักษาความปลอดภัยของทรัพยากรสารสนเทศของมหาวิทยาลัยจากการเข้าถึงตามแนวทาง ดังต่อไปนี้

(๑) บุคคลหรือส่วนงานที่ต้องการติดตั้งคอมพิวเตอร์แม่ข่ายของหน่วยงานต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้บังคับบัญชาของส่วนงาน และแจ้งข้อมูลการติดตั้งประกอบด้วยหมายเลขไอพี (IP Address) ชื่อโดเมน (Domain Name) ข้อมูลการติดต่อผู้รับผิดชอบ หมายเลขพอร์ต (Port Number) ที่ให้บริการ ให้แก่สำนักคอมพิวเตอร์ เพื่อการบันทึกข้อมูลและการดำเนินการต่อไป

(๒) ส่วนงานที่ต้องการขออนุญาตใช้งานพื้นที่เพื่อติดตั้งคอมพิวเตอร์แม่ข่าย แบบจัดตั้งคอมพิวเตอร์แม่ข่ายร่วมในศูนย์ข้อมูล (Co-Location) ในพื้นที่ของสำนักคอมพิวเตอร์ ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อแสดงถึงวัตถุประสงค์การใช้งาน ข้อมูลการติดต่อผู้รับผิดชอบ ชื่อเรียก (Hostname) และหมายเลขพอร์ต (Port Number) ที่ให้บริการ

(๓) ส่วนงานที่ต้องการขออนุญาตใช้งานพื้นที่ให้บริการในรูปแบบสร้างอยู่ในคอมพิวเตอร์แม่ข่ายเว็บ (Web Hosting)ของสำนักคอมพิวเตอร์ ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อแสดงถึงวัตถุประสงค์การใช้งาน ชื่อเว็บ ข้อมูลการติดต่อผู้รับผิดชอบ หมายเลขพอร์ตที่ให้บริการ ขนาดของพื้นที่เก็บข้อมูลที่ต้องการ

(๔) ส่วนงานที่ต้องการขออนุญาตใช้งานรูปแบบคอมพิวเตอร์แม่ข่ายส่วนตัวเสมือน (Virtual Private Server) ของสำนักคอมพิวเตอร์ ให้ทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการสำนักคอมพิวเตอร์ เพื่อแสดงถึงวัตถุประสงค์การใช้งาน หรือชื่อเรียกเสมือนแบบคอมพิวเตอร์แม่ข่ายส่วนตัวเสมือน (Virtual Private Server) ข้อมูลการติดต่อผู้รับผิดชอบ หมายเลขพอร์ตที่ให้บริการ ขนาดของฮาร์ดดิสก์ และขนาดของหน่วยความจำที่ต้องการ

(๕) ส่วนงานที่ขออนุญาตใช้งานพื้นที่ แบบจัดตั้งคอมพิวเตอร์แม่ข่ายร่วมในศูนย์ข้อมูล (Co-Location) แบบสร้างอยู่ในคอมพิวเตอร์แม่ข่ายเว็บ (Web Hosting)และแบบคอมพิวเตอร์แม่ข่ายส่วนตัวเสมือน (Virtual Private Server) ห้ามติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบหรือผู้ใช้งานอื่นๆ

(๖) หากสำนักคอมพิวเตอร์ ตรวจสอบว่าการใช้งานในข้อ (๑) (๒) (๓) และ (๔) ส่งผลกระทบต่อการทำงานของระบบหรือผู้ใช้งานอื่นๆ สำนักคอมพิวเตอร์ ขอสงวนสิทธิ์ในการระงับการให้บริการก่อนแล้วจึงแจ้งให้ผู้รับผิดชอบทราบในภายหลัง

(๗) ส่วนงานต้องกำหนดวิธีการควบคุมการใช้ช่องทางข้อมูล (Port) ที่คอมพิวเตอร์แม่ข่ายที่ใช้ในการเข้าถึงข้อมูลและให้สามารถรายงานการใช้ช่องทางข้อมูลเมื่อร้องขอให้กับสำนักคอมพิวเตอร์ และให้มีการตรวจสอบความถูกต้องของข้อมูลอย่างสม่ำเสมอ

(๘) วิธีการใดๆ ที่สามารถเข้าสู่คอมพิวเตอร์แม่ข่ายสำหรับการบริหารจัดการจากระยะไกล (Remote Administrator) และการเข้าสู่ระบบจากระยะไกล (Remote Login) จากเครือข่ายอินเตอร์เน็ต ให้ผู้ใช้งานแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอและต้องได้รับการอนุญาตจากสำนักคอมพิวเตอร์

ข้อ ๓๙ ส่วนงานที่ต้องการขอจดชื่อโดเมนต้องปฏิบัติตามแนวทางต่อไปนี้

(๑) กำหนดผู้รับผิดชอบชื่อโดเมนประกอบด้วยชื่อผู้รับผิดชอบ ส่วนงานต้นสังกัด และข้อมูลการติดต่อเช่น เบอร์โทรศัพท์ และอีเมล์ของมหาวิทยาลัย

(๒) ชื่อโดเมนที่ขอจดต้องเป็นชื่อโดเมนย่อย (Sub-domain) ของชื่อโดเมนของส่วนงานต้นสังกัด ในกรณีที่เครื่องแม่ข่ายนั้นเป็นเครื่องแม่ข่ายใช้งานภายในส่วนงานนั้น

(๓) ชื่อโดเมนที่ขอจดต้องถูกนำไปใช้ในงานเพื่อการศึกษาและภารกิจของส่วนงานหรือมหาวิทยาลัยเท่านั้น

ข้อ ๔๐ ส่วนงานที่จัดตั้งคอมพิวเตอร์แม่ข่ายภายในมหาวิทยาลัย ต้องกำหนดให้มีผู้ดูแลระบบและต้องมีห้องที่มีมาตรการควบคุมการเข้า-ออก และการนำอุปกรณ์เข้า-ออก ของส่วนงานนั้น และระบบรักษาความปลอดภัยของการควบคุมการเข้า-ออก เช่นระบบคีย์การ์ด (Key Card Access) ระบบตรวจสอบลายนิ้วมือ (Fingerprint Scanner) หรือระบบกล้องวงจรปิด (CCTV) เป็นต้น

ข้อ ๔๑ ผู้ดูแลระบบต้องบริหารควบคุมคอมพิวเตอร์แม่ข่ายและรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนด การแก้ไขหรือเปลี่ยนแปลงค่าต่างๆ (Configuration) ของซอฟต์แวร์ระบบปฏิบัติการ (Operating Systems Software) โดยให้มีการใช้ระบบซอฟต์แวร์ช่วยในการจัดการบริหารคอมพิวเตอร์แม่ข่าย (Server Management Software) ที่มีฐานข้อมูลคอมพิวเตอร์แม่ข่ายที่ทันสมัยและตรวจสอบได้ตลอดเวลา

ข้อ ๔๒ การกำหนดค่าอนุญาตการให้บริการของคอมพิวเตอร์แม่ข่ายในเครือข่ายหลัก หรือในแต่ละส่วนของเครือข่ายของหน่วยงานด้วยอุปกรณ์ป้องกัน เช่น ไฟร์วอลล์ ต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น โดยต้องระบุนโยบาย (Policy) ของอุปกรณ์ป้องกันให้กับคอมพิวเตอร์แม่ข่ายเป็นรายเครื่องที่ให้บริการจริง

ข้อ ๔๓ การเชื่อมต่อในลักษณะของการเข้าสู่ระบบจากระยะไกล Remote Login จากเครือข่ายอินเตอร์เน็ตมายังคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์ภายในเครือข่าย ต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และได้รับความเห็นชอบจากผู้บังคับบัญชาของส่วนงานและสำนักคอมพิวเตอร์

ข้อ ๔๔ คอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในส่วนงานที่ไม่จำเป็นต้องเข้าถึงข้อมูลจากอินเทอร์เน็ต ต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยต้องกำหนดให้มีการควบคุมการเข้าถึง

ข้อ ๔๕ คอมพิวเตอร์แม่ข่ายที่จัดตั้งขึ้นต้องมีการประสานเวลา (Synchronization) กับคอมพิวเตอร์แม่ข่ายเวลา (Network Time Server) ของสำนักคอมพิวเตอร์ หรือคอมพิวเตอร์แม่ข่ายเวลาที่เป็นมาตรฐานของประเทศ

ข้อ ๔๖ ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมหรือโพรโทคอลที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (bittorrent), อีมูล (emule), FTP, TELNET, RSH เป็นต้น เว้นแต่จะได้รับอนุญาตจากสำนักคอมพิวเตอร์

หมวด ๖
นโยบายด้านการใช้งานจดหมายอิเล็กทรอนิกส์
(E-mail Usage Policy)

ข้อ ๔๗ นโยบายนี้ครอบคลุมการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยที่เป็นโดเมนชื่อว่า @kmutnb.ac.th

ข้อ ๔๘ บุคลากรและส่วนงานของมหาวิทยาลัยให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัยในการติดต่องานราชการหรืองานที่เกี่ยวข้องกับมหาวิทยาลัย

ข้อ ๔๙ มหาวิทยาลัยต้องสนับสนุนให้บุคลากรและหน่วยงานของมหาวิทยาลัยให้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของมหาวิทยาลัย

ข้อ ๕๐ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ ต้องกำหนดให้มีการติดตั้งระบบกรองจดหมายอิเล็กทรอนิกส์ (E-mail Filter) เพื่อป้องกันการโจมตีแบบ SPAM ทั้งจากภายในและภายนอกเครือข่ายของมหาวิทยาลัย

ข้อ ๕๑ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ ต้องกำหนดให้มีระบบเก็บบันทึกจดหมายอิเล็กทรอนิกส์ (E-mail Archive) เป็นเวลาอย่างน้อย ๓๐ วัน หรือตามข้อกำหนดตามพระราชบัญญัติ ว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ สำหรับการตรวจสอบการรับส่งอีเมล์ย้อนหลัง

ข้อ ๕๒ มหาวิทยาลัยไม่อนุญาตให้ส่วนงานทำการติดตั้งคอมพิวเตอร์แม่ข่ายจดหมายอิเล็กทรอนิกส์ (E-Mail Server) เพื่อใช้งานภายในส่วนงาน เว้นแต่ได้รับอนุญาตจากสำนักคอมพิวเตอร์ และได้มีมาตรการควบคุมตามนโยบายของสำนักคอมพิวเตอร์ และต้องใช้ชื่อที่ใช้ระบุลงในคอมพิวเตอร์ (โดเมน) ภายใต้ชื่อ kmutnb.ac.th เท่านั้น

ข้อ ๕๓ การจดทะเบียนบัญชี (Account Registration) ผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (E-mail) สำหรับอาจารย์และเจ้าหน้าที่ให้อาจารย์หรือเจ้าหน้าที่ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของหน่วยงานโดยยื่นคำขอกับเจ้าหน้าที่ของสำนักคอมพิวเตอร์ ผ่านทางผู้บังคับบัญชาของส่วนงานต้นสังกัด หรือให้แสดงหลักฐานทางราชการว่าเป็นอาจารย์หรือเจ้าหน้าที่ของมหาวิทยาลัย หรือมีข้อมูลอยู่ในระบบสารสนเทศบุคคลากรของมหาวิทยาลัย

ข้อ ๕๔ การจดทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์สำหรับนักศึกษาให้นักศึกษารับบัญชีผู้ใช้ เมื่อได้ขึ้นทะเบียนเป็นนักศึกษาแล้ว โดยผู้ดูแลระบบจะจดทะเบียนบัญชีผู้ใช้ให้พร้อมกับการขึ้นทะเบียนเรียนของนักศึกษา

ข้อ ๕๕ เมื่อได้รับรหัสผ่านสำหรับการเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันที

ข้อ ๕๖ ผู้ใช้งานต้องไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือระบบอื่นๆ หรือในเอกสารใดๆ ที่ผู้อื่นสามารถเข้าถึงข้อมูลได้

ข้อ ๕๗ ผู้ใช้งานควรเปลี่ยนรหัสผ่านอย่างน้อยทุกๆ ๓-๖ เดือน หรือให้เปลี่ยนรหัสผ่านทันทีเมื่อได้รับแจ้งจากทางสำนักคอมพิวเตอร์ ในกรณีที่สงสัยว่ามีการรั่วไหลของรหัสผ่านดังกล่าว

ข้อ ๕๘ ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของจดหมายอิเล็กทรอนิกส์และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตนเอง

ข้อ ๕๙ ทุกครั้งหลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้งานต้องลงบันทึกออก (Logout) ทุกครั้ง

หมวด ๗
นโยบายด้านการควบคุมการจราจรข้อมูล
(Data Traffic Control Policy)

ข้อ ๖๐ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ มีหน้าที่ในการบริหารจัดการ ติดตั้ง และกำหนดค่าของไฟร์วอลล์ (Firewall) และ/หรือ เครื่อง Proxy ระหว่างเครือข่ายอินเตอร์เน็ตและเครือข่ายหลักและเครือข่ายของส่วนงานสำหรับการใช้งานด้านการควบคุมการจราจรข้อมูล

ข้อ ๖๑ ส่วนงานหรือส่วนงานที่มีเครือข่ายของส่วนงานต้องติดตั้งไฟร์วอลล์เพื่อเชื่อมต่อกับเครือข่ายหลักและกำหนดมีผู้รับผิดชอบในการจัดการไฟร์วอลล์ของส่วนงาน

ข้อ ๖๒ การกำหนดค่าเริ่มต้นพื้นฐานหรือค่าโดยปริยาย (Default) ของการควบคุมการจราจรข้อมูลของทั้งเครือข่ายหลักและเครือข่ายส่วนงานต้องเป็นการปฏิเสธ (Deny) ทั้งหมด

ข้อ ๖๓ การจราจรข้อมูลในทุกเส้นทางที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ตและบริการอินเทอร์เน็ตที่ไม่อนุญาตตามนโยบายด้านความมั่นคงปลอดภัยของเทคโนโลยีสารสนเทศ ต้องถูกขัดขวาง (Block) โดยไฟร์วอลล์โดยปริยาย

ข้อ ๖๔ ผู้ใช้งานที่เข้าถึงเครือข่ายอินเทอร์เน็ตต้องมีการลงบันทึกเข้า (Login) ด้วยบัญชีผู้ใช้ (Account) ก่อนการใช้งานทุกครั้งด้วยการพิสูจน์ตัวตน (Authentication) ที่ไฟร์วอลล์หรือที่เครื่องตัวแทน (Proxy Server)

ข้อ ๖๕ การเปลี่ยนแปลงการกำหนดค่าต่างๆ (Configuration) ของไฟร์วอลล์ เช่น นโยบายคอมพิวเตอร์แม่ข่ายที่อนุญาต บริการที่อนุญาต และการเชื่อมต่อที่อนุญาต ต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้ง และสามารถตรวจสอบย้อนหลังได้ไม่น้อยกว่า ๓๐ วัน

ข้อ ๖๖ ต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ (Configuration) ของไฟร์วอลล์เป็นประจำทุกสัปดาห์ หรือทุกครั้งก่อนการเปลี่ยนแปลงค่า

ข้อ ๖๗ การเข้าถึงไฟร์วอลล์ต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

ข้อ ๖๘ ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกไฟร์วอลล์ ต้องมีการจัดเก็บข้อมูลจราจรไม่น้อยกว่า ๙๐ วัน

ข้อ ๖๙ การเชื่อมต่อเครือข่ายอินเทอร์เน็ตของคอมพิวเตอร์หรืออุปกรณ์ที่เชื่อมต่อเครือข่ายที่นอกเหนือจากการใช้โพรโทคอลพื้นฐานที่ทางสำนักคอมพิวเตอร์อนุญาตให้ใช้งาน ต้องขออนุญาตอย่างเป็นลายลักษณ์อักษรจากสำนักคอมพิวเตอร์ ก่อน

ข้อ ๗๐ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ มีสิทธิที่จะระงับหรือขัดขวางการใช้งานของคอมพิวเตอร์หรืออุปกรณ์ที่เชื่อมต่อเครือข่าย ของหน่วยงานที่มีพฤติกรรมการใช้งานที่ผิดนโยบาย หรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัย จนกว่าจะได้รับการแก้ไขโดยให้มีการแจ้งเตือนอย่างเป็นลายลักษณ์อักษรไปยังส่วนงานนั้น

ข้อ ๗๑ ผู้ใช้งานที่ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ต้องถูกระงับสิทธิการใช้งานอินเทอร์เน็ตทันทีและเป็นระยะเวลาอย่างน้อย ๓๐ วัน และให้มีการแจ้งผู้ใช้งานอย่างเป็นลายลักษณ์อักษรด้วยบันทึกข้อความ (Memo) หรือด้วยจดหมายอิเล็กทรอนิกส์ (E-mail) และให้พิจารณาคืนสิทธิการใช้งานอินเตอร์เน็ตเมื่อเห็นว่าการใช้งานของผู้ใช้งานมีความปลอดภัยแล้ว

ข้อ ๗๒ ส่วนงานที่เชื่อมต่อกับเครือข่ายหลักของมหาวิทยาลัยด้วยอุปกรณ์เครือข่ายประเภท Gateway/Router/NAT ทุกประเภท ต้องมีการจัดเก็บข้อมูลบันทึกการใช้งาน (Log) อยู่ตลอดเวลาตามพระราชบัญญัติว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และ ต้องมีการสำรองข้อมูลบันทึกการใช้งาน (Log) อย่างน้อย ๙๐ วัน และต้องสามารถตรวจสอบย้อนหลังได้ตลอดเวลา

หมวด ๘
นโยบายด้านการตรวจจับและการป้องกันการบุกรุก
(Intrusion Detection System / Intrusion Prevention System Policy : IDS/IPS Policy)

ข้อ ๗๓ นโยบายด้านการตรวจจับและการป้องกันการบุกรุก จัดทำขึ้นเพื่อป้องกันทรัพยากรระบบสารสนเทศของมหาวิทยาลัย ให้มีความมั่นคงปลอดภัย และเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจจับและการป้องกันการบุกรุก พร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

ข้อ ๗๔ นโยบายนี้ครอบคลุมคอมพิวเตอร์แม่ข่ายและคอมพิวเตอร์ ในเครือข่ายหลักของมหาวิทยาลัยและเครือข่ายของส่วนงาน รวมถึงเส้นทางที่ข้อมูลอาจเดินทางภายในมหาวิทยาลัย นโยบายนี้ไม่ได้ครอบคลุมเส้นทางในเครือข่ายอินเทอร์เน็ต

ข้อ ๗๕ ระบบสารสนเทศที่สำคัญของมหาวิทยาลัยที่สามารถเข้าถึงได้จากเครือข่ายอินเทอร์เน็ตหรือเครือข่ายสาธารณะ (Public Network) ต้องผ่านการตรวจสอบจากระบบตรวจจับและป้องกันการบุกรุกโดยความรับผิดชอบของสำนักคอมพิวเตอร์

ข้อ ๗๖ สำนักคอมพิวเตอร์ มีความรับผิดชอบในการจัดระบบ DMZ สำหรับให้บริการคอมพิวเตอร์แม่ข่ายในเครือข่ายหลักและให้คอมพิวเตอร์แม่ข่ายทั้งหมดใน DMZ ต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ โดยให้สำนักคอมพิวเตอร์ เป็นผู้ตรวจสอบและเก็บบันทึกข้อมูลของผู้ขอติดตั้ง

ข้อ ๗๗ สำนักคอมพิวเตอร์ ต้องจัดให้มีกลไกสำหรับการตรวจสอบ และทำการปิดช่องโหว่ (Update Patch) หรือทำการปรับปรุงข้อมูลลายเซ็นการบุกรุก (Signature) ของระบบตรวจจับและการป้องกันการบุกรุก (IDS/IPS) เป็นประจำ

ข้อ ๗๘ สำนักคอมพิวเตอร์ ต้องจัดให้มีกลไกสำหรับการตรวจสอบเหตุการณ์ ข้อมูลจราจร พฤติกรรมการใช้งาน กิจกรรม และบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายหลัก และกำหนดให้มีการรายงานต่อคณะกรรมการบริหารของสำนักคอมพิวเตอร์ เป็นประจำทุกเดือน

ข้อ ๗๙ คอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่านระบบตรวจจับและป้องกันการบุกรุก ต้องมีการบันทึกผลการตรวจสอบและต้องสามารถตรวจสอบย้อนหลังได้

ข้อ ๘๐ ผลการตรวจสอบการบุกรุกทั้งหมด ตามข้อ ๗๘ และข้อ ๗๙ ต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

ข้อ ๘๑ พฤติกรรมการใช้งาน กิจกรรม หรือเหตุการณ์ทั้งหมด เช่น พฤติกรรมที่น่าสงสัย หรือการพยายามเข้าระบบ ทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จ ที่มีความเสี่ยงต่อการถูกบุกรุกหรือการโจมตี ต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

ข้อ ๘๒ ระบบตรวจจับและป้องกันการบุกรุก ต้องทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายหลักของมหาวิทยาลัย

ข้อ ๘๓ สำนักคอมพิวเตอร์และหน่วยงานที่มีเครือข่ายของตนเอง ต้องมีขั้นตอนการปฏิบัติการตอบสนองฉุกเฉิน (Emergency Response Procedure) ต่อเหตุการณ์ที่เกิดขึ้นอย่างเป็นลายลักษณ์อักษร ได้แก่ การรายงานผลการตรวจพบของเหตุการณ์ต่างๆ การดำเนินการเพื่อลดความเสียหาย การลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบ การป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคต และผู้รับผิดชอบการดำเนินการตามขั้นตอนการปฏิบัติการตอบสนองฉุกเฉิน

ข้อ ๘๔ คอมพิวเตอร์แม่ข่ายที่ติดตั้งในเครือข่ายหลักหรือเครือข่ายของส่วนงาน ควรติดตั้ง ระบบตรวจจับการบุกรุกแบบติดตั้งในเครื่อง (Host-based IDS) และให้มีการทำข้อมูลบันทึกการใช้งาน (Log) และตรวจสอบข้อมูลเหตุการณ์อย่างสม่ำเสมอ

ข้อ ๘๕ มหาวิทยาลัยโดยสำนักคอมพิวเตอร์ มีสิทธิในการยุติการเชื่อมต่อเครือข่ายของส่วนงานที่มีพฤติกรรมเสี่ยงต่อการบุกรุกเครือข่ายหลัก โดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า และไม่ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้นกับคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุก

ข้อ ๘๖ ผู้ใช้งานที่ถูกตรวจสอบและพบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของมหาวิทยาลัย โดยการพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบ หรือมีพฤติกรรมเสี่ยงต่อการทำงานของทรัพยากรสารสนเทศมหาวิทยาลัย จะถูกระงับการใช้ทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับพระราชบัญญัติ ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลหรือทรัพยากรสารสนเทศของมหาวิทยาลัยหรือความเสียหายส่วนบุคคล จะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

หมวด ๙
นโยบายด้านการใช้งานคอมพิวเตอร์และซอฟต์แวร์ที่จำเป็น
(Computer and Software Usage Policy)

ข้อ ๘๗ นโยบายนี้สำหรับการควบคุมการใช้งานคอมพิวเตอร์ส่วนบุคคล (Personal Computer) คอมพิวเตอร์พกพา (Notebook หรือ Laptop) คอมพิวเตอร์เสมือน (Virtual Personal Computer) แท็บเล็ต (Tablet) โทรศัพท์เคลื่อนที่ประเภท Smart Phone หรืออุปกรณ์เทียบเท่าคอมพิวเตอร์ เรียกรวมกันว่า “คอมพิวเตอร์” ที่เป็นทรัพย์สินของมหาวิทยาลัยและที่เป็นทรัพย์สินส่วนบุคคลของผู้ใช้งานที่นำมาใช้เชื่อมต่อกับเครือข่ายหลักหรือเครือข่ายของส่วนงานของมหาวิทยาลัย เพื่อให้เกิดการใช้งานอย่างปลอดภัยและไม่ให้มีผลกระทบต่อมหาวิทยาลัย

ข้อ ๘๘ ซอฟต์แวร์ที่นำมาติดตั้งใช้งานในคอมพิวเตอร์ของมหาวิทยาลัยต้องเป็นซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องตามกฎหมาย

ข้อ ๘๙ มหาวิทยาลัยไม่มีนโยบายสนับสนุนการละเมิดลิขสิทธิ์ซอฟต์แวร์หรือการใช้ซอฟต์แวร์อย่างผิดกฎหมาย และหากมีการละเมิดหรือการใช้งานซอฟต์แวร์อย่างผิดกฎหมาย ให้ถือว่าเป็นความรับผิดชอบของผู้ใช้งานเอง

ข้อ ๙๐ มหาวิทยาลัยหรือส่วนงานมีหน้าที่จัดหาซอฟต์แวร์ที่มีลิขสิทธิ์ที่จำเป็นสำหรับการใช้งานทั่วไปภายในมหาวิทยาลัยหรือภายในส่วนงานเพื่อเป็นการส่งเสริมให้มีการใช้งานซอฟต์แวร์อย่างถูกต้องตามกฎหมาย

ข้อ ๙๑ ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อทรัพย์สินที่มหาวิทยาลัยมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นทรัพย์สินของผู้ใช้งานเอง โดยกำหนดให้จัดทำแบบการขอใช้หรือขอยืมทรัพย์สินและให้กำหนดความรับผิดชอบของผู้ใช้งานในแบบการขอใช้หรือขอยืมทรัพย์สิน

ข้อ ๙๒ กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบทรัพย์สินของมหาวิทยาลัยที่ได้ขอยืมไม่ให้เกิดความเสียหายหรือสูญหาย

ข้อ ๙๓ ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายในกรณีที่ทรัพย์สินของมหาวิทยาลัยชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

ข้อ ๙๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมทรัพย์สินคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออื่นๆ ที่ตนเองได้ยืมจากมหาวิทยาลัย ไม่ว่าในกรณีใดๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาของส่วนงานที่เป็นผู้ดูแลทรัพย์สินนั้น

ข้อ ๙๕ ผู้ใช้งานทรัพย์สินคอมพิวเตอร์ส่วนบุคคล คอมพิวเตอร์พกพา หรืออื่นๆ ของมหาวิทยาลัยต้องมีหน้าที่รับผิดชอบในการปรับปรุงข้อมูลสำหรับตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดี (Malware) และปรับปรุงระบบปฏิบัติการด้วยทำการปิดช่องโหว่ (Update Patch) ให้ทันสมัยอยู่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นจากการโจมตี

ข้อ ๙๖ ทรัพย์สินและทรัพยากรสารสนเทศต่างๆ ที่มหาวิทยาลัยจัดเตรียมไว้ให้ใช้งานมีวัตถุประสงค์เพื่อการใช้งานตามภารกิจของมหาวิทยาลัยเท่านั้น ห้ามมิให้ผู้ใช้งานนำทรัพย์สินและทรัพยากรสารสนเทศต่างๆ ไปใช้ในกิจกรรมที่มหาวิทยาลัยไม่ได้กำหนดหรือไม่ได้อยู่ในภารกิจของมหาวิทยาลัย หรือทำให้เกิดความเสียหายต่อมหาวิทยาลัย และหากเกิดความเสียหายใดๆ ที่เกิดจากการละเมิดดังกล่าวให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ข้อ ๙๗ ผู้ใช้งานที่ต้องการนำคอมพิวเตอร์และอุปกรณ์ส่วนตัวมาเชื่อมต่อกับเครือข่ายหลักของมหาวิทยาลัยหรือเครือข่ายของส่วนงาน ต้องเป็นผู้ที่มีประวัติอยู่ในระบบสารสนเทศบุคลากรของมหาวิทยาลัย หรือเป็นนักศึกษาที่มีประวัติในระบบสารสนเทศเพื่องานทะเบียนและอยู่ในระหว่างการเป็นนักศึกษา หรือเป็นผู้ที่มีหลักฐานทางราชการที่แสดงได้ว่าผู้ใช้งานเป็นอาจารย์ เจ้าหน้าที่ หรือนักศึกษาของมหาวิทยาลัย เพื่อลงทะเบียนกับสำนักคอมพิวเตอร์ ก่อนใช้งาน

ข้อ ๙๘ ผู้ใช้งานที่นำคอมพิวเตอร์ส่วนตัวมาใช้งานต้องมีหน้าที่รับผิดชอบในการปรับปรุงข้อมูลสำหรับตรวจสอบไวรัสคอมพิวเตอร์ และโปรแกรมไม่ประสงค์ดี และปรับปรุงระบบปฏิบัติการด้วย Update Patch ให้ทันสมัยอยู่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นจากการโจมตี

ข้อ ๙๙ คอมพิวเตอร์ส่วนตัวของผู้ใช้งานต้องติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Antivirus Program) ตามที่มหาวิทยาลัยได้จัดหามาให้หรือที่ผู้ใช้งานจัดหาเอง และต้องปรับปรุงข้อมูลสำหรับตรวจสอบความปลอดภัย (Security Patch) ให้มีความทันสมัยอยู่ตลอดเวลาเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

ข้อ ๑๐๐ บรรดาข้อมูล ไฟล์ ซอฟต์แวร์ หรือสิ่งอื่นใด ที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

ข้อ ๑๐๑ ผู้ใช้งานต้องพึงระวังไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติ ผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบทราบโดยทันที

ข้อ ๑๐๒ เมื่อผู้ใช้งานพบว่าคอมพิวเตอร์ที่ตนเองใช้งานอยู่ติดไวรัสคอมพิวเตอร์ ผู้ใช้งานต้องไม่เชื่อมต่อคอมพิวเตอร์เข้าสู่เครือข่ายหลักหรือเครือข่ายของส่วนงาน และต้องแจ้งปัญหาดังกล่าวแก่ผู้ดูแลระบบทราบโดยทันที

ข้อ ๑๐๓ ห้ามผู้ใช้งาน ลักลอบ ทำสำเนา เปลี่ยนแปลง ลบทิ้ง ซึ่งข้อมูล ข้อความ เอกสาร หรือสิ่งใดๆ ที่เป็นทรัพย์สินของส่วนงานหรือของมหาวิทยาลัย หรือของผู้อื่น โดยไม่ได้รับอนุญาต และหากผู้ใช้งานได้ทำการละเมิดด้วยกระทำการดังกล่าวจะต้องถูกลงโทษทางวินัย และหากเป็นการกระทำผิดตามพระราชบัญญัติ ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ผู้ใช้งานนั้นจะต้องถูกดำเนินคดีตามกฎหมายอีกด้วย

ข้อ ๑๐๔ ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์ โปรแกรมไม่ประสงค์ดี หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่ระบบสารสนเทศที่สำคัญหรือทรัพยากรสารสนเทศของมหาวิทยาลัยหรือมาสู่คอมพิวเตอร์ของบุคคลอื่น

หมวด ๑๐
นโยบายด้านการบริหารจัดการข้อมูล ฐานข้อมูล และการพัฒนาระบบสารสนเทศเพื่อการใช้งาน
(Information and Database Management and Information System Development Policy)

ข้อ ๑๐๕ มหาวิทยาลัยมีพันธกรณีในการปฏิบัติตามพระราชบัญญัติ ว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ โดยมหาวิทยาลัยต้องดำเนินการทุกวิถีทางเพื่อให้มหาวิทยาลัยและส่วนงานต่างๆ ในมหาวิทยาลัยมีการดำเนินธุรกรรมอิเล็กทรอนิกส์ที่เกี่ยวข้องกับข้อมูลของมหาวิทยาลัยให้เป็นไปตามพันธกรณีดังกล่าว

ข้อ ๑๐๖ ข้อมูลทั้งหลายที่อยู่ภายในระบบสารสนเทศของมหาวิทยาลัย ถือเป็นทรัพย์สินของมหาวิทยาลัย ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย เว้นแต่จะได้รับอนุญาตจากมหาวิทยาลัยหรือผู้ได้รับมอบหมายจากมหาวิทยาลัย

ข้อ ๑๐๗ ผู้ใช้งานหรือผู้ใช้ข้อมูลต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลนั้นจะเป็นของมหาวิทยาลัยหรือส่วนงาน หรือเป็นข้อมูลของบุคคลภายนอกที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัย และหากไม่ทราบแน่ชัดเรื่องการใช้งานข้อมูลดังกล่าวว่าถูกต้องหรือไม่ ให้สอบถามที่หัวหน้าส่วนงานหรือสำนักคอมพิวเตอร์

ข้อ ๑๐๘ ผู้ใช้งานหรือผู้ใช้ข้อมูลห้ามปฏิเสธความรับผิดหากมีการละเมิดการใช้งานข้อมูลดังกล่าว หรือการใช้งานข้อมูลดังกล่าวในทางที่ผิดอันเป็นผลเสียหายต่อมหาวิทยาลัยหรือส่วนงาน

ข้อ ๑๐๙ ผู้ใช้งานหรือผู้ใช้ข้อมูลต้องมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของมหาวิทยาลัย ไม่ให้เกิดการสูญหาย การถูกนำไปใช้ในทางที่ผิด หรือการเผยแพร่โดยไม่รับอนุญาต ผู้ใช้งานหรือผู้ใช้ข้อมูลต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายจากการกระทำดังกล่าวนั้นด้วย

ข้อ ๑๑๐ ในกรณีที่ต้องการเชื่อมต่อกับระบบสารสนเทศที่สำคัญหรือทรัพยากรสารสนเทศของมหาวิทยาลัย ผู้ใช้งานหรือผู้ใช้ข้อมูลที่ขอเชื่อมต่อต้องได้รับอนุญาตจากมหาวิทยาลัยหรือผู้ได้รับมอบหมายจากมหาวิทยาลัย และต้องจัดเตรียมการเชื่อมต่อให้มีความปลอดภัยตามที่สำนักคอมพิวเตอร์เป็นผู้กำหนด

ข้อ ๑๑๑ ผู้ใช้งานหรือผู้ใช้ข้อมูลต้องป้องกัน ดูแล รักษาไว้ซึ่งความลับ ความถูกต้อง และความพร้อมใช้ของข้อมูล

ข้อ ๑๑๒ ผู้ใช้งานมีสิทธิโดยชอบธรรมที่จะเก็บ รักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามที่เห็นสมควร มหาวิทยาลัยจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคล และไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่มหาวิทยาลัยต้องการตรวจสอบข้อมูลหรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับมหาวิทยาลัย ซึ่งมหาวิทยาลัยอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบ ทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลา โดยไม่ต้องแจ้งให้เจ้าของข้อมูลหรือผู้ใช้งานทราบ

ข้อ ๑๑๓ ผู้ใช้งานหรือผู้ใช้ข้อมูลมีสิทธิที่จะพัฒนาระบบสารสนเทศเพื่อการใช้งานภายในมหาวิทยาลัย เว้นแต่การดำเนินการดังต่อไปนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่ทำซ้ำ เผยแพร่ หรือเปลี่ยนแปลงข้อมูลสารสนเทศของมหาวิทยาลัยโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายกลไกรักษาความปลอดภัยของข้อมูลสารสนเทศของมหาวิทยาลัยรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่าน การลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๓) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิและลำดับความสำคัญในการครอบครองทรัพยากรสารสนเทศมากกว่าที่มหาวิทยาลัยกำหนดให้

(๔) พัฒนาโปรแกรมใดๆ ที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์หรือโปรแกรมไม่ประสงค์ดี

(๕) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายการจำกัดสิทธิการใช้ (License) ของซอฟต์แวร์ลิขสิทธิ์

(๖) นำเสนอข้อมูลที่ผิดกฎหมาย ละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสม หรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทย ผ่านทางช่องทางการสื่อสารข้อมูลต่างๆ

ข้อ ๑๑๔ ผู้ใช้งานหรือผู้ใช้ข้อมูลที่ฝ่าฝืนในข้อ ๑๑๓ ทั้งโดยเจตนาหรือประมาท ต้องถูกลงโทษทางวินัย และถ้าการกระทำดังกล่าวขัดต่อพระราชบัญญัติ ว่าด้วย การกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ต้องถูกดำเนินคดีทางกฎหมายต่อไป

หมวด ๑๑
นโยบายด้านการสำรองข้อมูลและการกู้คืนระบบจากเหตุหายนะ
(Backup and Disaster Recovery Policy)

ข้อ ๑๑๕ นโยบายนี้ครอบคลุมการสำรองข้อมูลและการกู้คืนของระบบสารสนเทศที่สำคัญที่จัดตั้งขึ้นสำหรับการใช้งานภายในมหาวิทยาลัย ทั้งที่เป็นของมหาวิทยาลัยและของส่วนงาน

ข้อ ๑๑๖ ผู้ดูแลระบบมีหน้าที่เกี่ยวกับนโยบายด้านการสำรองข้อมูลและการกู้คืนระบบจากเหตุหายนะ ดังต่อไปนี้

(๑) ทำสำเนาซอฟต์แวร์ของระบบสารสนเทศที่สำคัญของมหาวิทยาลัยหรือของส่วนงานอย่างสม่ำเสมอหรือก่อนการเปลี่ยนแปลงหรือปรับปรุงเวอร์ชั่นของซอฟต์แวร์เพื่อป้องกันปัญหาระบบไม่สามารถใช้งานได้หรือไม่สามารถกู้คืนได้เมื่อเกิดปัญหาจากการเปลี่ยนแปลงหรือปรับปรุง

(๒) ผู้ดูแลระบบต้องทำการสำรองข้อมูลของระบบสารสนเทศที่สำคัญอย่างสม่ำเสมอ สำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงมากให้สำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง และสำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงปานกลางให้สำรองข้อมูลอย่างน้อย สัปดาห์ละ ๑ ครั้ง และสำหรับข้อมูลที่มีอัตราการเปลี่ยนแปลงน้อยให้สำรองข้อมูลอย่างน้อยเดือนละ ๑ ครั้ง

(๓) ผู้ดูแลระบบต้องมีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศที่สำคัญ โดยกำหนดให้มีขั้นตอนการปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

(๔) จัดเก็บข้อมูลที่สำรองแล้วในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งติดตั้งอยู่ที่สถานที่อื่นที่ไม่ใช่สถานที่เดียวกับสถานที่ติดตั้งระบบหรืออยู่ในสถานที่ที่ปลอดภัยจากภาวะคุมคาม (Threat) ต่างๆ ที่อาจเกิดขึ้นกับระบบหรือสถานที่ติดตั้งระบบได้

(๕) จัดทำแผนและระบบการทดสอบสื่อเก็บข้อมูลสำรองของระบบสารสนเทศที่สำคัญอย่างสม่ำเสมอเพื่อพิสูจน์ว่าสื่อที่เก็บสำรองข้อมูลยังสามารถใช้งานได้

ข้อ ๑๑๗ ข้อมูลของระบบสารสนเทศสำคัญที่จัดเก็บสำรองต้องมีการป้องกันข้อมูลรั่วไหล (Information Leak) ด้วยการเข้ารหัสลับ (Encryption)

ข้อ ๑๑๘ มหาวิทยาลัยและส่วนงานต้องมีการจัดทำแผนการกู้คืนระบบกรณีเกิดเหตุหายนะ (Disaster Recovery Plan) ของระบบสารสนเทศที่สำคัญให้สามารถกู้ระบบกลับคืนมาภายในระยะเวลาที่เหมาะสม และให้จัดตั้งคณะกรรมการเพื่อจัดทำแผนและรับผิดชอบในการดำเนินการตามแผน ดังกล่าว

ข้อ ๑๑๙ มหาวิทยาลัยมีหน้าที่ในการรักษาข้อมูลในระบบสารสนเทศที่สำคัญของมหาวิทยาลัยให้เป็นไปตามพระราชบัญญัติ ว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม และพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

ข้อ ๑๒๐ สำหรับส่วนงานที่จะจัดหาระบบสารสนเทศเพื่อการใช้งานภายในหน่วยงานที่เกี่ยวข้องกับการดำเนินงานของมหาวิทยาลัยและข้อมูลที่ใช้ในระบบมีความสำคัญตามพระราชบัญญัติ ว่าด้วย ธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ และที่แก้ไขเพิ่มเติม ต้องมีการกำหนดกลไกการสำรองข้อมูลและพื้นที่เพื่อจัดเก็บสำรองข้อมูลอย่างมีระบบเช่นเดียวกับระบบสารสนเทศที่สำคัญของมหาวิทยาลัย

หมวด ๑๒
บทลงโทษ

ข้อ ๑๒๑ หากบุคลากรคนใดทำผิดหรือกระทำการใดๆ อันเป็นการฝ่าฝืนประกาศนี้ ให้ถือว่าผู้นั้นกระทำความผิดวินัย และให้ดำเนินการทางวินัยตามหลักเกณฑ์ที่กำหนดไว้ในข้อบังคับมหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ ว่าด้วย การบริหารงานบุคคลพนักงานมหาวิทยาลัย พ.ศ. ๒๕๕๑

ข้อ ๑๒๒ กรณีบุคคลภายนอกกระทำผิดหรือกระทำการใดๆ อันเป็นการฝ่าฝืนประกาศนี้ และการกระทำดังกล่าวเป็นความผิดตามพระราชบัญญัติ ว่าด้วย การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ให้ผู้มีอำนาจดำเนินการกับผู้กระทำความผิดตามกฎหมาย

ทั้งนี้ ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๕ พฤศจิกายน พ.ศ. ๒๕๕๖

(ศาสตราจารย์ ดร.ธีรวุฒิ บุณยโสภณ)
อธิการบดี