ประกาศสำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

ที่ ๐๐๕/๒๕๕๕

เรื่อง นโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ

.....

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยบูรพา มีความมั่นคง ปลอดภัย และมิให้ผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยบูรพา และเป็นความผิดตามพระราชบัญญัติ ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๑. นิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

๑.๑ “ส่วนงาน” หมายถึง คณะ วิทยาลัย สถาบัน สำนัก หรือส่วนงานอื่นที่มีฐานะเทียบเท่าคณะ

๑.๒ “สำนักคอมพิวเตอร์” หมายถึง สำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

๑.๓ “ผู้อำนวยการ” หมายถึง ผู้อำนวยการสำนักคอมพิวเตอร์

๑.๔ “สินทรัพย์” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของมหาวิทยาลัยบูรพา ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์ และอยู่ภายใต้ขอบเขตการควบคุมตามมาตรฐาน ISO/IEC 27001

๑.๕ “ระบบเครือข่าย” หมายถึง เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยบูรพา ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์

๑.๖ “คณะกรรมการ” หมายถึง คณะกรรมการดูแลและบริหารความปลอดภัยในระบบสารสนเทศ ISO/IEC 27001

๑.๗ “ผู้ใช้งาน” หมายถึง ข้าราชการ พนักงาน ลูกจ้างของมหาวิทยาลัยบูรพา และนิสิต รวมถึงบุคคลอื่นที่มหาวิทยาลัย มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

๑.๘ “สิทธิของผู้ใช้งาน” หมายถึง สิทธิของผู้ใช้งานในการเข้าถึงระบบเครือข่ายและระบบสารสนเทศของมหาวิทยาลัย

๑.๙ “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

๑.๑๐ “ความมั่นคงปลอดภัยด้านสารสนเทศ” หมายถึง การดำเนินการในด้านต่าง ๆ ที่เกี่ยวข้อง เพื่อให้มั่นใจว่าระบบเครือข่าย และระบบสารสนเทศมีความปลอดภัย สามารถให้บริการได้ตลอดเวลา

๑.๑๑ “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง สาเหตุที่อาจจะเป็นไปได้ที่จะเกิดขึ้นและมีผลกระทบต่อการให้บริการกับระบบเครือข่ายและระบบสารสนเทศ

๑.๑๒ “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง เหตุการณ์ที่ไม่พึงประสงค์หรือไม่อาจคาดคิดที่จะเกิดขึ้น และมีผลกระทบต่อการให้บริการกับระบบเครือข่ายและระบบสารสนเทศ

๑.๑๓ “ผู้ดูแลระบบ” หมายถึง ข้าราชการหรือพนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

๒. บททั่วไป

๒.๑ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศฉบับนี้จัดทำขึ้นเพื่อกำหนดนโยบาย และแนวทางให้เกิดความมั่นคงปลอดภัยในระบบสารสนเทศ โดยมีขอบเขตครอบคลุม ระบบสารสนเทศของมหาวิทยาลัยบูรพา โดยมีวัตถุประสงค์เพื่อ

๒.๑.๑ ระบบสารสนเทศเกิดความมั่นคงปลอดภัย ป้องกันการบุกรุก ความเสียหายที่มีต่อข้อมูลในระบบสารสนเทศ

๒.๑.๒ ผู้ใช้งานระบบสารสนเทศ เกิดความมั่นใจ เมื่อระบบมีปัญหา สามารถกู้คืนกลับได้อย่างรวดเร็ว

๒.๒ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ได้จัดทำขึ้นเป็นลายลักษณ์อักษรและได้รับการอนุมัติจากผู้อำนวยการ โดยผ่านความเห็นชอบของคณะกรรมการประจำสำนักคอมพิวเตอร์ และได้เผยแพร่ให้บุคลากรทุกคนที่เกี่ยวข้องทราบและปฏิบัติตามอย่างมีประสิทธิภาพ

๒.๓ นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ทบทวนปรับปรุงให้ทันสมัยอย่างน้อยปีละ ๑ ครั้ง

๓. ความรับผิดชอบของผู้บริหาร

๓.๑ ผู้อำนวยการ เป็นผู้ลงนามอนุมัตินโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ

๓.๒ คณะกรรมการ มีหน้าที่ดังนี้

๓.๒.๑ ทบทวนนโยบาย และปรับปรุงให้ทันสมัยสอดคล้องกับผลการประเมินความเสี่ยงในระบบสารสนเทศ

๓.๒.๒ ผลักดันให้ผู้ใช้งานทุกคนตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูลในระบบสารสนเทศ และปฏิบัติตามกฎหมายที่เกี่ยวข้อง

๓.๒.๓ สนับสนุนด้านสินทรัพย์ต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบเครือข่ายมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายฉบับนี้

๓.๒.๔ คณะกรรมการ ต้องทบทวน ประสิทธิภาพของการให้บริการระบบสารสนเทศ และนโยบายด้านความมั่นคงปลอดภัย เพื่อวางแผนในการปรับปรุงแก้ไข และพัฒนาระบบให้มีประสิทธิภาพ ทุก ๆ ๑ ปี

๓.๓ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ ผู้อำนวยการจะเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

๔. การให้บริการระบบสารสนเทศของสำนักคอมพิวเตอร์

๔.๑ บริการชื่อผู้ใช้งาน (Username) และรหัสผ่านส่วนตัว (Password) สำหรับการเข้าใช้งานระบบสารสนเทศ

๔.๒ การเชื่อมต่อผ่านสายสัญญาณ และ ไร้สายเข้าสู่ระบบเครือข่าย

๔.๓ จัดทำ และให้บริการสื่อการเรียนการสอน (e-Learning)

๔.๔ บริการสืบค้นข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ต

๔.๕ บริการระบบจดหมายอิเล็กทรอนิกส์

๔.๖ บริการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบสารสนเทศ

๔.๗ บริการเว็บไซต์ของมหาวิทยาลัยบูรพา และ ส่วนงานต่าง ๆ

๔.๘ บริการระบบสารสนเทศภายในและภายนอกมหาวิทยาลัย

๔.๙ บริการสำรองข้อมูล

๔.๑๐ บริการอื่น ๆ ที่ได้รับมอบหมาย

๕. ระบบความมั่นคงปลอดภัยของระบบสารสนเทศ ทางกายภาพ และสิ่งแวดล้อม

๕.๑ สำนักคอมพิวเตอร์มีหน้าที่ดังนี้

๕.๑.๑ จัดทำบัญชีสินทรัพย์ระบบสารสนเทศ มีการบริหารจัดการสินทรัพย์อย่างชัดเจน และจัดหมวดหมู่สินทรัพย์ตามระดับความสำคัญ ความลับ คุณค่า เพื่อหาวิธีการบริหารจัดการที่เหมาะสม เพื่อนำข้อมูลของสินทรัพย์ไปใช้เพื่อประเมินความเสี่ยงต่าง ๆ

๕.๑.๒ กำหนดให้ห้องควบคุมระบบ (System Control Room) เป็นบริเวณที่ต้องรักษาความปลอดภัย และจัดให้มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาตเท่านั้น

๕.๑.๓ จัดทำแผนป้องกันอุบัติภัย เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่นๆทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามเป้าหมายที่กำหนด

๕.๑.๔ ดูแลอุปกรณ์ระบบเครือข่ายไร้สายที่ใช้งานภายในสำนักคอมพิวเตอร์ โดยควบคุมการใช้งานจากส่วนกลาง ซึ่งได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงในการเข้าใช้งานระบบเครือข่าย

๕.๑.๕ เมื่อผู้ใช้งานไม่มีการใช้งานเครือข่าย ภายใน ๓๐ นาที กำหนดให้เครื่องคอมพิวเตอร์ที่เชื่อมต่อระบบเครือข่ายยุติการเชื่อมต่อโดยอัตโนมัติ

๕.๑.๖ กำหนดสิทธิให้ผู้ใช้งานระบบเครือข่ายจากภายนอก (User Guest) ที่ได้รับการอนุญาตให้เข้าสู่ระบบสารสนเทศของมหาวิทยาลัยบูรพา ส่วนงานที่เกี่ยวข้องต้องได้รับอนุญาต จากผู้อำนวยการ เป็นลายลักษณ์อักษร เพื่อให้สิทธิการใช้งาน และ กำหนดระยะเวลาใช้งานที่แน่นอน

๕.๑.๗ ตรวจสอบความเหมาะสมของข้อมูล ที่เผยแพร่ออกสู่สาธารณะ ต้องไม่ขัดต่อกฎหมายที่เกี่ยวข้อง และ กลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

๕.๑.๘ แบ่งแยกเครือข่ายโดยแยกตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศด้วย VLAN

๕.๒ การควบคุมการนำเข้าและการส่งออก เครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศ ของสำนักคอมพิวเตอร์

๕.๒.๑ การนำฮาร์ดแวร์และซอฟต์แวร์ใหม่ มาติดตั้งใช้งาน จะต้องผ่านตรวจสอบ และหากต้องมีการทดสอบก่อนเชื่อมต่อกับระบบเดิม ห้ามมิให้ใช้ฐานข้อมูลจริง ในการทดสอบ

๕.๒.๒ เครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูล ที่ส่งออกไปภายนอก ผู้ครอบครองต้องตรวจสอบ และป้องกันการนำข้อมูลออกไปพร้อมอุปกรณ์ เพื่อให้มั่นใจได้ว่า ข้อมูลที่สำคัญไม่รั่วไหลสู่ภายนอก

๕.๒.๓ ผู้ครอบครองสื่อบันทึกข้อมูล ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟต์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือเขียนทับ ก่อนจำหน่ายอุปกรณ์ดังกล่าว

๕.๒.๔ ผู้ดูแลระบบ ต้องควบคุมการให้บริการของหน่วยงานภายนอก (Outsource) ที่เกี่ยวข้องกับระบบสารสนเทศ และให้ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศของสำนักคอมพิวเตอร์

๕.๒.๕ ผู้ดูแลระบบ ตรวจสอบระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือติดตั้งใหม่ ไม่ให้เกิดผลกระทบต่อระบบสารสนเทศ ก่อนนำระบบนั้นมาติดตั้งใช้งาน

๕.๒.๖ ผู้ดูแลระบบ ตรวจจับ ป้องกัน และกู้คืน ระบบสารสนเทศ จากโปรแกรมที่ไม่ประสงค์ดี หรือ โปรแกรมชนิดเคลื่อนที่ เช่น ไวรัส เวิร์ม โทรจัน สปายแวร์ ฯลฯ รวมทั้งมีการสร้างความตระหนักถึงอันตรายที่เกิดขึ้นจากโปรแกรมที่ไม่ประสงค์ดีเหล่านี้ และเผยแพร่วิธีการใช้งานระบบสารสนเทศอย่างปลอดภัยให้ผู้ใช้งาน

๕.๒.๗ ผู้ดูแลระบบ ต้องสำรองข้อมูลและทดสอบข้อมูลที่เก็บไว้อย่างสม่ำเสมอตามขั้นตอนการปฏิบัติงานเรื่องการสำรองข้อมูล

๕.๒.๘ ผู้ดูแลระบบ บริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบเครือข่ายและระบบสารสนเทศได้ตามสิทธิที่ได้รับ

๕.๒.๙ ผู้ดูแลระบบ ตรวจสอบ และป้องกันการเข้าถึงพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ไม่ว่าจะเป็นจากทางกายภาพหรือผ่านระบบเครือข่าย โดยอุปกรณ์เครือข่ายจะติดตั้งในตู้ที่มีการป้องกันด้วยกุญแจล็อค และมีการกำหนดสิทธิผู้ใช้และรหัสผ่านในการเข้าถึงพอร์ต

๕.๒.๑๐ผู้ดูแลระบบ ตรวจสอบและป้องกันการเข้าถึงพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ไม่ว่าจะเป็นจากทางกายภาพหรือผ่านระบบเครือข่าย

๕.๒.๑๑ผู้ดูแลระบบ จัดเก็บข้อมูลจราจรคอมพิวเตอร์ตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐

๖. ข้อกำหนดเกี่ยวกับประเภทข้อมูล

๖.๑ ประเภทข้อมูล แบ่งได้ดังนี้

๖.๑.๑ เอกสารกระดาษ

๖.๑.๒ แฟ้มข้อมูลอิเล็กทรอนิกส์

๖.๑.๓ ฐานข้อมูล

๖.๒ การลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

๖.๓ เวลาและช่องทางการเข้าถึงข้อมูล

๖.๓.๑ เอกสารกระดาษ จัดเก็บในตู้เอกสารพร้อมการป้องกันการเข้าถึง จัดทำแฟ้มระบุชื่อแฟ้มให้ชัดเจน เพื่อความรวดเร็วในการให้บริการ

๖.๓.๒ แฟ้มข้อมูลอิเล็กทรอนิกส์ จัดเก็บบนเครื่องแม่ข่าย โดยกำหนดสิทธิการเข้าถึง สามารถเข้าถึงได้ตลอดเวลา

๖.๓.๓ ฐานข้อมูล จัดเก็บบนเครื่องแม่ข่าย โดยกำหนดสิทธิการเข้าถึง สามารถเข้าถึงได้ตลอดเวลา

๗. แนวทางการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๗.๑ การเข้าถึงหรือควบคุมระบบสารสนเทศ

๗.๑.๑ ผู้ใช้งาน สามารถเข้าถึงข้อมูลได้ตามสิทธิ ความรับผิดชอบของตนเอง โดยผู้ดูแลระบบเป็นผู้กำหนดสิทธิการเข้าถึงข้อมูล รวมทั้งมีการทบทวนสิทธิการใช้งานอย่างสม่ำเสมอ

๗.๑.๒ ผู้ดูแลระบบ ต้องจัดให้มีระบบบันทึกและติดตามการใช้งานระบบสารสนเทศ และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบ

๗.๑.๓ ผู้ดูแลระบบ ต้องจัดทำบัญชีรายชื่อเจ้าหน้าที่ผู้รับผิดชอบระบบเพื่อรองรับการแจ้งและแก้ไขปัญหาที่จะเกิดขึ้นกับระบบ และจัดทำเป็นเอกสารประกาศไว้ให้ชัดเจน รวมทั้งมีการทบทวนบัญชีรายชื่ออย่างสม่ำเสมอ

๗.๒ การเข้าถึงหรือควบคุมระบบเครือข่าย

๗.๒.๑ ผู้ใช้งาน ต้องทำการยืนยันตัวตน (Authentication) ทุกครั้งที่ใช้บริการผ่านอุปกรณ์ Internet Access Management

๗.๒.๒ ผู้ดูแลระบบ ต้องตรวจสอบการโจมตี บุกรุก การใช้งานในลักษณะที่ผิดปกติ เพื่อความมั่นคงปลอดภัยของระบบเครือข่ายอย่างสม่ำเสมอ บันทึกผลการตรวจสอบและเหตุการณ์ที่เกิดขึ้นในระบบเครือข่าย

๗.๒.๓ มีการติดตั้งอุปกรณ์หรือโปรแกรมป้องกันการบุกรุกในระบบเครือข่าย

๗.๒.๔ มีการปิดพอร์ตที่ไม่มีการใช้งานเครือข่ายทุกพอร์ต หากหน่วยงานที่ต้องการเชื่อมต่อระบบเครือข่ายเพิ่มเติมจะต้องได้รับอนุญาตจากผู้อำนวยการเป็นลายลักษณ์อักษร เพื่อให้สิทธิการใช้งาน

๗.๒.๕ มีการควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) โดยการกำหนดจากส่วนกลาง

๗.๒.๖ การบริหารจัดการรหัสผ่าน ดำเนินการผ่าน Web Portal โดยจะได้รับรหัสผ่านใหม่จากบัญชีจดหมายอิเล็กทรอนิกส์สำรองโดยอัตโนมัติ

๗.๓ การเข้าถึงระบบปฏิบัติการ

๗.๓.๑ ผู้ดูแลระบบหรือผู้ใช้งาน ต้องทำการกำหนดรหัสผ่านสำหรับการเข้าถึงเครื่องคอมพิวเตอร์ส่วนบุคคล

๗.๓.๒ ผู้ดูแลระบบหรือผู้ใช้งาน ต้องทำการตั้งโปรแกรมถนอมหน้าจอพร้อมรหัสผ่านเมื่อไม่มีการใช้งานนานกว่า ๑๕ นาที

๗.๔ การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

๗.๔.๑ ระบบที่มีผลกระทบและความสำคัญสูงต่อมหาวิทยาลัย ได้แก่ ระบบงบประมาณ พัสดุ การเงิน และบัญชีกองทุนโดยเกณฑ์พึงรับ-พึงจ่าย ลักษณะ ๓ มิติ ระบบทะเบียนและสถิตินิสิต ต้องมีการควบคุมแยกเครื่องใช้งาน (Server) จากระบบอื่น ๆ

๗.๔.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๗.๔.๓ เพื่อเป็นการรักษาความปลอดภัยของข้อมูลอิเล็กทรอนิกส์ สำนักคอมพิวเตอร์ได้กำหนดช่องทางการเข้าถึงข้อมูลอิเล็กทรอนิกส์ที่สำคัญ โดยเข้าถึงได้ผ่านระบบเครือข่ายภายใน

๗.๔.๔ ผู้ดูแลระบบ ต้องจำกัดระยะเวลาการเชื่อมต่อระบบ โดยตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานในช่วงเวลาที่กำหนด

๗.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน

๗.๕.๑ ผู้ดูแลระบบ จะทำการทบทวนสิทธิการใช้งาน เมื่อบุคลากรมีการเปลี่ยนแปลงตำแหน่ง เลื่อนขั้น ย้ายส่วนงาน

๗.๕.๒ เมื่อบุคลากร ลาออก หรือนิสิต พ้นสภาพนิสิต ระบบจะทำการยกเลิกบัญชีผู้ใช้งานโดยอัตโนมัติ

๘. แนวทางปฏิบัติในการสำรองข้อมูล

๘.๑ ทำการสำรองข้อมูลและซอฟต์แวร์เก็บไว้ทุกวันด้วยวิธีการตั้งเวลาการทำงานไว้ที่เครื่องแม่ข่ายและส่งข้อมูลไปยังไซต์ข้อมูลสำรอง และทดสอบการกู้คืนอย่างน้อยปีละ ๑ ครั้ง

๘.๒ มีขั้นตอนวิธีการสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง

๙. แนวทางปฏิบัติการประเมินความเสี่ยงด้านสารสนเทศ

๙.๑ กำหนดขั้นตอนในการบริหารความเสี่ยง ตั้งแต่กระบวนการประเมินภัยคุกคามและผลกระทบต่อทรัพย์สิน และบริการในระบบสารสนเทศ

๙.๒ จัดทำรายงานผลการประเมินความเสี่ยงในระบบสารสนเทศ และ แผนการจัดการกับความเสี่ยงในระบบสารสนเทศ เพื่อให้มั่นใจได้ว่า ระบบสารสนเทศ ได้รับการบริหารอย่างปลอดภัย

๑๐.การใช้งานจดหมายอิเล็กทรอนิกส์

๑๐.๑ ในการส่งข้อมูลที่เกี่ยวข้องกับงาน และข้อมูลที่สำคัญ ต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ที่สำนักคอมพิวเตอร์จัดไว้ให้ในการส่งข้อมูลเท่านั้น เพื่อป้องกันการรั่วไหลของข้อมูล

๑๐.๒ จดหมายอิเล็กทรอนิกส์ในกล่องจดหมายจะถูกเก็บไว้บนระบบสำรอง ข้อมูลสูงสุด ๙๐ วัน โดยจดหมายที่ส่งเข้ามายังกล่องจดหมายก่อนวันสำรองข้อมูลประจำสัปดาห์จะสามารถกู้คืนได้หากสูญหาย โดยผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ต้องแจ้งให้ผู้ดูแลระบบทราบ

๑๑. ข้อกำหนดการใช้งานระบบเครือข่าย ระบบสารสนเทศ และความรับผิดชอบของผู้ใช้งาน

๑๑.๑ ผู้ที่มีความประสงค์ใช้งานระบบเครือข่าย ระบบสารสนเทศของมหาวิทยาลัย ให้นำบัตรแสดงตน มาทำการลงทะเบียนเพื่อขอบัญชีผู้ใช้งานและรหัสผ่านที่ห้องให้บริการของสำนักคอมพิวเตอร์

๑๑.๒ การใช้งานรหัสผ่าน จะต้องรักษารหัสผ่านของตนเองให้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้ หากมีผู้อื่นล่วงรู้ข้อมูลอันเป็นความลับนี้ และนำไปใช้งานในทางที่ผิด

๑๑.๓ ต้องทำการเปลี่ยนรหัสผ่านของตนเองอย่างน้อยทุก ๆ ๑๘๐ วัน โดยการตั้งรหัสผ่านใหม่จะต้องมีความยาวไม่น้อยกว่า ๘ ตัว แต่ไม่เกิน ๑๖ ตัว ประกอบไปด้วยตัวอักขระหรืออักษรพิเศษ และรหัสผ่านต้องไม่เป็นส่วนหนึ่งของชื่อบัญชีผู้ใช้งาน

๑๑.๔ ต้องทำการกำหนดรหัสผ่านสำหรับการเข้าถึงเครื่องคอมพิวเตอร์ส่วนบุคคล และทำการตั้งโปรแกรมถนอมหน้าจอพร้อมรหัสผ่านเมื่อไม่มีการใช้งานนานกว่า ๓๐ นาที

๑๑.๕ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร ต้องทำการยืนยันตัวบุคคลด้วยบัญชีผู้ใช้และรหัสผ่าน ผ่านระบบ VPN จึงจะสามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศขององค์กรได้

๑๑.๖ กรณีข้อมูลที่เป็นความลับของราชการ หรือ ข้อมูลที่สำคัญ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ หรืออาจใช้โปรแกรมช่วยในการเข้ารหัสข้อมูล

๑๑.๗ รับผิดชอบในการรับ ส่ง หรือจัดเก็บข้อมูลอันเป็นความลับ ภายในระบบเครือข่าย หรือส่งออกไปภายนอกระบบเครือข่าย ทั้งนี้ สามารถขอคำปรึกษา หรือการสนับสนุนจากผู้ดูแลระบบของสำนักคอมพิวเตอร์ เพื่อให้การรับและส่งข้อมูลมีความปลอดภัยมากขึ้นได้

๑๑.๘ ต้องดูแลและบำรุงรักษาฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล หรือสารสนเทศใด ๆ ที่เป็นของตนเองหรือ อยู่ในความรับผิดชอบของตนเอง ยกเว้นฮาร์ดแวร์ ซอฟต์แวร์ ข้อมูล หรือสารสนเทศนั้น ๆ อยู่ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์

๑๑.๙ รับผิดชอบต่อความเสียหายที่เกิดขึ้น หากผู้ใช้งานนำฮาร์ดแวร์ หรือซอฟต์แวร์มาติดตั้ง เปลี่ยนแปลง ทำซ้ำ หรือต่อเติม กับอุปกรณ์ ที่อยู่ภายในสำนักคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากสำนักคอมพิวเตอร์ หรือไม่มีการติดต่อประสานงาน และขอคำปรึกษาจากผู้ดูแลระบบก่อนติดตั้ง

๑๑.๑๐ ห้ามโอนสิทธิการใช้งานสินทรัพย์ที่ตนเองได้รับสิทธิให้ใช้ แก่บุคคลอื่นยกเว้นได้รับอนุญาตจากผู้อำนวยการ

๑๑.๑๑ ห้ามใช้งานสินทรัพย์หรือบริการที่ไม่ได้มีไว้สำหรับตนเอง และไม่ได้รับอนุญาตจากเจ้าของสินทรัพย์หรือ บริการนั้น ๆ

๑๑.๑๒ ห้ามใช้งานระบบเครือข่าย เพื่อกระทำสิ่งที่ผิดกฎหมาย และผิดไปจากนโยบายด้านความมั่นคงปลอดภัย

๑๑.๑๓ ห้ามทำลาย ทำให้เสียหาย แก้ไข เปลี่ยนแปลง ทำซ้ำ หรือเพิ่มเติมข้อมูล และสารสนเทศของผู้อื่นโดยมิชอบ

๑๑.๑๔ ห้ามปลอมแปลงตัวตนในระบบเครือข่าย เสมือนกับเข้าใช้งานในนามผู้อื่น

๑๑.๑๕ ห้ามเผยแพร่ข้อมูล หรือสารสนเทศที่เป็นเท็จ หรือดำเนินการใด ๆ ที่จะส่งผลให้เกิดความเสียหายแก่ผู้อื่นหรือมหาวิทยาลัยบูรพา

๑๑.๑๖ ห้ามเผยแพร่ หรือจัดเก็บข้อมูลที่มีลักษณะลามก อนาจาร และขัดต่อศีลธรรมอันดี และ ห้ามเผยแพร่ข้อมูลภาพตัดต่อ เติม หรือดัดแปลงภาพของบุคคลอื่น ด้วยวิธีการใด ๆ ซึ่งจะทำให้ผู้อื่นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

๑๑.๑๗ ห้ามใช้สินทรัพย์และบริการในระบบเครือข่าย เพื่อประกอบธุรกิจ

๑๑.๑๘ ห้ามกระทำการอันมีลักษณะ เป็นการละเมิดสินทรัพย์ทางปัญญาของผู้อื่น

๑๑.๑๙ ห้ามใช้กรรมวิธีใด ๆ ก็ตามที่ทำให้การสื่อสารข้อมูลเกิดการชะลอตัว หรือรบกวนจนระบบเครือข่าย หรือสินทรัพย์ หรือบริการอย่างหนึ่งอย่างใดไม่สามารถทำงานได้ตามปกติ

๑๑.๒๐ ห้ามทำลาย หรือพยายามทำลายระบบความมั่นคงปลอดภัยของระบบเครือข่าย

๑๑.๒๑ ห้ามนำฮาร์ดแวร์ หรือซอฟต์แวร์เข้ามาเชื่อมต่อกับระบบเครือข่าย โดยไม่ได้รับอนุญาตจากสำนักคอมพิวเตอร์

๑๑.๒๒ ห้ามลักลอบดักจับข้อมูลในระบบเครือข่าย

๑๒.การเปิดเผยข้อมูล การยกเลิกหรือสิ้นสุดการให้บริการระบบสารสนเทศ

๑๒.๑ ผู้อำนวยการ อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งาน เพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิหรือสินทรัพย์ของสำนักคอมพิวเตอร์ หรือของผู้ใช้งานอื่น

๑๒.๒ ผู้อำนวยการ อาจยกเลิกสิทธิ การเข้าใช้งานระบบเครือข่าย หากผู้ใช้งานมิได้เข้าใช้งานในระบบเครือข่ายภายในระยะเวลาติดต่อกันเกิน ๙๐ วัน

๑๒.๓ ผู้อำนวยการ อาจยกเลิกการให้บริการ หากพบว่าผู้ใช้งานละเมิดข้อตกลงการใช้งาน หรือ ทำให้การให้บริการระบบเครือข่ายขัดข้อง โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

๑๒.๔ กรณีผู้ใช้งาน เมื่อพ้นสภาพการเป็นผู้ใช้งาน สำนักคอมพิวเตอร์จะยกเลิกสิทธิการเป็นผู้ใช้งาน

๑๒.๕ กรณีผู้ใช้งานเป็นบุคลากรจากภายนอกที่ได้รับสิทธิเข้าใช้งานระบบเครือข่ายเพื่อปฏิบัติงานในส่วนที่รับผิดชอบ จะสิ้นสุดสิทธิการใช้งาน เมื่อจบงานตามสัญญาการทำงาน

๑๒.๖ กรณีผู้ใช้งาน ฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ การยกเลิกสิทธ์ผู้ใช้งานขึ้นอยู่กับดุลยพินิจของผู้อำนวยการ

ประกาศ ณ วันที่ ๑๐ พฤษภาคม พ.ศ. ๒๕๕๕

(ลงชื่อ)

(ผู้ช่วยศาสตราจารย์. ดร.สุรางคนา ธรรมลิขิต)
ผู้อำนวยการสำนักคอมพิวเตอร์