(สำเนา)

ประกาศสำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา
เรื่อง นโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ

.....

เพื่อให้ระบบสารสนเทศของมหาวิทยาลัยบูรพา มีความมั่นคง ปลอดภัย และมิให้ผู้กระทำด้วยประการใด ๆ ให้ระบบสารสนเทศไม่สามารถทำงานตามคำสั่งที่กำหนดไว้ หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก้ไข หรือทำลายข้อมูลของบุคคลอื่นในระบบสารสนเทศโดยมิชอบ หรือใช้ระบบสารสนเทศเพื่อเผยแพร่ข้อมูลอันเป็นเท็จ หรือมีลักษณะอันลามกอนาจาร ซึ่งอาจก่อให้เกิดความเสียหายแก่มหาวิทยาลัยบูรพา และเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

1. นิยามศัพท์ที่ใช้ในนโยบายฉบับนี้

1.1 “ส่วนงาน” หมายความว่า คณะ วิทยาลัย สถาบัน สำนัก หรือส่วนงานอื่นที่มีฐานะเทียบเท่าคณะ

1.2 “สำนักคอมพิวเตอร์” หมายความว่า สำนักคอมพิวเตอร์ มหาวิทยาลัยบูรพา

1.3 “ผู้อำนวยการ” หมายความว่า ผู้อำนวยการสำนักคอมพิวเตอร์

1.4 “ทรัพย์สิน” หมายความว่า ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศของมหาวิทยาลัยบูรพา ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์ และอยู่ภายใต้ขอบเขตการควบคุมตามมาตรฐาน ISO/IEC 27001

1.5 “ระบบเครือข่าย” หมายความว่า เครือข่ายคอมพิวเตอร์ของมหาวิทยาลัยบูรพา ภายใต้การกำกับดูแลของสำนักคอมพิวเตอร์

1.6 “คณะกรรมการ” หมายความว่า คณะกรรมการดูแลและบริหารความปลอดภัยในระบบสารสนเทศ ISO/IEC 27001

1.7 “ผู้ใช้งาน” หมายความว่า ข้าราชการ พนักงาน ลูกจ้างของมหาวิทยาลัยบูรพา และนิสิต รวมถึงบุคคลอื่นที่มหาวิทยาลัย มอบหมายให้ปฏิบัติงานตามสัญญา ข้อตกลง หรือใบสั่งซื้อ

1.8 “ผู้ดูแลระบบ” หมายความว่า ข้าราชการหรือพนักงานที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบเครือข่าย ซึ่งสามารถเข้าถึงโปรแกรมเครือข่าย เพื่อจัดการฐานข้อมูลของระบบเครือข่าย

2. บททั่วไป

2.1 นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศฉบับนี้จัดทำขึ้นเพื่อกำหนดนโยบาย และแนวทางให้เกิดความมั่นคงปลอดภัยในระบบสารสนเทศ โดยมีขอบเขตครอบคลุม ระบบสารสนเทศของมหาวิทยาลัยบูรพา โดยมีวัตถุประสงค์เพื่อ

2.1.1 ระบบสารสนเทศเกิดความมั่นคงปลอดภัย ป้องกันการบุกรุก ความเสียหายที่มีต่อข้อมูลในระบบสารสนเทศ

2.1.2 ผู้ใช้งานระบบสารสนเทศ เกิดความมั่นใจ เมื่อระบบมีปัญหา สามารถกู้คืนกลับได้อย่างรวดเร็ว

2.2 นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ได้จัดทำขึ้นเป็นลายลักษณ์อักษรและได้รับการอนุมัติ จาก ผู้อำนวยการ โดยผ่านความเห็นชอบของคณะกรรมการประจำสำนักคอมพิวเตอร์ และได้เผยแพร่ให้บุคลากรทุกคนที่เกี่ยวข้องทราบและปฏิบัติตามอย่างมีประสิทธิภาพ

2.3 นโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ ทบทวนปรับปรุงให้ทันสมัยอย่างน้อยปีละครั้ง

3. ความรับผิดชอบของผู้บริหาร

3.1 ผู้อำนวยการ เป็นผู้ลงนามอนุมัตินโยบายความมั่นคงปลอดภัยในระบบสารสนเทศ

3.2 คณะกรรมการ มีหน้าที่ดังนี้

3.2.1 ทบทวนนโยบาย และปรับปรุงให้ทันสมัยสอดคล้องกับผลการประเมินความเสี่ยงในระบบสารสนเทศ

3.2.2 ผลักดันให้ผู้ใช้งานทุกคนตระหนักถึงความสำคัญในการรักษาความปลอดภัยของข้อมูลในระบบสารสนเทศ และปฏิบัติตามกฎหมายที่เกี่ยวข้อง

3.2.3 สนับสนุนด้านทรัพย์สินต่าง ๆ เพื่อให้การบริหารจัดการและให้บริการระบบเครือข่ายมีความมั่นคงปลอดภัยและสอดคล้องกับนโยบายฉบับนี้ คณะกรรมการ ต้องทบทวนประสิทธิภาพของการให้บริการระบบสารสนเทศ และความมั่นคงปลอดภัย เพื่อวางแผนในการปรับปรุงแก้ไข และพัฒนาระบบให้มีประสิทธิภาพ ทุก ๆ 1 ปี

4. การให้บริการระบบสารสนเทศของสำนักคอมพิวเตอร์

4.1 บริการชื่อผู้ใช้งาน (Username) และรหัสผ่านส่วนตัว (Password) สำหรับการเข้าใช้งานระบบสารสนเทศ

4.2 การเชื่อมต่อผ่านสายสัญญาณ และ ไร้สายเข้าสู่ระบบเครือข่าย

4.3 จัดทำ และให้บริการสื่อการเรียนการสอน (E-Learning)

4.4 บริการสืบค้นข้อมูลผ่านระบบเครือข่ายอินเทอร์เน็ต และอินทราเน็ต

4.5 บริการระบบจดหมายอิเล็กทรอนิกส์

4.6 บริการเครื่องคอมพิวเตอร์แม่ข่ายสำหรับระบบสารสนเทศ

4.7 บริการเว็บไซต์ของมหาวิทยาลัยบูรพา และ ส่วนงานต่าง ๆ

4.8 บริการระบบสารสนเทศภายในและภายนอกมหาวิทยาลัย

4.9 บริการสำรองข้อมูล

4.10 บริการอื่น ๆ ที่ได้รับมอบหมาย

5. ระบบความมั่นคงปลอดภัยของระบบสารสนเทศ ทางกายภาพ และสิ่งแวดล้อม

5.1 สำนักคอมพิวเตอร์มีหน้าที่ดังนี้

5.1.1 จัดทำบัญชีทรัพย์สินระบบสารสนเทศ มีการบริหารจัดการทรัพย์สินอย่างชัดเจน และจัดหมวดหมู่ทรัพย์สินตามระดับความสำคัญ ความลับ คุณค่า เพื่อหาวิธีการบริหารจัดการที่เหมาะสม เพื่อนำข้อมูลของทรัพย์สินไปใช้เพื่อประเมินความเสี่ยงต่าง ๆ

5.1.2 กำหนดให้ ห้องควบคุมระบบ (System Control Room) เป็นบริเวณที่ต้องรักษาความปลอดภัย และจัดให้มีการควบคุมการเข้า-ออก เฉพาะผู้ได้รับอนุญาตเท่านั้น

5.1.3 จัดทำแผนป้องกันอุบัติภัย เช่น ไฟไหม้ น้ำท่วม แผ่นดินไหว หรือหายนะอื่นๆทั้งที่เกิดจากมนุษย์และธรรมชาติ เพื่อสามารถรับมือกับอุบัติภัยที่เกิดขึ้นและกู้คืนระบบให้สามารถกลับมาใช้งานได้ตามเป้าหมายที่กำหนด

5.1.4 ดูแลอุปกรณ์ระบบเครือข่ายที่ใช้งานภายในสำนักคอมพิวเตอร์ เช่นสายไฟ สายสื่อสาร และสายเคเบิลอื่นๆ ต้องได้รับการป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อสายสัญญาณ หรืออุปกรณ์ระบบเครือข่ายนั้น ๆ

5.1.5 เมื่อผู้ใช้งานไม่มีการใช้เครือข่าย ภายใน 30 นาที กำหนดให้เครื่องคอมพิวเตอร์ที่เชื่อมต่อระบบเครือข่ายยุติการเชื่อมต่อโดยอัตโนมัติ

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

5.1.7 ตรวจสอบความเหมาะสมของข้อมูล ที่เผยแพร่ออกสู่สาธารณะ ต้องไม่ขัดต่อกฎหมายที่เกี่ยวข้อง และ กลไกป้องกันการเข้าไปแก้ไขข้อมูลโดยไม่ได้รับอนุญาต

5.2 การควบคุมการนำเข้า และการส่งออก เครื่องคอมพิวเตอร์ และอุปกรณ์สารสนเทศของสำนักคอมพิวเตอร์

5.2.1 การนำฮาร์ดแวร์และซอฟต์แวร์ใหม่ มาติดตั้งใช้งาน จะต้องผ่านตรวจสอบ และหากต้องมีการทดสอบก่อนเชื่อมต่อกับระบบเดิม ห้ามมิให้ใช้ฐานข้อมูลจริง ในการทดสอบ

5.2.2 เครื่องคอมพิวเตอร์ หรือสื่อบันทึกข้อมูล ที่ส่งออกไปภายนอก ผู้ครอบครองต้องตรวจสอบ และป้องกันการนำข้อมูลออกไปพร้อมอุปกรณ์ เพื่อให้มั่นใจได้ว่า ข้อมูลที่สำคัญไม่รั่วไหลสู่ภายนอก

5.2.3 ผู้ครอบครองสื่อบันทึกข้อมูล ต้องตรวจสอบอุปกรณ์ที่มีสื่อบันทึกข้อมูลเพื่อดูว่าข้อมูลสำคัญและซอฟท์แวร์ลิขสิทธิ์ที่เก็บอยู่ในสื่อบันทึกดังกล่าวได้ถูกลบทิ้งหรือเขียนทับ ก่อนจำหน่ายอุปกรณ์ดังกล่าว

5.2.4 ผู้ดูแลระบบ ต้องควบคุมการให้บริการของหน่วยงานภายนอก (Outsource) ที่เกี่ยวข้องกับระบบสารสนเทศ และให้ปฏิบัติตามนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศของสำนักคอมพิวเตอร์

5.2.5 ผู้ดูแลระบบตรวจสอบระบบสารสนเทศใหม่ที่ปรับปรุงเพิ่มเติม หรือติดตั้งใหม่ไม่ให้เกิดผลกระทบต่อระบบสารสนเทศ ก่อนนำระบบนั้นมาติดตั้งใช้งาน

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

5.2.7 ผู้ดูแลระบบต้องสำรองข้อมูลและทดสอบข้อมูลที่เก็บไว้อย่างสม่ำเสมอตามขั้นตอนการปฏิบัติงานเรื่องการสำรองข้อมูล

5.2.8 ผู้ดูแลระบบบริหารจัดการบัญชีผู้ใช้งาน และรหัสผ่าน เพื่อให้ผู้ใช้งานสามารถใช้งานระบบเครือข่ายและระบบสารสนเทศได้ตามสิทธิ์ที่ได้รับ

5.2.9 ผู้ดูแลระบบตรวจสอบ และป้องกันการเข้าถึงพอร์ตที่ใช้ในการตรวจสอบและปรับแต่งระบบ ไม่ว่าจะเป็นจากทางกายภาพหรือผ่านระบบเครือข่าย

5.2.10 ผู้ดูแลระบบจัดเก็บข้อมูลจราจรคอมพิวเตอร์ตาม พรบ.ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

6. การใช้งานจดหมายอิเล็กทรอนิกส์

6.1 ในการส่งข้อมูลที่เกี่ยวข้องกับงาน และข้อมูลที่สำคัญ ต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ที่สำนักคอมพิวเตอร์จัดไว้ให้ในการส่งข้อมูลเท่านั้น เพื่อป้องกันการรั่วไหลของข้อมูล

6.2 จดหมายอิเล็กทรอนิกส์ในกล่องจดหมายจะถูกเก็บไว้บนระบบสำรอง ข้อมูลสูงสุด 90 วัน โดยจดหมายที่ส่งเข้ามายังกล่องจดหมายก่อนวันสำรองข้อมูลประจำสัปดาห์จะสามารถกู้คืนได้หากสูญหาย โดยผู้ใช้งานระบบจดหมายอิเล็กทรอนิกส์ต้องแจ้งให้ผู้ดูแลระบบทราบ

7. ข้อกำหนดการใช้งานระบบเครือข่าย สำหรับผู้ใช้งาน

เพื่อความปลอดภัยของระบบเครือข่าย ผู้ใช้งานจะต้องปฏิบัติดังต่อไปนี้

7.1 ต้องเปลี่ยนรหัสผ่านของตนเองทันที หลังจากได้รับ รหัสผ่านจากผู้ดูแลระบบ โดยการตั้งรหัสผ่านใหม่จะต้องมีความยาวไม่น้อยกว่า 8 อักขระ

7.2 ต้องทำการเปลี่ยนรหัสผ่านของตนเองอย่างน้อยทุก ๆ 180 วัน โดยการตั้งรหัสผ่านใหม่จะต้องมีความยาวไม่น้อยกว่า 8 อักขระ

7.3 ต้องจัดเก็บและรักษารหัสผ่านของตนเองให้เป็นความลับ และไม่สามารถปฏิเสธความรับผิดชอบได้ หากมีผู้อื่นล่วงรู้ข้อมูลอันเป็นความลับนี้ และนำไปใช้งานในทางที่ผิด

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

7.5 รับผิดชอบต่อความเสียหายที่เกิดขึ้น หากผู้ใช้งานนำฮาร์ดแวร์ หรือซอฟต์แวร์มาติดตั้ง เปลี่ยนแปลง ทำซ้ำ หรือต่อเติม กับอุปกรณ์ ที่อยู่ภายในสำนักคอมพิวเตอร์โดยไม่ได้รับอนุญาตจากสำนักคอมพิวเตอร์ หรือไม่มีการติดต่อประสานงาน และขอคำปรึกษาจากผู้ดูแลระบบก่อนติดตั้ง

7.6 รับผิดชอบในการรับ ส่ง หรือจัดเก็บข้อมูลอันเป็นความลับ ภายในระบบเครือข่าย หรือส่งออกไปภายนอกระบบเครือข่าย ทั้งนี้ สามารถขอคำปรึกษา หรือการสนับสนุนจากผู้ดูแลระบบของสำนักคอมพิวเตอร์ เพื่อให้การรับและส่งข้อมูลมีความปลอดภัยมากขึ้นได้

7.7 ห้ามโอนสิทธิ์การใช้งานทรัพย์สินที่ตนเองได้รับสิทธิ์ให้ใช้ แก่บุคคลอื่นยกเว้นได้รับอนุญาตจากผู้อำนวยการ

7.8 ห้ามใช้งานระบบเครือข่าย เพื่อกระทำสิ่งที่ผิดกฎหมาย และผิดไปจากนโยบายด้านความมั่นคงปลอดภัย

7.9 ห้ามใช้ชื่อและรหัสผ่านของผู้ใช้งานคนอื่น โดยไม่ได้รับอนุญาตจากเจ้าของชื่อผู้ใช้งาน และรหัสผ่านนั้น

7.10 ห้ามใช้งานทรัพย์สินหรือบริการที่ไม่ได้มีไว้สำหรับตนเอง และไม่ได้รับอนุญาตจากเจ้าของทรัพย์สินหรือ บริการนั้น ๆ

7.11 ห้ามทำลาย ทำให้เสียหาย แก้ไข เปลี่ยนแปลง ทำซ้ำ หรือเพิ่มเติมข้อมูล และสารสนเทศของผู้อื่นโดยมิชอบ

7.12 ห้ามปลอมแปลงตัวตนในระบบเครือข่าย เสมือนกับเข้าใช้งานในนามผู้อื่น

7.13 ห้ามเผยแพร่ข้อมูล หรือสารสนเทศที่เป็นเท็จ หรือดำเนินการใด ๆ ที่จะส่งผลให้เกิดความเสียหายแก่ผู้อื่นหรือมหาวิทยาลัยบูรพา

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

7.15 ห้ามใช้ทรัพย์สินและบริการในระบบเครือข่าย เพื่อประกอบธุรกิจ

7.16 ห้ามกระทำการอันมีลักษณะ เป็นการละเมิดทรัพย์สินทางปัญญาของผู้อื่น

7.17 ห้ามใช้กรรมวิธีใด ๆ ก็ตามที่ทำให้การสื่อสารข้อมูลเกิดการชะลอตัว หรือ รบกวนจนระบบเครือข่าย หรือทรัพย์สิน หรือบริการอย่างหนึ่งอย่างใดไม่สามารถทำงานได้ตามปกติ

7.18 ห้ามทำลาย หรือพยายามทำลายระบบความมั่นคงปลอดภัยของระบบเครือข่าย

7.19 ห้ามนำฮาร์ดแวร์ หรือซอฟต์แวร์เข้ามาเชื่อมต่อกับระบบเครือข่าย โดยไม่ได้รับอนุญาตจากสำนักคอมพิวเตอร์

7.20 ห้ามลักลอบดักจับข้อมูลในระบบเครือข่าย

8. การเปิดเผยข้อมูล การยกเลิกหรือสิ้นสุดการให้บริการระบบสารสนเทศ

8.1 ผู้อำนวยการ อาจเข้าถึงหรือเปิดเผยข้อมูลการสื่อสารของผู้ใช้งาน เพื่อปฏิบัติตามกฎหมายหรือตอบสนองต่อการเรียกร้องที่ชอบด้วยกฎหมายหรือกระบวนการทางกฎหมาย หรือเพื่อปกป้องสิทธิ์หรือทรัพย์สินของสำนักคอมพิวเตอร์ หรือของผู้ใช้งานอื่น

8.2 ผู้อำนวยการ อาจยกเลิกสิทธิ การเข้าใช้งานระบบเครือข่าย หากผู้ใช้งานมิได้ เข้าใช้งานในระบบเครือข่ายภายในระยะเวลาติดต่อกันเกิน 90 วัน

8.3 ผู้อำนวยการ อาจยกเลิกการให้บริการ หากพบว่าผู้ใช้งานละเมิดข้อตกลงการใช้งาน หรือ ทำให้การให้บริการระบบเครือข่ายขัดข้อง โดยไม่ต้องแจ้งให้ทราบล่วงหน้า

8.4 กรณีผู้ใช้งาน เมื่อพ้นสภาพการเป็นผู้ใช้งาน สำนักคอมพิวเตอร์จะยกเลิกสิทธิการเป็นผู้ใช้งาน

8.5 กรณีผู้ใช้งานเป็นบุคลากรจากภายนอกที่ได้รับสิทธิเข้าใช้งานระบบเครือข่าย เพื่อปฏิบัติงานในส่วนที่รับผิดชอบ จะสิ้นสุดสิทธิการใช้งาน เมื่อจบงานตามสัญญาการทำงาน

8.6 กรณีผู้ใช้งาน ฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยในระบบสารสนเทศ การยกเลิกสิทธ์ผู้ใช้งานขึ้นอยู่กับดุลยพินิจของผู้อำนวยการ

ประกาศ ณ วันที่ 10 กรกฎาคม พ.ศ. 2552

(ลงชื่อ) เสรี ชิโนดม

(นายเสรี ชิโนดม)

ผู้อำนวยการสำนักคอมพิวเตอร์

สำเนาถูกต้อง

เกศแก้ว มนต์วิเศษ

(นางเกศแก้ว มนต์วิเศษ)

เจ้าหน้าที่บริหารงานทั่วไป 8