นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ฉบับ ปี พ.ศ. 2565

งานสารสนเทศ

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

สารบัญ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)
ฉบับปี พ.ศ. 2565

1. บทนำ

สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) จัดตั้งขึ้นตามข้อตกลงความร่วมมือระหว่างรัฐบาลไทยและองค์การสหประชาชาติ โดยพระราชกฤษฎีกาจัดตั้งสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา พ.ศ. 2544 มีภารกิจในการจัดการศึกษาอบรมและให้การสนับสนุนการค้นคว้าวิจัยเพื่อส่งเสริมการค้าระหว่างประเทศและการพัฒนา แก่บุคลากรของประเทศต่าง ๆ โดยเฉพาะภูมิภาคเอเชีย มีบทบาทในการให้ความช่วยเหลือแก่ประเทศกำลังพัฒนา ในการเสริมสร้างศักยภาพและความสามารถในการแสวงประโยชน์จากกระแสโลกาภิวัฒน์และการเปิดเสรีในด้านต่าง ๆ

สถาบันมีระบบสารสนเทศเป็นส่วนประกอบสำคัญในการอำนวยความสะดวกในการดำเนินงานด้านการบริหารจัดการภายในสถาบัน การสื่อสารภายในและภายนอก รวมถึงการเผยแพร่ข่าวสาร ด้านวิชาการ ด้านการฝึกอบรมและให้การสนับสนุนเพื่อการค้นคว้าวิจัยแก่บุคลากรของประเทศต่าง ๆ ในภูมิภาคเอเชีย ด้านการค้าระหว่างประเทศ การเงิน การคลัง การลงทุน การพัฒนา เป็นต้น ซึ่งระบบสารสนเทศจะช่วยให้การเข้าถึงข้อมูล ตลอดจนการติดต่อสื่อสารมีความรวดเร็วและมีประสิทธิภาพ อีกทั้งยังช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของสถาบันที่เชื่อมต่อในระบบอินเทอร์เน็ต เช่น การรับส่งจดหมายอิเล็กทรอนิกส์ การมีเว็บไซต์สำหรับเป็นช่องทางในการประชาสัมพันธ์ข่าวสารต่างๆ ระบบบริหารจัดการสำนักงาน (e-office) ระบบงบประมาณบัญชีการเงิน เป็นต้น อย่างไรก็ตามสถาบัน มีความตระหนักว่าระบบสารสนเทศนั้นมีความเสี่ยงสูง และอาจก่อให้เกิดภัยอันตรายหรือสร้างความเสียหายต่อการปฏิบัติราชการได้เช่นกัน เพราะการใช้งานระบบเทคโนโลยีสารสนเทศเพื่อติดต่อเชื่อมโยงข้อมูลไปยังสถาบันต่าง ๆ รวมถึงการเชื่อมต่อกับอินเทอร์เน็ต ทำให้มีโอกาสถูกบุกรุกได้มากขึ้น ซึ่งอาจก่อให้เกิดอาชญากรรมทางคอมพิวเตอร์ได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับของทางสถาบัน ซึ่งอาจทำให้สถาบันสูญเสียชื่อเสียงและภาพพจน์ของสถาบัน ดังนั้นจึงมีความจำเป็นจะต้องตระหนักถึงการให้การดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัย ด้านสารสนเทศเป็นอย่างยิ่ง

ด้วยเหตุนี้สถาบัน จึงจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

2. วัตถุประสงค์

2.1 เพื่อสร้างความเชื่อมั่นว่าการใช้งานและการสร้างความมั่นคงปลอดภัยของระบบสารสนเทศภายในสถาบันเป็นไปอย่างมีระเบียบแบบแผน และสอดคล้องกับกฎหมายและข้อบังคับที่เกี่ยวข้อง

2.2 เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติและวิธีปฏิบัติ ให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบและบุคคลภายนอกที่ปฏิบัติงานร่วมกับหรือให้กับสถาบัน ตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้ระบบเทคโนโลยีสารสนเทศของสถาบันในการดำเนินงานและปฏิบัติตามอย่างเคร่งครัด

2.3 เพื่อทำการเผยแพร่ให้เจ้าหน้าที่ทุกระดับในสถาบันได้รับทราบ และพนักงานทุกคนจะต้องลงนามยอมรับและปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

3. นิยามศัพท์

3.1 “สถาบัน” หมายถึง สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.2 “หัวหน้าสถาบัน” หมายถึง หัวหน้าสถาบันต่าง ๆ ภายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) เช่น ผู้อำนวยการ รองผู้อำนวยการ เป็นต้น

3.3 “ผู้บังคับบัญชา” หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.4 “ทรัพยากร (Resource)” หมายถึง ฮาร์ดแวร์ ซอฟต์แวร์ และข้อมูลสารสนเทศ ภายใต้การดูแลของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.5 “เครือข่ายคอมพิวเตอร์” หมายถึง เครือข่ายคอมพิวเตอร์ของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.6 “ผู้ดูแลระบบ (System Administrator)” หมายถึง ผู้ซึ่งได้รับมอบหมายให้ทำหน้าที่ดูแลระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์

3.7 “บุคลากร” หมายถึง พนักงานและเจ้าหน้าที่ รวมถึง ลูกจ้าง หรือบุคคลอื่นที่ได้รับมอบหมายให้ปฏิบัติงานตามสัญญาของสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.8 “ฝ่ายเทคโนโลยีสารสนเทศ” หมายถึง กลุ่มงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบ คอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่งโปรแกรม และเครือข่ายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน)

3.9 “ผู้ใช้งานภายใน (Internal User)” หมายถึง บุคลากรภายในสถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) ที่มีบัญชีผู้ใช้งานที่ออกโดยฝ่ายเทคโนโลยีสารสนเทศ หรือ บุคคลหรือสถาบันภายนอกที่ได้รับอนุญาตให้ใช้เครือข่าย

3.10 “ผู้ใช้งานภายนอก (External User)” หมายถึง บุคลากรภายนอกที่สถาบันระหว่างประเทศเพื่อการค้าและการพัฒนา (องค์การมหาชน) อนุญาตให้มีสิทธิในการเข้าถึงเครือข่ายและข้อมูล โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในอำนาจหน้าที่ของตนเอง

3.11 “บัญชีผู้ใช้งาน (User Account)” หมายถึง บัญชีที่ผู้ใช้งานใช้ในการเข้าถึงและใช้งานระบบสารสนเทศ ซึ่งเป็นไปตามข้อตกลงระหว่างผู้ใช้งานกับผู้ให้บริการระบบสารสนเทศ

3.12 “การพิสูจน์ตัวตน” หมายถึง ขั้นตอนการยืนยันความถูกต้องของหลักฐาน (Identity) ที่แสดงว่าเป็นบุคคลที่กล่าวอ้างจริง

3.13 “สิทธิของผู้ใช้งาน” หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

3.14 “แนวทางปฏิบัติ (Guideline)” หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

3.15 “การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตสำหรับบุคคลภายนอก

3.16 “ความมั่นคงปลอดภัยระบบสารสนเทศ” หมายถึง การรักษาไว้ซึ่งความลับ (Confidentiality) ความถูกต้องของข้อมูล (Integrity) และความพร้อมในการใช้งาน (Availability) ของเครือข่าย ระบบ และข้อมูลสารสนเทศ

3.17 “เหตุการณ์ด้านความมั่นคงปลอดภัย” หมายถึง เหตุการณ์ที่แสดงความเป็นไปได้ถึงความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายความมั่นคงปลอดภัยระบบสารสนเทศ หรือเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัย

3.18 “สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสถาบันถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

3.19 “หน้าจอภาพรวม (Desktop)” หมายถึง พื้นที่หน้าจอหลักของระบบคอมพิวเตอร์ที่ปรากฏหลังจากที่เปิดเครื่องคอมพิวเตอร์ เพื่อเข้าสู่ระบบของคอมพิวเตอร์

3.20 “ข้อมูลคอมพิวเตอร์” หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมอิเล็กทรอนิกส์

3.21 “สารสนเทศ (Information)” หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลนำมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่น ๆ

3.22 “ระบบคอมพิวเตอร์” หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

3.23 “ระบบเทคโนโลยีสารสนเทศ (Information Technology System)” หมายถึงระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศ ที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ระบบเครือข่าย โปรแกรม ข้อมูล และสารสนเทศ เป็นต้น

3.24 “สินทรัพย์” หมายถึง ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศ และการสื่อสารของสถาบัน เช่น อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

3.25 “จดหมายอิเล็กทรอนิกส์ หรือ อีเมล (E-mail)” หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคน

3.26 “รหัสผ่าน (Password)” หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบ ยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

ส่วนที่ 1 นโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ
(Access Control Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดมาตรการควบคุมการเข้าถึงและควบคุมการใช้งานสารสนเทศและอุปกรณ์ในการประมวลผล กำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงตามนโยบายที่เกี่ยวข้องกับการกำหนดสิทธิ การอนุญาต หรือการมอบอำนาจของสถาบัน กำหนดกฎเกณฑ์การบริหารประเภทของข้อมูล ลำดับความสำคัญ (ชั้นของความลับ) ระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง ในการใช้งานสารสนเทศของสถาบันได้อย่างเหมาะสมและมีความปลอดภัย

2. แนวทางปฏิบัติในการเข้าถึงและควบคุมการใช้งานสารสนเทศ

2.1 การควบคุมการปลอดภัยทางกายภาพ สิ่งแวดล้อม และการเข้า-ออก สถานที่

2.1.1 สถานที่ตั้งของสถาบัน ต้องมีระบบรักษาความปลอดภัย (Security) ควบคุมการเข้า-ออกที่รัดกุมและอนุญาตให้เฉพาะบุคคลที่ได้รับสิทธิผ่านเข้าออกในสถาบันได้เท่านั้น บุคคลภายนอกที่มาติดต่อภายในสถาบันจะต้องได้รับการบันทึกข้อมูลประวัติ หรือได้รับการอนุญาตใช้พื้นที่ตามช่วงเวลาที่กำหนด

2.1.2 กำหนดให้มีระบบกล้องวงจรปิดบันทึกภาพเคลื่อนไหว เพื่อเฝ้าติดตามเหตุการณ์ ดูแลพื้นที่ส่วนกลาง บริเวณทางเข้าห้องปฏิบัติงาน รวมถึงห้องควบคุมระบบเครือข่าย ห้องเก็บเอกสาร และข้อมูลสำคัญ บริเวณบันไดทางออกฉุกเฉิน หรือบริเวณทางเชื่อมต่อการเข้า-ออกทั้งหมดของสถาบัน นอกจากนี้ระบบยังต้องมีเครื่องบันทึกภาพในส่วนของภาคบันทึก พร้อมกับมีอุปกรณ์สำรองไฟฟ้า (UPS) สำรองติดตั้งกับเครื่องบันทึกข้อมูลภาคบันทึก

2.1.3 ต้องมีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศ และอุปกรณ์ประมวลผลข้อมูลต่างๆ อย่างเหมาะสม โดยจัดทำเป็นเอกสาร หรือแผนผัง “การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ” เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่น ๆ ที่อาจเกิดขึ้นได้

2.1.4 มีการจัดสภาพแวดล้อมทางกายภาพเพื่อป้องกันบุคคลภายนอกบุกรุกเข้าสู่พื้นที่ภายในสถาบัน

2.1.5 ประตูหรือทางเข้าของห้องปฏิบัติงานของบุคลากร ห้องควบคุมระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย ต้องมีระบบที่สามารถล็อคได้ เพื่อป้องกันการบุกรุกทางกายภาพ

2.1.6 บุคลากรที่ปฏิบัติงานภายในสถาบันต้องปิดประตูและหน้าต่างให้ล็อคอยู่เสมอภายหลังเลิกงาน และนอกเวลาราชการ

2.1.7 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

2.1.8 รณรงค์หรือออกกฎให้บุคลากรสถาบันแขวนบัตรพนักงานเพื่อใช้ระบุตัวตนในเวลาที่อยู่ภายในอาคารสถาบัน

2.1.9 เอกสารกระดาษต้องจัดเก็บให้อยู่ห่างจากปลั๊กไฟ หรือบริเวณที่อาจก่อให้เกิดประกายไฟ

2.1.10 ต้องแยกพื้นที่สำหรับระบบเทคโนโลยีสารสนเทศของสถาบันออกจากพื้นที่ที่มีการดูแล หรือบริหารจัดการโดยผู้ให้บริการภายนอก

2.1.11 ต้องจัดให้มีอุปกรณ์ดับเพลิงภายในสถาบัน

2.1.12 ควรจัดพื้นที่หรือบริเวณส่งมอบผลิตภัณฑ์สำหรับบุคคลภายนอก ไว้ในบริเวณต่างหากเพื่อหลีกเลี่ยงการเข้าถึงพื้นที่อื่น ๆ ภายในสถาบัน และต้องตรวจสอบวัสดุหรืออุปกรณ์ที่เป็นอันตรายก่อนที่จะโอนย้ายวัสดุนั้นไปยังพื้นที่ที่มีการใช้งาน

2.1.13 ห้ามไม่ให้มีการนำอาหาร เครื่องดื่ม และสูบบุหรี่ในบริเวณหรือพื้นที่ห้องควบคุมระบบเครือข่าย ระบบคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์แม่ข่าย

2.1.14 ต้องจัดวางอุปกรณ์ในพื้นที่หรือบริเวณที่เหมาะสม ไม่ให้เกิดความเสี่ยงทางกายภาพ เพื่อความสะดวก และความปลอดภัยต่อการเข้าปฏิบัติงานของบุคลากร

2.1.15 ดำเนินการตรวจสอบ สอดส่อง ระดับอุณหภูมิ และดูแลสภาพแวดล้อมภายในบริเวณห้องควบคุมระบบเครือข่าย ระบบคอมพิวเตอร์ ระบบเครื่องคอมพิวเตอร์แม่ข่ายอย่างสม่ำเสมอเพื่อป้องกันความเสียหายต่ออุปกรณ์ที่อยู่ในบริเวณดังกล่าว

2.1.16 มีมาตรการป้องกันอุปกรณ์ไฟฟ้าเสียหายจากการที่กระแสไฟฟ้าไม่แน่นอน หรือไฟฟ้ากระชากอันจะทำให้ระบบสารสนเทศ ข้อมูลสารสนเทศ และอุปกรณ์ไฟฟ้าเกิดความเสียหาย โดยให้มีการติดตั้งระบบสำรองไฟฟ้า (UPS) และต้องทดสอบระบบอย่างสม่ำเสมอ โดยทดสอบให้ตรงตามคำแนะนำที่ผู้ผลิตได้ระบุไว้

2.2 ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control)

2.2.1 มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

2.2.2 ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของสถาบัน

2.2.3 ต้องกำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2.3 การควบคุม และการอนุญาตให้เข้าถึงระบบ

2.3.1 ผู้ดูแลระบบ ต้องกำหนดสิทธิการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอทุก 6 เดือน เป็นอย่างน้อย ทั้งนี้ ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบตามความจำเป็นในการใช้งาน

2.3.2 ผู้ดูแลระบบ หรือผู้ที่ได้รับมอบหมายเท่านั้นที่สามารถแก้ไขเปลี่ยนแปลงสิทธิการเข้าถึงข้อมูล และระบบสารสนเทศได้

2.3.3 ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน และตรวจตราการละเมิดความปลอดภัย ที่มีต่อระบบสารสนเทศที่สำคัญ

2.3.4 ผู้ดูแลระบบ ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

2.4 ข้อมูล ลำดับชั้นความลับของข้อมูล เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

2.4.1 ประเภทข้อมูลของสถาบันแบ่งได้ดังนี้

2.4.1.1 ข้อมูลสารสนเทศด้านการบริหาร ได้แก่

1) ข้อมูลที่เกี่ยวข้องกับคณะกรรมการและอนุกรรมการ
2) ข้อมูลที่เกี่ยวข้องกับสำนักบริหาร
3) ข้อมูลที่เกี่ยวข้องกับสำนักผู้อำนวยการ
4) ข้อมูลที่เกี่ยวข้องกับสำนักยุทธศาสตร์และสารสนเทศ

2.4.1.2 ข้อมูลสารสนเทศด้านวิชาการ ได้แก่

1) ข้อมูลที่เกี่ยวข้องกับสำนักพัฒนาขีดความสามารถทางการค้าและการพัฒนา
2) ข้อมูลที่เกี่ยวข้องกับสำนักความร่วมมือระหว่างประเทศ
3) ข้อมูลที่เกี่ยวข้องกับสำนักพัฒนาและส่งเสริมการวิจัย

2.4.2 ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ.2544 ซึ่งระเบียบ ดังกล่าวเป็นมาตรการที่ละเอียด รอบคอบ ถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์ และในการรักษาความปลอดภัย ของเอกสารอิเล็กทรอนิกส์ โดยได้กำหนดกระบวนการ และกรรมวิธีต่อเอกสารที่สำคัญไว้ โดยการกำหนดชั้นความลับตามความสำคัญของข้อมูลในเอกสาร กำหนดไว้ 3 ระดับ ได้แก่ ลับ ลับมากลับที่สุด และมีการกำหนดความรับผิดชอบ ให้แก่ผู้มีอำนาจกำหนดชั้นความลับ เป็นผู้พิจารณากำหนดระดับชั้นความลับของเอกสาร และการยกเลิกหรือปรับระดับชั้นความลับของเอกสารตามความจำเป็น

2.4.3 ระดับชั้นการเข้าถึงกำหนดให้มีมาตรการควบคุมต่าง ๆ เช่น ข้อมูลที่ไม่เป็น สาธารณะ ข้อมูลลับ ข้อมูลสำคัญ ข้อมูลใช้เฉพาะภายในการบริหารงานในสถาบัน ตามลำดับของสารสนเทศ แต่ละประเภท ดังนี้

2.4.3.1 ข้อมูลสารสนเทศประเภทเอกสาร ต้องมีการกำหนดสิทธิและระดับการเข้าถึงข้อมูลให้เหมาะสมกับผู้ใช้และหน้าที่รับผิดชอบ บุคคลอื่นที่ต้องการเข้าถึงข้อมูลสารสนเทศดังกล่าวนี้ จะต้องมีการทำหนังสือขออนุญาตใช้ข้อมูลผ่านผู้บังคับบัญชาที่เกี่ยวข้องตามลำดับ

2.4.3.2 ข้อมูลสารสนเทศอิเล็กทรอนิกส์ ต้องมีการกำหนดสิทธิและระดับการเข้าถึงข้อมูลและระบบสารสนเทศให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบทั้งนี้ผู้ใช้งานจะต้องได้รับอนุญาตจากผู้ดูแลระบบ ตามความจำเป็นในการใช้งาน บุคคลอื่นที่ต้องการเข้าถึงข้อมูลสารสนเทศดังกล่าวนี้ จะต้องมีการทำหนังสือขออนุญาตใช้ข้อมูลผ่านผู้บังคับบัญชาที่เกี่ยวข้องตามลำดับ

2.4.4 เวลาที่ได้เข้าถึง

2.4.4.1 การเข้าถึงสารสนเทศของสถาบันในเวลาทำการปกติ จันทร์-ศุกร์ เวลา 09.00–17.00 น.)

2.4.4.2 การเข้าถึงในช่วงเวลาพิเศษเป็นรายครั้ง ต้องระบุช่วงเวลาและจำนวนระยะเวลาการเข้าถึง และต้องรับอนุญาตจากผู้บริหารสถาบันก่อน

2.4.5 ช่องทางการเข้าถึง

2.4.5.1 ติดต่อด้วยตนเอง (เข้าถึงได้ในวันจันทร์-ศุกร์ เวลา 09.00–17.00 น.)

2.4.5.2 เคาน์เตอร์บริการ (เข้าถึงได้ในวันจันทร์-ศุกร์ เวลา 09.00–17.00 น.)

2.4.5.3 โทรศัพท์หรือโทรสาร (เข้าถึงได้ในวันจันทร์-ศุกร์ เวลา 09.00–17.00 น.)

2.4.5.4 หนังสือหรือบันทึกข้อความ (เข้าถึงได้ในวันจันทร์-ศุกร์ เวลา 09.00–17.00 น.)

2.4.5.5 ระบบแลน (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

2.4.5.6 ระบบอินทราเน็ต (เข้าถึงได้ทั้งในและนอกเวลาราชการ)

2.4.5.7 ระบบอินเทอร์เน็ต (เข้าถึงได้ทุกช่วงเวลา)

2.4.5.8 ระบบจดหมายอิเล็กทรอนิกส์ (เข้าถึงได้ทุกช่วงเวลา)

2.4.5.9 เว็บไซต์ (เข้าถึงได้ทุกช่วงเวลา หรือ ในช่วงเวลาพิเศษที่กำหนด)

2.4.5.10 การประชุมทางไกล (เข้าถึงได้ในเวลาราชการ หรือ ในช่วงเวลาพิเศษเป็นรายครั้ง)

2.5 การใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

2.5.1 มีการควบคุมการเข้าถึงสารสนเทศ โดยจัดทำข้อปฏิบัติสำหรับการควบคุมการเข้าถึงสารสนเทศ (อ้างถึง 2.2 ข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ)

2.5.2 มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย โดยกำหนดสิทธิที่เกี่ยวข้องกับระบบสารสนเทศ ควบคุม และตรวจสอบการเข้าถึงข้อมูลที่มีความลับในลำดับชั้นต่าง ๆ ตามที่ได้รับอนุญาต

2.6 การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

2.6.1 สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัย และผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือ รู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

2.6.2 การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

2.6.3 การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุม และจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

2.6.4 การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

2.6.5 การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

2.7 การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clean Desk and Clear Screen Policy) สำหรับบุคลากร

2.7.1 ต้องมีการจัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย เช่น ในตู้เอกสารที่มีกุญแจล็อค และไม่ทิ้งเอกสารที่สำคัญไว้บนโต๊ะ เพื่อความปลอดภัยของทรัพย์สินของสถาบัน

2.7.2 ต้องไม่เก็บบันทึกไฟล์ข้อมูลสำคัญไว้บนหน้าจอภาพรวม (Desktop) ของคอมพิวเตอร์ หากมีความจำเป็นต้องบันทึกไว้บนหน้าจอรวมดังกล่าว จะต้องทำการสำรองข้อมูลเก็บไว้ในฮาร์ดดิสก์อื่นที่มีความปลอดภัย

2.7.3 ต้องไม่บันทึก หรือแสดง ชื่อผู้ใช้งาน หรือรหัสผ่าน หรือข้อมูลที่แสดงถึงวิธีการเข้าถึงการใช้งานสารสนเทศ เครื่องคอมพิวเตอร์ ระบบสารสนเทศ และอุปกรณ์ในการประมวลผล

2.7.4 ต้องป้องกันเครื่องโทรสาร เมื่อไม่มีผู้ใช้งาน และป้องกันตู้หรือบริเวณที่ใช้ในการรับ-ส่งเอกสารไปรษณีย์ เพื่อความปลอดภัยของข้อมูล

2.7.5 ห้ามผู้ที่ไม่ได้รับอนุญาตใช้อุปกรณ์ต่าง ๆ ของสถาบัน เช่น เครื่องคอมพิวเตอร์ กล้องดิจิตอล เครื่องพิมพ์ เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น

2.7.6 นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

2.7.7 ต้องทำการทำลายข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการเปลี่ยนหรือทดแทนอุปกรณ์

2.7.8 ต้องทำการทำลายข้อมูลที่บันทึกอยู่ในอุปกรณ์ฮาร์ดดิสก์หรือสื่อบันทึกข้อมูลก่อนทำการทำลายหรือจำหน่าย โดยมีวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	**วิธีทำลาย**
กระดาษ	ใช้วิธีการหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้วิธีการหักหรือหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหมสหรัฐอเมริกา DOD 5220.33-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็น จำนวนหลายรอบ)

2.7.9 ต้องลบข้อมูลออกจากฐานข้อมูลที่มีอายุตั้งแต่ 5 ปีขึ้นไป และสำรองข้อมูลลงฮาร์ดดิสก์ภายนอก (External Hard Disk) หรือสื่อข้อมูลสำรอง (Backup Media) และจัดเก็บไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล

2.7.10 ต้องได้รับความเห็นชอบจากผู้บังคับบัญชาในการทำลายสื่อบันทึกข้อมูล หรือลบข้อมูลอิเล็กทรอนิกส์ออกจากฐานข้อมูล

2.7.11 โปรแกรมประยุกต์ที่ใช้ในสถาบันต้องเป็นโปรแกรมที่มีลิขสิทธิ์ถูกต้อง

ส่วนที่ 2 นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ (Security Awareness Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อเผยแพร่แนวนโยบายและแนวปฏิบัติให้กับบุคลากรในสถาบัน และบุคคลที่เกี่ยวข้องกับสถาบัน ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

2. แนวทางปฏิบัติในการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศ

2.1 จัดให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อย 1 ครั้ง ในระยะเวลา 5 ปี

2.2 ฝ่ายเทคโนโลยีสารสนเทศต้องจัดฝึกอบรมแนวปฏิบัติตามแนวนโยบายอย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามแนวนโยบายเข้ากับหลักสูตรอบรมต่าง ๆ ตามแผนการฝึกอบรมของสถาบันที่มีอยู่แล้ว

2.3 ฝ่ายเทคโนโลยีสารสนเทศต้องติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อควรระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ เพื่อสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยระบบสารสนเทศให้แก่บุคลากรในสถาบัน

ส่วนที่ 3 นโยบายการบริหารจัดการรหัสผ่าน
(Password Management Policy)

1. **วัตถุประสงค์ของนโยบาย**

เพื่อให้ผู้ใช้งานได้มีแนวทางปฏิบัติที่มีความมั่นคงปลอดภัยเกี่ยวกับการใช้รหัสผ่าน เพื่อการระบุตัวตน และสร้างความปลอดภัยจากบุคคลที่ไม่ได้รับอนุญาตเข้ามาล่วงรู้รหัสผ่าน อันส่งผลกระทบต่อความมั่นคงปลอดภัยต่อระบบเทคโนโลยีสารสนเทศของสถาบัน

2. แนวปฏิบัติในการบริหารจัดการรหัสผ่าน

2.1 ผู้ใช้งานภายในและผู้ใช้งานภายนอกต้องลงทะเบียนบัญชีผู้ใช้ เพื่อขอใช้งานรหัสผ่าน โดยต้องทำการกรอกข้อมูลคำร้องขอใช้งานของสถาบัน โดยยื่นคำขอกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

2.2 ผู้ใช้งานภายในและผู้ใช้งานภายนอกต้องลงนามยินยอมในสัญญาเรื่องการเก็บรักษารหัสผ่านไว้เป็นความลับ ซึ่งข้อความดังกล่าวรวมอยู่ในเงื่อนไขในเอกสารคำร้องขอใช้งานแล้ว

2.3 สำหรับผู้ใช้งานรายใหม่จะได้รับรหัสผ่านครั้งแรก (Default Password) และเมื่อมีการเข้าสู่ระบบใด ๆ ในครั้งแรกนั้น ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

2.4 การกำหนดรหัสผ่าน ผู้ใช้งานภายในและผู้ใช้งานภายนอกต้องดำเนินการ ดังนี้

2.4.1 การกำหนดรหัสผ่านต้องไม่ใช้คำศัพท์ที่มาจากพจนานุกรม ชื่อผู้ใช้งาน ชื่อหนัง หรือชื่อสถานที่ และต้องไม่ใช้ข้อมูลที่เกี่ยวข้องกับสถาบัน หรือเป็นข้อมูลส่วนตัวของผู้ใช้งานซึ่งอาจง่ายแก่การคาดเดา เช่น รหัสประจำตัวเจ้าหน้าที่ หมายเลขโทรศัพท์ วันเกิด หรือ ชื่อบุคคลในครอบครัว เป็นต้น

2.4.2 ต้องไม่กำหนดรหัสผ่านที่ประกอบด้วยตัวอักษรหรือตัวเลขที่เรียงซ้ำกันเกินกว่า 3 ตัว หรือเรียงกัน ตามลำดับ เช่น aaaabbbb, 11111111, abcdefg หรือ 123456 เป็นต้น

2.4.3 รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร

2.4.4 รหัสผ่านต้องมีส่วนประกอบของตัวอักษร ตัวเลข และอักขระพิเศษ ผสมกัน ดังนี้

2.4.4.1 ตัวอักษรพิมพ์ใหญ่ เช่น A, B, C, D, ...

2.4.4.2 ตัวอักษรพิมพ์เล็ก เช่น a, b, c, d, ...

2.4.4.3 ตัวเลข เช่น 0, 1, 2, 3, ...

2.4.4.4 อักขระพิเศษ เช่น !, @, #, $, ...

2.5 ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่าน อย่างน้อยทุก 90 วัน

2.6 ผู้ใช้งานภายในและผู้ใช้งานภายนอกต้องเปลี่ยนรหัสผ่าน อย่างน้อยทุก 180 วัน

2.7 ระบบสารสนเทศของสถาบันต้องมีการแนะนำผู้ใช้งานในการกำหนดรหัสผ่านที่มีคุณภาพ เช่น รหัสผ่านที่ผู้ใช้งานกำหนดนั้นอยู่ในระดับอ่อน ปานกลาง หรือแข็งแกร่ง เป็นต้น

2.8 เวลาป้อนรหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญญาลักษณ์แทนตัวอักษรนั้น เช่น ‘X’หรือ ‘O’ ในการพิมพ์แต่ละอักษร

2.9 ต้องไม่ส่งรหัสผ่านบนระบบเครือข่าย ต้องดำเนินการรักษาความลับให้รหัสผ่านก่อนส่งรหัสผ่านระบบเครือข่าย

2.10 ผู้ใช้งานภายในและผู้ใช้งานภายนอก ต้องไม่เก็บรหัสผ่านไว้ในเครื่องคอมพิวเตอร์ในรูปแบบที่สามารถอ่านได้ หรือไม่ควรเก็บรักษารหัสผ่านไว้ในที่ที่บุคคลอื่นสามารถเห็นหรือเข้าถึงได้ง่าย เช่น บนเครื่องคอมพิวเตอร์ บนโต๊ะทำงาน เป็นต้น และต้องเก็บข้อมูลรหัสผ่านไว้ต่างหากจากข้อมูลอื่น

2.11 หากมีเหตุที่น่าเชื่อถือได้ว่ามีการเปิดเผยรหัสผ่าน ผู้ใช้งานต้องรายงานเหตุการณ์ไปยังผู้ดูแลระบบหรือเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ และให้ดำเนินการเปลี่ยนรหัสผ่านทันที

2.12 ถ้าพบว่ารหัสผ่านของตนถูกล็อคโดยไม่ทราบสาเหตุ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบหรือเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศทราบ

2.13 รหัสผ่านของผู้ใช้งานภายในที่ลาออก หรือผู้ใช้งานภายนอกที่สิ้นสุดการจ้างงานหรือย้ายงาน ต้องทำการยกเลิกสิทธิของผู้ใช้งานในระบบภายใน 30 วัน

ส่วนที่ 4 นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่าย
(Network Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อให้มีการกำหนดมาตรฐานและการควบคุมการเข้าถึงเครือข่าย โดยการกำหนดผู้ใช้งานภายใน และผู้ใช้งานภายนอก รวมถึงสิทธิของผู้ใช้งานภายในและผู้ใช้งานภายนอก ซึ่งผู้ใช้งานทุกประเภทจะต้องผ่านการยืนยันหรือการพิสูจน์ตัวตนก่อนที่จะสามารถเข้าถึงและใช้งานระบบเครือข่ายได้ นอกจากนั้น นโยบายนี้ยังจะใช้ในการกำหนดแนวทางการดูแลอุปกรณ์เครือข่าย ควบคุมการออกแบบ การเชื่อมต่อ และเส้นทางการเดินทางของข้อมูลบนเครือข่ายด้วย

2. แนวปฏิบัติในการควบคุมการเข้าถึงเครือข่าย

2.1 การรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย (Server)

2.1.1 ให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศของสถาบัน ทำการกำหนดผู้ใช้งานภายในที่มีสิทธิเข้าถึงระบบคอมพิวเตอร์แม่ข่าย หรือผู้ดูแลระบบ ให้มีสิทธิสำหรับการดูแลระบบคอมพิวเตอร์แม่ข่ายเท่านั้น ผู้ใช้งานอื่น ๆ ให้ผู้ดูแลระบบกำหนดให้สามารถเข้าถึงบริการหรือข้อมูลสารสนเทศที่แต่ละบุคคลได้รับอนุญาตเท่านั้น

2.1.2 บุคคลที่นอกเหนือจากข้อ 2.1.1 ต้องไม่มีสิทธิเข้าถึงระบบคอมพิวเตอร์แม่ข่ายเพื่อทำการเปลี่ยนแปลงค่า (Configure) ต่าง ๆ หรือดูแลระบบคอมพิวเตอร์แม่ข่ายโดยเด็ดขาด

2.1.3 ต้องมีขั้นตอนหรือวิธีปฏิบัติสำหรับผู้ดูแลระบบในการตรวจสอบการรักษาความปลอดภัยระบบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าต่าง ๆ ในลักษณะที่ผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งมีการรายงานต่อผู้บังคับบัญชาโดยทันที

2.1.4 ผู้ดูแลระบบต้องเปิดใช้บริการ (Service) หรือพอร์ท (Port) เท่าที่จำเป็น ทั้งนี้หากบริการหรือพอร์ทที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัย ฝ่ายเทคโนโลยีสารสนเทศจำเป็นต้องมีมาตรการป้องกันเพิ่มเติม

2.1.5 ผู้ดูแลระบบต้องดำเนินการติดตั้งซอฟต์แวร์ปรับปรุง (Patch) ที่จำเป็นของระบบงานสำคัญเพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบ (System Software) บนระบบคอมพิวเตอร์แม่ข่าย อย่างสม่ำเสมอ

2.2 การบริหารจัดการและการตรวจสอบเครือข่าย

2.2.1 ต้องมีการแบ่งแยกเครือข่าย (Network Segmentation) ให้เป็นสัดส่วนตามการใช้งานเป็นเครือข่ายภายนอกสถาบัน และเครือข่ายภายในสถาบัน เช่น เครือข่ายของฝ่ายบริหาร ที่รวมสำนักผู้อำนวยการ สำนักยุทธศาสตร์และสารสนเทศ และเครือข่ายของฝ่ายวิชาการที่รวมสำนักพัฒนาขีดความสามารถทางการค้าและการพัฒนา สำนักความร่วมมือระหว่างประเทศและสำนักพัฒนาและส่งเสริมการวิจัย เป็นต้น ทั้งนี้ต้องมีการควบคุมดูแล โดยวิธีต่อไปนี้

2.2.1.1 ผู้ดูแลระบบต้องควบคุมไม่ให้มีการเปิดเผยแผนการใช้หมายเลขเครือข่าย (IP Address) ต่อบุคคลภายนอกสถาบัน และบุคคลภายในสถาบันที่ไม่มีสิทธิ

2.2.1.2 ผู้ดูแลระบบต้องกำหนดให้มีการแบ่งการใช้หมายเลขเครือข่าย (IP Address) สำหรับการแบ่งเครือข่ายย่อย (Sub-Network)

2.2.1.3 ผู้ดูแลระบบต้องกำหนดมาตรการการบังคับและควบคุมการใช้เส้นทางเครือข่าย (Network Routing Control) เพื่อให้สามารถเชื่อมเครือข่ายภายนอกสถาบันผ่านช่องทางที่กำหนดไว้

2.2.2 ต้องมีการควบคุมการเชื่อมต่อระหว่างเครือข่ายภายนอกสถาบันและภายในสถาบัน และควบคุมการเข้าถึงเครือข่ายภายในสถาบัน อย่างน้อยโดยวิธีต่อไปนี้

2.2.2.1 ต้องมีระบบป้องกันการบุกรุก เช่น กำแพงไฟ (Firewall) ระหว่างเครือข่ายภายในสถาบัน และเครือข่ายภายนอกสถาบัน

2.2.2.2 ต้องมีระบบตรวจสอบการบุกรุกและการใช้งานในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยใช้ระบบตรวจจับการบุกรุก (Intrusion Detection System) หรือโดยวิธีการตรวจสอบการบุกรุกผ่านเครือข่าย การตรวจสอบการใช้งานที่ผิดปกติ และการตรวจสอบการแก้ไขเปลี่ยนแปลงค่าในเครือข่ายโดยผู้ไม่มีสิทธิ

2.2.3 ผู้ดูแลระบบ และฝ่ายเทคโนโลยีสารสนเทศต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่ายภายในสถาบันและเครือข่ายภายนอกสถาบัน รวมถึงการระบุอุปกรณ์ต่าง ๆ บนเครือข่าย เช่น อุปกรณ์กระจายสัญญาณข้อมูล (Switch) หรือ อุปกรณ์จัดเส้นทาง (Router) พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

2.2.4 ผู้ดูแลระบบต้องตรวจสอบเกี่ยวกับความปลอดภัยของอุปกรณ์คอมพิวเตอร์ก่อนเชื่อมต่อกับเครือข่ายภายในสถาบัน เช่น ตรวจสอบไวรัส ตรวจสอบการกำหนดค่า Parameter ต่าง ๆ เกี่ยวกับการรักษาความปลอดภัย เป็นต้น และต้องตัดการเชื่อมต่อเครื่องคอมพิวเตอร์ (Physical Disconnect) และจุดเชื่อมต่อการให้บริการ (Disable Port) ที่ไม่มีความจำเป็นต้องเชื่อมต่อกับเครือข่ายภายในสถาบัน ออกจากเครือข่ายโดยสิ้นเชิง

2.2.5 ต้องกำหนดบุคคลรับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของเครือข่ายภายในสถาบัน และอุปกรณ์ต่าง ๆ ที่เชื่อมต่อกับเครือข่ายอย่างชัดเจน และต้องมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละหนึ่งครั้ง นอกจากนี้ หากมีการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ก็ควรแจ้งบุคคลหรือผู้ใช้งานที่เกี่ยวข้องให้รับทราบทุกครั้ง

2.2.6 การใช้เครื่องมือต่าง ๆ (Tools) เพื่อตรวจสอบเครือข่ายภายในสถาบัน ต้องได้รับการอนุมัติจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

2.2.7 ผู้ดูแลระบบและฝ่ายเทคโนโลยีสารสนเทศ ต้องกำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่าย และเครือข่าย เพื่อทำการบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ (Log-in Log-out Logs) บันทึกการพยายามเข้าสู่ระบบ (Login Attempts) เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน

2.2.8 ผู้ใช้งานภายนอกที่จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และเครือข่ายของสถาบัน ต้องได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

2.2.9 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลางของสถาบัน ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับเครือข่ายของสถาบันโดยไม่ได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ

2.3 การยืนยันหรือการพิสูจน์ตัวบุคคลสำหรับผู้ใช้งานภายใน

2.3.1 ผู้ใช้งานภายในที่จะเข้าใช้งานเครือข่ายภายในสถาบัน ต้องทำการระบุตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

2.3.2 ต้องมีการตรวจสอบผู้ใช้งานภายในทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงเครือข่ายภายในสถาบัน ซึ่งจะต้องมีวิธีการยืนยันหรือการพิสูจน์ตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริงอย่างน้อยโดยการใช้รหัสผ่าน (Password)

2.4 ข้อปฏิบัติสำหรับผู้ติดต่อจากหน่วยงานภายนอก

2.4.1 ผู้ติดต่อจากหน่วยงานภายนอกทุกคน ต้องทำการลงบันทึกข้อมูลในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์

2.4.2 เจ้าหน้าที่ต้องตรวจสอบความถูกต้องของข้อมูลที่บันทึกในเอกสารแบบฟอร์มการเข้า - ออกห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสถาบัน เป็นประจำทุกเดือน

2.4.3 ผู้ใช้งานที่จะเข้าใช้งานระบบต้องแสดงตัวตน (Identification) ด้วยชื่อผู้ใช้งาน (Username) ทุกครั้ง

2.4.4 ในกรณีที่ผู้ใช้งานต้องการเข้าถึงเครือข่ายจากภายนอกสถาบัน โดยต้องการสิทธิ์ในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสถาบันจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศ ในการเข้าสู่ระบบเครือข่ายจะต้องเชื่อมผ่านด้วยวิธีการ Remote Access VPN หรือ FTP โดยผู้ใช้งานจะต้องพิสูจน์ยืนยันตัวตน (Authentication) ด้วยการป้อนชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อยืนยันตัวตนของผู้ใช้งานในการเข้าถึงเครือข่ายในส่วนที่ได้รับอนุญาต

2.4.5 มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง เช่น การใช้รหัสผ่าน (Password) เป็นต้น

2.4.6 ตรวจสอบผู้ใช้งานเมื่อมีการเข้าสู่ระบบสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

ส่วนที่ 5 นโยบายการรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย
(Wireless Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดมาตรฐานการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN) โดยการกำหนดสิทธิของผู้ใช้ในการเข้าถึงระบบให้เหมาะสมตามหน้าที่ความรับผิดชอบในการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ ทั้งนี้ ผู้ใช้ระบบต้องผ่านการพิสูจน์ตัวตนจริงจากระบบ ว่าได้รับอนุญาตจากผู้ดูแลระบบ เพื่อสร้างความมั่นคงปลอดภัยของการใช้งานระบบเครือข่ายไร้สาย

2. แนวปฏิบัติในการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

2.1 การติดตั้งระบบเครือข่ายไร้สาย (Wireless) ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

2.2 ห้ามผู้ใช้งานภายใน และผู้ใช้งานภายนอก นำอุปกรณ์ Wireless มาติดตั้ง หรือ เปิดใช้งานเองในสถาบัน ไม่ว่าจะเป็น Access point, Wireless Router, Wireless USB Client หรือ Wireless Card โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา

2.3 ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายของสถาบัน จะต้องทำการลงทะเบียนกับผู้ดูแลระบบและต้องได้รับพิจารณาอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศอย่างเป็นลายลักษณ์อักษร

2.4 ผู้ดูแลระบบต้องทำการลงทะเบียนกำหนดสิทธิผู้ใช้งานภายใน และผู้ใช้งานภายนอกในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงาน ก่อนเข้าใช้ระบบเครือข่ายไร้สาย รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

2.5 ผู้ดูแลระบบต้องทำการลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

2.6 ผู้ดูแลระบบต้องกำหนดตำแหน่งการวางอุปกรณ์ Access Point (AP) ให้เหมาะสม เพื่อเป็นการควบคุมไม่ให้สัญญาณของอุปกรณ์กระจายออกไปนอกบริเวณที่ใช้งาน และเพื่อป้องกันไม่ให้ผู้โจมตีสามารถรับส่งสัญญาณจากภายนอกอาคาร หรือบริเวณขอบเขตที่ควบคุมได้

2.7 ผู้ดูแลระบบต้องทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าดีฟอลต์ (Default) มาจากผู้ผลิตทันทีที่นำ Access Point มาใช้งาน

2.8 ผู้ดูแลระบบต้องกำหนด ชื่อล็อกอินและรหัสผ่านสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย และผู้ดูแลระบบต้องเลือกใช้ชื่อล็อกอินและรหัสผ่านที่มีความคาดเดาได้ยากเพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสได้โดยง่าย

2.9 ผู้ดูแลระบบต้องกำหนดค่าให้ WEP หรือ WPA ในการเข้ารหัสข้อมูลระหว่าง Access Point และ Wireless LAN Client เพื่อให้ยากต่อการดักจับ จะช่วยให้ปลอดภัยมากยิ่งขึ้น

2.10 ผู้ดูแลระบบควรเลือกใช้วิธีการควบคุม MAC Address และชื่อผู้ใช้งาน (Username) รหัสผ่าน (Password) ของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address ชื่อผู้ใช้งานและรหัสผ่าน ตามที่กำหนดไว้เท่านั้นให้เข้าใช้เครือข่ายไร้สายได้

2.11 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผล

การตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้หัวหน้าฝ่ายเทคโนโลยีสารสนเทศทราบทันที

ส่วนที่ 6 นโยบายการรักษาความมั่นคงปลอดภัยของจดหมายอิเล็กทรอนิกส์
(E-mail Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน ซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ ไม่ละเมิดสิทธิกระทำการใด ๆ ที่จะสร้างปัญหาหรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์

2.1 ในการลงทะเบียนบัญชีผู้ใช้บริการจดหมายอิเล็กทรอนิกส์ (e-mail) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของสถาบัน โดยยื่นคำขอกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ

2.2 สำหรับผู้ใช้รายใหม่จะได้รับรหัสผ่านตั้งต้นในการเข้าจดหมายอิเล็กทรอนิกส์ และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้น ให้ทำการเปลี่ยนรหัสผ่านโดยทันที

2.3 ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

2.4 ควรเปลี่ยนรหัสผ่านทุก 60 วัน

2.5 รหัสผ่านจดหมายอิเล็กทรอนิกส์ เวลาป้อนรหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมา แต่ต้องแสดงออกมาในรูปแบบของสัญลักษณ์แทนตัวอักษรนั้น เช่น ‘X’หรือ ‘O’ ในการพิมพ์แต่ละอักษร

2.6 ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ไม่เกิน 3 ครั้ง

2.7 ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้บริการและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ของตน

2.8 การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของสถาบันผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของสถาบันเท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของสถาบันขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

2.9 ผู้ใช้งานควรระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์ เพื่อไม่ให้เกิดความเสียหายต่อสถาบันหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรม และไม่แสวงหาประโยชน์หรืออนุญาตให้ผู้อื่นแสวงหาผลประโยชน์ในเชิงธุรกิจจากการใช้งานจดหมายอิเล็กทรอนิกส์ผ่านระบบเครือข่ายของสถาบัน

2.10 การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของสถาบัน

2.11 หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ควรทำการออกจากระบบทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

2.12 ผู้ใช้งาน ควรทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ก่อนทำการเปิด เพื่อทำการตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัส เป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

2.13 ผู้ใช้งานไม่ควรเปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์หรือข้อความที่ได้รับจากผู้ส่งที่ไม่รู้จัก

2.14 ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

2.15 ห้ามไม่ให้ผู้ใช้งานนำบัญชีจดหมายอิเล็กทรอนิกส์ (E-mail Address) ซึ่งเป็นของสถาบัน ไปเผยแพร่สู่บุคคลอื่น ไม่ว่าจะเป็นทางใดก็ตาม เช่น การโพสต์ในเว็บบอร์ดในชุดคำถาม หรือแบบสอบถามจากผู้ค้า เป็นต้น เว้นแต่การเผยแพร่นั้นเป็นไปเพื่อผลประโยชน์ต่อสถาบันหรือได้รับอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

2.16 ผู้ใช้งานควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ของตนเองทุกวัน และควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ของตนให้เหลือจำนวนน้อยที่สุด

2.17 ผู้ใช้งานควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์

2.18 ผู้ใช้งาน ควรโอนย้ายจดหมายอิเล็กทรอนิกส์ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตน เพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้นไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์

2.19 ผู้ดูแลระบบจะปิดสิทธิ์การใช้งานภายใน 7 วัน และดำเนินการลบจดหมายอิเล็กทรอนิกส์ ภายใน 60 วัน หลังจากผู้ใช้งานจดหมายอิเล็กทรอนิกส์ พ้นสภาพจากการเป็นเจ้าหน้าที่ของสถาบัน

ส่วนที่ 7 นโยบายการรักษาความมั่นคงปลอดภัยของอินเทอร์เน็ต
(Internet Security Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดมาตรการการใช้งานอินเทอร์เน็ตของสถาบันซึ่งผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้งานอินเทอร์เน็ต ผู้ใช้จะต้องเข้าใจกฎเกณฑ์ต่าง ๆ ที่ผู้ดูแลระบบเครือข่ายวางไว้ไม่ละเมิดสิทธิกระทำการใด ๆ ที่จะสร้างปัญหา หรือไม่เคารพกฎเกณฑ์ที่วางไว้ และจะต้องปฏิบัติตามคำแนะนำของผู้ดูแลระบบเครือข่ายนั้นอย่างเคร่งครัด จะทำให้การใช้งานอินเทอร์เน็ตเป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

2. แนวทางปฏิบัติในการใช้เครือข่ายอินเทอร์เน็ต

2.1 การลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต ต้องทำการกรอกข้อมูลคำขอใช้บริการเครือข่ายอินเทอร์เน็ตของสถาบัน โดยยื่นคำขอกับเจ้าหน้าที่ฝ่ายเทคโนโลยีสารสนเทศ โดยผู้ใช้งานต้องเป็นบุคลากรของสถาบัน สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากหัวหน้าฝ่ายเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย

2.2 ไม่ใช้ระบบอินเทอร์เน็ตของสถาบัน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับสถาบัน

2.3 ผู้ดูแลระบบ ต้องกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานอินเทอร์เน็ต ที่ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น และห้ามผู้ใช้ทำการเชื่อมต่อระบบคอมพิวเตอร์ผ่านช่องทางอื่น เช่น Dial-up Modem ยกเว้นแต่ว่ามีเหตุผลความจำเป็นและต้องทำการขออนุญาตจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

2.4 เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ก่อนทำการเชื่อมต่ออินเทอร์เน็ตผ่านเว็บเบราว์เซอร์ (Web Browser) ต้องมีการติดตั้งโปรแกรมป้องกันไวรัส และทำการอุดช่องโหว่ของระบบปฏิบัติการและเว็บเบราว์เซอร์

2.5 ผู้ใช้งานจะถูกกำหนดสิทธิในการเข้าถึงแหล่งข้อมูลตามหน้าที่ความรับผิดชอบ เพื่อประสิทธิภาพของเครือข่ายและความปลอดภัยทางข้อมูลของสถาบัน

2.6 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบัน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านทางอินเทอร์เน็ต

2.7 ห้ามผู้ใช้งานนำเข้าข้อมูลคอมพิวเตอร์ใด ๆ ที่มีลักษณะอันเป็นเท็จ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร อันเป็นความผิดเกี่ยวกับการก่อการร้าย หรือภาพที่มีลักษณะอันลามก และไม่ทำการเผยแพร่หรือส่งต่อข้อมูลคอมพิวเตอร์ดังกล่าวผ่านอินเทอร์เน็ต

2.8 ห้ามผู้ใช้งานนำเข้าข้อมูลคอมพิวเตอร์ที่เป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ตัดต่อเติม หรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์ หรือวิธีการอื่นใด ทั้งนี้ จะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชัง หรือได้รับความอับอาย

2.9 ผู้ใช้งานมีหน้าที่ตรวจสอบความถูกต้องและความน่าเชื่อถือของข้อมูลคอมพิวเตอร์ที่อยู่บนอินเทอร์เน็ตก่อนนำข้อมูลไปใช้งาน

2.10 ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานผ่านบัญชีของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้นั้นต้องเป็นผู้รับผิดชอบ

2.11 ระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต การดาวน์โหลด การอัพเดท (Update) โปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์ ไม่ดาวน์โหลดไฟล์ขนาดใหญ่ แต่หากมีความจำเป็นให้ปฏิบัตินอกเวลาทำงาน

2.12 ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

2.13 ใช้งานระบบอินเทอร์เน็ตเสร็จแล้ว ให้ปิดเว็บเบราว์เซอร์ที่ใช้งาน และออกจากเครือข่ายอินเทอร์เน็ตด้วยการออกจาก Authentication เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น ๆ

ส่วนที่ 8 นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ
(Operating System Access Control Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อให้มีการกำหนดมาตรฐานและการควบคุมการเข้าถึงระบบปฏิบัติการ โดยการกำหนดขั้นตอนปฏิบัติเพื่อเข้าใช้งานระบบปฏิบัติการ การควบคุมการใช้งานการระบุและยืนยันตัวตนของผู้ใช้งาน การจำกัดและควบคุมการใช้โปรแกรมอรรถประโยชน์ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ ตลอดถึงการยุติการใช้ระบบงานสารสนเทศเมื่อว่างเว้นการใช้งานในระยะเวลาหนึ่ง พร้อมทั้งนโยบายการบริหารจัดการรหัสผ่าน

2. แนวปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ

2.1 แนวปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย

2.1.1 ผู้ใช้งานต้องกำหนดรหัสผ่านในการใช้งานเครื่องคอมพิวเตอร์ที่รับผิดชอบ

2.1.2 ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ (Screen Saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งานหลังจากนั้นเมื่อต้องการใช้งานผู้ใช้บริการต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน

2.1.3 ก่อนการเข้าใช้ระบบปฏิบัติการต้องใส่ชื่อผู้ใช้งานและรหัสผ่านทุกครั้ง

2.1.4 ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้งานและรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสถาบันร่วมกัน

2.1.5 ผู้ใช้งานต้องทำการออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

2.1.6 ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

2.1.7 ซอฟต์แวร์ที่สถาบันใช้มีลิขสิทธิ์ผู้ใช้งานสามารถขอใช้งานได้ตามหน้าที่ความจำเป็นและห้ามไม่ให้ผู้ใช้งานทำการติดตั้งหรือใช้งานซอฟต์แวร์อื่นใดที่ไม่มีลิขสิทธิ์หากตรวจพบถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานรับผิดชอบแต่เพียงผู้เดียว

2.1.8 ซอฟต์แวร์ที่สถาบันจัดเตรียมไว้ให้ผู้ใช้งานถือเป็นสิ่งจำเป็นห้ามมิให้ผู้ใช้งานทำการติดตั้งถอดถอนเปลี่ยนแปลงแก้ไขหรือทำสำเนาเพื่อนำไปใช้งานที่อื่น

2.1.9 ห้ามใช้ทรัพยากรทุกประเภทที่เป็นของสถาบันเพื่อประโยชน์ทางการค้า

2.1.10 ห้ามผู้ใช้งานนำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรม กรณีผู้ใช้สร้างเว็บเพ็จบนเครือข่ายคอมพิวเตอร์

2.1.11 ห้ามผู้ใช้งานระบบสารสนเทศของสถาบันเพื่อควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

2.2 แนวปฏิบัติการระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication)

2.2.1 ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบสารสนเทศเพื่อป้องกันผู้ไม่มีสิทธิเข้าใช้งานระบบสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาดผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

2.2.2 ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ (Account) ต้องเป็นผู้รับผิดชอบในผลต่าง ๆอันจะเกิดขึ้นจากการใช้บัญชีผู้ใช้บริการ (Account) ของเครื่องคอมพิวเตอร์และระบบเครือข่าย เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

2.2.3 ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่นห้ามโอนจำหน่ายหรือจ่ายแจกให้ผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

2.2.4 ผู้ใช้งานต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้บริการ (Account) ของตนเองและทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

2.3 แนวปฏิบัติการใช้งานโปรแกรมประเภทอรรถประโยชน์ (Use of System Utilities)

2.3.1 กำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติการใช้งานโปรแกรมอรรถประโยชน์ระดับสิทธิของผู้ขออนุมัติและการระบุและพิสูจน์ตัวตนสำหรับการเข้าไปใช้งานโปรแกรมอรรถประโยชน์เพื่อจำกัดและควบคุมการใช้งาน

2.3.2 ต้องจัดเก็บโปรแกรมอรรถประโยชน์ออกจากซอฟต์แวร์สำหรับระบบงาน

2.3.3 มีการจำกัดผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมอรรถประโยชน์

2.3.4 ต้องยกเลิกหรือลบทิ้งโปรแกรมอรรถประโยชน์และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมอรรถประโยชน์ได้

2.4 แนวปฏิบัติการหมดเวลาใช้งานระบบสารสนเทศ (Session Time-out)

2.4.1 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศทำการพักหน้าจอหลังจากที่ไม่มีกิจกรรมการใช้งานช่วงระยะเวลา 15 นาที เพื่อป้องกันผู้อื่นเห็นข้อมูลบนหน้าจอ

ส่วนที่ 9 นโยบายการรักษาความมั่นคงปลอดภัย
การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ
(Application and Information Access Control Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อจำกัดการเข้าถึงสารสนเทศ จำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่นให้สอดคล้องกับนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศของสถาบันที่ได้กำหนดไว้ และให้มีการควบคุมระบบซึ่งไวต่อการรบกวนให้มีสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุม ปกป้องความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และการสื่อสารเคลื่อนที่ และการปฏิบัติงานจากภายนอกสถาบัน

2. แนวทางปฏิบัติในการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

2.1 การจำกัดการเข้าถึงสารสนเทศ (Information access restriction)

2.1.1 ผู้ดูแลระบบ ต้องกำหนดขั้นตอนปฏิบัติอย่างเป็นทางการในการให้สิทธิต่าง ๆ แก่บุคลากรใหม่ของสถาบัน เพื่อเข้าใช้งานโปรแกรมประยุกต์หรือแอพพลิเคชั่นและระบบสารสนเทศได้ ตามสิทธิในการปฏิบัติงานของแต่ละบุคคล

2.1.2 ผู้ดูแลระบบ มีหน้าที่ในการตรวจสอบการอนุมัติและกำหนดสิทธิในการผ่านเข้าสู่ระบบให้แก่ผู้ใช้งานโดยในการขออนุญาตเข้าระบบงานนั้น จะต้องมีการทำเป็นเอกสารเพื่อขอสิทธิในการเข้าสู่ระบบและกำหนดให้มีการลงนามอนุมัติ เอกสารดังกล่าวต้องมีการจัดเก็บไว้เป็นหลักฐาน

2.1.3 เจ้าของข้อมูล และ “เจ้าของระบบงาน” จะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่จำเป็นต้องรู้ตามหน้าที่งานเท่านั้น เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่ ดังนั้นการกำหนดสิทธิในการเข้าถึงระบบงาน ต้องกำหนดตามความจำเป็น ขั้นต่ำในการใช้งานตามภารกิจเท่านั้น

2.1.4 ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของผู้ใช้งาน (บุคลากรตามขั้นตอนในข้อที่ 2.1.1) ดังนี้

2.1.4.1 ในการให้สิทธิจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

2.1.4.2 การกำหนดชื่อผู้ใช้หรือรหัสผ่านตั้งต้นของผู้ใช้งานต้องไม่ซ้ำกัน

2.1.4.3 กำหนดเปลี่ยนแปลงและการยกเลิกรหัสผ่าน เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน ตลอดจนระงับสิทธิการใช้งานชั่วคราว ในกรณีที่ผู้บริหารเห็นว่าผู้ใช้งานดังกล่าวมีความเสี่ยงที่ก่อให้เกิดความเสียหายในการใช้งานโปรแกรมประยุกต์และระบบสารสนเทศ

2.1.4.4 ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีกำหนดระยะเวลาการใช้งานและระงับการใช้งาน ทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

2.1.4.5 การส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้บริการด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่น หรือการส่งจดหมายอิเล็กทรอนิกส์ (E-mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

2.1.5 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

2.1.5.1 ต้องมีควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

2.1.5.2 ต้องกำหนดรายชื่อผู้ใช้งานและรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

2.1.5.3 การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

2.1.5.4 กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

2.1.5.5 กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสถาบัน หรือกรณีที่ต้องส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ผู้ใช้งานคอมพิวเตอร์ดังกล่าวต้องทำการสำรองข้อมูล และลบข้อมูลที่เป็นความลับที่เก็บอยู่ในเครื่องคอมพิวเตอร์ออกเสียก่อน

2.2 แนวปฏิบัติการจัดการกับระบบซึ่งไวต่อการรบกวน

2.2.1 ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน ได้แก่ เว็บไซต์สถาบัน ระบบบริหารจัดการสำนักงาน (e-office) และ ระบบงบประมาณ บัญชีและการเงิน ถ้าระบบใดเสียหายจะส่งผลต่อการปฏิบัติงาน จึงต้องแยกออกจากระบบงานอื่นๆ ของสถาบัน และมีผู้รับผิดชอบหลัก

2.2.2 ระบบซึ่งไวต่อการรบกวน และมีความสำคัญสูงต่อสถาบัน ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงาน หรือเครื่องคอมพิวเตอร์แยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น เข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว และให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกสถาบัน(Mobile Computing and Teleworking)

2.3 แนวปฏิบัติงานจากภายนอกสถาบัน (Teleworking)

2.3.1 การเข้าสู่ระบบจากระยะไกล (Remote access) สู่ระบบเครือข่ายคอมพิวเตอร์ของสถาบันให้เกิดช่องทางที่มีความเสี่ยงสูงต่อความปลอดภัยของข้อมูลและทรัพยากรของสถาบัน การควบคุมบุคคลที่เข้าสู่ระบบของสถาบันจากระยะไกลจึงต้องมีการกำหนดมาตรการการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน

2.3.2 วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้ จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสถาบันก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้และผู้ใช้ต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบและข้อมูลอย่างเคร่งครัด

2.3.3 ก่อนทำการให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบัน อย่างเพียงพอและต้องได้รับอนุมัติจากผู้บังคับบัญชา

2.3.4 การควบคุมพอร์ท (Port) ที่ใช้ในการเข้าสู่ระบบ ต้องมีการดูแลและการจัดการโดยผู้ดูแลระบบ

2.3.5 การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ไม่ควรเปิดพอร์ตและโมเด็มที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น ช่องทางดังกล่าวควรตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้เมื่อมีการร้องขอที่จำเป็นเท่านั้น

2.3.6 ต้องกำหนดให้ระบบเทคโนโลยีสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง ระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยง (ในที่สาธารณะหรือพื้นที่ภายนอกสถาบัน) เป็นต้น มีการจำกัดช่วงระยะเวลาการเชื่อมต่อ

2.4 แนวปฏิบัติในการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงานภายนอก หรือ Outsource

2.4.1 ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกัน ทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่ม ปฏิบัติงานจากระยะไกล

2.4.2 ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะมีการปฏิบัติงานจากระยะไกลและระบบงานต่าง ๆ ภายในสถาบัน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

2.4.3 ต้องกำหนดมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล (ซึ่งรวมถึงตึก อาคาร สำนักงาน และสิ่งแวดล้อมภายนอก) เพื่อป้องกันการขโมยอุปกรณ์การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดีเพื่อเข้าสู่ระบบงานของสถาบัน

2.4.4 ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบันในสถานที่ดังกล่าว

2.4.5 ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้เครือข่ายจากที่บ้านเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน รวมทั้งมาตรการควบคุมการใช้เครือข่ายไร้สายที่บ้าน

2.4.6 ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบันจากระยะไกลมีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ (Firewall) ตามที่สถาบันต้องการ

2.4.7 ต้องมีการจัดเตรียมอุปกรณ์สeหรับการปฏิบัติงานจากระยะไกล การจัดเก็บข้อมูล และอุปกรณ์สื่อสารไว้ให้กับผู้ปฏิบัติงานจากระยะไกล

2.4.8 ไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน จากระยะไกล ถ้าอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุมหรือดูแลของสถาบัน

2.4.9 ต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่าง ๆ ของสถาบันที่อนุญาตให้เข้าถึงได้จากระยะไกล

2.4.10 ต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

2.5 การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

ผู้ดูแลระบบต้องกำหนดแนวปฏิบัติอย่างเป็นทางการสำหรับการใช้งานอุปกรณ์คอมพิวเตอร์ประเภท พกพา อาทิ เครื่องคอมพิวเตอร์โน้ตบุ๊ก รวมทั้งกำหนดมาตรการการใช้งานอย่าง เหมาะสม โดยมีแนวทางปฏิบัติดังนี้

2.5.1 ต้องวิเคราะห์และประเมินความเสี่ยงจากลักษณะการใช้งานอุปกรณ์คอมพิวเตอร์ประเภท พกพา

2.5.2 สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์ประเภท พกพา เช่น การใช้งานในที่สาธารณะ ห้องประชุมนอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกสถาบัน เป็นต้น

2.5.3 ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์ฯ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสข้อมูล

2.5.4 ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลสำคัญหรือข้อมูลลับในอุปกรณ์ฯ

2.5.5 สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์ฯ อย่างสม่ำเสมอ

2.5.6 ต้องควบคุมการเข้าถึงระบบงานของสถาบัน จากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตสาธารณะ

2.5.7 ต้องระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของสถาบันจากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา

2.5.8 ต้องควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของสถาบัน

2.5.9 ผู้ติดต่อจากหน่วยงานภายนอกที่นำอุปกรณ์คอมพิวเตอร์หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานเข้ามาปฏิบัติงานภายในห้องปฏิบัติการเครือข่ายและคอมพิวเตอร์ของสถาบัน จะต้องลงบันทึกรายการอุปกรณ์ในแบบฟอร์มการขออนุญาต เข้า - ออกพื้นที่ ให้ถูกต้องชัดเจน และต้องได้รับอนุญาตจากเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชา ด้วยการลงนามอย่างเป็นลายลักษณ์อักษร

2.5.10 กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารให้ชัดเจน โดยมีการจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้ผู้เกี่ยวข้องรับทราบโดยทั่วกัน เช่น พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่ใช้งานเครือข่ายไร้สาย (Wireless area) เป็นต้น

ส่วนที่ 10 นโยบายการสำรองและกู้คืนข้อมูล
(Backup and Recovery Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่องโดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจเพื่อลดความเสี่ยงที่อาจจะเกิดขึ้นกับข้อมูลและสามารถนำข้อมูลกลับมาใช้งานได้

2. วัตถุประสงค์ของนโยบาย

2.1 แนวปฏิบัติในการคัดเลือกการสำรองข้อมูล

2.1.1 มีการจัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของสถาบัน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรองและจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ 1ครั้ง

2.1.2 กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบและกำหนดความถี่ในการสำรองข้อมูลหากระบบใดที่มีการเปลี่ยนแปลงบ่อยควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้นโดยให้มีวิธีการสำรองข้อมูลดังนี้

2.1.2.1 กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้และความถี่ในการสำรอง

2.1.2.2 กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรองเช่นการสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

2.1.2.3 บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูลได้แก่ ผู้ดำเนินการวัน เวลาชื่อข้อมูลที่สำรองสำเร็จ ไม่สำเร็จเป็นต้น

2.1.2.4 ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วนเช่นซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศข้อมูล Configuration ข้อมูลในฐานข้อมูลเป็นต้น

2.1.2.5 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูลโดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึง ระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน

2.1.2.6 จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับสถาบัน ควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับสถาบัน เช่น ไฟไหม้ เป็นต้น

2.1.2.7 ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลนอกสถานที่

2.1.2.8 ทดสอบการบันทึกข้อมูลสำรองอย่างสม่ำเสมอเพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

2.1.2.9 จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้ตรวจสอบ และทดสอบประสิทธิภาพ และประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

2.1.2.10 กำหนดให้มีการใช้งานการเข้ารหัสข้อมูลกับข้อมูลลับที่ได้สำรองเก็บไว้

2.2 แนวปฏิบัติในการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินใน กรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

2.2.1 มีการจัดทำแผนเตรียมความพร้อมฉุกเฉินกรณีที่ไม่สามารถดำเนินการด้วยวิธีทางอิเล็กทรอนิกส์โดยมีรายละเอียดอย่างน้อยดังนี้

2.2.1.1 มีการกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

2.2.1.2 มีการประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้นและกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วง ทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

2.2.1.3 มีการกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

2.2.1.4 มีการกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูลและทดสอบกู้คืนข้อมูลที่สำรองไว้

2.2.1.5 มีการกำหนดช่องทางในการติดต่อกับผู้ให้บริการภายนอก เช่น ผู้ให้บริการเครือข่าย ฮาร์ดแวร์ซอฟต์แวร์เป็นต้นเมื่อเกิดเหตุจำเป็นที่จะต้องติดต่อ

2.2.1.6 การสร้างความตระหนักหรือให้ความรู้แก่เจ้าหน้าที่ผู้ที่เกี่ยวข้องกับขั้นตอนการปฏิบัติหรือสิ่งที่ต้องทำเมื่อเกิดเหตุเร่งด่วนเป็นต้น

2.2.2 มีการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจอย่างน้อยปีละ 1 ครั้ง

2.3 แนวปฏิบัติในการสำรองและกู้คืนข้อมูล

2.3.1 การสำรองข้อมูล

2.3.1.1 ผู้ดูแลระบบต้องตั้งค่าระบบให้มีการสำรองข้อมูลโดยอัตโนมัติหรือทำการสำรองข้อมูลของระบบ ซึ่งอยู่ในความรับผิดชอบของตนเองตามความเหมาะสมของแต่ละระบบไม่ต่ำกว่า 1 ครั้งต่อเดือน

2.3.1.2 ผู้ดูแลระบบต้องตั้งค่าสำรองข้อมูลอัตโนมัติสำหรับเครื่องคอมพิวเตอร์แม่ข่ายของเว็บไซต์ (Web Server)

2.3.1.3 ผู้ใช้งานเครื่องคอมพิวเตอร์ทั่วไปจะต้องทำการสำรองข้อมูลในเครื่องคอมพิวเตอร์ของตนเองตามความเหมาะสมไม่น้อยกว่า 1 ครั้งต่อปี โดยจัดเก็บไว้ที่สำรองข้อมูลกลางที่ผู้ดูแลระบบจัดเตรียมไว้ให้

2.3.1.4 เมื่อสถาบันประกาศให้มีการสำรองข้อมูลเนื่องจากจะได้มีการดำเนินการที่อาจส่งผลต่อข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้ ผู้ใช้จะต้องทำการสำรองข้อมูลดังกล่าวภายในระยะเวลาที่กำหนด

2.3.1.5 หากผู้ดูแลระบบหรือผู้ใช้งานเครื่องคอมพิวเตอร์เห็นว่าข้อมูลใด เป็นข้อมูลสำคัญให้พิมพ์ (Print) ออกมาเก็บสำรองไว้ในรูปของเอกสารกระดาษ (Hard Copy)

2.3.1.6 ฝ่ายเทคโนโลยีสารสนเทศของสถาบันต้องทำการทดสอบกู้ข้อมูลสำรองในทุกระบบโดยต้องมีการทดสอบอย่างน้อยปีละหนึ่งครั้ง ซึ่งการทดสอบดังกล่าวต้องใช้ข้อมูลสำรองจากระบบที่ใช้งานจริงแต่ทดสอบบนระบบทดสอบ

2.3.1.7 ผู้ดูแลระบบต้องทำการสำรองข้อมูลอิเล็กทรอนิกส์ของสถาบันและเก็บรักษาไว้ตามแนวทางปฏิบัติการเก็บรักษาข้อมูลของสถาบันโดยต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลที่สำคัญด้วย

2.3.2 การกู้คืนข้อมูล

2.3.2.1 ผู้ใช้งานจะต้องเปิดใช้งานการกู้คืน (Recovery) ของระบบปฏิบัติการตลอดเวลา

2.3.2.2 ผู้ดูแลระบบจะต้องจัดหาเครื่องคอมพิวเตอร์ อุปกรณ์และการติดตั้งซอฟต์แวร์ใหม่เพื่อทดแทนของเดิมที่เสียหาย

2.3.2.3 ผู้ดูแลระบบจะต้องทำการบำรุงรักษาระบบคอมพิวเตอร์และอุปกรณ์สนับสนุนเพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับระบบ

ส่วนที่ 11 นโยบายการรักษาความมั่นคงปลอดภัย การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit and Assessment policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อให้มีมาตรการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ที่อาจมีผลต่อความมั่นคงปลอดภัยด้านระบบสารสนเทศของสถาบัน

2. แนวทางปฏิบัติในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

2.1 สถาบันต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านความมั่นคงปลอดภัยด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) หรือกระบวนการการทำงานที่เกี่ยวข้องกับสารสนเทศของสถาบัน อย่างน้อยปีละ 1 ครั้ง

2.2 ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ดำเนินการโดยผู้ตรวจสอบภายในสถาบันที่ได้รับการแต่งตั้งจากสถาบัน (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor)

2.3 มาตรการในการตรวจประเมินระบบสารสนเทศ ต้องปฏิบัติดังนี้

2.3.1 กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย

2.3.2 กำหนดให้สิทธิให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านอย่างเดียว (Read only)

2.3.3 ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งานรวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือจัดเก็บไว้โดยมีการป้อนกันเป็นอย่างดี

2.3.4 กำหนดให้มีการเฝ้าระวังการเข้าถึงระบบของผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลแสดงการเข้าถึงนั้น (log) ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

2.3.5 ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ ควรกำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้น จากการเข้าถึงโดยไม่ได้รับอนุญาต

2.4 ต้องสรุปผลการตรวจสอบและการประเมินความเสี่ยง พร้อมข้อเสนอแนะต่อผู้อำนวยการสถาบัน เพื่อให้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของสถาบัน

ส่วนที่ 12 นโยบายและแนวปฏิบัติการใช้สื่อสังคมออนไลน์
(Guidelines for Uses of Social Media)

1. วัตถุประสงค์ของนโยบาย

เพื่อเป็นแนวทางในการกำกับดูแลการเผยแพร่ข้อมูลและการเข้าถึงสื่อเครือข่ายสังคมออนไลน์ของสถาบัน รวมถึงบริการอิเล็กทรอนิกส์ ตลอดจนการแสดงความคิดเห็นของบุคลากรในสถาบัน ผ่านสื่อเครือข่ายสังคมออนไลน์ให้เป็นไปอย่างถูกต้องเหมาะสม มีความเป็นระเบียบเรียบร้อยและเกิดประโยชน์สูงสุด

2. แนวทางปฏิบัติในการใช้สื่อสังคมออนไลน์มีดังนี้

2.1 ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอกนิกส์ที่สถาบันจัดให้ในการลงทะเบียนหรือประกาศข้อมูลใดๆ ในสื่อสังคมออนไลน์ เช่น เว็บบอร์ด บล็อก หรือกระดานข่าว เป็นต้น เว้นแต่การลงทะเบียนหรือประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนนึงของการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายจากสถาบัน

2.2 ผู้ใช้งานที่ต้องสื่อสารกับบุคคลภายนอกในการปฏิบัติงานของสถาบันผ่านสื่อสังคมออนไลน์ ให้ใช้แนวปฏิบัติดังนี้

2.2.1 การนำเสนอข่าวสารของสถาบัน โดยการใช้สื่อสังคมออนไลน์ ควรมีหลักในการอ้างอิงถึงสถาบัน ด้วยชื่อ รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงความเป็นสถาบัน หรือด้วยมาตรการอื่นที่ยืนยันสถานะ และความมีตัวตน

2.2.2 การนำเสนอข้อมูลข่าวสารของสถาบันต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในสังคม และไม่ยุยงให้เกิดความรุนแรงจนนำไปสู่ความขัดแย้งหรือเสียหายในสังคม

2.2.3 ผู้ใช้งานต้องใช้ความระมัดระวังในการเผยแพร่ข้อมูลข่าวสาร โดยไม่ละเมิดลิขสิทธิ์ของข้อมูล ข่าวสาร ภาพ หรืออื่น ๆ ที่ผลิตโดยบุคคลอื่น

2.2.4 การคัดลอกข้อความใด ๆ จากสื่อสังคมออนไลน์ ควรทำต่อเมื่อได้รับอนุญาตจากเจ้าของข้อความนั้น ๆ ในกรณีที่จำเป็นต้องคัดลอกข้อความจากสื่อสังคมออนไลน์เพื่อประโยขน์ในการเผยแพร่ข้อมูลข่าวสาร ผู้ใช้งานต้องอ้างอิงแหล่งที่มาของข้อความและข่าวสารเหล่านั้น โดยรับรู้ถึงสิทธิ์และลิขสิทธิ์ของบุคคลหรือสถาบันผู้เป็นเจ้าของข้อมูลดังกล่าว

2.2.5 ผู้ใช้งานใช้ความระมัดระวังในการนำเสนอข้อมูลข่าวสารของสถาบัน โดยเน้นหลักความถูกต้องและใช้ภาษาที่เหมาะสม หลีกเลี่ยงการแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของสถาบันในลักษณะที่อาจก่อให้เกิดที่เข้าใจความคลาดเคลื่อนไปจากความเป็นจริง

2.3 ผู้ใช้งานควรหลีกเลี่ยงการใช้งานสื่อสังคมออนไลน์ผ่านทางระบบสารสนเทศของสถาบัน เพื่อไม่ให้สถาบันตกอยู่ในความเสี่ยงเกินความจำเป็น

ส่วนที่ 13 นโยบายด้านความรับผิดชอบ
(Responsibility Policy)

1. วัตถุประสงค์ของนโยบาย

เพื่อกำหนดความรับผิดชอบที่ชัดเจน กรณีเครือข่าย ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศของสถาบันเกิดความเสียหาย หรืออันตรายใด ๆ แก่สถาบันหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2. หน้าที่ความรับผิดชอบแยกตามตำแหน่งงานที่เกี่ยวข้อง ดังนี้

2.1 ผู้บริหารระดับสูงสุด (Chief Executive Office : CEO)

2.1.1 กำกับให้มีการกำหนดจัดทำปรับปรุงนโยบายความมั่นคงปลอดภัยอยู่เสมอ

2.1.2 กำกับให้มีการควบคุม และปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด ห้ามมิให้ผู้ใดฝ่าฝืน หรือละเลยการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.1.3 มอบหมายอำนาจหน้าที่ให้ผู้ดูแลควบคุม และถือปฏิบัติตามนโยบายความมั่นคงปลอดภัยอย่างเคร่งครัด

2.1.4 รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิด ความเสียหาย หรืออันตรายใด ๆ แก่สถาบันหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

2.2 ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Office : CIO)

2.2.1 เป็นผู้บังคับบัญชาสูงสุดในการปฏิบัติการฉุกเฉินที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ

2.2.2 มีอำนาจสั่งการให้ทุกหน่วยหยุดปฏิบัติการและระงับเหตุฉุกเฉินที่เกิดขึ้นในระบบเทคโนโลยีสารสนเทศ

2.2.3 ทำหน้าที่แทนผู้อำนวยการระงับเหตุฉุกเฉินตามที่ได้รับมอบหมาย หรือขณะที่ ผู้อำนวยการระงับเหตุฉุกเฉินไม่อยู่

2.2.4 ประชุมร่วมกับคณะกรรมการจัดการระบบเครือข่ายคอมพิวเตอร์ และคณะกรรมการอื่นที่เกี่ยวข้อง

2.2.5 ประเมินสถานการณ์ และสั่งการให้ปรับเปลี่ยนแผนฯ ตามความเหมาะสม

2.2.6 รายงานข้อมูลและผลการปฏิบัติงานให้ ผู้บริหารระดับสูง ทราบ

2.2.7 ผู้ประสานงานและบริหารการกับดูแลสภาพความพร้อมของระบบเครือข่าย (เจ้าหน้าที่สารสนเทศ)

2.2.8 วิเคราะห์สถานการณ์ในที่เกิดเหตุ แล้วแจ้งเหตุต่อ CIO

2.2.9 มีอำนาจสั่งการให้ใช้แผนปฏิบัติการฉุกเฉิน จนกว่าผู้อำนวยการระงับเหตุฉุกเฉินจะมาถึงที่เกิดเหตุ

2.2.10 ประสานงานกับหน่วยงานที่เกี่ยวข้อง เช่น ช่างไฟฟ้า ยานพาหนะและหน่วยดับเพลิง เป็นต้น

2.2.11 รายงานให้ผู้อำนวยการทราบถึงสถานการณ์ และให้สั่งการแนวทางการระงับเหตุฉุกเฉิน

2.2.12 ตรวจสอบความเสียหายของทรัพย์สินและอาคารที่เกิดเหตุ

2.3 ผู้ดูแลระบบเครือข่าย และผู้ช่วยดูแลระบบเครือข่าย (LAN Administrator and Staffs)

2.3.1 กรณีเกิดเพลิงไหม้ให้ดำเนินการนำอุปกรณ์ดับเพลิงเข้าทำการดับเพลิง

2.3.2 พิจารณาแจ้งสถานีดับเพลิง หรือหน่วยงานภายนอกอื่นๆ

2.3.3 ตัดกระแสไฟฟ้าที่จ่ายให้พื้นที่ที่เกิดเหตุฉุกเฉิน

2.3.4 ป้องกันชีวิต ทรัพย์สิน และสิ่งแวดล้อม ให้ได้รับความเสียหายน้อยที่สุด

2.3.5 หลังจากเหตุการณ์ฉุกเฉินได้สงบลงแล้วให้รีบดำเนินการตรวจสอบ วัสดุ อุปกรณ์ที่ชำรุดเสียหาย แล้วรายงานให้ CIO ทราบ อุปกรณ์ที่ต้องตรวจสอบ ได้แก่

- ทำการตรวจสอบระบบ firewall
- ทำการตรวจสอบ Virus, Worm, Spy ware
- ทำการตรวจสอบ UPS
- ทำการตรวจสอบ Transaction log files
- ทำการตรวจสอบการใช้งานข้อมูลระบบงานที่สำคัญ
- ทำการตรวจสอบการเปลี่ยนแปลงของไฟล์ต่าง ๆ
- ทำการตรวจสอบความถูกต้องของไฟล์ข้อมูล
- ทำการตรวจสอบค่า Configuration ของระบบ

2.3.6 เตรียมเครื่องมือ อุปกรณ์ ทั้งทางด้าน Hardware และ software ตลอดจนอุปกรณ์ที่เกี่ยวข้อง เพื่อดำเนินการกู้ระบบโดยเร็ว

2.3.7 ประสานและขอความช่วยเหลือจากหน่วยงานภายนอกในการกู้ระบบ

2.3.8 ทำการสำรองข้อมูลตามที่กำหนด ทุก 6 เดือน

2.3.9 ต้องเก็บสิ่งที่สำคัญที่เกี่ยวข้องในระบบสารสนเทศไว้ในสถานที่ที่ปลอดภัย โดยแยกเก็บไว้ต่างหากจากห้องควบคุมระบบ เช่น โปรแกรมและแฟ้มข้อมูล, รายชื่อโปรแกรม, เอกสารที่เกี่ยวกับระบบปฏิบัติการและโปรแกรม, รายการฮาร์ดแวร์สำรอง, สำเนาคู่มือ

2.3.10 นำระบบสำรองข้อมูลออกมาใช้เพื่อให้ระบบสามารถดำเนินการต่อไปได้

2.4 ที่ปรึกษาด้านเทคนิค (บุคคลภายนอก)

2.4.1 ให้คำปรึกษาในเรื่องเกี่ยวกับระบบสารสนเทศ และวิธีการจัดการในการระงับเหตุฉุกเฉินที่ปลอดภัยต่อชีวิต ทรัพย์สิน และสิ่งแวดล้อมมากที่สุด

2.4.2 ติดต่อขอคำปรึกษาด้านเทคนิคจากผู้เชี่ยวชาญหรือหน่วยราชการที่เกี่ยวข้อง

2.4.3 ให้คำปรึกษาวิธีการกู้ระบบสารสนเทศกลับคืนมาโดยเร็ว หลังจากเหตุฉุกเฉินสงบแล้ว

2.5 หัวหน้าหน่วยงานที่เกิดเหตุ (On-site manager)

2.5.1 แจ้งเหตุฉุกเฉิน และเคลื่อนย้ายตนเอง และผู้อื่นออกจากที่เกิดเหตุโดยเร็ว

2.5.2 ให้ข้อมูลเกี่ยวกับสถานที่เกิดเหตุแก่ประธานศูนย์ประสานงานรักษาความปลอดภัย ระบบเทคโนโลยีสารสนเทศ

2.5.3 นำทรัพย์สินที่ขนย้ายออกมาเก็บเข้าที่โดยต้องตรวจสภาพ และสอบทานบัญชีทรัพย์สินที่จัดทำขึ้นมา และทำรายงานเสนอผู้บังคับบัญชาตามลำดับขั้น

2.6 ระดับนโยบาย

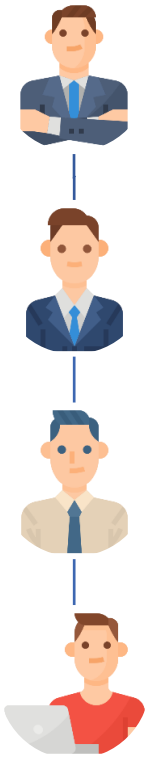
2.6.1 ให้ผู้บริหารระดับสูง ซึ่งมีหน้าที่ดูแลรับผิดชอบด้านสารสนเทศของหน่วยงานที่ทำหน้าที่ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) และผู้อำนวยการสำนัก เป็นผู้รับผิดชอบในการสั่งการตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศติดตามและกำกับดูแล ควบคุมตรวจสอบ รวมทั้งให้ข้อเสนอแนะแก่เจ้าหน้าที่ระดับปฏิบัติการ

2.7 แนวทางปฏิบัติของผู้รับผิดชอบ

2.7.1 CIO/ผู้ที่ได้รับมอบหมาย รับผิดชอบกำกับดูแลการปฏิบัติงานของผู้ปฏิบัติงาน อย่างใกล้ชิด ให้ความคิดเห็น เสนอแนะวิธีการ และแนวทางแก้ไขปัญหาจากสถานการณ์ ความเสี่ยงของระบบฐานข้อมูล และสารสนเทศ วางแผนการปฏิบัติงาน ติดตามการ ปฏิบัติงานตามแผนการบริหารความเสี่ยงและตรวจสอบ ระบบความมั่นคงและความปลอดภัยของฐานข้อมูลและสารสนเทศ พร้อมรายงานผลการดำเนินการ รวมทั้งรับผิดชอบ ดังนี้

- ควบคุมการเข้า - ออกห้อง Server ตามการกำหนดสิทธิ์การเข้าถึง Server
- กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ Server และอุปกรณ์เชื่อมโยงเครือข่าย (Network) ของระบบการเชื่อมโยงเครือข่ายฐานข้อมูลทั้งหมดให้ สามารถใช้งานได้ตามปกติตลอด 24 ชั่วโมง
- กำกับดูแล การติดตั้ง รื้อถอน ดูแล ตรวจสอบ การเชื่อมโยงการสื่อสารผ่านเครือข่ายทางระบบ LAN, Internet, Intranet ที่ให้บริการใน สถาบัน
- กำกับดูแลรักษาการทำงานระบบดับเพลิงอัตโนมัติของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ให้สามารถทำงานได้ตลอดเวลาเมื่อเกิดสถานการณ์ไฟไหม้
- แก้ไขปัญหา อุปสรรค สถานการณ์ความเสี่ยงและความเสียหายที่เกิดขึ้นกับระบบเชื่อมโยงเครือข่ายของระบบฐานข้อมูลสรสนเทศ
- รายงานผลการปฏิบัติงาน สถานการณ์ที่เกิดขึ้นกับระบบเครือข่ายและระบบฐานข้อมูลและสารสนเทศ ให้แก่ผู้บังคับบัญชาระดับสูงสุดทราบอย่างสม่ำเสมอ
- กำกับดูแล การติดตาม ตรวจสอบ (Monitor) การเข้าใช้งานและการเข้าถึงงานระบบการทำงานของเครื่องคอมพิวเตอร์แม่ข่าย (Server) ตามสิทธิ์การเข้าถึงระบบ
- กำกับดูแล การป้องกันการถูกเจาะระบบ และแก้ไขปัญหาการถูกเจาะเข้า ระบบฐานข้อมูลจากบุคคลภายนอก (Hacker) โดยไม่ได้รับอนุญาตตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- กำกับดูแล ตรวจสอบ บำรุงรักษาอุปกรณ์ป้องกันการถูกเจาะระบบจากบุคคลภายนอกและโปรแกรมปฏิบัติการทั้งหมดที่ติดตั้งอยู่ใน Server ของระบบฐานข้อมูลทั้งหมด ที่ให้บริการในเว็บไซต์ ให้สามารถใช้งานได้ตามปกติตลอด 24 ชั่วโมง
- กำกับดูแล ตรวจสอบในการกำหนดแก้ไขหรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบอื่น

2.8 แผนผังสายการบังคับบัญชา (Lines of Authority)



Chief Executive Officer (CEO)

ผู้อำนวยการ สถาบัน

Chief Information Officer (CIO)

รองผู้อำนวยการ (บริหาร)

ผู้อำนวยการสำนัก

ผู้อำนวยการสำนักยุทธศาสตร์และสารสนเทศ

กลุ่มงานสารสนเทศ

- นักเทคโนโลยีสารสนเทศ
- นักออกแบบสื่อประชาสัมพันธ์