ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันบัณฑิตพัฒนบริหารศาสตร์
พ.ศ. ๒๕๖๔

เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ผ่านระบบเทคโนโลยีหรือเครือข่ายคอมพิวเตอร์ของสถาบันบัณฑิตพัฒนบริหารศาสตร์มีความมั่นคงปลอดภัยและเชื่อถือได้ สถาบันบัณฑิตพัฒน-บริหารศาสตร์จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยมีวัตถุประสงค์ ดังนี้

๑. เพื่อให้การใช้ระบบสารสนเทศเป็นไปอย่างเหมาะสม สามารถดำเนินงานได้อย่างต่อเนื่อง ป้องกันปัญหาจากการใช้งานในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของสถาบัน

๒. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ และระบบเครือข่ายคอมพิวเตอร์ของสถาบัน ทำให้การดำเนินงานเป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ และขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันให้ได้รับการปรับปรุงอย่างต่อเนื่อง

๔. เพื่อเผยแพร่นโยบายและแนวปฏิบัตินี้ ให้บุคลากร นักศึกษา และบุคคลภายนอกที่ปฏิบัติงานร่วมกับสถาบันได้รับทราบ และถือปฏิบัติตามอย่างเคร่งครัด

๕. เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๖. เพื่อส่งเสริมให้บุคลากร และนักศึกษาของสถาบัน มีความรู้ ความเข้าใจ และสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน

อาศัยอำนาจตามความในมาตรา ๔๐ (๑) แห่งพระราชบัญญัติสถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. ๒๕๖๒ ประกอบกับมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ สถาบันบัณฑิตพัฒนบริหารศาสตร์ จึงออกประกาศดังนี้

ข้อ ๑. ประกาศนี้เรียกว่า “ประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์ เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. ๒๕๖๔”

ข้อ ๒. ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓. การจัดทำนโยบาย

๓.๑ ให้ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

๓.๒ ให้จัดทำนโยบายและแนวปฏิบัติได้เป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสถาบัน

๓.๓ กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน ดังนี้

ส่วนที่ ๑ การควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้บริหารส่วนงานเจ้าของระบบ

ส่วนที่ ๒ ระบบสารสนเทศและระบบสำรองสารสนเทศ

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) หน่วยงานเจ้าของระบบ

ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) สำนักงานตรวจสอบภายใน

๓.๔ มีการทบทวนและปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔. รายละเอียดของเอกสารแนบท้ายประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสถาบันบัณฑิตพัฒนบริหารศาสตร์ ซึ่งมีสาระสำคัญสอดคล้องตามมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ ประกอบด้วย ๔ องค์ประกอบ ได้แก่

๔.๑ คำนิยาม

๔.๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๔.๓ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ๓ ส่วน ได้แก่

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ ประกอบด้วย

๑) การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)

๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๕) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access control)

๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ส่วนที่ ๒ ระบบสารสนเทศและระบบสำรองสารสนเทศ

ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๔.๔ ภาคผนวก เรื่อง ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังนี้

๑. ข้อปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒. ข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน

๓. ข้อปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน

๔. ข้อปฏิบัติการใช้งานรหัสผ่าน

๕. ข้อปฏิบัติการใช้งานบริการเครือข่าย

๖. ข้อปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์

๗. ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

๘. ข้อปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

ข้อ ๕. สถาบันบัณฑิตพัฒนบริหารศาสตร์ขอสงวนสิทธิ์ในการติดตั้งเครื่องมือฮาร์ดแวร์ ซอฟต์แวร์ เพื่อบันทึกและเฝ้าระวังการใช้คอมพิวเตอร์และเครือข่าย เพื่อคงไว้ซึ่งการให้บริการอย่างปลอดภัย มีประสิทธิภาพและเป็นไปตามกฎหมาย ทั้งนี้ สถาบันบัณฑิตพัฒนบริหารศาสตร์ คงไว้ซึ่งอำนาจในการจำกัด ระงับหรือเพิกถอนสิทธิ์การใช้ระบบสารสนเทศ และดำเนินการสืบสวน เมื่อได้รับรายงานการแจ้งเตือนหรือตรวจพบการกระทำใดที่อาจก่อให้เกิดปัญหาความมั่นคงปลอดภัย ปัญหาเสถียรภาพ หรือการกระทำที่ขัดต่อนโยบาย หรือพระราชบัญญัติสถาบันบัณฑิตพัฒนบริหารศาสตร์ หรือกฎหมายของรัฐ

ข้อ ๖. สำนักเทคโนโลยีสารสนเทศ มีหน้าที่ในการกำหนดหลักเกณฑ์ แนวปฏิบัติในการจำกัด ระงับหรือเพิกถอนสิทธิ์การใช้เครือข่ายของผู้ฝ่าฝืน ตลอดจนระงับหรือจำกัดการเข้าถึงคอมพิวเตอร์ที่มีข้อมูลขัดต่อหลักเกณฑ์ แนวปฏิบัติ นโยบาย พระราชบัญญัติสถาบันบัณฑิตพัฒนบริหารศาสตร์ หรือกฎหมายของรัฐ ในกรณีสำคัญให้สำนักเทคโนโลยีสารสนเทศรายงานเหตุแห่งการฝ่าฝืนนั้น ให้อธิการบดีสถาบันบัณฑิตพัฒนบริหารศาสตร์พิจารณาดำเนินการทางวินัยและทางกฎหมายต่อไป

ข้อ ๗. กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สถาบัน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ กำหนดให้อธิการบดี เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ประกาศ ณ วันที่ ๓๐ พฤศจิกายน พ.ศ. ๒๕๖๔

(ศาสตราจารย์ ดร.กำพล ปัญญาโกเมศ)

อธิการบดีสถาบันบัณฑิตพัฒนบริหารศาสตร์

เอกสารแนบท้ายประกาศสถาบันบัณฑิตพัฒนบริหารศาสตร์

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ พ.ศ. ๒๕๖๔

คำนำ

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นสิ่งสำคัญที่ต้องปฏิบัติอย่างต่อเนื่อง และจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือจากทุกฝ่ายที่เกี่ยวข้อง การกำหนดนโยบายและแนวปฏิบัติเพื่อใช้เป็นแนวทางในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศจะช่วยให้การใช้ระบบสารสนเทศเป็นไปอย่างเหมาะสม มีประสิทธิภาพ เป็นการป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของสถาบัน ด้วยเหตุผลดังกล่าวสถาบันจึงได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๔ ขึ้น เพื่อเผยแพร่ให้ บุคลากร นักศึกษาในสถาบัน และบุคคลภายนอกที่ปฏิบัติงานร่วมกับสถาบันได้รับทราบ และให้ความร่วมมือปฏิบัติตามอย่างเคร่งครัดต่อไป

สำนักเทคโนโลยีสารสนเทศ
สถาบันบัณฑิตพัฒนบริหารศาสตร์
๒๕๖๔

สารบัญ

หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้ หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันบัณฑิตพัฒนบริหารศาสตร์สามารถดำเนินงานได้อย่างเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัย ใช้งานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยใด ๆ สถาบันบัณฑิตพัฒนบริหารศาสตร์จึงเห็นสมควรจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ เพื่อให้บุคลากรและนักศึกษาทุกคนที่เกี่ยวข้องได้นำไปปฏิบัติอย่างเคร่งครัด

วัตถุประสงค์

๑.๑. เพื่อให้การใช้ระบบสารสนเทศสามารถดำเนินงานได้อย่างเหมาะสมและมีประสิทธิภาพ มีความมั่นคงปลอดภัย ใช้งานได้อย่างต่อเนื่อง ป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง ซึ่งอาจส่งผลให้เกิดภัยคุกคามในลักษณะต่าง ๆ ต่อระบบสารสนเทศของสถาบัน

๑.๒. เพื่อให้เกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศ หรือเครือข่ายคอมพิวเตอร์ของสถาบัน ทำให้การดำเนินงานเป็นไปได้อย่างมีประสิทธิภาพและประสิทธิผล

๑.๓. เพื่อกำหนดมาตรฐาน แนวทางปฏิบัติ วิธีปฏิบัติ และขอบเขตของการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันให้ได้รับการปรับปรุงอย่างต่อเนื่อง

๑.๔. เพื่อเผยแพร่นโยบายและแนวปฏิบัตินี้ ให้บุคลากร นักศึกษา และบุคคลภายนอกที่ปฏิบัติงานร่วมกับสถาบันได้รับทราบ และถือปฏิบัติตามอย่างเคร่งครัด

๑.๕. เพื่อให้มีการดำเนินการตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอ

๑.๖. เพื่อส่งเสริมให้บุคลากร และนักศึกษาของสถาบัน มีความรู้ ความเข้าใจ และสร้างความตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน

องค์ประกอบ

สาระสำคัญของนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ ประกอบด้วย ๓ องค์ประกอบ ได้แก่

๑.๑. คำนิยาม

๑.๒. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑.๓. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วย ๓ ส่วน ได้แก่

ส่วนที่ ๑. การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ ประกอบด้วย

๑.๑) การควบคุมการเข้าถึงการใช้งานสารสนเทศ (Access Control)

๑.๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

๑.๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
๑.๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๑.๕) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
๑.๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
๑.๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
๑.๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ส่วนที่ ๒. ระบบสารสนเทศและระบบสำรองของสารสนเทศ ประกอบด้วย
๒.๑) พิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน
๒.๒) การทดสอบและการกู้คืน
๒.๓) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๓. การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

คำนิยาม

๑. **สถาบัน** หมายความว่า สถาบันบัณฑิตพัฒนบริหารศาสตร์

๒. **สำนัก** หมายความว่า สำนักเทคโนโลยีสารสนเทศซึ่งเป็นหน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษา ระบบคอมพิวเตอร์ ระบบชุดคำสั่ง ชุดคำสั่ง โปรแกรมและระบบเครือข่ายภายในสถาบัน

๓. **ผู้บริหารระดับสูงสุด** หมายความว่า ผู้ดำรงตำแหน่งอธิการบดี

๔. **ผู้บริหาร** หมายความว่า ผู้ดำรงตำแหน่งรองอธิการบดี ผู้ช่วยอธิการบดี คณบดี รองคณบดี ผู้อำนวยการสำนัก รองผู้อำนวยการสำนัก เลขานุการคณะ/สำนัก ผู้อำนวยการกอง

๕. **ผู้ใช้งาน** หมายความว่า ผู้ใช้งานภายในสถาบันและผู้ที่ได้รับอนุญาตให้ใช้ระบบสารสนเทศของสถาบัน

๖. **ผู้ดูแลระบบ (System Administrator)** หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บริหาร ให้มีหน้าที่รับผิดชอบในการดูแลรักษา หรือจัดการระบบสารสนเทศ และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

๗. **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

๘. **สิทธิทั่วไป** หมายความว่า สิทธิตามสถานภาพการใช้งานของผู้ใช้งาน ที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

๙. **สิทธิจำเพาะ** หมายความว่า สิทธิตามตำแหน่งหน้าที่และความรับผิดชอบ ที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

๑๐. **สิทธิพิเศษ** หมายความว่า สิทธิในการเข้าถึงข้อมูลและสารสนเทศที่สูงกว่าสิทธิทั่วไป มีการให้สิทธิชั่วคราวและมีกำหนดระยะเวลาในการใช้งาน

๑๑. **สินทรัพย์** หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตน และไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับสถาบัน ได้แก่ ข้อมูล ระบบสารสนเทศ และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร ได้แก่ อุปกรณ์ระบบเครือข่าย และซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๑๒. **เจ้าของระบบ** หมายความว่า ผู้บริหารที่รับผิดชอบต่อระบบสารสนเทศและข้อมูลในระบบสารสนเทศ โดยเจ้าของระบบเป็นผู้รับผิดชอบข้อมูลนั้น ๆ และเป็นผู้ได้รับผลกระทบโดยตรงหากข้อมูลในระบบสารสนเทศเหล่านั้นเกิดสูญหายหรือเกิดรั่วไหล

๑๓. **บุคคลภายนอก** หมายความว่า บุคคลภายนอกที่สถาบันอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๔. **หน่วยงานภายนอก** หมายความว่า องค์กรหรือหน่วยงานภายนอกที่สถาบันอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้งานตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๑๕. **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้แก่ผู้ใช้งาน เพื่อเข้าถึงหรือใช้งานระบบเครือข่ายหรือระบบสารสนเทศหรืออุปกรณ์ประมวลผลข้อมูลและสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตใช้งานเช่นนั้นสำหรับผู้ใช้งานที่เป็นบุคคลภายนอกหรือหน่วยงานภายนอก

๑๖. **การเปลี่ยนแปลงสถานภาพ** หมายความว่า การเปลี่ยนแปลงที่มีผลต่อสิทธิการเข้าถึงหรือเข้าใช้งานระบบสารสนเทศ ได้แก่ การลาออก การเปลี่ยนตำแหน่ง การโอนย้าย การสิ้นสุดการจ้าง การพ้นสภาพ

๑๗.ข้อมูล หมายความว่า ข่าวสาร เอกสาร ข้อเท็จจริงเกี่ยวกับบุคคล สิ่งของหรือเหตุการณ์ที่มีอยู่ในรูปของตัวเลข ภาษา ภาพ สัญลักษณ์ต่างๆ ที่มีความหมายเฉพาะตัว ซึ่งยังไม่มีการประมวลสำหรับการนำไปใช้ได้อย่างมีประสิทธิภาพ

๑๘.สารสนเทศ หมายความว่า ข้อมูลที่เป็นประโยชน์ต่อสถาบัน เกิดจากการนำข้อมูล ผ่านระบบการประมวลผล คำนวณ วิเคราะห์หรือแปลความหมาย อย่างเป็นระบบตามหลักวิชาการ ที่สามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่น ๆ

๑๙.ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์ หรือ ชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงาน ให้อุปกรณ์ หรือชุดอุปกรณ์ ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

๒๐.ระบบสารสนเทศ หมายความว่า ระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ระบบเครือข่าย ระบบปฏิบัติการ โปรแกรมประยุกต์ ข้อมูลสารสนเทศ เป็นต้น

๒๑.ระบบเครือข่าย หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่าง ๆ ของสถาบันได้ ได้แก่ ระบบแลน **(LAN)** ระบบอินทราเน็ต **(Intranet)** และระบบอินเทอร์เน็ต **(Internet)**

๒๒.จดหมายอิเล็กทรอนิกส์ (e-Mail) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่ายภาพกราฟิก ภาพเคลื่อนไหว ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ ผ่านโพรโตคอล ต่าง ๆ ได้แก่ **SMTP, POP3, IMAP** เป็นต้น

๒๓.บัญชีผู้ใช้ (Account) หมายความว่า ชื่อบัญชีและรหัสผ่านของผู้เข้าถึงในการใช้งานระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่าย

๒๔.รหัสผ่าน (Password) หมายความว่า ชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ ที่ถูกกำหนดขึ้นเพื่อใช้ในการเข้าใช้งานระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

๒๕.Single Sign-on หมายความว่า ความสามารถของระบบในการยืนยันตัวตน **(Authentication)** ที่รองรับการให้ผู้ใช้งานลงชื่อเข้าใช้งานระบบ **(Login)** ครั้งเดียว แล้วสามารถเข้าใช้งานระบบหลายระบบได้โดยไม่ต้องลงชื่อเข้าใช้งานซ้ำอีก

๒๖.การเข้ารหัสลับ (Encryption) หมายความว่า การนำข้อมูลมาเข้ารหัสลับเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสลับไว้จะต้องเข้าโปรแกรมถอดรหัสลับเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

๒๗.อุปกรณ์จัดเส้นทาง (Router) หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

๒๘.การยืนยันตัวตน (Authentication) หมายความว่า เป็นขั้นตอนในการยืนยันตัวตนของผู้ใช้งานระบบโดยทั่วไปแล้วจะเป็นการยืนยันโดยใช้ชื่อบัญชีและรหัสผ่าน

๒๙.อุปกรณ์ป้องกันการบุกรุก (Firewall) หมายความว่า ซอฟต์แวร์หรือฮาร์ดแวร์ในระบบเครือข่าย ที่ทำหน้าที่คอยตรวจสอบข้อมูลต่างๆ ระหว่างเครือข่าย หรือระหว่างเครื่องคอมพิวเตอร์ต่างๆ เพื่อคอยป้องกันการโจมตี สแปม และผู้บุกรุกต่างๆ ที่ไม่หวังดีต่อระบบ

๓๐.SSID (Service Set Identifier) หมายความว่า ชื่อระบุเครือข่ายไร้สาย

๓๑.**WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสลับเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายซึ่งได้รับการพัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

๓๒.**VPN (Virtual Private Network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว ที่การรับส่งข้อมูลจริงทำโดยการเข้ารหัสลับแล้วทำการรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

๓๓.**แผนผังระบบเครือข่าย (Network Diagram)** หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสถาบัน

๓๔.**มาตรฐาน (Standard)** หมายความว่า บรรทัดฐานที่ใช้ในการปฏิบัติเพื่อให้ได้ผลบรรลุตามวัตถุประสงค์หรือเป้าหมาย

๓๕.**แนวปฏิบัติ** หมายความว่า แนวทางที่แนะนำให้ปฏิบัติตาม เพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

๓๖.**ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของระบบเครือข่ายหรือระบบสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

๓๗.**เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือเกิดมาตรการป้องกันที่ล้มเหลว หรือเกิดเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๓๘.**สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายความว่า สถานการณ์ที่ระบบสารสนเทศถูกบุกรุกโจมตีและความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม รวมถึงสถานการณ์ที่เกิดจากภัยพิบัติ

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันบัณฑิตพัฒนบริหารศาสตร์

นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันบัณฑิตพัฒนบริหารศาสตร์ จัดทำขึ้นเพื่อกำหนดแนวทางและวิธีปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องและเป็นไปตามนโยบายที่กำหนดไว้ โดยมีรายละเอียดดังต่อไปนี้

ข้อ ๑ มีข้อกำหนดการควบคุมการเข้าถึงการใช้งานสารสนเทศ (access control) ดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลและสารสนเทศ โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) มีการกำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของหน่วยงาน

(๓) มีการกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ข้อ ๒ มีข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๓ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต ดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

(๕) การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (review of user access rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๔ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลและสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ต้องกำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ ได้แก่ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัสลับ มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๕ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต ดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แค่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๒) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

(๕) การแบ่งแยกเครือข่าย (segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงานให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานตามภารกิจ

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการใช้งานตามภารกิจ

ข้อ ๖ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต ดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

(๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

(๔) การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

ข้อ ๗ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม ดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและผู้ดูแลระบบในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking)

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

ข้อ ๘ มีการจัดทำระบบสำรองของสารสนเทศ ตามแนวทางต่อไปนี้

(๑) พิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) จัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) มีการกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) มีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๙ มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยมีเนื้อหาดังนี้

(๑) จัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในของหน่วยงาน (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันบัณฑิตพัฒนบริหารศาสตร์

องค์ประกอบของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ส่วนที่ ๑ การเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ ประกอบด้วย

๑) การควบคุมการเข้าถึงการใช้งานสารสนเทศ (Access Control)
๒) ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)
๓) การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)
๔) การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)
๕) การควบคุมการเข้าถึงเครือข่าย (Network Access Control)
๖) การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)
๗) การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)
๘) การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

ส่วนที่ ๒ การสำรองระบบสารสนเทศ ประกอบด้วย

๑) การพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน
๒) การทดสอบและการกู้คืน
๓) การทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

ส่วนที่ ๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

องค์ประกอบแต่ละส่วนที่กล่าวข้างต้นประกอบด้วย วัตถุประสงค์ รายละเอียดของมาตรฐาน และขั้นตอนปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน แนวปฏิบัตินี้ จัดเป็นมาตรฐานในการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสถาบัน ซึ่งบุคลากร และนักศึกษา รวมทั้งบุคคลหรือหน่วยงานภายนอกที่ปฏิบัติงานร่วมกับสถาบัน จะต้องปฏิบัติตามอย่างเคร่งครัด

ส่วนที่ ๑ การควบคุมการเข้าถึงการใช้งานสารสนเทศ

แนวปฏิบัติในการควบคุมการเข้าถึงการใช้งานสารสนเทศนี้ เป็นมาตรการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อุปกรณ์เครือข่าย และระบบสารสนเทศของสถาบัน โดยระบุถึงข้อกำหนดการใช้งานตามภารกิจ การบริหารจัดการและการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีขั้นตอนปฏิบัติในการควบคุมการเข้าถึงระบบปฏิบัติการ โปรแกรมประยุกต์ สารสนเทศ ระบบเครือข่าย และระบบเครือข่ายไร้สาย

วัตถุประสงค์

๑) เพื่อให้มีแนวทางปฏิบัติในการรักษาความมั่นคงปลอดภัย สำหรับการควบคุมการเข้าถึงการใช้งานระบบสารสนเทศของสถาบัน

๒) เพื่อให้ผู้รับผิดชอบและผู้มีส่วนเกี่ยวข้อง ได้แก่ ผู้บริหาร อาจารย์ ผู้ใช้งาน ผู้ดูแลระบบ เจ้าของข้อมูลหรือเจ้าของระบบ รวมทั้งบุคคลหรือหน่วยงานภายนอก ได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้บริหารส่วนงานเจ้าของระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

๑. การควบคุมการเข้าถึงการใช้งานสารสนเทศ (Access Control)

๑.๑. จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน จำแนกตามกลุ่มทรัพยากร โดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน รวมถึงผู้รับผิดชอบในทรัพย์สิน

๑.๒. กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ซึ่งเกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือ การมอบอำนาจ ดังนี้

๑.๒.๑. กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง ได้แก่

(๑) อ่านอย่างเดียว

(๒) สร้างข้อมูล

(๓) เพิ่มข้อมูล

(๔) แก้ไขข้อมูล

(๕) ลบข้อมูล

(๖) อนุมัติสิทธิ

(๗) ไม่มีสิทธิ

๑.๒.๒. กำหนดเกณฑ์การบริหารจัดการสิทธิกำหนดไว้ ดังนี้

(๑) จัดทำแบบฟอร์มลงทะเบียนผู้ใช้งานระบบสารสนเทศเพื่อตรวจสอบสิทธิ และดำเนินการตามขั้นตอน

(๒) การลงทะเบียนผู้ใช้งาน

(๓) ต้องจัดทำเอกสารแสดงถึงสิทธิ และความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๔) ต้องบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๕) กำหนดหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

(๕.๑.) ต้องเป็นนักศึกษา บุคลากรของสถาบัน หรือบุคคลภายนอกที่ได้รับอนุญาตให้ใช้สินทรัพย์สารสนเทศของสถาบัน และยังไม่สิ้นสุดสถานภาพการเป็นผู้ใช้งาน

(๕.๒.) ผู้ใช้งานต้องได้รับอนุญาตจากเจ้าของข้อมูล และได้รับมอบหมายจากผู้บังคับบัญชา

(๕.๓.) ได้รับการอนุมัติจากผู้อำนวยการสำนัก หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๖) กำหนดหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศ ได้แก่

(๖.๑.) การตัดออกจากทะเบียน การโยกย้ายหน่วยงาน การระงับการปฏิบัติงาน หรือเมื่อสิ้นสุดสถานภาพการเป็นผู้ใช้งาน

(๖.๒.) การใช้งานที่ขัดต่อข้อกำหนดการใช้งานระบบสารสนเทศ

(๗) บริหารจัดการสิทธิของผู้ใช้งาน โดยแสดงรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึง และใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ ดังนี้

(๗.๑.) ต้องมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งานที่เหมาะสมต่อสถานภาพการเป็นผู้ใช้งานหรือตามหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งาน

(๗.๒.) ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ หรือตามความจำเป็นในการใช้งาน

(๗.๓.) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

(๘) ต้องมีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน

(๙) การทบทวนสิทธิในการเข้าถึงระบบของผู้ใช้งาน ผู้ดูแลระบบต้องทบทวนสิทธิในการเข้าถึงระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๑๐) ต้องจัดการฝึกอบรมเกี่ยวกับการสร้างความรู้ความเข้าใจถึงภัยและผลกระทบที่เกิดขึ้นจากการใช้งานระบบสารสนเทศ และความตระหนักเรื่องความมั่นคงปลอดภัย และกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๑.๒.๓. ผู้ใช้งานที่ต้องการเข้าใช้ระบบสารสนเทศของสถาบันจะต้องได้รับการอนุญาตเป็นลายลักษณ์อักษรจากผู้อำนวยการสำนักหรือผู้ที่ได้รับมอบหมาย

๑.๓. การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลให้ใช้แนวทางตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ โดยกำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ ดังนี้

๑.๓.๑. การจัดแบ่งประเภทของข้อมูล ดังนี้

(๑) ข้อมูลทั่วไปที่เปิดเผยได้

(๒) ข้อมูลเฉพาะที่ต้องกำหนดสิทธิ ได้แก่

(๒.๑.) ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลด้านการเงิน ข้อมูลนักศึกษา

(๒.๒.) ข้อมูลสารสนเทศตามพันธกิจ ได้แก่ ข้อมูลด้านการเรียนการสอน ข้อมูลด้านการวิจัย ข้อมูลด้านบริการวิชาการ

(๒.๓.) ข้อมูลสารสนเทศสนับสนุนการปฏิบัติงาน ได้แก่ ข้อมูลด้านทรัพยากรด้านสถานที่และสิ่งอำนวยความสะดวก

๑.๓.๒. การจัดแบ่งระดับความสำคัญของข้อมูล ดังนี้

(๑) ข้อมูลที่มีระดับความสำคัญมากที่สุด คือ ข้อมูลที่มีผลกระทบในระดับที่มีนัยสำคัญต่อการดำเนินงานของสถาบันและการดำรงอยู่ของหน่วยงาน ได้แก่ ข้อมูลนักศึกษา ข้อมูลการเงิน

(๒) ข้อมูลที่มีระดับความสำคัญมาก คือ ข้อมูลที่มีผลกระทบในระดับที่มีนัยสำคัญต่อการดำเนินงานของสถาบัน ได้แก่ ข้อมูลยุทธศาสตร์ ข้อมูลนโยบาย

(๓) ข้อมูลที่มีระดับความสำคัญปานกลาง คือ ข้อมูลที่มีผลกระทบในระดับที่ไม่มีนัยสำคัญต่อการดำเนินงานของสถาบัน

(๔) ข้อมูลที่มีระดับความสำคัญน้อย คือ ข้อมูลที่ไม่มีผลกระทบต่อการดำเนินงานของสถาบัน

๑.๓.๓. การจัดแบ่งลำดับชั้นความลับของข้อมูล ดังนี้

(๑) ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายกับสถาบันอย่างร้ายแรงที่สุด

(๒) ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายกับสถาบันอย่างร้ายแรง

(๓) ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายกับสถาบัน

(๔) ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

๑.๓.๔. การจัดแบ่งระดับชั้นการเข้าถึง ดังนี้

(๑) เข้าถึงได้ทุกกลุ่มผู้ใช้งาน

(๒) เข้าถึงได้เฉพาะกลุ่มผู้ใช้งานที่ได้รับสิทธิ

(๓) เข้าถึงได้เฉพาะกลุ่มผู้มีสิทธิในการบริหารจัดการระบบสารสนเทศ

๑.๓.๕. กำหนดเวลาที่สามารถเข้าถึงข้อมูลสารสนเทศ และระบบสารสนเทศได้ ดังนี้

(๑) ตลอดเวลา

(๒) เวลาราชการ

(๓) นอกเวลาราชการ

(๔) วันหยุดราชการและวันหยุดนักขัตฤกษ์

(๕) ช่วงเวลาพิเศษเป็นรายครั้ง

๑.๓.๖. ต้องกำหนดจำนวนช่องทางที่สามารถเข้าถึง

(๑) ผู้ใช้งานเข้าใช้บริการผ่านระบบเครือข่ายของสถาบันได้ตลอด 24 ชั่วโมง

(๒) ผู้ใช้งานเข้าใช้บริการผ่านระบบเครือข่ายอินเทอร์เน็ตภายนอกสถาบัน ใช้ผ่านระบบ VPN ได้ตลอด 24 ชั่วโมง

๒. ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

ข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศแบ่งเป็น ๒ ส่วนคือ การควบคุมการเข้าถึงสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๑. การควบคุมการเข้าถึงสารสนเทศ

๒.๑.๑. กำหนดแนวทางการควบคุมการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศ ตามสถานะของผู้ใช้งาน ดังนี้

(๑) สำหรับนักศึกษา เป็นนักศึกษาที่ได้ลงทะเบียนเรียนจนจบการศึกษา หรือพ้นสภาพนักศึกษา หรือศิษย์เก่า

(๒) สำหรับบุคลากร เป็นบุคลากรที่ได้รายงานตัวหรือได้รับมอบหมายหน้าที่รับผิดชอบ จนกระทั่งได้รับการอนุมัติการลาออก หรือพ้นสภาพการเป็นบุคลากรของสถาบัน

(๓) สำหรับผู้มีส่วนเกี่ยวข้อง (Stakeholder) ได้แก่ ร้านค้า ผู้รับเหมา (Vendor) หรือผู้มีส่วนเกี่ยวข้องอื่น ๆ ตามช่วงเวลาที่มาปฏิบัติงานและได้ขออนุญาตไว้เป็นลายลักษณ์อักษร

(๔) สำหรับผู้เข้ารับการอบรม ในช่วงเวลาที่เข้ารับการอบรม โดยผู้จัดการอบรมจะต้องขออนุญาตไว้เป็นลายลักษณ์อักษรเพื่อเข้าใช้งาน

๒.๑.๒. ต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๒.๑.๓. ต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๒.๑.๔. ต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

๒.๒. การปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒.๒.๑. หากจำเป็นต้องมีการเข้าถึงสารสนเทศเกินสิทธิที่ได้รับเพื่อให้บรรลุงานตามภารกิจ ให้ผู้ใช้งานเขียนคำร้องเพื่อให้ผู้ดูแลระบบสร้างบัญชีผู้ใช้งาน (User Account) เป็นกรณีพิเศษ และต้องกำหนดระยะเวลาในการใช้งานของบัญชีผู้ใช้งานที่สร้างขึ้นใหม่ด้วย

๒.๒.๒. ผู้ดูแลระบบต้องประสานงานกับกองบริหารทรัพยากรบุคคลหรือหน่วยงานต้นสังกัด เพื่อแก้ไขปรับปรุง เพิ่ม ยกเลิก บัญชีผู้ใช้งาน เมื่อมีการปรับเปลี่ยนตำแหน่ง ลาออก เพิ่มบุคลากร เพื่อปรับปรุงสิทธิการเข้าถึงของบัญชีผู้ใช้งาน

๒.๒.๓. ในเรื่องของการปรับปรุงข้อกำหนดในการใช้งาน ให้มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจ และข้อกำหนดด้านความมั่นคงปลอดภัย

๓. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

เพื่อกำหนดเป็นมาตรการการเข้าถึงระบบสารสนเทศของผู้ใช้งาน มิให้บุคคลที่ไม่มีหน้าที่ที่เกี่ยวข้องในการทำงานเข้าถึงระบบสารสนเทศและเครือข่ายภายในโดยไม่ได้รับอนุญาต รวมทั้งจำกัดสิทธิในการใช้งานระบบสารสนเทศ เพื่อให้สามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบสารสนเทศของสถาบัน โดยกำหนดแนวปฏิบัติในการควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาต และสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ ดังนี้

๓.๑. การสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ

ต้องดำเนินการตามข้อปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในภาคผนวก

๓.๒. การแบ่งกลุ่มบัญชีผู้ใช้

เพื่อควบคุมการเข้าถึงและใช้งานสารสนเทศและระบบสารสนเทศโดยระบุชื่อบัญชีผู้ใช้งานแยกกันแบบรายบุคคล ไม่ซ้ำซ้อนกัน ดังนี้

๓.๒.๑. นักศึกษา

๓.๒.๒. บุคลากร

๓.๒.๓. อาจารย์พิเศษ นักวิจัย กรรมการ ที่ปรึกษา

๓.๒.๔. บุคคลภายนอกที่เข้าอบรมหรือสัมมนา

๓.๒.๕. บุคคลอื่น ๆ ที่สถาบันมอบสิทธิให้

๓.๓. การลงทะเบียนผู้ใช้งาน (User Registration)

ต้องดำเนินการตามข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน ในภาคผนวก

๓.๔. การบริหารจัดการสิทธิของผู้ใช้งาน (User Management)

ต้องดำเนินการตามข้อปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน ในภาคผนวก โดยมีรายละเอียดที่เกี่ยวกับการควบคุมและจำกัดสิทธิ เพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิพิเศษ และสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

๓.๔.๑. ผู้ใช้งานที่มีชื่ออยู่ในบัญชีรายชื่อผู้ใช้งานมีสิทธิทั่วไปในการเข้าถึงระบบสารสนเทศพื้นฐานตามกลุ่มผู้ใช้งาน

๓.๔.๒. ให้หน่วยงานเจ้าของระบบเป็นผู้กำหนดสิทธิจำเพาะหรือสิทธิพิเศษรวมถึงกำหนดระยะเวลาในการใช้งาน

๓.๔.๓. การแจ้งขอใช้สิทธิ/เปลี่ยนแปลงสิทธิในการเข้าถึงและใช้งานข้อมูลสารสนเทศและระบบสารสนเทศจะต้องจัดทำเป็นลายลักษณ์อักษร

(๑) ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้

(๒) ส่งถึงผู้บริหารของหน่วยงานเจ้าของระบบ

(๓) เก็บเอกสารไว้เป็นหลักฐานอ้างอิงทั้งฝ่ายผู้ขอและผู้อนุญาต

(๔) หน่วยงานเจ้าของระบบส่งเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

๓.๔.๔. การให้สิทธิพิเศษกับผู้ใช้งาน ต้องได้รับความเห็นชอบจากอธิการบดีหรือผู้ที่ได้รับมอบหมายจากอธิการบดี

๓.๔.๕. การแจ้งยกเลิกสิทธิการใช้งานระบบสารสนเทศ

(๑) ผู้บริหารของหน่วยงานที่ขอใช้แจ้งยกเลิกสิทธิของผู้ใช้

(๒) ผู้ดูแลระบบทำการยกเลิกสิทธิในการใช้งานระบบตามคำขอและลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๓.๔.๖. ผู้ดูแลระบบต้องทำการเพิกถอนหรือเปลี่ยนแปลงสิทธิการเข้าถึงและใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน หรือพ้นสภาพการเป็นนักศึกษาหรือบุคลากร หรือเมื่อผู้ใช้งานสิ้นสุดสภาพการใช้งาน

๓.๕. การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

๓.๕.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ เข้าด้วยกัน

๓.๕.๒. ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นทราบ

๓.๕.๓. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๓.๕.๔. ผู้ดูแลระบบต้องกำหนดการใช้งานบัญชีผู้ใช้งานและรหัสผ่านกำหนดรหัสผ่านเริ่มต้นแยกเป็นรายบุคคล ให้กับผู้ใช้ให้ยากต่อการเดา เพื่อให้สามารถติดตามการใช้งานและกำหนดเป็นความรับผิดชอบของแต่ละคนได้

๓.๕.๕. ผู้ดูแลระบบต้องส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานภายในสถาบันด้วยวิธีการที่ปลอดภัย และผู้ใช้งานต้องทำการเปลี่ยนรหัสผ่านทันทีเมื่อเข้าใช้งานระบบงานครั้งแรก

๓.๕.๖. เพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่าน ผู้ใช้งานต้องทำความเข้าใจและยอมรับสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งาน

๓.๕.๗. ผู้ใช้งานต้องทำการยืนยันตัวตน ที่ถูกต้อง ก่อนเปลี่ยนรหัสผ่าน

๓.๕.๘. ข้อมูลรหัสผ่านของผู้ใช้งานบนหน้าจอในระหว่างที่ผู้ใช้งานนั้นกำลังใส่ข้อมูลให้แสดงเป็นเครื่องหมายดอกจัน (*) บนหน้าจอ หรือเครื่องหมายอื่นที่ทำให้ข้อมูลเป็นความลับ

๓.๕.๙. ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชาของหน่วยงานเจ้าของระบบ โดยต้องกำหนดระยะเวลาใช้งาน และระงับการใช้งานทันทีเมื่อพ้นระยะเวลาสิทธิพิเศษที่ได้รับ

๓.๖. การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights)

ผู้ดูแลระบบหรือเจ้าของระบบต้องมีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศ และทบทวนสิทธิของผู้ใช้งานที่มีการเปลี่ยนแปลงสถานภาพ ได้แก่ การเปลี่ยนตำแหน่ง ย้ายหน่วยงาน หรือสิ้นสุดการจ้างงาน ดังนี้

๓.๖.๑. สิทธิการเข้าถึงข้อมูลของผู้ใช้งานต้องได้รับการพิจารณาทบทวนทุกครั้งที่มีการปรับเปลี่ยนสถานะ ได้แก่ การย้ายหน่วยงาน การเลื่อนตำแหน่ง การเปลี่ยนหน้าที่รับผิดชอบ หรือการยกเลิกการจ้าง

๓.๖.๒. สิทธิการเข้าถึงข้อมูลต้องได้รับการทบทวนและจัดสรรใหม่เมื่อมีการโยกย้ายบุคลากรระหว่างหน่วยงาน

๓.๖.๓. สิทธิการเข้าถึงพิเศษต้องได้รับการพิจารณาทบทวนตามระยะเวลาที่ได้รับอนุมัติการใช้งานและหรือทุกครั้งที่มีการปรับเปลี่ยนสิทธิการใช้งาน เพื่อให้มั่นใจได้ว่าไม่มีการได้สิทธิพิเศษกับผู้ใช้งานที่ไม่ได้รับมอบอำนาจ

๓.๖.๔. ต้องมีการทบทวนอย่างน้อย ปีละ ๑ ครั้ง

(๑) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานที่ได้รับสิทธิทั่วไปและผู้ใช้งานที่ได้รับสิทธิพิเศษ อย่างน้อยปีละ ๑ ครั้ง

(๒) ต้องทบทวนสิทธิการเข้าถึงของผู้ใช้งานที่มีสิทธิระดับผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้ง

(๓) สิทธิการเข้าถึงการใช้งานสำหรับผู้ใช้งาน หมดอายุเมื่อผู้ใช้งานพ้นสภาพหรือผู้ใช้งานที่ได้รับสิทธิพิเศษไม่มีการใช้งานติดต่อกันเกิน ๑ปี

๓.๖.๕. บันทึกการเปลี่ยนแปลงสิทธิของผู้ใช้งานทุกครั้ง เพื่อใช้ในการทบทวนสิทธิการเข้าถึงผู้ใช้งานประจำปี

๔. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๔.๑. การใช้งานรหัสผ่าน (Password Use)

ผู้ใช้งานต้องดำเนินการตามข้อปฏิบัติการใช้งานรหัสผ่าน ในภาคผนวก

๔.๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์

๔.๒.๑. ต้องมีการป้องกันการเข้าถึงอุปกรณ์จากผู้ที่ไม่มีสิทธิ โดยการล็อคหน้าจอด้วยรหัสผ่านเพื่อไม่ให้บุคคลอื่นเข้าถึงอุปกรณ์ได้โดยง่าย

๔.๒.๒. ต้องทำการใส่รหัสผ่านให้ถูกต้องเพื่อปลดล็อกหน้าจอ หากอุปกรณ์นั้นไม่ได้ใช้งานเป็นระยะเวลา ๓๐ นาที

๔.๒.๓. ต้องออกจากระบบ (Logout) ทันทีเมื่อเสร็จสิ้นการทำงาน

๔.๓. การควบคุมสินทรัพย์ด้านสารสนเทศและการใช้งานระบบคอมพิวเตอร์

๔.๓.๑. จัดเก็บเอกสารและสื่อบันทึกข้อมูลที่มีข้อมูลสารสนเทศสำคัญมากหรือเป็นความลับ ไว้ในตู้เซฟหรือสถานที่ที่มีการป้องกันและมีความปลอดภัย

๔.๓.๒. การเข้าถึงข้อมูล สื่อบันทึกข้อมูล หรือสินทรัพย์ด้านสารสนเทศ ต้องเป็นผู้เป็นเจ้าของหรือผู้ได้รับมอบหมาย ผู้ได้รับสิทธิเป็นลายลักษณ์อักษรเท่านั้น

๔.๓.๓. มีกลไกการยืนยันตัวตน ก่อนเข้าใช้งานเครื่องคอมพิวเตอร์หรือระบบสารสนเทศของสถาบัน โดยบัญชีผู้ใช้งาน หรือการใช้อุปกรณ์สร้างรหัสผ่าน (Token) เป็นต้น

๔.๓.๔. ต้องมีมาตรการหรือเทคนิคในการป้องกันข้อมูลที่มีความสำคัญก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานหรือเผยแพร่ต่อ

๔.๓.๕. สำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อนส่งเครื่องคอมพิวเตอร์หรืออุปกรณ์ไปตรวจซ่อม เพื่อป้องกันการสูญหายหรือการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๔.๓.๖. โปรแกรมต่าง ๆ ที่ติดตั้งบนเครื่องคอมพิวเตอร์ของสถาบัน เป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้นห้ามผู้ใช้งานคัดลอกโปรแกรมและนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว แก้ไข หรือนำไปให้ผู้อื่นใช้งานเพราะเป็นการกระทำที่ผิดกฎหมาย

๔.๓.๗. ไม่เก็บข้อมูลสำคัญของสถาบันไว้บนเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลที่เป็นสมบัติส่วนบุคคล

๔.๓.๘. เอกสารสำคัญหรือเป็นความลับต้องขออนุมัติจากผู้บังคับบัญชาทุกครั้งเมื่อมีการนำออกจากหน่วยงานหรือสถาบัน

๔.๓.๙. ตู้หรือจุดบริการที่ใช้รับส่งเอกสารไปรษณีย์ รวมถึงเครื่องโทรสาร จะต้องมีการป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตหรือไม่มีสิทธิ สามารถเข้าถึงหรือใช้งานได้

๔.๓.๑๐. ต้องมีการควบคุมและป้องกันจากผู้ไม่ได้รับอนุญาตในการใช้งานอุปกรณ์ถ่ายภาพ หรืออุปกรณ์ทำสำเนา ได้แก่ กล้องถ่ายภาพ เครื่องสแกนเอกสาร และเครื่องสำเนาเอกสาร เป็นต้น เพื่อป้องกันไม่ให้มีการทำสำเนาข้อมูลสารสนเทศที่สำคัญ

๔.๓.๑๑. เอกสารสำคัญหรือเป็นความลับซึ่งได้รับการพิมพ์ออกมาจากเครื่องพิมพ์ จะต้องถูกเก็บออกจากเครื่องพิมพ์ทันทีเมื่อมีการพิมพ์แล้วเสร็จ

๔.๓.๑๒. เมื่อมีความจำเป็นต้องทำลายข้อมูลลับบนสื่อบันทึกข้อมูล ให้ปฏิบัติตามข้อปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล ในภาคผนวก

๔.๔. การใช้การเข้ารหัสลับกับข้อมูลที่เป็นความลับ

ผู้ดูแลระบบหรือเจ้าของระบบนำการเข้ารหัสลับ มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๔.๔.๑. การเข้ารหัสลับจะนำมาใช้กับข้อมูลที่เป็นความลับ หรือมีความสำคัญมาก ได้แก่ ข้อมูลนักศึกษา ข้อมูลการเงิน ข้อมูลยุทธศาสตร์ ข้อมูลนโยบาย

๔.๔.๒. การเข้ารหัสลับที่ใช้กับข้อมูลที่เป็นความลับ หรือมีความสำคัญมาก ต้องเข้ารหัสด้วยขั้นตอนวิธี (Algorithm) ที่มีความเป็นมาตรฐานสากล ได้แก่ TLS, AES

๔.๕. การใช้งานบริการเครือข่ายให้ผู้ใช้งานปฏิบัติตามข้อปฏิบัติการใช้งานบริการเครือข่าย ในภาคผนวก

๔.๖. การใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ผู้ใช้งานปฏิบัติตามข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ ในภาคผนวก

๔.๗. การระงับบัญชีจดหมายอิเล็กทรอนิกส์

๔.๗.๑. บัญชีจดหมายอิเล็กทรอนิกส์เป็นสิทธิพิเศษเฉพาะ (Privilege) ที่สถาบันเอื้ออำนวยให้ผู้ใช้ซึ่งผู้ใช้ไม่สามารถโอนสิทธิให้แก่ผู้อื่นใช้ได้ สถาบันคงไว้ซึ่งอำนาจในการจำกัด ระงับ หรือเพิกถอนสิทธิให้แก่ผู้ใช้โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า หากได้รับแจ้งหรือตรวจพบการกระทำใดที่ขัดกับนโยบายหรืออาจก่อให้เกิดปัญหา ความมั่นคงปลอดภัย หรือเสถียรภาพของระบบ หรือการกระทำที่ขัดต่อนโยบายหรือกฎหมายแห่งรัฐ การระงับใช้บัญชีจดหมายอิเล็กทรอนิกส์

๔.๗.๒. เมื่อผู้ใช้พ้นสภาพการเป็นบุคลากรของสถาบัน บัญชีจดหมายอิเล็กทรอนิกส์นั้นจะถูกระงับไป

๔.๗.๓. ผู้ใช้ที่พ้นสภาพการเป็นบุคลากรของสถาบัน สามารถร้องขอการขยายสิทธิการใช้บัญชีผู้ใช้เพื่อคงสิทธิการใช้บัญชีจดหมายอิเล็กทรอนิกส์เดิมไว้ โดยยื่นคำร้องผ่านผู้บริหารต้นสังกัด พร้อมแนบเหตุผลความจำเป็นส่งถึงสำนักเทคโนโลยีสารสนเทศ การอนุญาตและระยะเวลาการขยายสิทธิให้เป็นอำนาจของผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๔.๗.๔. บัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ของผู้ใช้ สามารถถูกระงับการใช้งาน โดยคำร้องขอจากผู้บริหารของหน่วยงาน หากพบว่ามีการใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ใช้ในสังกัดของหน่วยงานที่ขัดกับนโยบายฉบับนี้

๔.๗.๕. บัญชีของผู้ใช้จดหมายอิเล็กทรอนิกส์ สามารถถูกระงับการใช้งานโดยทันทีโดยผู้ดูแลระบบ หากตรวจพบว่ามีการใช้งานที่ส่งผลกระทบต่อการให้บริการระบบเครือข่ายมีประสิทธิภาพด้อยลง หรือขัดต่อนโยบาย ไม่ว่าจะเป็นการใช้โดยผู้ใช้หรือการลักลอบเข้าใช้โดยผู้อื่น ทั้งนี้สำนักเทคโนโลยีสารสนเทศมีสิทธิระงับการใช้บัญชีจดหมายอิเล็กทรอนิกส์นั้น ๆ โดยไม่ต้องแจ้งให้ผู้ใช้ทราบล่วงหน้า

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต โดยให้ปฏิบัติ ดังนี้

๕.๑. ผู้ดูแลระบบต้องออกแบบและแบ่งแยกระบบเครือข่าย ตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ โดยประกอบด้วย โซนภายใน (Internal Zone) โซนภายนอก (External Zone) เพื่อให้การบริหารจัดการและควบคุมเป็นระบบ และป้องกันการบุกรุกได้อย่างมีประสิทธิภาพ

๕.๒. การยืนยันตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกสถาบัน ผู้ดูแลระบบต้องกำหนดให้มีการยืนยันตัวตนก่อนที่จะอนุญาตให้ผู้ใช้ที่อยู่ภายนอกสถาบันสามารถเข้าใช้งานเครือข่าย และระบบสารสนเทศของสถาบัน ได้แก่

๕.๒.๑. การยืนยันตัวตน ด้วยชื่อผู้ใช้งาน (Username)

๕.๒.๒. การยืนยันตัวตน ด้วยการใช้รหัสผ่าน (Password)

๕.๒.๓. การเข้าสู่ระบบสารสนเทศของสถาบัน จะต้องมีการตรวจสอบผู้ใช้งานอีกครั้ง

๕.๒.๔. การเข้าสู่ระบบจากระยะไกล เพื่อเพิ่มความปลอดภัยของการรับส่งข้อมูล ต้องมีการใช้การเข้ารหัสลับ ได้แก่ SSL, TLS

๕.๓. การใช้งานเครือข่ายจากแหล่ง หรือสถานที่ที่ได้รับอนุญาต ผู้ดูแลระบบต้องจัดทำกระบวนการยืนยันตัวตนในการเชื่อมต่อระหว่างเครือข่ายของสถาบันและเครือข่ายภายนอกว่ามาจากแหล่งหรือสถานที่ที่ได้รับอนุญาตเท่านั้น

๕.๔. ความมั่นคงปลอดภัยสำหรับการใช้บริการเครือข่าย ผู้ดูแลระบบต้องจัดทำข้อกำหนดหรือข้อตกลงสำหรับคุณสมบัติด้านความมั่นคงปลอดภัยของบริการเครือข่ายแต่ละประเภทที่ใช้งานร่วมกันระหว่างสถาบันกับหน่วยงานภายนอก

๕.๕. การควบคุมผู้ใช้งานในการใช้งานเครือข่าย ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งาน เพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น ได้แก่

๕.๕.๑. ใช้ Monitoring Tool เพื่อตรวจสอบการเชื่อมต่อทางระบบเครือข่าย

๕.๕.๒. มีระบบการตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องแม่ข่าย

๕.๕.๓. ควบคุมไม่ให้มีการเปิดให้บริการบนระบบเครือข่ายโดยไม่ได้รับอนุญาต

๕.๖. การจำกัดเส้นทางการเข้าถึงเครือข่ายที่ใช้งานร่วมกัน ผู้ดูแลระบบต้องกำหนดตารางของการใช้เส้นทางบนระบบเครือข่าย (Network routing Control) บนอุปกรณ์จัดเส้นทาง (Router) หรืออุปกรณ์กระจายสัญญาณ เพื่อควบคุมผู้ใช้งานเฉพาะเส้นทางที่ได้รับอนุญาต ดังนี้

๕.๖.๑. ควบคุมไม่ให้มีการเปิดเผยการใช้หมายเลขเครือข่าย (IP Address) ของหน่วยงาน

๕.๖.๒. กำหนดให้มีการแปลงหมายเลขเครือข่ายและชื่อโดเมน เพื่อแยกเครือข่ายย่อยหรือเครือข่ายภายในและภายนอก

๕.๖.๓. กำหนดให้มีการแปลงหมายเลขเครือข่ายย่อย

๕.๖.๔. กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย หรือจำกัดสิทธิในการใช้บริการเครือข่ายของหน่วยงาน

๕.๖.๕. จำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องแม่ข่าย เพื่อไม่อนุญาตให้ผู้ใช้บริการสามารถใช้เส้นทางอื่น ๆ ได้ นอกจากเส้นทางที่ได้กำหนดไว้ให้เท่านั้น

๕.๖.๖. กำหนดมาตรการการบังคับใช้เส้นทางเครือข่าย ให้สามารถเชื่อมต่อเครือข่ายปลายทางผ่านช่องทางที่กำหนดไว้ หรือจำกัดสิทธิในการเข้าใช้บริการระบบเครือข่ายของสถาบัน

๕.๗. ผู้ดูแลระบบต้องกำหนด IP Address ให้กับอุปกรณ์ที่เชื่อมต่อเครือข่ายเพื่อให้สามารถระบุถึงอุปกรณ์เครือข่ายได้อย่างถูกต้อง ในกรณีที่ไม่สามารถใช้ IP Address ระบุถึงอุปกรณ์ได้ กำหนดให้ผู้ใช้งานต้องลงทะเบียน MAC address อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่าย เพื่อให้สามารถระบุอุปกรณ์เครือข่ายตัวนั้นได้อย่างถูกต้อง

๕.๘. ผู้ดูแลระบบจะต้องทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ ทั้งการเข้าถึงทางกายภาพและผ่านทางเครือข่าย ได้แก่

๕.๘.๑. ต้องตรวจสอบ และปิดพอร์ตที่ไม่มีการใช้งานอยู่เสมอ

๕.๘.๒. ต้องควบคุมการเข้าถึงระบบผ่านอุปกรณ์ป้องกันการบุกรุก (firewall) ของระบบเครือข่าย

๕.๘.๓. การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผ่านช่องทางที่สำนักเทคโนโลยีสารสนเทศจัดเตรียมไว้ให้

๕.๘.๔. ควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับการวิเคราะห์ปัญหาและการตั้งค่าระบบทางกายภาพ โดยให้ใช้การล็อกอินเข้ามาใช้งาน

๕.๘.๕. บันทึกการเข้า-ออกพื้นที่บริเวณศูนย์ข้อมูลหลัก (Data Center) ได้แก่ เจ้าหน้าที่ผู้รับผิดชอบที่เกี่ยวข้อง และ เจ้าหน้าที่ผู้ดูแลระบบ เป็นต้น

๕.๘.๖. ห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง เข้าไปในศูนย์ข้อมูลหลัก (Data Center) หากจำเป็นให้เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบนำพาเข้าไป

๕.๘.๗. ติดตั้งเครื่องควบคุมบันทึกการเข้าออกห้องศูนย์ข้อมูลหลัก (Data Center) ที่ประตูเข้าออกและติดตั้งกล้องโทรทัศน์วงจรปิดกันการโจรกรรม

๕.๙. การขอใช้งานพอร์ตดังกล่าวต้องได้รับอนุญาตจากผู้อำนวยการสำนัก หรือผ่านช่องทางที่สำนักจัดเตรียมไว้ให้

๕.๑๐. ต้องเก็บอุปกรณ์ที่เชื่อมต่อเครือข่ายไว้ในห้องที่มีการควบคุมการเข้าถึง และจะเข้าได้เฉพาะผู้ที่ได้รับอนุญาตเท่านั้น หรือล็อกกุญแจเพื่อป้องกันการเชื่อมต่อโดยไม่ได้รับอนุญาต

๕.๑๑. ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

เพื่อให้ผู้ใช้งานได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบปฏิบัติการ รวมทั้งทำความเข้าใจตลอดจนปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพยากรและข้อมูลของหน่วยงานให้มีความลับความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ โดยให้ปฏิบัติ ดังนี้

๖.๑. กำหนดขั้นตอนการปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัยสำหรับระบบที่มีความความสำคัญสูงหรือมีความเสี่ยงสูง หมายถึง การล็อคอินเข้าสู่ระบบปฏิบัติการเครื่องคอมพิวเตอร์แม่ข่ายต่าง ๆ ทั้งหมด

๖.๒. การเข้าถึงระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของผู้ใช้งานทั่วไป จะต้องควบคุมโดยวิธียืนยันตัวตนด้วยบัญชีผู้ใช้งานและรหัสผ่าน และจำกัดการเข้าถึงระบบปฏิบัติการเฉพาะอินทราเน็ต

๖.๓. ผู้ดูแลระบบต้องกำหนดให้มีการระบุและยืนยันตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งาน

๖.๓.๑. ผู้ใช้งานต้องลงบันทึกเข้า (Login) สำหรับเครื่องคอมพิวเตอร์ โดยใช้ชื่อบัญชีผู้ใช้ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๖.๓.๒. ผู้ใช้งานที่เป็นเจ้าของบัญชีผู้ใช้บริการ ต้องเป็นผู้รับผิดชอบในผลต่าง ๆ อันเกิดจากการใช้ชื่อบัญชีผู้ใช้ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๖.๔. การบริหารจัดการรหัสผ่าน ผู้ดูแลระบบต้องจัดให้มีระบบหรือวิธีการในการตรวจสอบคุณภาพของรหัสผ่านและมีวิธีการควบคุมดูแลให้ผู้ใช้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนด ได้แก่

๖.๔.๑. กำหนดให้รหัสผ่านต้องมีมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยผสมชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ เข้าด้วยกัน

๖.๔.๒. ต้องให้ผู้ใช้งานลงนามเพื่อเก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับและไม่เปิดเผยให้ผู้อื่นทราบ

๖.๔.๓. กำหนดรหัสผ่านชั่วคราวให้กับผู้ใช้ให้ยากต่อการเดา

๖.๔.๔. ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย หลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

๖.๔.๕. ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว

๖.๔.๖. ควรมีการแจ้งเตือนให้ผู้ใช้งานเปลี่ยนรหัสผ่าน ๑ สัปดาห์ ก่อนถึงรอบระยะเวลาการเปลี่ยนรหัสผ่านที่กำหนดไว้

๖.๔.๗. ระบบมีการแจ้งเตือนเมื่อผู้ใช้งานกรอกรหัสผ่านผิด และจะระงับการเข้าถึงระบบทันที เมื่อกรอกรหัสผ่านผิดเกิน ๓ ครั้ง โดยผู้ใช้งานต้องแจ้งผู้ดูแลระบบเพื่อทำการยกเลิกการระงับ

๖.๕. ผู้ใช้งานต้องมีวิธีการตัดเวลาการใช้งานเครื่องคอมพิวเตอร์ เมื่อเครื่องคอมพิวเตอร์ นั้นไม่ได้ใช้งานเป็นระยะเวลาหนึ่ง ได้แก่ การล็อคหน้าจอ และการใช้รหัสผ่านในการเข้าสู่ระบบปฏิบัติการ เป็นต้น

๖.๖. การใช้งานโปรแกรมอรรถประโยชน์ (Use of System Utilities)

ผู้ดูแลระบบต้องแนะนำผู้ใช้งานให้จำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมอรรถประโยชน์บางชนิดสามารถทำให้ผู้ใช้งานไม่ปลอดภัย โดยให้ปฏิบัติตามข้อปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์ ในภาคผนวก

๖.๗. การหมดเวลาใช้งานระบบ (Session Time-Out)

ผู้ดูแลระบบต้องให้ผู้ใช้งานยุติการใช้งานระบบ (Session Time-Out) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่ง โดยให้ปฏิบัติ ดังนี้

๖.๗.๑. ให้ยุติการใช้งานระบบเมื่อว่างเว้นจากการใช้งานเกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงหรือความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานให้สั้นลง ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

๖.๗.๒. ถ้าไม่มีการใช้งานระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

๖.๗.๓. เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องมีการกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามที่กำหนด

๖.๘. การจำกัดระยะเวลาการเชื่อมต่อระบบ (Limitation of Connection Time)

ผู้ดูแลระบบต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากขึ้น สำหรับระบบ หรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง โดยให้ปฏิบัติ ดังนี้

๖.๘.๑. ต้องจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศหรือแอปพลิเคชันที่มีความเสี่ยง หรือมีความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุด โดยการเชื่อมต่อหนึ่งครั้งอนุญาตให้ใช้งานไม่เกิน ๔ ชั่วโมง

๖.๘.๒. ต้องพิสูจน์ตัวตนเพื่อเข้าใช้งานระบบสารสนเทศอีกครั้งหลังจากที่ระบบได้ตัดการใช้งานนั้นไปแล้ว

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

๗.๑. การจำกัดการเข้าถึงสารสนเทศ (Information Access Restriction)

ผู้ดูแลระบบต้องจำกัดหรือควบคุมผู้ใช้งานในการเข้าถึงหรือเข้าใช้งานระบบสารสนเทศและฟังก์ชันต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชัน โดยให้กำหนดหลักเกณฑ์ในการจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานที่สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศ

๗.๑.๑. ต้องจำกัดหรือควบคุมผู้ใช้งาน ในการเข้าถึงระบบสารสนเทศและฟังก์ชันต่าง ๆ ตามข้อกำหนดการบริหารจัดการสิทธิของผู้ใช้งาน

๗.๑.๒. ต้องมีการยืนยันตัวตน ก่อนการเข้าใช้งานโปรแกรมประยุกต์และระบบสารสนเทศ

๗.๑.๓. ต้องควบคุมหรือจำกัดสิทธิผู้ใช้งานในการเข้าถึงระบบซึ่งถูกเข้าถึงจากอีกระบบหนึ่ง

๗.๑.๔. ต้องควบคุมหรือจำกัดการนำข้อมูลเฉพาะที่เกี่ยวข้องและจำเป็นสำหรับการนำไปใช้งานออกจากระบบ

๗.๑.๕. ต้องแสดงเฉพาะข้อมูลพื้นฐานเพื่อให้ผู้ใช้งานได้รับทราบเท่าที่จำเป็นเท่านั้น

๗.๑.๖. ต้องแสดงรายละเอียดเท่าที่จำเป็นของระบบหลังจากที่ผู้ใช้งานล็อกอินเสร็จแล้ว

๗.๑.๗. ต้องแสดงข้อความเตือนห้ามผู้ไม่มีสิทธิเข้าถึงระบบ

๗.๑.๘. ต้องจำกัดไม่ให้ระบบแสดงความช่วยเหลือใด ๆ กรณีมีเหตุการณ์ไม่พึงประสงค์เกิดขึ้นกับระบบ

๗.๑.๙. ต้องตรวจสอบข้อมูลการล็อกอินหลังจากที่ผู้ใช้งานใส่ข้อมูลทั้งหมดครบถ้วนแล้ว

๗.๑.๑๐. ต้องจำกัดไม่ให้ระบบแสดงข้อความผิดพลาดจากการทำงานหรือการใช้งานในลักษณะที่เปิดเผยข้อมูลภายในของระบบ

๗.๑.๑๑. ต้องจำกัดจำนวนครั้งที่ผู้ใช้งานสามารถใส่ข้อมูลการล็อกอินผิด

๗.๑.๑๒. ต้องกำหนดการหน่วงระยะเวลาที่ผู้ใช้งานสามารถเชื่อมโยงกลับเข้ามายังระบบได้ภายหลังจากที่ใส่ข้อมูลการล็อกอินผิดเกินกว่าจำนวนครั้งที่กำหนด

๗.๑.๑๓. ต้องส่งข้อความเตือนไปยังผู้ดูแลระบบให้ทราบว่ามีผู้ใช้งานพยายามล็อกอินแต่ผิดพลาดเป็นจำนวนหลายครั้ง

๗.๑.๑๔. ต้องจำกัดช่วงระยะเวลาที่นานที่สุดที่ให้ผู้ใช้งานจะต้องล็อกอินเข้าใช้งานให้สำเร็จ

๗.๑.๑๕. ต้องบันทึกข้อมูลการล็อกอินทั้งที่สำเร็จและไม่สำเร็จ

๗.๑.๑๖. ต้องแสดงวัน/เวลาที่ล็อกอินครั้งที่แล้ว ทั้งที่สำเร็จและไม่สำเร็จ

๗.๒. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน

๗.๒.๑. ต้องมีการจัดระดับความสำคัญของระบบงาน ซึ่งไวต่อการรบกวน หรือมีผลกระทบสูงต่อสถาบัน

๗.๒.๒. ต้องแยกระบบซึ่งไวต่อการรบกวนออกจากระบบงานอื่น ๆ ได้แก่ ระบบบริการการศึกษา ระบบทะเบียน ระบบสารสนเทศด้านการบริหาร (MIS) ระบบการบริหารการเงินการคลังภาครัฐแบบอิเล็กทรอนิกส์ (GFMIS) หรือแยกเครือข่ายออกจากเครือข่ายผู้ใช้งานทั่วไป

๗.๒.๓. ต้องควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีห้องปฏิบัติงานแยกเป็นสัดส่วน และกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้นเข้าไปปฏิบัติงานในห้องควบคุมดังกล่าว

๗.๒.๔. ต้องมีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (mobile computing and teleworking) ที่เกี่ยวข้องกับระบบดังกล่าว

๗.๒.๕. ทำการควบคุมการเข้าใช้งานจากเครือข่ายภายในและเครือข่ายภายนอก

๗.๓. การควบคุมอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่

๗.๓.๑. สร้างความตระหนักเพื่อให้ผู้ใช้งานระมัดระวังและป้องกันการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ในที่สาธารณะ ห้องประชุม นอกสถานที่ ซึ่งรวมถึงการเชื่อมต่อผ่านทางเครือข่ายสาธารณะภายนอกสถาบัน

๗.๓.๒. ป้องกันข้อมูลที่จัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ จากการถูกเข้าถึงโดยไม่ได้รับอนุญาต ด้วยการเข้ารหัสลับ

๗.๓.๓. ไม่อนุญาตให้บุคคลภายนอกสามารถเข้าถึงข้อมูลที่มีความสำคัญหรือเป็นความลับในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๓.๔. สำรองข้อมูลสำคัญที่อยู่ในอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ อย่างสม่ำเสมอ

๗.๓.๕. มีการควบคุมการเข้าถึงระบบงานของสถาบันจากระยะไกล โดยการใช้อุปกรณ์คอมพิวเตอร์ประเภทพกพา ซึ่งเชื่อมต่อผ่านทางเครือข่ายสาธารณะ

๗.๓.๖. มีการระบุและพิสูจน์ตัวตนที่มีความมั่นคงปลอดภัย สำหรับการเข้าถึงระบบงานของสถาบันจากระยะไกลโดยการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๗.๓.๗. มีการควบคุมการติดตั้งโปรแกรมไม่พึงประสงค์ ในอุปกรณ์คอมพิวเตอร์ประเภทพกพาของสถาบัน

๗.๔. การจ้างเหมาพัฒนา บำรุงรักษาระบบ ผู้ดูแลระบบต้องกำหนดการเข้าถึงระบบสารสนเทศสำหรับผู้ปฏิบัติงานจากภายนอก (Outsource)

๗.๔.๑. ต้องจัดให้มีการควบคุมการใช้งาน ได้แก่ กำหนดสิทธิในการใช้งานเฉพาะที่จำเป็นขั้นต่ำ ตรวจสอบว่าระบบสารสนเทศที่อนุญาตให้ใช้งานนั้นมีเฉพาะข้อมูลที่จำเป็นต้องใช้งาน

๗.๔.๒. ต้องมีวิธีการยืนยันตัวตนสำหรับผู้ใช้งานภายนอก ก่อนที่จะอนุญาตให้เข้ามาใช้งานระบบสารสนเทศ ได้แก่ การกำหนดชื่อผู้ใช้ และรหัสผ่าน สำหรับเข้าใช้งานระบบสารสนเทศ

๗.๔.๓. จัดเก็บบันทึกข้อมูลการเข้า-ออกพื้นที่ของผู้ปฏิบัติงานจากภายนอก (Outsource) และบันทึกการเข้าใช้งานระบบเครือข่ายของสถาบัน

๗.๔.๔. ระบบที่มีความสำคัญสูงไม่อนุญาตให้ทดสอบบนระบบจริง (Production) แต่ต้องทดสอบบนระบบทดสอบ (Test) ให้เสร็จสิ้นก่อนจึงจะนำมาติดตั้งบนระบบจริง และก่อนการติดตั้งระบบจริงต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๗.๔.๕. บุคคลหรือหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของสถาบันจะต้อง ทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๗.๔.๖. บุคคลหรือหน่วยงานภายนอก ที่ทำงานให้กับหน่วยงานภายในสถาบัน ไม่ว่าจะทำงานอยู่ภายในองค์กรหรือนอกสถานที่ ต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลขององค์กร

๗.๔.๗. บุคคลหรือหน่วยงานภายนอก ซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูล จะต้องมีการกำหนดการเข้าใช้งานให้เฉพาะกับบุคคลที่จำเป็นเท่านั้น และให้บุคคลหรือหน่วยงานภายนอกลงนามในสัญญาในการไม่เปิดเผยข้อมูล

๗.๕. การปฏิบัติงานจากภายนอกสถาบัน (Teleworking) ให้ปฏิบัติดังนี้

๗.๕.๑. การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องทำการยืนยันตัวตน ทุกครั้งที่ใช้งาน

๗.๕.๒. ต้องมีมาตรการการรักษาความมั่นคงปลอดภัยทางกายภาพสำหรับสถานที่ที่จะมีการปฏิบัติงานของผู้ใช้งานจากระยะไกล เพื่อป้องกันการขโมยอุปกรณ์ การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และการเชื่อมต่อจากระยะไกลโดยผู้ไม่ประสงค์ดี

๗.๕.๓. ต้องมีการรักษาความปลอดภัยของข้อมูล ได้แก่ การเข้ารหัสลับ เป็นต้น

๗.๕.๔. วิธีการใด ๆ ก็ตามที่สามารถเข้าสู่ระบบสารสนเทศและเครือข่ายได้จากระยะไกลต้องได้รับการอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศก่อน และมีการควบคุมอย่างเข้มงวดก่อนนำมาใช้ และผู้ใช้งานต้องปฏิบัติตามข้อกำหนดของการเข้าสู่ระบบสารสนเทศอย่างเคร่งครัด

๗.๕.๕. กรณีที่หน่วยงานภายนอกต้องการขอสิทธิในการเข้าสู่ระบบจากระยะไกลต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับสถาบันอย่างเพียงพอ ที่ผ่านการรับรองจากหน่วยงานเจ้าของระบบ และได้รับการอนุมัติจากผู้ดูแลระบบ

๗.๕.๖. มีการควบคุมพอร์ต (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องได้รับอนุมัติอย่างถูกต้องและเหมาะสมแล้วเท่านั้น และต้องไม่เปิดพอร์ตที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น

๗.๕.๗. การอนุญาตให้ผู้ใช้งานเข้าสู่ระบบจากระยะไกล ต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ช่องทางดังกล่าวต้องถูกตัดการเชื่อมต่อ เมื่อไม่ได้ใช้งานแล้ว และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

๗.๕.๘. ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นที่ไม่เกี่ยวข้องเข้าถึงระบบสารสนเทศของสถาบัน

๗.๕.๙. ผู้ใช้งานต้องตรวจสอบว่าอุปกรณ์ที่ใช้ในการเข้าถึงระบบสารสนเทศของสถาบันมีการติดตั้งระบบป้องกันไวรัสและการใช้งานอุปกรณ์ป้องกันผู้บุกรุก

๗.๖. การควบคุมหน่วยงานภายนอกเข้าถึงระบบสารสนเทศ

๗.๖.๑. หน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศและการสื่อสารของสถาบัน จะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุมัติจากผู้บริหารของหน่วยงาน

๗.๖.๒. จัดทำเอกสารแบบฟอร์มสำหรับหน่วยงานภายนอก โดยต้องมีรายละเอียดในการเข้าระบบสารสนเทศอย่างน้อย ดังนี้

(๑) เหตุผลในการขอใช้งาน

(๒) ระยะเวลาในการใช้งาน

(๓) การตรวจสอบความปลอดภัยของอุปกรณ์ที่เชื่อมต่อเครือข่าย

(๔) การกำหนดการป้องกันในเรื่องการเปิดเผยข้อมูล

๗.๖.๓. หน่วยงานภายนอกที่ทำงานให้กับสถาบันทุกหน่วยงาน จำเป็นต้องลงนามในสัญญาการไม่เปิดเผยข้อมูลของสถาบัน โดยสัญญาต้องทำให้เสร็จก่อนให้สิทธิในการเข้าสู่ระบบสารสนเทศ

๗.๖.๔. ผู้ให้บริการจากหน่วยงานภายนอก ต้องจัดทำคู่มือการปฏิบัติงาน และเอกสารที่เกี่ยวข้อง รวมทั้งปรับปรุงให้ทันสมัย และหากมีการปรับเปลี่ยนจะต้องแก้ไขให้ถูกต้อง เพื่อใช้ควบคุมและตรวจสอบการให้บริการของผู้ให้บริการว่าเป็นไปตามข้อกำหนด

๗.๖.๕. เจ้าของโครงการซึ่งรับผิดชอบต่อโครงการที่มีการเข้าถึงข้อมูลโดยหน่วยงานภายนอก ต้องกำหนดการเข้าใช้งานเฉพาะบุคคลที่จำเป็นเท่านั้น และให้หน่วยงานภายนอกลงนามในสัญญาไม่เปิดเผยข้อมูล และผู้ดูแลระบบต้องควบคุมการปฏิบัติงานนั้น ๆ ให้มีความปลอดภัยทั้ง ๓ ด้าน คือ การรักษาความลับ (Confidentiality) การรักษาความถูกต้องของข้อมูล (Integrity) และการรักษาความพร้อมที่จะให้บริการ (Availability)

๗.๗. การทบทวนการควบคุมการเข้าถึงการใช้งานสารสนเทศ ต้องทำการทบทวน อย่างน้อยปีละ ๑ ครั้ง

๘. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๘.๑. ผู้ใช้งานต้องทำการยืนยันตัวตน ก่อนเข้าใช้งาน

๘.๒. ผู้ดูแลระบบต้องลงทะเบียนอุปกรณ์ทุกตัวที่ใช้ติดต่อระบบเครือข่ายไร้สาย

๘.๓. ผู้ดูแลระบบต้องเปลี่ยนค่า SSID ที่ถูกกำหนดเป็นค่า default โดยผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (access point) มาใช้งาน

๘.๔. ผู้ดูแลระบบต้องเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์ไร้สาย

๘.๕. ผู้ดูแลระบบต้องกำหนดค่ามาตรฐานความปลอดภัยโดยใช้ WPA (Wi-Fi protected access) หรือดีกว่าในการเข้ารหัสลับระหว่างอุปกรณ์ของผู้ใช้งาน และอุปกรณ์กระจายสัญญาณ (access point)

ส่วนที่ ๒ นโยบายระบบสารสนเทศและระบบสำรองของสารสนเทศ

วัตถุประสงค์

๑) เพื่อให้ระบบสารสนเทศของสถาบันให้บริการได้อย่างต่อเนื่อง

๒) เพื่อกำหนดมาตรฐาน แนวปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับสถาบันให้เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) ผู้บริหารส่วนงานเจ้าของระบบ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. การพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน

๑.๑. จัดทำรายการระบบสารสนเทศที่สำคัญของสถาบัน และกำหนดระบบสารสนเทศที่จะทำการสำรองและจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน และทบทวนอย่างน้อยปีละ ๑ ครั้ง

๑.๒. ต้องมีการสำรองระบบสารสนเทศหลัก และกำหนดความถี่ในการสำรองระบบ หากระบบมีการเปลี่ยนแปลงมาก ให้มีความถี่ในการสำรองมากขึ้น

๑.๓. ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบสารสนเทศ และระบบสำรอง

๑.๔. ต้องกำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง

๑.๕. ต้องกำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง ได้แก่ การสำรองข้อมูลแบบเต็ม (Full Backup) หรือการสำรองข้อมูลแบบส่วนต่าง (Incremental Backup)

๑.๖. ต้องบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๑.๗. ต้องจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานต้องห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน ได้แก่ ไฟไหม้ เป็นต้น

๑.๘. ต้องกำหนดให้มีการใช้งานการเข้ารหัสลับข้อมูลในการสำรองข้อมูลที่สำคัญ ด้วยขั้นตอนวิธี (Algorithm) ที่มีความเป็นมาตรฐานสากล

๒. การทดสอบและการกู้คืน

๒.๑. ต้องจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๒.๒. ใช้ข้อมูลทันสมัยที่สุด (Latest Update) ที่ได้สำรองไว้หรือตามความเหมาะสมเพื่อกู้คืนระบบ

๒.๓. หากความเสียหายที่เกิดขึ้นมีผลกระทบต่อการให้บริการหรือการใช้งาน ให้แจ้งผู้ใช้งานทราบตามช่องทางการสื่อสารต่าง ๆ ทันที พร้อมทั้งรายงาน ความคืบหน้าการกู้คืนระบบเป็นระยะจนกว่าจะดำเนินการเสร็จสิ้นอย่างสมบูรณ์

๒.๔. ต้องตรวจสอบและทดสอบสภาพพร้อมใช้งานและขั้นตอนปฏิบัติในการกู้คืนข้อมูล อย่างน้อยปีละ ๑ ครั้ง

๓. การเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง ในสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด สำนักเทคโนโลยีสารสนเทศต้องกำหนดแผนโดยความร่วมมือกับหน่วยงานเจ้าของระบบ เพื่อการเตรียมความพร้อมกรณีฉุกเฉินดังกล่าว และเพื่อให้สามารถปรับใช้แผนได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ โดยมีข้อปฏิบัติ ดังนี้

๓.๑. ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒. ต้องมีการกำหนดหน้าที่และความรับผิดชอบของผู้ดูแลระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๓. หน่วยงานเจ้าของระบบ ต้องดำเนินการตามแผนฉุกเฉินตามสถานการณ์ ซึ่งระบุใน “แผนบริหารความต่อเนื่องในภาวะฉุกเฉินสถาบันบัณฑิตพัฒนบริหารศาสตร์”

๓.๔. หน่วยงานเจ้าของระบบ ต้องกำหนดกระบวนการการทำงานในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๕. หน่วยงานเจ้าของระบบ ต้องนำข้อมูลที่เกิดขึ้นในช่วงที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เข้าสู่ระบบหลังจากทำการกู้คืนระบบเรียบร้อยแล้ว

๓.๖. หน่วยงานเจ้าของระบบ ต้องทำการทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

วัตถุประสงค์

๑) เพื่อให้ระบบสารสนเทศของสถาบันให้บริการได้อย่างต่อเนื่อง

๒) เพื่อกำหนดมาตรฐาน แนวปฏิบัติและความรับผิดชอบของผู้ดูแลระบบในการปฏิบัติงานให้กับสถาบันให้เป็นไปอย่างเคร่งครัด และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ผู้รับผิดชอบ

๑) ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๒) ผู้ดูแลระบบที่ได้รับมอบหมาย

๓) สำนักงานตรวจสอบภายใน

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๑. **ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment)** อย่างน้อยปีละ ๑ ครั้ง

๒. **รายงานผลการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ** เสนอต่อคณะกรรมการบริหารความเสี่ยงของสถาบันบัณฑิตพัฒนบริหารศาสตร์ อย่างน้อยปีละ ๑ ครั้ง

๓. **กรณีระบบสารสนเทศหรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ** แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ “อธิการบดี” เป็นผู้รับผิดชอบความเสี่ยง ความเสียหายหรืออันตรายที่เกิดขึ้นโดยตรง รวมถึงในกรณีที่มีข้อร้องเรียน และฟ้องร้องภายใต้กฎหมายพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และที่แก้ไขเพิ่มเติม

๔. **ต้องกำหนดให้มีการตรวจสอบและประเมินความเสี่ยง** ดำเนินการโดยเจ้าหน้าที่ของสำนักงานตรวจสอบภายในของสถาบัน

ภาคผนวก

ภาคผนวก
ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๑. ข้อปฏิบัติการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

เพื่อเผยแพร่นโยบายและแนวปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง ได้มีความรู้ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตลอดจนสามารถนำไปปฏิบัติได้อย่างถูกต้อง

๑.๑. มีการให้ความรู้ความเข้าใจแก่บุคลากรเกี่ยวกับการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างสม่ำเสมอ โดยใช้วิธีการเสริมเนื้อหาเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในทุกครั้งที่มีการจัดฝึกอบรมการใช้งานระบบสารสนเทศของสถาบันเมื่อมีการปรับปรุงหรือเปลี่ยนแปลงการใช้งานระบบสารสนเทศ

๑.๒. จัดสัมมนาหรือกิจกรรมเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรและบุคคลที่เกี่ยวข้อง โดยการจัดกิจกรรมดังกล่าวอย่างน้อยปีละ 1 ครั้ง และอาจเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้

๑.๓. มีการประชาสัมพันธ์ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในลักษณะเกร็ดความรู้ หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ อาทิเช่น การประชาสัมพันธ์ผ่าน iNEWS ผ่านสื่อโซเชียลต่าง ๆ ของสำนักเทคโนโลยีสารสนเทศ และสถาบัน เป็นต้น

๑.๔. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับ ติดตาม ประเมินผล และสำรวจความต้องการของผู้ใช้บริการ

๒. ข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน

๒.๑. จัดทำแบบฟอร์มขอใช้งานระบบสารสนเทศให้ผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์มเพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน โดยสำนักเทคโนโลยีสารสนเทศหรือเจ้าของระบบเป็นผู้จัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

๒.๒. จัดทำเอกสารแสดงถึงสิทธิความรับผิดชอบของผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานซึ่งต้องลงนามรับทราบ

๒.๓. ในกรณีผู้ใช้งานต้องการระบุชื่อบัญชีผู้ใช้งานแบบกลุ่มภายใต้หน่วยงานเดียวกันที่มีบัญชีรายชื่อเดียวกัน ให้ผู้ใช้งานหรือผู้ขอมีบัญชีผู้ใช้งานระบุรายชื่อผู้ใช้และผู้ที่รับผิดชอบในการดูแลบัญชีผู้ใช้ และแจ้งเป็นลายลักษณ์อักษรถึงสำนักเทคโนโลยีสารสนเทศ

๒.๔. ตรวจสอบว่าผู้ใช้ได้รับมอบหมายสิทธิจากเจ้าของระบบ สำหรับการใช้งานระบบสารสนเทศ และบริการอย่างถูกต้อง ต้องมีการอนุมัติรับรองการได้สิทธิจากผู้บริหารอย่างชัดเจน

๒.๕. ตรวจสอบบัญชีผู้ใช้งาน โดยไม่มีการลงทะเบียนผู้ใช้งานมาก่อน

๒.๖. กำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศ โดยทันทีเมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

๒.๗. เมื่อมีการเปลี่ยนแปลงบัญชีผู้ใช้งานหรือผู้รับผิดชอบในการดูแลบัญชีผู้ใช้งานจะต้องเป็นลายลักษณ์อักษรถึงสำนักเทคโนโลยีสารสนเทศ

๒.๘. ตรวจสอบและมอบหมายสิทธิ หลักเกณฑ์ในการอนุญาตหรือการเพิกถอนสิทธิให้เข้าถึงระบบสารสนเทศ ต้องเป็นไปตามแนวปฏิบัติการบริหารจัดการการเข้าถึงของผู้ใช้งานที่กำหนดไว้

๓. ข้อปฏิบัติการบริหารจัดการสิทธิของผู้ใช้งาน

๓.๑. ตรวจสอบข้อมูลในแบบฟอร์ม ซึ่งข้อมูลจะต้องครบถ้วนทั้งหมด พร้อมทั้งต้องมีลายเซ็นของผู้ขอเข้าใช้งานระบบ ลายเซ็นของบุคคลผู้มีสิทธิอนุญาตในการลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

๓.๒. ตรวจสอบความซ้ำซ้อนของบัญชีผู้ใช้งาน

๓.๓. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารแก่ผู้ใช้โดยให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่ และต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๓.๔. กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด โดยให้มีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และให้มีการกำหนดสิทธิพิเศษที่ได้รับด้วยว่าการเข้าถึงได้นั้นสามารถเข้าถึงได้ในระดับใดบ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๓.๕. ผู้ใช้งานต้องลงนามรับทราบสิทธิและหน้าที่เกี่ยวกับการใช้งานระบบเทคโนโลยีสารสนเทศของสถาบันเป็นลายลักษณ์อักษร และต้องปฏิบัติตามอย่างเคร่งครัด

๓.๖. การแจ้งยกเลิกสิทธิการใช้งานระบบเทคโนโลยีสารสนเทศ ผู้บริหารหน่วยงานของผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม และยื่นคำขอกับผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ

๓.๗. ผู้ดูแลระบบยกเลิกสิทธิการใช้งานระบบตามคำขอในแบบฟอร์มและลบชื่อผู้ใช้งานออกจากระบบงานที่เกี่ยวข้องทั้งหมด

๓.๘. กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ โดยต้องให้สิทธิเฉพาะที่เกี่ยวกับการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

๓.๙. มีการทบทวนสิทธิการใช้งานอย่างน้อยปีละ ๑ ครั้ง

๔. ข้อปฏิบัติการใช้งานรหัสผ่าน

๔.๑. เลือกรหัสผ่านที่ปลอดภัยและเก็บรักษารหัสผ่านไว้เป็นความลับอยู่ตลอดเวลา

๔.๒. ไม่อนุญาตให้ผู้อื่นใช้บัญชีของตน หากเกิดปัญหาจากการให้ใช้บัญชี ได้แก่ การละเมิดลิขสิทธิ์ หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ต้องเป็นผู้รับผิดชอบ เว้นแต่จะมีหลักฐานพิสูจน์ได้ว่าไม่ได้เป็นผู้กระทำ

๔.๓. ไม่ลักลอบใช้รหัสผ่าน หรือถอดรหัสผ่านของผู้ใช้อื่น หรือการกระทำอื่นใดเพื่อให้ได้มาซึ่งรหัสผ่านของผู้อื่น

๔.๔. รายงานการล่วงละเมิดความปลอดภัยในระบบให้ผู้ดูแลระบบทราบในทันที

๔.๕. ตั้งรหัสผ่านที่ยากต่อการคาดเดาโดยผู้อื่น

๔.๖. กำหนดให้รหัสผ่านมีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมชุดของตัวอักษร หรืออักขระ หรือตัวเลข หรือสัญลักษณ์ เข้าด้วยกัน

๔.๗. หลีกเลี่ยงการกำหนดรหัสผ่านจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ปรากฏในพจนานุกรม

๔.๘. หลีกเลี่ยงการใช้ตัวอักษรเรียงกัน ได้แก่ abcd 1234 และเลี่ยงการใช้ตัวอักษรซ้ำกัน ได้แก่ aaaa 8888

๔.๙. หลีกเลี่ยงการใช้รหัสผ่านเดียวกัน และเลี่ยงการใช้รหัสผ่านเดียวกันกับระบบงานอื่น ๆ ยกเว้นระบบที่มีการใช้ Single Sign-on หรือมีการยืนยันตัวบุคคลผ่านระบบบริหารจัดการบัญชีผู้ใช้งาน

๔.๑๐. หลีกเลี่ยงการจดหรือบันทึกรหัสผ่านไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

๔.๑๑. หลีกเลี่ยงการกำหนดให้เครื่องคอมพิวเตอร์จดจำรหัสผ่านของตนเองไว้

๔.๑๒. ควรเปลี่ยนรหัสผ่านทันที เมื่อทราบว่ารหัสผ่านของตนอาจถูกเปิดเผยหรือ มีผู้อื่นล่วงรู้

๔.๑๓. ควรเปลี่ยนรหัสผ่านหลังจากที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากการทำงาน

๔.๑๔. ควรเปลี่ยนรหัสผ่านทุกรอบระยะเวลา ๖ เดือน

๔.๑๕. ควรเปลี่ยนรหัสผ่านโดยไม่ใช้รหัสผ่านเดิมที่เคยตั้งมาแล้ว

๕. ข้อปฏิบัติการใช้งานบริการเครือข่าย

๕.๑. ห้ามผู้ใช้งานกระทำการใด ๆ เกี่ยวกับข้อมูลที่เป็นการขัดต่อกฎหมายหรือศีลธรรมอันดี แห่งสาธารณชน โดยผู้ใช้งานรับรองว่าหากมีการกระทำการใด ๆ ดังกล่าว ย่อมถือว่าอยู่นอกเหนือความรับผิดชอบของสถาบัน

๕.๒. ห้ามผู้ใช้งานกระทำการใด ๆ ที่เข้าข่ายลักษณะเพื่อการค้าหรือการแสวงหาผลกำไรผ่านเครื่องคอมพิวเตอร์และเครือข่าย ได้แก่ การประกาศแจ้งความการซื้อ หรือการจำหน่ายสินค้าการนำข้อมูลไปซื้อขาย การรับบริการค้นหาข้อมูลโดยคิดค่าบริการ การให้บริการโฆษณาสินค้า หรือการเปิดบริการอินเทอร์เน็ตแก่บุคคลทั่วไปเพื่อแสวงหากำไร

๕.๓. ผู้ใช้งานต้องไม่ละเมิดต่อผู้อื่น คือ ผู้ใช้งานต้องไม่อ่าน เขียน ลบ เปลี่ยนแปลงหรือแก้ไขใด ๆ ในส่วนที่มิใช่ของตนโดยไม่ได้รับอนุญาต การบุกรุก (Hack) เข้าสู่บัญชีผู้ใช้งาน (User Account) ของผู้อื่น การเผยแพร่ข้อความใด ๆ ที่ก่อให้เกิดความเสียหายเสื่อมเสียแก่ผู้อื่น การใช้ภาษาไม่สุภาพหรือการเขียนข้อความที่ทำให้ผู้อื่นเสียหาย ถือเป็นการละเมิดสิทธิของผู้อื่นทั้งสิ้น ผู้ใช้งานต้องรับผิดชอบแต่เพียงฝ่ายเดียว สถาบันไม่มีส่วนร่วมรับผิดชอบความเสียหายดังกล่าว

๕.๔. ห้ามมิให้ผู้ใดเข้าใช้งานโดยมิได้รับอนุญาต การบุกรุกหรือพยายามบุกรุกเข้าสู่ระบบถือว่าเป็นการพยายามรุกล้ำเขตหวงห้ามของทางราชการ

๕.๕. ผู้ใช้งานได้รับบัญชีผู้ใช้งาน (User Account) เป็นการเฉพาะบุคคลเท่านั้น ผู้ใช้งานจะโอน หรือจ่ายแจกสิทธินี้ให้กับผู้อื่นไม่ได้

๕.๖. ผู้ใช้งานต้องเป็นผู้รับผิดชอบผลต่าง ๆ อันอาจจะเกิดมีขึ้น รวมถึงผลเสียหายต่าง ๆ ที่เกิดจากบัญชีผู้ใช้งาน (User Account) นั้น ๆ เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

๕.๗. ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้เฉพาะบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๕.๘. ห้ามเปิดหรือใช้งานโปรแกรมประเภท Peer-to-Peer หรือโปรแกรมที่มีความเสี่ยงเว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชาหรือสำนักเทคโนโลยีสารสนเทศ

๖. ข้อปฏิบัติการใช้งานโปรแกรมอรรถประโยชน์

ผู้ดูแลระบบต้องจำกัดและควบคุมการใช้งานโปรแกรมอรรถประโยชน์ (System Utility) เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๖.๑. จัดทำรายการบัญชีรายชื่อโปรแกรมอรรถประโยชน์ที่อนุญาตให้ใช้งานได้เท่านั้น

๖.๒. จำกัดสิทธิและกำหนดสิทธิการเข้าถึงการใช้งานโปรแกรมอรรถประโยชน์ให้เฉพาะผู้ที่ได้รับสิทธิเท่านั้น

๖.๓. ต้องใช้โปรแกรมอรรถประโยชน์ที่มีลิขสิทธิ์ถูกต้อง

๖.๔. ผู้ใช้งานที่ต้องการใช้งานโปรแกรมอรรถประโยชน์ ต้องแจ้งความจำเป็นในการขอใช้และทำการขออนุญาตจากผู้ดูแลระบบ พร้อมระบุเหตุผลความต้องการใช้งาน โดยต้องมีการลงนามเห็นชอบจากผู้บังคับบัญชาของผู้ใช้งาน และได้รับอนุมัติจากผู้อำนวยการสำนักเป็นลายลักษณ์อักษร

๖.๕. จัดเก็บโปรแกรมอรรถประโยชน์ไว้ในสื่อภายนอก ถ้าไม่ต้องใช้งานเป็นประจำ

๖.๖. ทำการเก็บบันทึกการเรียกใช้งานโปรแกรมเหล่านี้

๖.๗. ทำการถอดถอนโปรแกรมอรรถประโยชน์ที่ไม่จำเป็นออกจากระบบ

๖.๘. ทำการตรวจสอบบันทึกการเรียกใช้งานอย่างสม่ำเสมอ

๗. ข้อปฏิบัติในการใช้จดหมายอิเล็กทรอนิกส์ (e-mail)

๗.๑. ผู้ใช้งานมีหน้าที่และความรับผิดชอบโดยพึงระวังไม่ให้ผู้อื่นเข้าถึงรหัสผ่านเพื่อใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตนเองโดยมิชอบ ผู้ใช้ต้องรักษารหัสผ่านเป็นความลับเฉพาะตัวและไม่อนุญาตให้ผู้อื่นเข้าใช้จดหมายอิเล็กทรอนิกส์ในนามของตนเองในทุกกรณี ผู้ใช้เป็นผู้รับผิดชอบต่อผลกระทบและผลทางกฎหมายจากการใช้จดหมายอิเล็กทรอนิกส์ และการอนุญาตให้ผู้อื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ในนามของตนเอง

๗.๒. ผู้ใช้งานพึงทราบว่าผู้ดูแลระบบไม่มีสิทธิที่จะถามหรือร้องขอให้ผู้ใช้เปิดเผยรหัสผ่านประจำตัวเพื่อเข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์

๗.๓. ผู้ใช้ต้องไม่เข้าใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้อื่นไม่ว่าจะได้รับอนุญาตหรือไม่ก็ตาม

๗.๔. การใช้จดหมายอิเล็กทรอนิกส์ ในลักษณะต่อไปนี้เป็นสิ่งต้องห้าม

๗.๔.๑. เพื่อประกอบธุรกิจส่วนตัว หรือเพื่อบุคคลอื่น

๗.๔.๒. การเผยแพร่จดหมายลูกโซ่

๗.๔.๓. การเผยแพร่ข้อมูลชั้นความลับของสถาบัน

๗.๔.๔. การปลอมแปลงหรือดัดแปลงชื่อผู้ส่งให้เข้าใจผิดว่าจดหมายอิเล็กทรอนิกส์นั้น ๆ ส่งมาจากบุคคลอื่น

๗.๔.๕. การปกปิดหรือดัดแปลงชื่อผู้ส่งในลักษณะที่ทำให้ไม่ทราบชื่อผู้ส่ง

๗.๔.๖. การปลอมแปลงหรือดัดแปลงส่วนหัวจดหมาย ได้แก่ เส้นทาง วันเวลาที่ส่ง

๗.๔.๗. การเผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่กล่าวร้ายต่อบุคคลหรือกลุ่มบุคคล

๗.๔.๘. การเผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่เป็นการดูหมิ่น เหยียดหยาม หรือทำให้เกิดการแบ่งแยกทาง ศาสนา เชื้อชาติ หรือเพศ

๗.๔.๙. การเผยแพร่ข้อความ ภาพ วีดีโอ เสียง ที่มีลักษณะหยาบคาย หรือลามกอนาจาร

๗.๔.๑๐. การเผยแพร่โปรแกรมหรืองาน หรือรหัสผ่านสำหรับใช้เข้าถึงโปรแกรมหรืองาน ในลักษณะที่ละเมิดลิขสิทธิ์

๗.๔.๑๑. การส่งจดหมายอิเล็กทรอนิกส์ กระจายความคิดเห็นส่วนบุคคลที่มีต่อสังคม การเมือง ศาสนา ไปยังผู้รับที่ไม่เคยแจ้งความประสงค์จะรับข่าวสาร

๗.๔.๑๒. การกระทำซึ่งส่งผลกระทบต่อประสิทธิภาพการให้บริการระบบสารสนเทศ

๗.๔.๑๓. การกระจายไวรัสหรือรหัสโปรแกรมที่เป็นอันตรายต่อความมั่นคงปลอดภัยด้านสารสนเทศ

๘. ข้อปฏิบัติการทำลายข้อมูลหรือกำจัดสื่อบันทึกข้อมูล

๘.๑. เมื่อต้องทำลายข้อมูลอิเล็กทรอนิกส์ ผู้รับผิดชอบข้อมูลอิเล็กทรอนิกส์ต้องเป็นผู้ทำลายข้อมูล

๘.๒. กำหนดวิธีการทำลายข้อมูลอิเล็กทรอนิกส์บนสื่อบันทึกข้อมูล ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลายใช้ใหม่ได้	วิธีทำลาย	ระยะเวลาทำลาย
กระดาษ		ทำลายด้วยเครื่องทำลายเอกสาร	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
Flash Drive	ใช้วิธีการ Format	- ทำลายข้อมูล ตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
แผ่น CD/DVD	ใช้วิธีการ Format	ใช้วิธีการหัก ทุบหรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
เทป		ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทำลาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด
ฮาร์ดดิสก์	ใช้วิธีการ Format	- ทำลายข้อมูลตามมาตรฐาน DoD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย	เก็บรักษาไว้อย่างน้อย ๑ ปีหรือตามที่กฎหมายกำหนด