ประกาศสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย พ.ศ. ๒๕๖๒

ด้วยปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบเทคโนโลยีสารสนเทศ มีความรุนแรงเพิ่มขึ้นทั้งในประเทศและต่างประเทศ อีกทั้งยังมีแนวโน้มที่จะส่งผลกระทบต่อภาครัฐและภาคธุรกิจมากขึ้นทำให้ผู้ประกอบการตลอดจนองค์กรภาครัฐและภาคเอกชนที่มีการดำเนินงานใดๆ ในรูปของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศขององค์กรขาดความเชื่อมั่นต่อการทำธุรกรรมทางอิเล็กทรอนิกส์ในทุกรูปแบบ ประกอบกับคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ตระหนักถึงความจำเป็นที่จะส่งเสริมและผลักดันให้ประเทศสามารถยกระดับการแข่งขันกับประเทศอื่นๆ โดยการนำระบบสารสนเทศและการสื่อสารมาประยุกต์ใช้ประกอบการทำธุรกรรมทางอิเล็กทรอนิกส์อย่างแพร่หลาย จึงเห็นความสำคัญที่จะนำกฎหมายข้อบังคับต่างๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ ทั้งในส่วนที่ต้องกระทำ และในส่วนที่ต้องงดเว้นการกระทำเพื่อช่วยให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของหน่วยงานมีความมั่นคงปลอดภัยและมีความน่าเชื่อถือ

เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย หรือต่อไปนี้เรียกว่า “สถาบัน” เป็นไปอย่างเหมาะสม มีความมั่นคงปลอดภัย และเชื่อถือได้ สามารถดำเนินงานได้อย่างต่อเนื่อง รวมถึงการป้องกันปัญหาที่อาจเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สถาบัน และเพื่อการดำเนินงานเป็นไปตามความในมาตรา ๕ มาตรา ๖ และมาตรา ๗ ภายใต้พระราชกฤษฎีกา กำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ ๒๕๔๙ ซึ่งกำหนดให้หน่วยงานของรัฐจัดทำประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานหรือองค์กร หรือส่วนงานของหน่วยงาน หรือองค์กรตามมาตรา ๕ (๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

สถาบันจึงเห็นควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน โดยความเห็นชอบของคณะกรรมการบริหารสถาบัน จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย พ.ศ. ๒๕๖๒”

ข้อ ๒ ในประกาศนี้

๒.๑ **สถาบัน** หมายถึง สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

๒.๒ **หน่วยงาน** หมายถึง สำนักงาน สำนักวิชา ศูนย์ สาขาวิชา ฝ่าย หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่น ในสังกัดสถาบัน

๒.๓ **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบัน

๒.๔ **ผู้บริหารระดับสูงสุดของหน่วยงาน** (Chief Executive Officer: CEO) หมายถึง อธิการบดีสถาบัน

๒.๕ **ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ** (Chief Information Officer: CIO) หมายถึง รองอธิการบดีสถาบันที่ได้รับมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสถาบัน

๒.๖ **ผู้บริหาร** หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี หัวหน้าสาขาวิชา ผู้อำนวยการสำนักงาน ผู้อำนวยการศูนย์ หัวหน้าฝ่าย หัวหน้าหน่วยงาน

๒.๗ **นโยบาย** หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๘ **หน่วยเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบงานสารสนเทศภายในสถาบัน

๒.๙ **หัวหน้าหน่วยเทคโนโลยีสารสนเทศ** หมายถึง ผู้บังคับบัญชาของบุคลากรที่ปฏิบัติหน้าที่ในหน่วยเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแล การใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน

๒.๑๐ **ผู้ใช้งาน** หมายถึง คณะกรรมการบริหารสถาบัน บุคลากร หรือลูกจ้างของสถาบัน และให้หมายความรวมถึงบุคคลอื่นที่สถาบันว่าจ้างหรือให้มาปฏิบัติงานให้แก่สถาบัน รวมทั้งบุคลากรที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบัน

๒.๑๑ **บุคคลภายนอก** หมายถึง บุคคลที่ไม่ได้สังกัดอยู่ในสถาบัน แต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

๒.๑๒ **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน

๒.๑๓ **ผู้ดูแลระบบ** (System Administrator) หมายถึง ผู้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิ์ในการเข้าถึงระบบสารสนเทศ เช่น การให้สิทธิ์ เพิ่มสิทธิ์ ลดสิทธิ์ ยกเลิกสิทธิ์ พัฒนา ปรับปรุง ดูแลและบำรุงรักษาระบบสารสนเทศ

๒.๑๔ **บุคลากร** หมายถึง ผู้บริหาร บุคลากรสายวิชาการ บุคลากรสายสนับสนุนวิชาการ ลูกจ้างประจำ และลูกจ้างชั่วคราว

๒.๑๕ **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงาน โดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

๒.๑๖ **สินทรัพย์** หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับสถาบัน ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อุปกรณ์ระบบคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

๒.๑๗ **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนในการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

๒.๑๘ **ระบบคอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์ เครื่องบริการ และอุปกรณ์อื่นๆ ที่เชื่อมการทำงานเข้าด้วยกัน เพื่อให้สามารถทำงาน ประมวลผล หรือติดต่อสื่อสารข้อมูลร่วมกันหรือระหว่างกันได้โดยอัตโนมัติ

๒.๑๙ **ระบบสื่อสาร** (Communication System) หมายถึง ระบบที่ประกอบด้วย ผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล (ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจร ทางสาย เช่น สายเคเบิล (Cable) โคแอกเชียล (Coaxial Cable) วิทยาการเส้นใยนำแสง (Fiber Optic) และระบบไร้สาย เช่น ไมโครเวฟ (Microwave) ดาวเทียม (Satellite) รวมทั้งอุปกรณ์อื่นๆ เช่น ฮับ (Hub) การสลับ (Switching) อุปกรณ์จัดเส้นทาง (Router)

๒.๒๐ **สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลให้มีหมายถึงโดยผ่านการประมวลผล การจัดระเบียบให้ข้อมูล ซึ่งอาจอยู่ในรูปของตัวเลขข้อความหรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผนการตัดสินใจและอื่นๆ

๒.๒๑ **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสาร หรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

๒.๒๒ **VPN (Virtual Private Network)** หมายถึง เครือข่ายส่วนตัวเสมือน ซึ่งในการรับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะ แล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นจากต้นทางไปจนถึงปลายทาง

๒.๒๓ **อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)** หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในระบบเครือข่ายไร้สาย

๒.๒๔ **SSID (Service Set Identifier)** หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

๒.๒๕ **WEP (Wire Equivalent Privacy)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้ในการเข้ารหัสข้อมูล ดังนั้นทุกเครื่องในระบบเครือข่ายที่รับ-ส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

๒.๒๖ **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาให้มีความปลอดภัยมากกว่า WEP

๒.๒๗ **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในระบบเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

๒.๒๘ **อินเทอร์เน็ต** หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเชื่อมโยง

๒.๒๙ **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์หรืออุปกรณ์เครือข่าย ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

๒.๓๐ **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ** (Information System Workspace) หมายถึง พื้นที่ที่สถาบันอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น

๑) พื้นที่ทำงานทั่วไป หมายถึง พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน และอุปกรณ์ต่อพ่วงต่าง ๆ

๒) พื้นที่ทำงานของผู้ดูแลระบบ

๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย

๔) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

๒.๓๑ **เครื่องคอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

๒.๓๒ **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

๒.๓๓ **ระบบจดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน

๒.๓๔ **เครือข่ายสังคมออนไลน์** หมายถึง เว็บไซต์หรือแอปพลิเคชั่นที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะ โดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประภทต่าง ๆ

๒.๓๕ **รหัสผ่าน** (Password) หมายถึง ชุดตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

๒.๓๖ **บัญชีผู้ใช้** (Account) ความถึง สัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกันมีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกันเพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชีหรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

๒.๓๗ **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๒.๓๘ **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

๒.๓๙ **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิด การห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ

๒.๔๐ **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง การเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒.๔๑ **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด ซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

๒.๔๒ **ความเสี่ยง** (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าหรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ เป้าประสงค์ และเป้าหมายของสถาบัน

๒.๔๓ **ประเมินความเสี่ยง** (Risk Assessment) หมายถึง กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศ รวมทั้งผลกระทบจากการสูญเสียสารสนเทศหรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตรการรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป

๒.๔๔ **สารสนเทศที่กำหนดชั้นความลับ** หมายถึง สารสนเทศในรูปข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใดๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหา จำกัดการเข้าถึงและหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึกประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่หรือเตรียมจะใช้ตลอดจนวัสดุหรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว

๒.๔๕ **ภัย** (Threat) หมายถึง อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศโดยคน (Person) สิ่งต่างๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนา อันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงานหรือการกระทำอื่นๆ ตามความต้องการของภัยนั้น

๒.๔๖ **ความอ่อนแอ** (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่องใดๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกันสามารถนำไปใช้ประโยชน์ เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้นๆ ได้ ความอ่อนแอที่มีอยู่ของระบบสารสนเทศและความรุนแรงที่เกิดจากภัยนั้นซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากันในแต่ละพื้นที่ใช้งานระบบสารสนเทศฯ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศฯ แต่ละแห่ง ควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด

๒.๔๗ **ระบบสำรอง (Disaster Recovery Site : DR Site)** หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

ข้อ ๓ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามประกาศฉบับนี้ มีเนื้อหาประกอบด้วย

๓.๑. นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒. แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๔ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้มี ๒ ส่วน ดังนี้

๔.๑. ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานมีส่วนร่วมในการจัดทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้บุคลากรและผู้เกี่ยวข้องทั้งหมดทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ของสถาบัน

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติให้ชัดเจน

(๔) ทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๔.๒. ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงและการใช้งานระบบสารสนเทศ มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งานอย่างทั่วถึง เพื่อให้ผู้ใช้งานสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก รวดเร็ว และให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ มีนโยบายการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยแยกประเภทและจัดเก็บเป็นหมวดหมู่ มีระบบสำรอง ระบบสารสนเทศและระบบคอมพิวเตอร์ที่สมบูรณ์และสภาพพร้อมใช้งาน และมีแผนฉุกเฉินเพื่อให้ระบบสามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ ต้องดำเนินการอย่างสม่ำเสมอ โดยกำหนดให้ต้องตรวจสอบประเมินความเสี่ยง และกำหนดมาตรการควบคุมความเสี่ยงด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

(๔) กำหนดหน้าที่และความรับผิดชอบเกี่ยวกับการรายงานเหตุการณ์ที่เสี่ยงต่อความมั่นคงปลอดภัยที่เกิดขึ้น

(๕) การสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศหรือระบบคอมพิวเตอร์ มีนโยบายในการสร้างความรู้ความเข้าใจ โดยจัดทำคู่มือ การฝึกอบรมและเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน

ข้อ ๕ ข้อกำหนดการเข้าถึงและควบคุมการใช้งานระบบสารสนเทศ

๕.๑. ต้องควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๕.๒. กำหนดหลักเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึงตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ์

๕.๓. กำหนดประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่เข้าถึงได้ และช่องทางการเข้าถึง

๕.๔. มีวิธีการบริหารจัดการเข้าถึงข้อมูลและระบบสารสนเทศของผู้ใช้งานแต่ละประเภทที่เหมาะสมและตรวจสอบได้ เพื่อป้องกันการเข้าถึงของผู้ไม่ได้รับอนุญาต

๕.๕. ต้องควบคุมการเข้าถึงระบบเครือข่ายและการใช้บริการผ่านระบบเครือข่าย รวมทั้งการเชื่อมต่อระบบเครือข่ายทั้งจากภายในสถาบันและจากภายนอกสถาบัน เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศหรือระบบสารสนเทศโดยไม่ได้รับอนุญาต

๕.๖. ต้องควบคุมการเข้าถึงระบบปฏิบัติการ เพื่อป้องกันการใช้งานอุปกรณ์ในการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

๕.๗. ต้องควบคุมการเข้าถึงโปรแกรมและระบบสารสนเทศ เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๖ ต้องบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศ ดังนี้

๖.๑. สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก เข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๖.๒. การลงทะเบียนผู้ใช้งาน ต้องกำหนดให้มีขั้นตอนปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อต้องอนุญาตเข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อยกเลิกการอนุญาตดังกล่าว

๖.๓. การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ใน

ภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๖.๔. ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๗ ต้องกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ ดังนี้

๗.๑. การใช้งานรหัสผ่าน ต้องกำหนดแนวทางปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่าน

๗.๒. การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน ต้องกำหนดแนวทางปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์ สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

๗.๓. การปฏิบัติตามนโยบายควบคุมการไม่ทิ้งสินทรัพย์สารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย โดยต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ สารสนเทศ ฯลฯ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อไม่ใช้งาน

ข้อ ๘ การจัดทำระบบสำรองระบบสารสนเทศ ตามแนวทางต่อไปนี้

๘.๑. ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองให้อยู่ในสภาพพร้อมใช้งาน

๘.๒. ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมฉุกเฉินดังกล่าว ให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการปฏิบัติงานตามภารกิจ

๘.๓. ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรที่ดูแลรับผิดชอบระบบสารสนเทศระบบสำรอง และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการอิเล็กทรอนิกส์

๘.๔. ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๘.๕. ต้องปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรองปีละ ๑ ครั้ง

ข้อ ๙ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ มีดังนี้

๙.๑. กำหนดให้ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศปีละ ๑ ครั้ง

๙.๒. ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๐ ต้องประกาศนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน พ.ศ. ๒๕๖๒ ให้ผู้เกี่ยวข้องทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและแนวปฏิบัติดังนี้

๑๐.๑. หนังสือเวียนภายในสถาบัน

๑๐.๒. ประกาศบนเว็บไซต์ภายในสถาบัน

ข้อ ๑๑ หน่วยงานภายในสถาบันที่ต้องบริหารจัดการระบบเทคโนโลยีสารสนเทศสามารถกำหนดแนวปฏิบัติในการรักษาความมั่นคงด้านสารสนเทศของหน่วยงานได้เอง ทั้งนี้ ต้องให้สอดคล้องกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน พ.ศ. ๒๕๖๒

ข้อ ๑๒ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสถาบัน โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสาร “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย พ.ศ. ๒๕๖๒” ซึ่งบุคลากรของสถาบันและบุคคลภายนอกต้องถือปฏิบัติอย่างเคร่งครัดต่อไป

ข้อ ๑๓ หากระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สถาบันหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย พ.ศ. ๒๕๖๒ ให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๔ ให้หน่วยเทคโนโลยีสารสนเทศ เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้และกำหนดให้ทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๕ บรรดาประกาศ ระเบียบ และคำสั่งอื่นใดที่ได้กำหนดไว้แล้วซึ่งขัดกับประกาศนี้ ให้ใช้ประกาศนี้แทน

ประกาศนี้ให้ใช้บังคับตั้งแต่วันที่ประกาศ เป็นต้นไป

ประกาศ ณ วันที่ 12 เดือน พฤศจิกายน พ.ศ 2562

(ลงชื่อ)

(ผู้ช่วยศาสตราจารย์ ดร.วรุณยุพา รอยกุลเจริญ)
อธิการบดี สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย (Information Security Policy)

๑. หลักการและเหตุผล

ตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินกิจกรรมหรือการให้บริการต่างๆ มีความมั่นคงปลอดภัย เชื่อถือได้ สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย ได้กำหนดนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขึ้น เพื่อให้ระบบเทคโนโลยีสารสนเทศของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย หรือต่อไปนี้เรียกว่า “สถาบัน” เป็นไปอย่างเหมาะสม มีประสิทธิภาพ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยให้สามารถดำเนินงานได้อย่างต่อเนื่อง และป้องกันภัยคุกคามต่างๆ สถาบันจึงเห็นสมควรกำหนดนโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ ให้มีมาตรฐาน แนวปฏิบัติ ขั้นตอนปฏิบัติ ครอบคลุมด้านการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศ ตามพระราชกฤษฎีกาฯ และตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

๒. วัตุประสงค์

๒.๑. เพื่อกำหนดมาตรฐานแนวทางปฏิบัติของการรักษาความมั่นคงปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

๒.๒. เพื่อให้เกิดความเชื่อมั่นด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน และทำให้การดำเนินงานต่างๆ เป็นไปอย่างมีประสิทธิภาพและประสิทธิผล

๒.๓. เพื่อเผยแพร่นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้บุคลากรสถาบันทุกระดับและบุคคลภายนอกที่ปฏิบัติงานให้กับสถาบัน มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญและถือปฏิบัติตามนโยบายนี้อย่างเคร่งครัด

๒.๔. เพื่อให้มีระบบตรวจสอบและประเมินความเสี่ยงในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศอย่างสม่ำเสมอทุกปี

๓. องค์ประกอบของนโยบาย

คำนิยาม

ส่วนที่ ๑ นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

ส่วนที่ ๒ นโยบายการจัดทำระบบสำรองสารสนเทศ

ส่วนที่ ๓ นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

ส่วนที่ ๔ นโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยด้านสารสนเทศ

ส่วนที่ ๕ นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

ส่วนที่ ๖ แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ

คำนิยาม

คำนิยามที่ใช้ในนโยบายนี้

- **สถาบัน** หมายถึง สถาบันการพยาบาลศรีสวรินทิราสภากาชาดไทย
- **หน่วยงาน** หมายถึง สำนักงาน สำนักวิชา ศูนย์ สาขาวิชา ฝ่าย หรือหน่วยงานที่เรียกชื่อเป็นอย่างอื่น ในสังกัดสถาบัน
- **ผู้บังคับบัญชา** หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบัน
- **ผู้บริหารระดับสูงสุดของหน่วยงาน** (Chief Executive Officer: CEO) หมายถึง อธิการบดีสถาบัน
- **ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ** (Chief Information Officer: CIO) หมายถึงรองอธิการบดีสถาบันที่ได้รับมอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศของสถาบัน
- **ผู้บริหาร** หมายถึง อธิการบดี รองอธิการบดี ผู้ช่วยอธิการบดี หัวหน้าสาขาวิชา ผู้อำนวยการสำนักงาน ผู้อำนวยการศูนย์ หัวหน้าฝ่าย หัวหน้าหน่วยงาน
- **นโยบาย** หมายถึง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- **หน่วยเทคโนโลยีสารสนเทศ** หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศและการสื่อสาร ให้คำปรึกษา พัฒนาปรับปรุง บำรุงรักษาระบบคอมพิวเตอร์ ระบบเครือข่ายคอมพิวเตอร์ และระบบงานสารสนเทศ ภายในสถาบัน
- **หัวหน้าหน่วยเทคโนโลยีสารสนเทศ** หมายถึง ผู้บังคับบัญของบุคลากรที่ปฏิบัติหน้าที่ในหน่วยเทคโนโลยีสารสนเทศ ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบาย มาตรฐาน การควบคุมดูแล การใช้งานระบบเทคโนโลยีสารสนเทศของสถาบัน
- **ผู้ใช้งาน** หมายถึง คณะกรรมการสถาบัน บุคลากร หรือลูกจ้างของสถาบัน และให้หมายความรวมถึงบุคคลอื่น ที่สถาบันว่าจ้างหรือให้มาปฏิบัติงานให้แก่สถาบัน รวมทั้งบุคลากรที่ปฏิบัติงานเกี่ยวข้องกับระบบสารสนเทศ และบุคคลภายนอกที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์ และระบบเครือข่ายของสถาบัน
- **บุคคลภายนอก** หมายถึง บุคคลที่ไม่ได้สังกัดอยู่ในสถาบัน แต่ได้รับอนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่าง ๆ ของสถาบัน โดยจะได้รับสิทธิ์ในการใช้ระบบตามหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล
- **สิทธิของผู้ใช้งาน** หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน
- **ผู้ดูแลระบบ** (System Administrator) หมายถึง ผู้บริหารจัดการบัญชีรายชื่อผู้มีสิทธิ์ในการเข้าถึงระบบสารสนเทศ เช่น การให้สิทธิ์ เพิ่มสิทธิ์ ลดสิทธิ์ ยกเลิกสิทธิ์ พัฒนา ปรับปรุง ดูแลและบำรุงรักษาระบบสารสนเทศ
- **บุคลากร** หมายถึง ผู้บริหาร บุคลากรสายวิชาการ บุคลากรสายสนับสนุนวิชาการ ลูกจ้างประจำ และลูกจ้างชั่วคราว
- **เจ้าของข้อมูล** หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบงานโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

- **สินทรัพย์** หมายถึง สิ่งใดก็ตามที่มีคุณค่าสำหรับสถาบัน ได้แก่ ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสาร อุปกรณ์ระบบคอมพิวเตอร์ อุปกรณ์ระบบเครือข่าย ซอฟต์แวร์ที่มีลิขสิทธิ์ เป็นต้น

- **ระบบเทคโนโลยีสารสนเทศ** (Information Technology System) หมายถึง ระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์และระบบเครือข่าย มาช่วยในการสร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนในการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลสารสนเทศ เป็นต้น

- **ระบบคอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์ เครื่องบริการ และอุปกรณ์อื่นๆ ที่เชื่อมการทำงานเข้าด้วยกัน เพื่อให้สามารถทำงาน ประมวลผล หรือติดต่อสื่อสารข้อมูลร่วมกันหรือระหว่างกันได้โดยอัตโนมัติ

- **ระบบสื่อสาร** (Communication System) หมายถึง ระบบที่ประกอบด้วย ผู้รับ ผู้ส่ง และสื่อกลางในระบบสื่อสารที่ใช้ในการส่งผ่านข้อมูล (ตัวอักษร ตัวเลข ภาพ เสียง เป็นต้น) ทั้งระบบวงจรทางสาย เช่น สายเคเบิล (Cable) โคแอกเชียล (Coaxial Cable) วิทยาการเส้นใยนำแสง (Fiber Optic) และระบบไร้สาย เช่น ไมโครเวฟ (Microwave) ดาวเทียม (Satellite) รวมทั้งอุปกรณ์อื่นๆ เช่น ฮับ (Hub) การสลับ (Switching) อุปกรณ์จัดเส้นทาง (Router)

- **สารสนเทศ** (Information) หมายถึง ข้อเท็จจริงที่ได้จากข้อมูลให้มีหมายถึงโดยผ่านการประมวลผลการจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย เช่น รายงาน ตาราง แผนภูมิ เป็นต้น และสามารถนำไปใช้ประโยชน์ในการบริหารการวางแผนการตัดสินใจและอื่นๆ

- **ระบบเครือข่าย** หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูล และสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของหน่วยงานได้ เช่น ระบบเครือข่ายแบบมีสาย (LAN) และระบบเครือข่ายแบบไร้สาย (Wireless LAN) เป็นต้น

- **VPN (Virtual Private Network)** หมายถึง เครือข่ายส่วนตัวเสมือน ซึ่งในการรับ-ส่งข้อมูลจริงจะทำโดยการเข้ารหัสเฉพาะ แล้วรับ-ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นจากต้นทางไปจนถึงปลายทาง

- **อุปกรณ์กระจายสัญญาณไร้สาย (Access Point)** หมายถึง อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในระบบเครือข่ายไร้สาย

- **SSID (Service Set Identifier)** หมายถึง บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุก ๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

- **WEP (Wire Equivalent Privacy)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย โดยอาศัยชุดตัวเลขมาใช้ในการเข้ารหัสข้อมูล ดังนั้น ทุกเครื่องในระบบเครือข่ายที่รับ-ส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

- **WPA (Wi-Fi Protected Access)** หมายถึง ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาให้มีความปลอดภัยมากกว่า WEP

- **ไฟร์วอลล์ (Firewall)** หมายถึง เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในระบบเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

- **อินเทอร์เน็ต** หมายถึง เครือข่ายคอมพิวเตอร์ขนาดใหญ่ที่เชื่อมโยงเครือข่ายทั่วโลกเข้าด้วยกัน โดยอาศัยเครือข่ายโทรคมนาคมเชื่อมโยง

- **ข้อมูลจราจรทางคอมพิวเตอร์** หมายถึง ข้อมูลเกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ หรืออุปกรณ์เครือข่าย ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ เวลา ปริมาณ ระยะเวลา ชนิดของบริการ หรืออื่น ๆ ที่เกี่ยวข้องกับการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

- **พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ** (Information System Workspace) หมายถึง พื้นที่ที่สถาบันอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยแบ่งเป็น
    ๑) พื้นที่ทำงานทั่วไป หมายถึง พื้นที่ที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน และอุปกรณ์ต่อพ่วงต่าง ๆ
    ๒) พื้นที่ทำงานของผู้ดูแลระบบ
    ๓) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ หรือระบบเครือข่าย
    ๔) พื้นที่ใช้งานระบบเครือข่ายไร้สาย

- **เครื่องคอมพิวเตอร์** หมายถึง เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

- **ข้อมูลคอมพิวเตอร์** หมายถึง ข้อมูล ข้อความคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

- **ระบบจดหมายอิเล็กทรอนิกส์** (E-mail) หมายถึง ระบบที่บุคคลใช้ในการรับ-ส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหวและเสียง โดยผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียว หรือหลายคน

- **เครือข่ายสังคมออนไลน์** หมายถึง เว็บไซต์หรือแอปพลิเคชั่นที่ผู้ใช้งานสามารถนำเสนอและเผยแพร่ข้อมูลข่าวสารได้ด้วยตนเองออกสู่สาธารณะโดยใช้อุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารประภทต่าง ๆ

- **รหัสผ่าน** (Password) หมายถึง ชุดตัวอักษร หรืออักขระ หรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

- **บัญชีผู้ใช้** (Account) หมายถึง เป็นสัญลักษณ์หรือชุดของตัวอักษรเรียงติดต่อกันมีลักษณะเป็นหนึ่งเดียว (Unique) ไม่ซ้ำกันเพื่อเป็นการระบุตัว (Identification) เจ้าของบัญชีหรือกลุ่มคนที่สามารถเข้าถึงระบบได้ บัญชีผู้ใช้เป็นเครื่องมือรักษาความปลอดภัยที่ใช้ควบคู่กับรหัสผ่าน (Password)

- **ชุดคำสั่งไม่พึงประสงค์** หมายถึง ชุดคำสั่งที่มีผลทำให้คอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไขเปลี่ยนแปลง หรือเพิ่มเติม ขัดข้อง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายถึง การอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึง หรือใช้งานเครือข่ายหรือระบบสารสนเทศทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอกตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

- **ความมั่นคงปลอดภัยด้านสารสนเทศ** หมายถึง การธำรงไว้ซึ่งความลับความถูกต้องครบถ้วนและสภาพพร้อมใช้งานของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง ความรับผิดการห้ามปฏิเสธความรับผิดและความน่าเชื่อถือ
- **เหตุการณ์ด้านความมั่นคงปลอดภัย** หมายถึง การเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลวหรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย
- **สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด** หมายถึง สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบของหน่วยงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม
- **ความเสี่ยง** (Risk) หมายถึง โอกาสที่จะเกิดความผิดพลาด ความเสียหาย การรั่วไหล ความสูญเปล่าหรือเหตุการณ์ที่ไม่พึงประสงค์ ซึ่งอาจเกิดขึ้นในอนาคต และมีผลกระทบหรือทำให้การดำเนินงานไม่ประสบความสำเร็จตามวัตถุประสงค์ เป้าประสงค์ และเป้าหมายของสถาบัน
- **ประเมินความเสี่ยง** (Risk Assessment) หมายถึง กระบวนการวิเคราะห์ภัยและความอ่อนแอของระบบสารสนเทศรวมทั้งผลกระทบจากการสูญเสียสารสนเทศหรือการสูญเสียความสามารถในการรักษาความปลอดภัยของระบบสารสนเทศ การประเมินความเสี่ยงใช้เป็นพื้นฐานในการกำหนดมาตร การรักษาความปลอดภัยที่เหมาะสมให้ระบบสารสนเทศต่อไป
- **สารสนเทศที่กำหนดชั้นความลับ** หมายถึง สารสนเทศในรูปข้อมูลหรือข่าวสารที่บันทึกไว้ในแบบใดๆ ที่กำหนดชั้นความลับตามความสำคัญของเนื้อหาจำกัดการเข้าถึงและหรือจำกัดให้ทราบเท่าที่จำเป็น และให้รวมถึงจานบันทึกประมวลลับ รหัส และรหัสผ่านที่กำลังใช้อยู่หรือเตรียมจะใช้ตลอดจนวัสดุหรือเอกสารทุกอย่างที่บันทึกเรื่องดังกล่าว
- **ภัย** (Threat) หมายถึง อันตรายที่อาจเกิดขึ้นกับระบบสารสนเทศโดยคน (Person) สิ่งต่างๆ (Thing) หรือเหตุการณ์ (Event) ทั้งเจตนาและไม่เจตนาอันเป็นเหตุทำให้ข้อมูลข่าวสารของระบบสารสนเทศถูกเปิดเผย เปลี่ยนแปลง บิดเบือน ทำลาย ปฏิเสธการทำงานหรือการกระทำอื่นๆ ตามความต้องการของภัยนั้น
- **ความอ่อนแอ** (Vulnerability) หมายถึง จุดอ่อนหรือข้อบกพร่องใดๆ ก็ตามของระบบสารสนเทศที่ภัยในรูปแบบที่เหมาะกันสามารถนำไปใช้ประโยชน์เพื่อก่อให้เกิดอันตรายต่อระบบสารสนเทศนั้นๆ ได้ ความอ่อนแอที่มีอยู่ของระบบสารสนเทศและความรุนแรงที่เกิดจากภัยนั้นซึ่งภัยประเภทเดียวกันอาจมีระดับความเสี่ยงไม่เท่ากันในแต่ละพื้นที่ใช้งานระบบสารสนเทศ ความเสี่ยงเป็นสิ่งที่ใช้ตัดสินว่า ณ พื้นที่ใช้งานระบบสารสนเทศแต่ละแห่งควรจัดเตรียมระบบการรักษาความปลอดภัยให้หนาแน่นเพียงใด
- **ระบบสำรอง (Disaster Recovery Site : DR Site)** หมายถึง ระบบคอมพิวเตอร์สำรองซึ่งประกอบด้วยฮาร์ดแวร์ ซอฟต์แวร์ อุปกรณ์คอมพิวเตอร์ และอุปกรณ์เครือข่ายที่จำเป็น ที่สามารถทำงานได้ทันทีที่ระบบหลักมีปัญหา

ส่วนที่ ๑
นโยบายการควบคุมการเข้าถึงและการใช้งานระบบสารสนเทศ

วัตถุประสงค์

๑. เพื่อควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูลโดยคำนึงถึงการใช้งานและความมั่งคงปลอดภัย

๒. เพื่อกำหนดกฎเกณฑ์ที่เกี่ยวกับการอนุญาตให้เข้าถึงการกำหนดสิทธิ์และการมอบอำนาจของหน่วยงาน

๓. เพื่อให้ผู้ใช้งานได้รับรู้เข้าใจและสามารถปฏิบัติตามแนวทางที่กำหนดโดยเคร่งครัดและตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ

ผู้รับผิดชอบ

๑. หน่วยเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็กทรอนิกส์

แนวปฏิบัติ

๑. การควบคุมการเข้าถึงสารสนเทศ (Access Control)

๑.๑. ผู้ดูแลระบบจะอนุญาตให้ผู้ใช้งานเข้าถึงระบบสารสนเทศที่ต้องการใช้งานได้ต่อเมื่อได้รับอนุญาตจากผู้รับผิดชอบ/เจ้าของข้อมูล/เจ้าของระบบตามความจำเป็นต่อการใช้งานเท่านั้น

๑.๒. บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิ์ในการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้บังคับบัญชา

๑.๓. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานของผู้ใช้งานและหน้าที่ความรับผิดชอบในการปฏิบัติงานของผู้ใช้งานระบบสารสนเทศรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ ดังนี้

(๑.๓.๑) กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ์หรือการมอบอำนาจดังนี้

(๑.๓.๑.๑) กำหนดสิทธิ์ของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ์

(๑.๓.๑.๒) กำหนดเกณฑ์การระงับสิทธิ์มอบอำนาจให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๑.๓.๑.๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้บังคับบัญชาหรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๑.๓.๒) การแบ่งประเภทของข้อมูลและการจัดลำดับความสำคัญหรือลำดับชั้นความลับของข้อมูลใช้แนวทางปฏิบัติชั้นความลับตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ซึ่งระเบียบดังกล่าวเป็นมาตรการที่ละเอียดรอบคอบถือว่าเป็นแนวทางที่เหมาะสมในการจัดการเอกสารอิเล็กทรอนิกส์และในการรักษาความปลอดภัยของเอกสารอิเล็กทรอนิกส์โดยได้กำหนดกระบวนการและกรรมวิธีต่อเอกสารที่สำคัญไว้ดังนี้

(๑.๓.๒.๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ได้แก่ ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลการบริหารงานบุคคล ข้อมูลงบประมาณการเงินและบัญชี ข้อมูลการพัสดุ และทรัพย์สินเป็นต้น
- ข้อมูลสารสนเทศด้านการศึกษา ข้อมูลวิชาการ และนักศึกษา การวิจัย เป็นต้น

(๑.๓.๒.๒) จัดแบ่งระดับความสำคัญของข้อมูลออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๑.๓.๒.๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

- ข้อมูลลับที่สุด หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรงที่สุด
- ข้อมูลลับมาก หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายอย่างร้ายแรง
- ข้อมูลลับ หมายถึง หากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหาย
- ข้อมูลทั่วไป หมายถึง ข้อมูลที่สามารถเปิดเผยหรือเผยแพร่ทั่วไปได้

(๑.๓.๒.๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้รับมอบหมาย

(๑.๓.๒.๕) รูปแบบของเอกสารอิเล็กทรอนิกส์แบ่งได้ดังนี้

- รูปแบบเอกสารข้อความ (Text Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์ปกติเมื่อเปิดไฟล์จะสามารถเห็นตัวอักษรในไฟล์และพอที่จะอ่านข้อความนั้นได้ซึ่งมีรูปแบบย่อยอีกหลายรูปแบบ เช่น TEXT

Format, Document Format, PDF Format (Portable Document Format)

- รูปแบบเอกสารภาพ (Image Format) เป็นไฟล์ที่ผลิตจากเครื่องมือที่เป็นซอฟต์แวร์มีรูปแบบที่ใช้เช่น JPEG Format, PNG or GIF Format, Bitmapping Format เป็นต้น

๑.๔. ผู้ดูแลระบบต้องจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของหน่วยงานและตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบสารสนเทศ

๑.๕. ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศและการแก้ไขเปลี่ยนแปลงสิทธิ์ต่างๆ เพื่อเป็นหลักฐานในการตรวจสอบ

๑.๖. ผู้ดูแลระบบต้องจัดให้มีการบันทึกการผ่านเข้า-ออกสถานที่ตั้งของระบบสารสนเทศเพื่อเป็นหลักฐานในการตรวจสอบ

๑.๗. เวลาการเข้าถึงระบบสารสนเทศดังนี้

(๑.๗.๑) การเข้าถึงสารสนเทศในเวลาปฏิบัติงาน (๐๘.๓๐ น. – ๑๖.๓๐ น.)

(๑.๗.๒) การเข้าถึงสารสนเทศนอกเวลาปฏิบัติงาน (นอกช่วงเวลา ๐๘.๓๐ น. – ๑๖.๓๐ น.)

(๑.๗.๓) การเข้าถึงสารสนเทศในช่วงวันหยุด (วันหยุดราชการและวันหยุดนักขัตฤกษ์)

๑.๘. ช่องทางการเข้าถึงระบบสารสนเทศ

(๑.๘.๑) ระบบเครือข่ายภายในสถาบัน

(๑.๘.๒) ระบบเครือข่ายภายนอกสถาบัน

(๑.๘.๓) เข้าถึงโดยผ่านระบบที่จัดไว้ให้ เช่น VPN

๑.๙. ข้อกำหนดการใช้งานตามภารกิจ เพื่อควบคุมการเข้าถึงสารสนเทศ (business requirements for access control) โดยแบ่งการจัดทำข้อปฏิบัติเป็น ๒ ส่วน คือ

(๑.๙.๑) มีการควบคุมการเข้าถึงสารสนเทศ โดยให้กำหนดแนวทางการควบคุมการเข้าถึงเทคโนโลยีสารสนเทศ และสิทธิที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ

(๑.๙.๒) มีการปรับปรุงให้สอดคล้องกับข้อกำหนดการใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

๒. การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑. การสร้างความรู้ความเข้าใจให้กับผู้ใช้งาน

(๒.๑.๑) กำหนดหลักสูตรฝึกอบรมเกี่ยวกับการสร้างความตระหนักเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

(๒.๑.๒) ฝึกอบรมให้ความรู้ความเข้าใจกับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบเทคโนโลยีสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๒.๒. การลงทะเบียนผู้ใช้

(๒.๒.๑) จัดทำแบบฟอร์มการลงทะเบียนผู้ใช้งาน สำหรับระบบเทคโนโลยีสารสนเทศของสถาบัน

(๒.๒.๒) ผู้ดูแลระบบต้องตรวจสอบบัญชีผู้ใช้งาน เพื่อไม่ให้มีการลงทะเบียนซ้ำซ้อน

(๒.๒.๓) ผู้ดูแลระบบต้องตรวจสอบและให้สิทธิ์ในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบและมีความสอดคล้องกับนโยบายความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน

(๒.๒.๔) ผู้ดูแลระบบต้องมอบเอกสารรับรองสิทธิ์การเข้าถึงแก่ผู้ใช้งาน เพื่อแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศ รวมทั้งกำหนดให้ผู้ใช้งานทำการลงนามในเอกสารดังกล่าวหลังจากได้ทำความเข้าใจ

(๒.๒.๕) ผู้ดูแลระบบต้องกำหนดให้มีการถอดถอนสิทธิการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยทันที เมื่อผู้ใช้งานนั้นทำการลาออกหรือเปลี่ยนตำแหน่งงาน

(๒.๒.๖) การลงทะเบียนผู้ใช้งาน ผู้ดูแลระบบต้องทำการตรวจสอบหรือทบทวนบัญชีผู้ใช้งานทั้งหมด เพื่อป้องกันการเข้าถึงระบบเทคโนโลยีสารสนเทศโดยไม่ได้รับอนุญาต

(๒.๒.๗) การลงทะเบียนผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

(๒.๒.๗.๑) บุคลากรของสถาบัน อาจารย์พิเศษ นักวิจัย และผู้ติดต่อของหน่วยงานหน่วยเทคโนโลยีสารสนเทศ จะสร้างบัญชีเจ้าหน้าที่ใหม่หลังจากที่ได้รับแจ้งจากหน่วยทรัพยากรบุคคล ป้อนข้อมูลบุคลากรเข้าระบบสารสนเทศทรัพยากรบุคคล

(๒.๒.๗.๒) บุคคลอื่น ๆ ที่สถาบันมอบสิทธิ์ให้ เช่น อาสาสมัครที่ทำงานในหน่วยงาน บุคคลที่ทำงานในหน่วยงาน บุคคลที่สถาบันมอบสิทธิ์ให้ สามารถลงทะเบียนขอใช้งานบัญชีผู้ใช้ โดยติดต่อที่หน่วยเทคโนโลยีสารสนเทศ โดยมีหนังสือรับรองจากผู้บริหารระดับสาขาวิชา/หน่วยงานขึ้นไปและแสดงบัตรประชาชน หรือหนังสือเดินทาง พร้อมสำเนาที่รับรองสำเนาถูกต้อง ๑ ฉบับ

(๒.๒.๘) การจัดการสิทธิ์ผู้ใช้งานระบบเทคโนโลยีสารสนเทศ

(๒.๒.๘.๑) เมื่อบุคลากรของหน่วยงาน ลาออก หรือเปลี่ยนแปลงหน้าที่ความรับผิดชอบในระบบที่เคยขอสิทธิ์การใช้งานไว้ ต้องรีบแจ้งเพื่อเปลี่ยนสิทธิ์หรือถอดถอนสิทธิ์ออกจากระบบทันที

(๒.๒.๘.๒) การแจ้งขอใช้สิทธิ์/เปลี่ยนแปลงสิทธิ์ในการเข้าถึงและใช้งานข้อมูลสารสนเทศ และระบบสารสนเทศจะต้องทำเป็นลายลักษณ์อักษร ระบุเหตผล และความจำเป็น

- ลงชื่อโดยผู้บริหารของหน่วยงานที่ขอใช้
- ส่งถึงผู้บริหารระดับสูงสุดของสถาบัน
- เก็บเอกสารไว้เป็นหลักฐานอ้างอิง
- ผู้บริหารระดับสูงสุดของสถาบันสำเนาเอกสารการอนุญาตให้ผู้ดูแลระบบเพื่อดำเนินการ

(๒.๒.๘.๓) ให้อำนาจกับผู้ดูแลระบบในการระงับสิทธิ์ ในกรณีตรวจพบว่ามีการกระทำความผิดตามนโยบายการเข้าถึงและควบคุมการใช้งานสารสนเทศ

๒.๓. ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์ โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย

(Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และได้รับความเห็นชอบเป็นลายลักษณ์อักษร

๒.๔. การทบทวนสิทธิ์การเข้าถึง

(๒.๔.๑) ต้องมีกระบวนการทบทวนบัญชีผู้ใช้และสิทธิ์การใช้งานระบบสารสนเทศ และปรับปรุงบัญชีผู้ใช้อย่างน้อยปีละ ๑ ครั้ง

(๒.๔.๒) ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิ์การใช้งาน

(๒.๔.๒.๑) กรณีบุคลากร เมื่อพ้นสภาพการเป็นบุคลากรของสถาบัน ต้องดำเนินการภายใน ๓ วัน

(๒.๔.๒.๒) กรณีบุคลากร เมื่อมีการเปลี่ยนแปลงตำแหน่งงานภายในสถาบัน ต้องดำเนินการภายใน ๗ วัน

(๒.๔.๒.๓) กรณีที่ไม่ใช่บุคลากรของสถาบัน จะหมดอายุตามวันที่ระบุในเอกสารขอเปิดบัญชี หรือ เมื่อไม่มีการเข้าใช้งานติดต่อกันเกิน ๓ เดือน

๒.๕. การบริหารจัดการสิทธิ์การใช้งานและรหัสผ่าน

(๒.๕.๑) ผู้ดูแลระบบที่รับผิดชอบระบบงานนั้น ๆ ต้องกำหนดสิทธิ์ของผู้ใช้งานในการเข้าถึงระบบเทคโนโลยีสารสนเทศแต่ละระบบ รวมทั้งกำหนดสิทธิ์แยกตามหน้าที่ที่รับผิดชอบ

(๒.๕.๒) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(๒.๕.๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๒.๕.๔) ส่งมอบรหัสผ่าน (Password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่มีการป้องกันในการส่งรหัสผ่าน (Password)

(๒.๕.๕) กำหนดให้ผู้ใช้งานตอบยืนยันการได้รับรหัสผ่าน (Password)

(๒.๕.๖) กำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่าน (Password) ผิดพลาดได้ไม่เกิน ๓ ครั้ง

(๒.๕.๗) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๒.๕.๘) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าสามารถเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๖. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ มีดังต่อไปนี้

(๒.๖.๑) ควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒.๖.๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๒.๖.๓) ต้องกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๒.๖.๔) การรับ-ส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๒.๖.๕) ควรกำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๒.๖.๖) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำสินทรัพย์ออกนอกหน่วยงาน เช่น บำรุงรักษาตรวจซ่อม ให้ดำเนินการสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๒.๗. ระบบงานสารสนเทศที่จะต้องเชื่อมโยงกัน (Business Information Systems) ให้ผู้บังคับบัญชาพิจารณาประเด็นต่างๆ ทางด้านความมั่นคงปลอดภัยและจุดอ่อนต่าง ๆ ก่อนตัดสินใจใช้ข้อมูลร่วมกันในระบบงานหรือระบบเทคโนโลยีสารสนเทศที่จะเชื่อมโยงเข้าด้วยกัน เช่น ระหว่างหน่วยงานที่มาขอเชื่อมโยง

(๒.๗.๑) กำหนดนโยบายและมาตรการเพื่อควบคุมป้องกันและบริหารจัดการการใช้ข้อมูลร่วมกัน

(๒.๗.๒) พิจารณาจำกัดหรือไม่อนุญาตการเข้าถึงข้อมูลส่วนบุคคล

(๒.๗.๓) พิจารณาว่ามีบุคลากรใดบ้างที่มีสิทธิ์หรือได้รับอนุญาตให้เข้าใช้งาน

(๒.๗.๔) พิจารณาเรื่องการลงทะเบียนผู้ใช้งาน

(๒.๗.๕) ไม่อนุญาตให้มีการใช้งานข้อมูลสำคัญหรือข้อมูลลับร่วมกันในกรณีที่ระบบไม่มีมาตรการป้องกันเพียงพอ

๓. การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

๓.๑. การใช้งานรหัสผ่าน ผู้ใช้งานต้องปฏิบัติ ดังนี้

(๓.๑.๑) ผู้ใช้งานมีหน้าที่ในการป้องกันดูแลรักษาข้อมูลบัญชีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) โดยผู้ใช้งานแต่ละคนต้องมีบัญชีชื่อผู้ใช้งาน (Username) ของตนเอง ห้ามใช้ร่วมกับผู้อื่น รวมทั้งห้ามทำการเผยแพร่แจกจ่ายทำให้ผู้อื่นล่วงรู้รหัสผ่าน (Password)

(๓.๑.๒) กำหนดรหัสผ่านประกอบด้วยตัวอักษรไม่น้อยกว่า ๖ ตัวอักษรซึ่งต้องประกอบด้วยตัวเลข (Numerical character) ตัวอักษร (Alphabet) และตัวอักษรพิเศษ (Special character)

(๓.๑.๓) ไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัว

(๓.๑.๔) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๓.๑.๕) ไม่ใช้โปรแกรมคอมพิวเตอร์ช่วยในการจำรหัสผ่านส่วนบุคคลอัตโนมัติ (save password) สำหรับเครื่องคอมพิวเตอร์ส่วนบุคคลที่ผู้ใช้งานครอบครองอยู่

(๓.๑.๖) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น

(๓.๑.๗) กำหนดรหัสผ่านเริ่มต้นให้กับผู้ใช้งานให้ยากต่อการเดา และการส่งมอบรหัสผ่านให้กับผู้ใช้งานต้องเป็นไปอย่างปลอดภัย

(๓.๑.๘) ผู้ใช้งานต้องเปลี่ยนรหัสผ่าน (Password) ไม่เกิน ๑๘๐ วัน หรือทุกครั้งที่มีการแจ้งเตือนให้เปลี่ยนรหัสผ่าน

๓.๒. การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานจะต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๓.๓. การกระทำใด ๆ ที่เกิดจากการใช้บัญชีของผู้ใช้งาน (Username) อันมีกฎหมายกำหนดให้เป็นความผิดไม่ว่าการกระทำนั้นจะเกิดจากผู้ใช้งานหรือไม่ก็ตามให้ถือว่าเป็นความรับผิดชอบส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

๓.๔. ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนที่จะใช้สินทรัพย์หรือระบบสารสนเทศของหน่วยงาน และหากการพิสูจน์ตัวตนนั้นมีปัญหาไม่ว่าจะเกิดจากรหัสผ่านล็อก หรือเกิดจากความผิดพลาดใดๆ ผู้ใช้งานต้องแจ้งให้ผู้ดูแลระบบทราบทันทีโดยปฏิบัติตามแนวทาง ดังนี้

(๓.๔.๑) คอมพิวเตอร์ทุกประเภทก่อนการเข้าถึงระบบปฏิบัติการต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓.๔.๒) การใช้งานระบบคอมพิวเตอร์อื่นในเครือข่ายจะต้องทำการพิสูจน์ตัวตนทุกครั้ง

(๓.๔.๓) การใช้งานอินเทอร์เน็ต (Internet) ต้องทำการพิสูจน์ตัวตนและต้องมีการบันทึกข้อมูลซึ่งสามารถบ่งบอกตัวตนบุคคลผู้ใช้งานได้

(๓.๔.๔) เมื่อผู้ใช้งานไม่อยู่ที่เครื่องคอมพิวเตอร์ต้องทำการล็อกหน้าจอทุกครั้งและต้องทำการพิสูจน์ตัวตนก่อนการใช้งานทุกครั้ง

(๓.๔.๕) เครื่องคอมพิวเตอร์ทุกเครื่องต้องทำการตั้งเวลาพักหน้าจอ (screen saver) โดยตั้งเวลาอย่างน้อย ๑๕ นาที หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๓.๔.๖) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๓.๕. ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูลไม่ว่าข้อมูลนั้นจะเป็นของสถาบันหรือเป็นข้อมูลของบุคคลภายนอก

๓.๖. ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่เปลี่ยนแปลงทำซ้ำหรือทำลายโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๓.๗. ผู้ใช้งานมีส่วนร่วมในการดูแลรักษาและรับผิดชอบต่อข้อมูลของสถาบันและข้อมูลของผู้รับบริการ หากเกิดการสูญหายโดยนำไปใช้ในทางที่ผิด การเผยแพร่โดยไม่ได้รับอนุญาตผู้ใช้งานต้องมีส่วนร่วมในการรับผิดชอบต่อความเสียหายนั้นด้วย

๓.๘. ผู้ใช้งานต้องป้องกันดูแลรักษาไว้ซึ่งความลับ ความถูกต้องและความพร้อมใช้ของข้อมูลตลอดจนเอกสารสื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศต่างๆ ที่เสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์

๓.๙. ผู้ใช้งานมีสิทธิ์โดยชอบธรรมที่จะเก็บรักษา ใช้งานและป้องกันข้อมูลส่วนบุคคลตามเห็นสมควร สถาบันจะให้การสนับสนุนและเคารพต่อสิทธิส่วนบุคคลและไม่อนุญาตให้บุคคลหนึ่งบุคคลใดทำการละเมิดต่อข้อมูลส่วนบุคคลโดยไม่ได้รับอนุญาตจากผู้ใช้งานที่ครอบครองข้อมูลนั้น ยกเว้นในกรณีที่หน่วยงานต้องการตรวจสอบข้อมูล หรือคาดว่าข้อมูลนั้นเกี่ยวข้องกับหน่วยงาน ซึ่งหน่วยงานอาจแต่งตั้งให้ผู้ทำหน้าที่ตรวจสอบทำการตรวจสอบข้อมูลเหล่านั้นได้ตลอดเวลาโดยไม่ต้องแจ้งให้ผู้ใช้งานทราบ

๓.๑๐. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมประเภท Peer-to-Peer (หมายถึงวิธีการจัดเครือข่ายคอมพิวเตอร์แบบหนึ่งที่กำหนดให้เครื่องคอมพิวเตอร์ในเครือข่ายทุกเครื่องเหมือนกันหรือเท่าเทียมกันหมายถึงแต่ละเครื่องต่างมีโปรแกรมหรือมีแฟ้มข้อมูลเก็บไว้เองการจัดแบบนี้ทำให้สามารถใช้โปรแกรมหรือแฟ้มข้อมูลของเครื่องคอมพิวเตอร์เครื่องใดก็ได้แทนที่จะต้องใช้จากเครื่องบริการแฟ้ม (File Server) เท่านั้น) หรือโปรแกรมที่มีความเสี่ยงในระดับเดียวกัน เช่น บิทเทอร์เรนท์ (Bittorrent), อีมูล (Emule) เป็นต้น เว้นแต่จะได้รับอนุญาตจากผู้บังคับบัญชา

๓.๑๑. ห้ามเปิดหรือใช้งาน (Run) โปรแกรมออนไลน์ทุกประเภทเพื่อความบันเทิง เช่น การดูหนังฟัง เพลง เกมส์ เป็นต้น ในระหว่างเวลาปฏิบัติงาน

๓.๑๒. ห้ามใช้สินทรัพย์ของหน่วยงานที่จัดเตรียมให้เพื่อการเผยแพร่ข้อมูล ข้อความรูปภาพ หรือสิ่งอื่นใดที่มีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อภารกิจของสถาบัน

๓.๑๓. ห้ามใช้สินทรัพย์ของหน่วยงานเพื่อการรบกวนก่อให้เกิดความเสียหาย หรือใช้ในการโจรกรรมข้อมูล หรือสิ่งอื่นใดอันเป็นการขัดต่อกฎหมายและศีลธรรม หรือกระทบต่อภารกิจของสถาบัน

๓.๑๔. ห้ามใช้สินทรัพย์ของสถาบันเพื่อประโยชน์ทางการค้า

๓.๑๕. ห้ามกระทำการใดๆ เพื่อการดักข้อมูลไม่ว่าจะเป็นข้อความภาพ เสียง หรือสิ่งอื่นใดในเครือข่ายระบบสารสนเทศของสถาบันโดยเด็ดขาดไม่ว่าจะด้วยวิธีการใดๆ ก็ตาม

๓.๑๖. ห้ามกระทำการรบกวน ทำลาย หรือทำให้ระบบสารสนเทศของหน่วยงานต้องหยุดชะงัก

๓.๑๗. ห้ามใช้ระบบสารสนเทศของสถาบัน เพื่อการควบคุมคอมพิวเตอร์หรือระบบสารสนเทศภายนอกโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๓.๑๘. ห้ามกระทำการใด ๆ อันมีลักษณะเป็นการลักลอบใช้งาน หรือรับรู้รหัสส่วนบุคคลของผู้อื่นไม่ว่าจะเป็นกรณีใดๆ เพื่อประโยชน์ในการเข้าถึงข้อมูลหรือเพื่อการใช้ทรัพยากรก็ตาม

๓.๑๙. ห้ามติดตั้งอุปกรณ์หรือกระทำการใดๆ เพื่อเข้าถึงระบบสารสนเทศของสถาบันโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๔. การบริหารจัดการสินทรัพย์ (Assets Management)

๔.๑. ผู้ใช้งานต้องไม่เข้าไปในศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) และห้องระบบเครือข่ายที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๔.๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) และห้องระบบเครือข่าย เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๔.๓. ผู้ใช้งานต้องไม่นำเครื่องมือหรืออุปกรณ์อื่นใดเชื่อมเข้าระบบเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

๔.๔. ผู้ใช้งานต้องไม่คัดลอกหรือทำสำเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กำกับการใช้งานก่อนได้รับอนุญาตและผู้ใช้งานต้องไม่ใช้หรือลบแฟ้มข้อมูลของผู้อื่นไม่ว่ากรณีใด ๆ

๔.๕. ผู้ใช้งานต้องทำลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูลก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	**วิธีทำลาย**
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ใช้การทำลายข้อมูลบน Flash Drive ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกา ซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร

เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	- ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ตามมาตรฐาน DOD 5220.22 M ของกระทรวงกลาโหมสหรัฐอเมริกาซึ่งเป็นมาตรฐานการทำลายข้อมูลโดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๔.๖. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Assetlists) ที่ผู้ใช้งานต้องรับผิดชอบการรับหรือคืนสินทรัพย์จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

๔.๗. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

๔.๘. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุดหรือสูญหายตามมูลค่าทรัพย์สินหากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๔.๙. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมเครื่องคอมพิวเตอร์หรือโน้ตบุ๊กไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากผู้บังคับบัญชา

๔.๑๐. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งานโดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนดหรือทำให้เกิดความเสียหายต่อสถาบัน

๔.๑๑. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๔.๑๐ ให้ถือเป็นความผิดส่วนบุคคลโดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

๕. การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๕.๑. ผู้ใช้งานที่ได้รับอนุญาตเข้าถึงระบบเครือข่าย สามารถเข้าใช้ได้เฉพาะบริการในระบบเครือข่ายตามสิทธิ์ที่ได้รับอนุญาตเท่านั้น

๕.๒. ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์ อุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์ ระบบเครือข่ายต้องได้รับอนุญาตจากผู้ดูแลระบบหรือเจ้าหน้าที่ที่ได้รับมอบหมาย และต้องปฏิบัติตามนโยบายโดยเคร่งครัด

๕.๓. ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติม หรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๕.๔. การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) จะต้องมีข้อปฏิบัติหรือกระบวนการให้มีการยืนยันตัวบุคคลก่อนได้รับอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบเทคโนโลยีสารสนเทศของหน่วยงานได้ ดังนี้

(๕.๔.๑) ผู้ใช้งานที่จะเข้าใช้งานระบบต้องพิสูจน์ตัวตนผู้ใช้ด้วยบัญชีผู้ใช้งาน (Username) ทุกครั้ง

(๕.๔.๒) ให้มีการตรวจสอบผู้ใช้งานทุกครั้งก่อนที่จะอนุญาตให้เข้าถึงระบบข้อมูล โดยจะต้องมีวิธีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง ด้วยการใช้รหัสผ่าน (Password) หรือการใช้สมาร์ทการ์ด

(๕.๔.๓) จะต้องมีวิธีการในการตรวจสอบเพื่อพิสูจน์ตัวตน สำหรับการเข้าสู่ระบบเทคโนโลยีสารสนเทศของหน่วยงาน อย่างน้อย ๑ วิธี

(๕.๔.๔) ผู้ดูแลระบบต้องตรวจสอบผู้ใช้งานเมื่อมีการเข้าสู่ระบบเทคโนโลยีสารสนเทศของหน่วยงานจากอินเทอร์เน็ต

๕.๕. การระบุอุปกรณ์ที่นำมาเชื่อมต่อบนเครือข่าย

(๕.๕.๑) ผู้ดูแลระบบมีการเก็บบัญชีการขอเชื่อมต่อเครือข่าย ได้แก่ รายชื่อผู้ขอใช้บริการ รายละเอียดเครื่องคอมพิวเตอร์ที่ขอใช้บริการ IP Address และสถานที่ติดตั้ง

(๕.๕.๒) ผู้ดูแลระบบต้องจำกัดผู้ใช้งานที่สามารถเข้าใช้อุปกรณ์ได้

(๕.๕.๓) กรณีอุปกรณ์ที่มีการเชื่อมต่อจากเครือข่ายภายนอกต้องมีการระบุหมายเลขอุปกรณ์ว่าสามารถเข้าเชื่อมต่อกับเครือข่ายภายในได้หรือไม่สามารถเชื่อมต่อได้

(๕.๕.๔) อุปกรณ์เครือข่ายต้องสามารถตรวจสอบ IP Address ของทั้งต้นทางและปลายทางได้

(๕.๕.๕) การเข้าใช้งานอุปกรณ์บนเครือข่ายต้องทำการพิสูจน์ตัวตนของผู้ใช้ทุกครั้ง

(๕.๕.๖) อุปกรณ์ที่นำมาเชื่อมต่อได้รับหมายเลขไอพีแอดเดรสตามที่กำหนดโดยผู้ดูแลระบบเครือข่าย

(๕.๕.๗) เก็บข้อมูลการใช้ Mac Address จากเครื่องบริการกำหนดค่าหมายเลขไอพีแอดเดรส (DHCP Server) หรือจาก ARP Table บนสวิทช์ L3

๕.๖. การป้องกันพอร์ตที่ใช้สำหรับทดสอบและปรับแต่งระบบ

(๕.๖.๑) ต้องควบคุมพอร์ตและหมายเลขไอพีแอดเดรสที่ใช้สำหรับตรวจสอบและปรับแต่งระบบให้เข้าถึงอุปกรณ์เครือข่ายอย่างรัดกุม

(๕.๖.๒) ต้องกำหนดรหัสผ่านสำหรับตรวจสอบและปรับปรุงอุปกรณ์เครือข่าย เมื่อใช้การเชื่อมต่อโดยตรงบนตัวอุปกรณ์

(๕.๖.๓) ไม่อนุญาตให้เชื่อมต่อพอร์ตโดยตรงจากเครือข่ายภายนอกสถาบัน แต่ให้เชื่อมต่อโดยตรงบนตัวอุปกรณ์

(๕.๖.๔) อุปกรณ์เครือข่ายคอมพิวเตอร์ที่สำคัญต้องจัดเก็บในห้องอุปกรณ์เครือข่ายที่ควบคุมความปลอดภัย

(๕.๖.๕) ต้องปิดพอร์ตหรือปิดบริการ บนอุปกรณ์เครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

(๕.๖.๖) ต้องตรวจสอบและปิดพอร์ตของระบบหรืออุปกรณ์ที่ไม่มีความจำเป็นในการเข้าใช้งานอย่างสม่ำเสมออย่างน้อยสัปดาห์ละ ๑ ครั้ง

๕.๗. กำหนดให้มีการแบ่งแยกเครือข่าย ดังต่อไปนี้

(๕.๗.๑) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอกและอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(๕.๗.๒) แบ่งแยกเครือข่ายตามกลุ่มของบริการ กลุ่มผู้ใช้งาน และระบบงานต่างๆ ของสถาบัน

(๕.๗.๓) ต้องแบ่งแยกเครือข่ายภายในออกเป็นเครือข่ายย่อยๆ

(๕.๗.๔) ต้องใช้เกตเวย์เพื่อควบคุมการเข้าถึงเครือข่ายภายในและเครือข่ายภายนอกหน่วยงานซึ่งสอดคล้องกับนโยบายควบคุมการเข้าถึงและนโยบายการใช้งานบริการเครือข่ายของหน่วยงาน

๕.๘. ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสถาบันต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุกและต้องมีความสามารถในการตรวจจับโปรแกรมไม่ประสงค์ดี และอนุญาตการเชื่อมต่อเฉพาะหมายเลขไอพีแอดเดรสที่กำหนดให้เท่านั้น

๕.๙. ต้องมีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของหน่วยงานในลักษณะที่ผิดปกติ โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่ายการใช้งานในลักษณะที่ผิดปกติและการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง

๕.๑๐. IP address ของระบบงานเครือข่ายภายในจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ เพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายได้โดยง่าย

๕.๑๑. การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายต้องได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑๒. ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่ายเพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(๕.๑๒.๑) ต้องมีวิธีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

(๕.๑๒..๒) ควรมีวิธีการจำกัดเส้นทางเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

(๕.๑๒.๓) ต้องจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(๕.๑๒.๔) ต้องป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็น IP Address ภายในของระบบเครือข่ายภายในของสถาบัน

(๕.๑๒..๕) ต้องกำหนดการป้องกันเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจนและต้องทบทวนการกำหนดค่า Parameter ต่างๆ เช่น IP Address อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนดแก้ไขหรือเปลี่ยนแปลงค่า parameter ต้องแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๑๓. กำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(๕.๑๓.๑) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรเพื่อขออนุญาตจากผู้บังคับบัญชาของหน่วยงานหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

(๕.๑๓.๒) ผู้ดูแลระบบควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม ต้องไม่เปิด Port ที่ใช้ทิ้งเอาไว้โดยไม่จำเป็น และช่องทางดังกล่าวจะต้องตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วโดยอัตโนมัติ และจะเปิดให้ใช้ได้ต่อเมื่อมีการร้องขอที่จำเป็นเท่านั้น

(๕.๑๓.๓) วิธีการใด ๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการอนุญาตจากผู้บังคับบัญชาของหน่วยงานหรือผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

(๕.๑๓.๔) การเข้าสู่ระบบจากระยะไกล ผู้ใช้งานต้องแสดงหลักฐาน ระบุเหตุผลหรือความจำเป็นในการดำเนินงานกับหน่วยงานอย่างเพียงพอ

(๕.๑๓.๕) การเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบของหน่วยงาน

(๕.๑๓.๖) การเข้าสู่ระบบต้องมีการใช้มาตรการรักษาความปลอดภัยที่เพิ่มขึ้นจากมาตรฐานการเข้าสู่ระบบภายใน เช่น การใช้ VPN SSL เป็นต้น

(๕.๑๓.๗) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานสามารถเชื่อมต่อกับระบบระยะไกลได้เพียงหนึ่งการเชื่อมต่อในขณะเวลาเดียวกัน

(๕.๑๓.๘) ผู้ดูแลระบบต้องกำหนด Port ที่ใช้ในการเข้าสู่ระบบ และจะต้องตรวจสอบและติดตามการใช้งานเป็นประจำอย่างน้อยเดือนละ ๑ ครั้ง

๕.๑๔. การควบคุมการจัดการเส้นทางบนเครือข่าย

(๕.๑๔.๑) อนุญาตเส้นทางเครือข่ายเฉพาะกลุ่มหมายเลขไอพีแอดเดรสที่กำหนด

(๕.๑๔.๒) มีเกตเวย์เพื่อกรองข้อมูลที่ไหลเวียนในเครือข่าย และต้องควบคุมการไหลของข้อมูลผ่านเครือข่าย

(๕.๑๔.๓) ต้องกำหนดเส้นทางการไหลของข้อมูลบนระบบเครือข่ายที่สอดคล้องกับการควบคุมการเข้าถึงและการใช้บริการบนเครือข่าย

(๕.๑๔.๔) ต้องจำกัดการใช้เส้นทางบนระบบเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์แม่ข่ายเพื่อระงับการใช้จากเส้นทางอื่น

(๕.๑๔.๕) ต้องตรวจสอบหมายเลขไอพีแอดเดรสของต้นทางและปลายทาง

๖. การควบคุมการเข้าถึงระบบเครือข่ายไร้สาย (Wireless LAN Access Control)

๖.๑. ผู้ใช้งานที่ต้องการเข้าถึงระบบเครือข่ายไร้สายภายในสถาบันจะต้องทำการลงทะเบียนกับผู้ดูแลระบบ และได้รับพิจารณาอนุญาตจากผู้บริหารหน่วยงานที่เป็นเจ้าของระบบเครือข่ายไร้สายนั้น

๖.๒. ผู้ดูแลระบบเครือข่ายไร้สายต้องดำเนินการดังต่อไปนี้

(๖.๒.๑) ต้องทำการลงทะเบียนกำหนดสิทธิ์ผู้ใช้งานในการเข้าถึงระบบเครือข่ายไร้สายให้เหมาะสมกับหน้าที่ความรับผิดชอบในการปฏิบัติงานก่อนเข้าใช้ระบบเครือข่ายไร้สายรวมทั้งมีการทบทวนสิทธิ์การเข้าถึงอย่างสม่ำเสมอ

(๖.๒.๑.๑) ต้องทำการลงทะเบียนอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ทุกตัวที่ใช้ในระบบเครือข่ายไร้สาย

(๖.๒.๑.๒) ต้องควบคุม ป้องกันสัญญาณของอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) ไม่ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สาย

(๖.๒.๑.๓) ต้องทำการเปลี่ยนค่า SSID (Service SetIdentifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณไร้สาย (Access Point) มาใช้งาน

(๖.๒.๑.๔) ต้องทำการเปลี่ยนค่าชื่อบัญชีผู้ใช้และรหัสผ่านในการเข้าสู่ระบบสำหรับการตั้งค่าการทำงานของอุปกรณ์กระจายสัญญาณ และต้องเลือกใช้บัญชีรายชื่อและรหัสผ่านที่คาดเดาได้ยาก เพื่อป้องกันผู้โจมตีไม่ให้สามารถเดาหรือเจาะรหัสผ่านได้โดยง่าย

(๖.๒.๑.๕) ต้องเข้ารหัสข้อมูลระหว่าง wireless LAN Client และอุปกรณ์กระจายสัญญาณ ไร้สาย ด้วยวิธีที่มีประสิทธิภาพไม่ด้อยกว่าวิธี WPA2 (Wi-Fi Protected Access) เพื่อให้ยากต่อการดักจับข้อมูลและทำให้ปลอดภัยมากขึ้น

(๖.๒.๑.๖) ควรเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และ/หรือชื่อผู้ใช้ (Username) รหัสผ่าน (Password) ของผู้ใช้บริการที่มีสิทธิ์ในการเข้าใช้งานระบบเครือข่ายไร้สายโดยจะอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และ/หรือชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(๖.๒.๑.๗) ควรกำหนดให้ผู้ใช้บริการในระบบเครือข่ายไร้สายติดต่อสื่อสารได้เฉพาะกับ VPN (Virtual Private Network) เพื่อช่วยป้องกันการบุกรุกในระบบเครือข่ายไร้สาย

(๖.๒.๑.๘) ต้องติดตั้งอุปกรณ์ป้องกันการบุกรุก (Firewall) ระหว่างเครือข่ายไร้สายกับเครือข่ายภายในสถาบัน

(๖.๒.๑.๑) ต้องใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายอย่างสม่ำเสมอ เพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สายและเมื่อตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติให้ผู้ดูแลระบบรายงานต่อผู้บังคับบัญชาทราบโดยทันที

๗. การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๗.๑. ผู้ดูแลระบบต้องกำหนดชื่อผู้ใช้และรหัสผ่านให้กับผู้ใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของหน่วยงาน

๗.๒. กำหนดขั้นตอนการปฏิบัติเพื่อเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยแสดงวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย โดยมีแนวปฏิบัติ ดังนี้

(๗.๒.๑) ต้องไม่ให้ระบบแสดงรายละเอียดสำคัญหรือความผิดพลาดต่างๆ ของระบบก่อนที่การเข้าสู่ระบบจะเสร็จสมบูรณ์

(๗.๒.๒) ระบบสามารถยุติการเชื่อมต่อเครื่องปลายทางได้ เมื่อพบว่ามีการพยายามคาดเดารหัสผ่านจากเครื่องปลายทาง

(๗.๒.๓) จำกัดระยะเวลาสำหรับใช้ในการป้อนรหัสผ่าน

(๗.๒.๔) จำกัดการเชื่อมต่อโดยตรงสู่ระบบปฏิบัติการผ่านทาง Command Line เนื่องจากอาจสร้างความเสียหายให้กับระบบได้

๗.๓. ระบุและยืนยันตัวตนของผู้ใช้งาน (User Identification and Authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงที่สามารถระบุตัวตนของผู้ใช้งานและเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติ ดังนี้

(๗.๓.๑) การพิสูจน์ตัวตนสำหรับผู้ใช้งาน ผู้ดูแลระบบเทคโนโลยีสารสนเทศต้องให้มีการพิสูจน์ตัวตนสำหรับผู้ใช้งานเป็นรายบุคคลก่อนที่จะอนุญาตให้เข้าใช้งานระบบ

(๗.๓.๒) ผู้ใช้งานต้องทำการพิสูจน์ตัวตนทุกครั้งก่อนใช้ระบบเทคโนโลยีสารสนเทศ เพื่อป้องกันผู้ไม่มีสิทธิ์เข้าใช้งานระบบเทคโนโลยีสารสนเทศ หากการระบุและยืนยันตัวตนของผู้ใช้งานมีปัญหาหรือเกิดความผิดพลาด ผู้ใช้งานแจ้งให้ผู้ดูแลระบบทำการแก้ไข

(๗.๓.๓) ผู้ใช้งานต้องเก็บรักษาบัญชีผู้ใช้บริการ (Account) ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือแจกจ่ายให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

(๗.๓.๔) ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้ชื่อบัญชีผู้ใช้บริการ (Account) ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

๗.๔. การบริหารจัดการรหัสผ่าน (Password Management System)

(๗.๔.๑) ต้องจำกัดระยะเวลาในการป้อนรหัสผ่าน หากผู้ใช้งานป้อนรหัสผ่านผิดเกินจำนวนครั้งที่กำหนด ระบบจะทำการล็อกสิทธิ์การเข้าถึงของผู้ใช้งาน ทำให้ไม่สามารถใช้งานได้จนกว่าผู้ดูแลระบบจะปลดล็อกให้

(๗.๔.๒) ระบบสามารถยุติการเชื่อมต่อจากเครื่องปลายทางได้ เมื่อพบว่ามีความพยายามในการเดารหัสผ่านจากเครื่องปลายทาง

(๗.๔.๓) มีระบบให้ผู้ใช้งานสามารถเปลี่ยนและยืนยันรหัสผ่านได้ด้วยตนเอง

(๗.๔.๔) ต้องจัดเก็บไฟล์ข้อมูลรหัสผ่านของผู้ใช้งานแยกต่างหากจากข้อมูลของระบบงาน

(๗.๔.๕) ไม่แสดงข้อมูลรัหสผ่านในหน้าจอของผู้ใช้งานระหว่างที่ผู้ใช้งานกำลังใส่ข้อมูลรหัสผ่านของตนเอง แต่แสดงเป็นเครื่องหมายจุดหรือดอกจันบนหน้าจอแทน

(๗.๔.๖) เมื่อได้ดำเนินการติดตั้งระบบแล้ว ให้ยกเลิกชื่อผู้ใช้งานหรือเปลี่ยนรหัสผ่านของทุกชื่อผู้ใช้ที่ได้ถูกกำหนดไว้เริ่มต้นที่มาพร้อมกับการติดตั้งระบบโดยทันที

๗.๕. การใช้งานโปรแกรมประเภทยูทิลิตี้ (Use of system utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมยูทิลิตี้สำหรับโปรแกรมคอมพิวเตอร์ที่สำคัญ เนื่องจากการใช้งานโปรแกรมยูทิลิตี้บางชนิดสามารถทำให้ผู้ใช้หลีกเลี่ยงมาตรการป้องกันทางด้านความมั่นคงปลอดภัยของระบบได้ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้วให้ดำเนินการ ดังนี้

(๗.๕.๑) การใช้งานโปรแกรมยูทิลิตี้ต้องได้รับการอนุมัติจากผู้ดูแลระบบและต้องมีการพิสูจน์ยืนยันตัวตนสำหรับการเข้าไปใช้งานโปรแกรมยูทิลิตี้เพื่อจำกัดและควบคุมการใช้งาน

(๗.๕.๒) โปรแกรมที่ติดตั้ง ต้องเป็นโปรแกรมที่สถาบันได้ซื้อลิขสิทธิ์ถูกต้องตามกฎหมาย

(๗.๕.๓) ต้องจัดเก็บโปรแกรมยูทิลิตี้ออกจากซอฟต์แวร์สำหรับระบบงาน

(๗.๕.๔) มีการจำกัดสิทธิ์ผู้ที่ได้รับอนุญาตให้ใช้งานโปรแกรมยูทิลิตี้

(๗.๕.๕) ต้องยกเลิกหรือลบทิ้งโปรแกรมยูทิลิตี้และซอฟต์แวร์ที่เกี่ยวข้องกับระบบงานที่ไม่มีความจำเป็นในการใช้งานรวมทั้งต้องป้องกันไม่ให้ผู้ใช้งานสามารถเข้าถึงหรือใช้งานโปรแกรมยูทิลิตี้ได้

(๗.๕.๖) ห้ามผู้ใช้งานคัดลอกโปรแกรมต่าง ๆ แล้วนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

๗.๖. การกำหนดเวลาใช้งานระบบสารสนเทศ (Session time-out)

(๗.๖.๑) ให้กำหนดหลักเกณฑ์การยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานเป็นเวลาไม่เกิน ๓๐ นาที หากเป็นระบบที่มีความเสี่ยงสูงหรือมีความสำคัญสูง ให้กำหนดระยะเวลายุติการใช้งานเมื่อว่างเว้นจาการใช้งานให้สั้นลงหรือเป็นเวลาไม่เกิน ๑๕ นาที ตามความเหมาะสม เพื่อป้องกันการเข้าถึงข้อมูลสำคัญโดยไม่ได้รับอนุญาต

(๗.๖.๒) ถ้าไม่มีการใช้ระบบ ต้องทำการยกเลิกการใช้โปรแกรมประยุกต์และการเชื่อมต่อเข้าสู่ระบบโดยอัตโนมัติ

(๗.๖.๓) เครื่องปลายทางที่ตั้งอยู่ในพื้นที่ที่มีความเสี่ยงสูงต้องกำหนดระยะเวลาให้ทำการปิดเครื่องโดยอัตโนมัติ หลังจากที่ไม่มีการใช้งานเป็นระยะเวลาตามกำหนด

๗.๗. การจำกัดระยะเวลาการเชื่อมต่อระบบเทคโนโลยีสารสนเทศ (Limitation of connection time)

(๗.๗.๑) กำหนดหลักเกณฑ์ในการจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ สำหรับระบบสารสนเทศที่มีความเสี่ยงสูงหรือมความสำคัญสูง เพื่อให้ผู้ใช้งานสามารถใช้งานได้นานที่สุดภายในระยะเวลาที่กำหนดเท่านั้น เช่น กำหนดให้ใช้งานได้ ๓ ชั่วโมงต่อการเชื่อมต่อ ๑ ครั้ง เป็นต้น และกำหนดให้ใช้งานได้เฉพาะในช่วงเวลาทำการตามปกติของหน่วยงานเท่านั้น

(๗.๗.๒) กำหนดช่วงเวลาสำหรับการเชื่อมต่อระบบเครือข่ายจากเครื่องปลายทางจะต้องพิจารณาถึงระดับความเสี่ยงของที่ตั้งของเครื่องปลายทางด้วย

(๗.๗.๓) กำหนดให้ระบบสารสนเทศ เช่น ระบบงานที่มีความสำคัญสูง และ/หรือระบบงานที่มีการใช้งานในสถานที่ที่มีความเสี่ยงในที่สาธารณะ หรือพื้นที่ภายนอกสำนักงาน มีการจำกัดช่วงเวลาการเชื่อมต่อ

๘. การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๘.๑. ให้หน่วยงาน กำหนดมาตรการควบคุมการเข้าใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงานเพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกหรือบุคคลภายนอกที่ต้องการสิทธิในการเข้าใช้ระบบเทคโนโลยีสารสนเทศของหน่วยงานจะต้องขออนุญาตจากผู้บังคับบัญชาหรือจากผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา

๘.๒. ผู้ดูแลระบบต้องกำหนดสิทธิ์การเข้าถึงข้อมูลและระบบข้อมูลให้เหมาะสมกับการเข้าใช้งานระบบ และหน้าที่ความรับผิดชอบของเจ้าหน้าที่ในการปฏิบัติงานก่อนเข้าใช้ระบบเทคโนโลยีสารสนเทศ รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างสม่ำเสมอ

๘.๓. ผู้ดูแลระบบ ควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน และตรวจตราการละเมิดความปลอดภัยที่มีต่อระบบข้อมูล

๘.๔. ผู้ดูแลระบบ จัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาตเพื่อเป็นหลักฐานในการตรวจสอบ

๘.๕. ผู้ดูแลระบบ ต้องกำหนดการลงทะเบียนบุคลากรใหม่ของสถาบัน ต้องกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามความจำเป็นรวมทั้งขั้นตอนปฏิบัติ สำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๘.๖. ผู้ดูแลระบบต้องกำหนดสิทธิ์การใช้งานระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (E-Mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิ์เฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ์ดังกล่าวอย่างสม่ำเสมอ

๘.๗. ผู้ดูแลระบบต้องกำหนดระยะเวลาในการเชื่อมต่อระบบสารสนเทศที่ใช้ในการปฏิบัติงานระบบสารสนเทศต่างๆ เมื่อผู้ใช้งานไม่มีการใช้งานระบบสารสนเทศเกิน ๑๕ นาที ระบบจะยุติการใช้งาน ผู้ใช้งานต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนเข้าระบบสารสนเทศอีกครั้ง

๘.๘. ผู้ดูแลระบบต้องบริหารจัดการสิทธิ์การใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

(๘.๘.๑) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่าน (Password) เมื่อผู้ใช้งานระบบลาออกหรือพ้นจากตำแหน่งหรือยกเลิกการใช้งาน

(๘.๘.๒) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(๘.๘.๓) กำหนดชื่อผู้ใช้งานหรือรหัสผู้ใช้งานต้องไม่ซ้ำกัน

(๘.๘.๔) ในกรณีมีความจำเป็นต้องให้สิทธิ์พิเศษกับผู้ใช้งานที่มีสิทธิ์สูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่งและมีการกำหนดสิทธิ์พิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้างและต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๘.๙. ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงานรวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(๑) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(๒) ต้องกำหนดรายชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้งานข้อมูลในแต่ละชั้นความลับของข้อมูล

(๓) กำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(๔) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากลเช่น SSL, VPN หรือ XML Encryption เป็นต้น

(๕) กำหนดการเปลี่ยนรหัสผ่าน (Password) ตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูล

(๖) กำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของหน่วยงาน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

๘.๑๐. ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน จะต้องดำเนินการ ดังนี้

(๑) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อสถาบัน ได้แก่ ระบบ FMIS เป็นระบบที่ใช้ในการปฏิบัติงานด้านการเงิน การบัญชี และการพัสดุ ของสถาบันจะได้รับการแยกออกจากระบบงานอื่นๆ ของหน่วยงาน

(๒) ต้องมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ โดยมีพื้นที่ปฏิบัติงานแยกเป็นสัดส่วน และต้องมีการกำหนดสิทธิให้เฉพาะผู้ที่มีสิทธิใช้ระบบเท่านั้น เข้าปฏิบัติงานในพื้นที่ควบคุมดังกล่าว

๘.๑๑. การใช้งานอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ต้องปฏิบัติ ดังต่อไปนี้

(๑) ตรวจสอบความพร้อมของเครื่องคอมพิวเตอร์และอุปกรณ์ที่จะนำไปใช้งานว่าอยู่ในสภาพพร้อมใช้งานหรือไม่และตรวจสอบโปรแกรมมาตรฐานว่าถูกต้องตามลิขสิทธิ์

(๒) ระมัดระวังไม่ให้บุคคลภายนอกคัดลอกข้อมูลจากเครื่องคอมพิวเตอร์ที่นำไปใช้ได้เว้นแต่ข้อมูลที่ได้มีการเผยแพร่เป็นการทั่วไป

(๓) เมื่อหมดความจำเป็นต้องใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่แล้วให้รีบนำส่งคืนเจ้าหน้าที่ที่รับผิดชอบทันที

(๔) เจ้าหน้าที่ผู้รับผิดชอบในการรับคืนต้องตรวจสอบสภาพความพร้อมใช้งานของอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่รับคืนด้วย

(๕) หากปรากฏว่าความเสียหายที่เกิดขึ้นนั้นเกิดจากความประมาทอย่างร้ายแรงของผู้นำไปใช้ ผู้นำไปใช้ต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

(๖) การใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ทั้งของส่วนตัวและอุปกรณ์ของสถาบัน

(๖.๑) ต้องล็อกหรือยึดเครื่องให้อยู่กับที่กรณีนำเครื่องไปใช้ในที่สาธารณะ หรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย

(๖.๒) ต้องเปิดใช้ระบบล็อกหน้าจออัตโนมัติหรือปิดเครื่องอัตโนมัติเมื่อไม่ได้ใช้งาน และในกรณีที่ไม่ได้ใช้งานเป็นการชั่วคราวต้องล็อกหน้าจอทุกครั้ง

(๖.๓) ผู้ใช้ต้องตั้งรหัสผ่านเพื่อเข้าใช้งานคอมพิวเตอร์แบบพกพา

(๖.๔) ไม่ใช้คอมพิวเตอร์พกพาร่วมกับบุคคลอื่น

(๖.๕) ต้องตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส ก่อนการใช้งานสื่อบันทึกข้อมูลพกพาต่าง ๆ

(๖.๖) ไม่เก็บข้อมูลสำคัญของหน่วยงานไว้บนอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ที่ใช้งานอยู่ หากจำเป็นต้องจัดเก็บข้อมูลบนอุปกรณ์ดังกล่าวจะต้องเข้ารหัสข้อมูลทุกครั้ง

(๖.๗) ห้ามใช้อุปกรณ์คอมพิวเตอร์และสื่อสารพกพา เป็นอุปกรณ์กระจายสัญญาณเครือข่ายไร้สายภายในสถาบัน

(๖.๘) ต้องจัดการกับโปรแกรมไม่พึงประสงค์ในอุปกรณ์ประเภทพกพา เช่น ติดตั้งโปรแกรมป้องกันมัลแวร์ ปรับปรุงระบบปฏิบัติการให้ทันสมัย ไม่ติดตั้งซอฟต์แวร์ผิดกฎหมาย ไม่ติดตั้งซอฟต์แวร์ที่ไม่รู้จัก ฯลฯ

(๖.๙) มีกระบวนการจัดการกรณีที่อุปกรณ์คอมพิวเตอร์พกพาเกิดการสูญหายหรือถูกขโมย เช่น เปิดระบบล็อกไบออส เข้ารหัสไฟส์ข้อมูล เข้ารหัสฮาร์ดดิสก์ ติดตั้งโปรแกรมติดตามเครื่อง ฯลฯ

(๗) การสำรองข้อมูลและการกู้คืน

(๗.๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกข้อมูลสำรอง (Backup Media) เช่น ซีดี ดีวีดี ฮาร์ดดิสก์ภายนอก (External Harddisk) เป็นต้น

(๗.๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อบันทึกข้อมูลสำรองไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูล และทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

๘.๑๒. การควบคุมผู้รับเหมาช่วง (Outsource) กรณีการจ้างเหมาบำรุงรักษา ดูแล และพัฒนาระบบสารสนเทศ

(๑) มีกระบวนการคัดเลือกผู้รับเหมาช่วงโดยเฉพาะ และต้องกำหนดคุณสมบัติของผู้รับเหมาช่วงที่ชัดเจน เช่น ต้องมีประสบการณ์ มีลูกค้าอ้างอิงน่าเชื่อถือ หรือใบรับรองทางด้านทักษะวิชาชีพตามมาตรฐานสากล มีความพร้อมด้านเทคโนโลยีของการรับเหมาช่วงทั้งในส่วนของ ฮาร์ดแวร์และซอฟต์แวร์ รวมถึงระบบสนับสนุนอื่น ๆ เพื่อให้ได้รับเหมาช่วงที่มีคุณสมบัติตรงตามมาตรฐานที่หน่วยงานต้องการ

(๒) มีข้อตกลงหรือสัญญาอย่างชัดเจนในการว่าจ้างผู้รับเหมาช่วง และต้องกำหนดขอบเขตและระดับการรับเหมาช่วงอย่างชัดเจน และผู้รับเหมาช่วงต้องนำเสนอรายละเอียดงานขอบเขตงานอย่างครบถ้วน

(๓) หน่วยงานต้องเข้าตรวจสอบรายละเอียดการปฏิบัติงานของผู้รับเหมาช่วงได้ เช่น ร่วมกำหนดวิธีทำงาน การตรวจติดตามคุณภาพของผู้รับเหมาช่วงเป็นระยะ ๆ ตามที่กำหนดไว้ หรือการสุ่มตรวจสอบการปฏิบัติงานในจุดที่สำคัญ เพื่อพิจารณากระบวนการที่ผู้รับเหมาช่วงใช้ในการปฏิบัติงาน และเพื่อประเมินความสม่ำเสมอของผู้รับเหมาช่วงในการกระทำตามข้อกำหนดของหน่วยงาน

(๔) ต้องควบคุมการเข้าถึงของข้อมูลที่ชัดเจน มีระบบบันทึกการเข้าถึงข้อมูล และการสำรองข้อมูลทุกขั้นตอน จำกัดการเข้าถึงข้อมูลสำคัญหรือให้ใช้ข้อมูลจากชุดจำลองแทนข้อมูลจริง

(๕) มีหลักเกณฑ์และกระบวนการในการตรวจรับงานที่ส่งมอบโดยผู้รับเหมาช่วงที่ชัดเจน เพื่อให้ได้งานตรงตามมาตรฐานที่กำหนด

๙. การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์และการป้องกันโปรแกรมไม่ประสงค์ดี (Software Licensing and intellectual property and Preventing Malware)

๙.๑. สถาบันได้ให้ความสำคัญต่อเรื่องทรัพย์สินทางปัญญา และไม่สนับสนุนการใช้ซอฟต์แวร์ที่ละเมิดลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ สถาบันถือว่าเป็นความผิดส่วนบุคคลผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๙.๒. เครื่องคอมพิวเตอร์ของผู้ใช้งานติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ (Anti virus) ตามที่หน่วยงานได้ประกาศให้ใช้ เว้นแต่เครื่องคอมพิวเตอร์นั้นเป็นเครื่องเพื่อการศึกษาโดยต้องได้รับอนุญาตจากผู้บังคับบัญชา

๙.๓. บรรดาข้อมูลไฟล์ซอฟต์แวร์หรือสิ่งอื่นใดที่ได้รับจากผู้ใช้งานอื่นต้องได้รับการตรวจสอบไวรัสคอมพิวเตอร์และโปรแกรมไม่ประสงค์ดีก่อนนำมาใช้งานหรือเก็บบันทึกทุกครั้ง

๙.๔. ผู้ใช้งานต้องทำการปรับปรุงข้อมูลสำหรับตรวจสอบและปรับปรุงระบบปฏิบัติการ (Update patch) ให้ใหม่เสมอเพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้น

๙.๕. ผู้ใช้งานต้องพึงระวังไวรัสและโปรแกรมไม่ประสงค์ดีตลอดเวลา รวมทั้งเมื่อพบสิ่งผิดปกติผู้ใช้งานต้องแจ้งเหตุแก่ผู้ดูแลระบบ

๙.๖. เมื่อผู้ใช้งานพบว่าเครื่องคอมพิวเตอร์ติดไวรัสผู้ใช้งานต้องไม่เชื่อมต่อเครื่องคอมพิวเตอร์เข้าสู่เครือข่ายและต้องแจ้งแก่ผู้ดูแลระบบ

๙.๗. ห้ามลักลอบทำสำเนาเปลี่ยนแปลง ลบทิ้งซึ่งข้อมูลข้อความเอกสารหรือสิ่งใดๆ ที่เป็นสินทรัพย์ของหน่วยงานหรือของผู้อื่นโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๙.๘. ห้ามทำการเผยแพร่ไวรัสคอมพิวเตอร์มัลแวร์หรือโปรแกรมอันตรายใดๆ ที่อาจก่อให้เกิดความเสียหายมาสู่สินทรัพย์ของหน่วยงาน สิทธิ์ที่จะพัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ สามารถดำเนินการได้แต่ต้องไม่ดำเนินการ ดังนี้

(๑) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใด ๆ ที่จะทำลายกลไกรักษาความปลอดภัยระบบรวมทั้งการกระทำในลักษณะเป็นการแอบใช้รหัสผ่านการลักลอบทำสำเนาข้อมูลบุคคลอื่นหรือแกะรหัสผ่านของบุคคลอื่น

(๒) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ซึ่งทำให้ผู้ใช้งานมีสิทธิ์และลำดับความสำคัญในการครอบครองทรัพยากรระบบมากกว่าผู้ใช้งานอื่น

(๓) พัฒนาโปรแกรมใดที่จะทำซ้ำตัวโปรแกรมหรือแฝงตัวโปรแกรมไปกับโปรแกรมอื่นในลักษณะเช่นเดียวกับหนอนหรือไวรัสคอมพิวเตอร์

(๔) พัฒนาโปรแกรมหรือฮาร์ดแวร์ใดๆ ที่จะทำลายระบบจำกัดสิทธิ์การใช้ (License) ซอฟต์แวร์

(๕) นำเสนอข้อมูลที่ผิดกฎหมายละเมิดลิขสิทธิ์ แสดงข้อความรูปภาพไม่เหมาะสมหรือขัดต่อศีลธรรมประเพณีอันดีงามของประเทศไทยกรณีที่ผู้ใช้งานสร้างเว็บเพจบนเครือข่ายคอมพิวเตอร์

๙.๙. การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced software development)

(๑) จัดให้มีการควบคุมโครงการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๒) พิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดในการพัฒนาซอฟต์แวร์โดยผู้รับจ้างให้บริการจากภายนอก

(๓) พิจารณากำหนดเรื่องการสงวนสิทธิ์ที่จะตรวจสอบด้านคุณภาพและความถูกต้องของซอฟต์แวร์ที่จะมีการพัฒนาโดยผู้ให้บริการภายนอกโดยระบุไว้ในสัญญาจ้างที่ทำกับผู้ให้บริการภายนอกนั้น

(๔) ให้มีการตรวจสอบโปรแกรมไม่ประสงค์ดีในซอฟต์แวร์ต่างๆ ที่จะทำการติดตั้งก่อนดำเนินการติดตั้ง

(๕) หลังจากการส่งมอบการพัฒนาซอฟแวร์จากหน่วยงานภายนอก หน่วยงานต้องดำเนินการเปลี่ยนรหัสผ่านต่างๆ

๑๐. การปฏิบัติงานจากภายนอกสำนักงาน (Teleworking)

๑๐.๑. ต้องมีการกำหนดมาตรการและการเตรียมการต่าง ๆ ที่จำเป็นก่อน ซึ่งรวมถึงการเตรียมการป้องกันทางกายภาพสำหรับสถานที่ที่จะอนุญาตการปฏิบัติงานของผู้ใช้งานจากระยะไกล ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๑๐.๒. ต้องมีการกำหนดมาตรการที่มีความมั่นคงปลอดภัยสำหรับระบบสื่อสารข้อมูลระหว่างสถานที่ที่จะปฏิบัติงานจากระยะไกลและระบบงานภายในสถาบัน ก่อนที่จะอนุญาตให้เริ่มปฏิบัติงานจากระยะไกล

๑๐.๓. ต้องกำหนดให้ผู้ปฏิบัติงานจากระยะไกลไม่อนุญาตให้ครอบครัวหรือเพื่อนของตนเองเข้าถึงระบบเทคโนโลยีสารสนเทศภายในสถาบัน

๑๐.๔. ต้องมีการกำหนดมาตรการควบคุมสำหรับการใช้งานเครือข่ายจากที่บ้านหรือเครือข่ายสาธารณะเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของสถาบัน รวมทั้งมาตรการควบคุมการใช้บริการเครือข่ายไร้สายที่บ้านหรือที่สาธารณะ

๑๐.๕. ต้องมีการตรวจสอบว่าอุปกรณ์ที่เป็นของส่วนตัวซึ่งใช้ในการเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกล มีการป้องกันไวรัสและการใช้งานไฟร์วอลล์ตามที่หน่วยงานกำหนด

๑๐.๖. ต้องมีการจัดเตรียมอุปกรณ์สำหรับการปฏิบัติงานจากระยะไกลการจัดเก็บข้อมูลและอุปกรณ์สื่อสารไว้ให้กับผู้ใช้งานจากระยะไกล

๑๐.๗. ผู้ใช้งานจากระยะไกลทุกคนต้องผ่านการพิสูจน์ตัวตนเพื่อเพิ่มความปลอดภัยจะต้องมีการตรวจสอบ เช่น รหัสผ่านหรือวิธีการเข้ารหัส เป็นต้น

๑๐.๘. หน่วยงานไม่อนุญาตให้ใช้งานอุปกรณ์ที่เป็นของส่วนตัวเพื่อเข้าถึงระบบเทคโนโลยีสารสนเทศของหน่วยงานจากระยะไกลหากอุปกรณ์ดังกล่าวไม่อยู่ภายใต้การควบคุม ดูแล ตามนโยบายความมั่นคงปลอดภัยของหน่วยงาน

๑๐.๙. หน่วยงานต้องกำหนดชนิดของงานที่อนุญาตและไม่อนุญาตให้ทำสำหรับการปฏิบัติงานจากระยะไกล ชั่วโมงการทำงานในสถานที่ดังกล่าว ชั้นความลับของข้อมูลที่อนุญาตให้ใช้งานได้ และระบบงานและบริการต่างๆ ของหน่วยงานที่อนุญาตและไม่อนุญาตให้เข้าถึงได้จากระยะไกล

๑๐.๖. หน่วยงานต้องกำหนดขั้นตอนปฏิบัติสำหรับการขออนุมัติและการขอยกเลิกการปฏิบัติงานจากระยะไกล การกำหนดหรือปรับปรุงสิทธิการเข้าถึงระบบงาน และการคืนอุปกรณ์ที่ใช้งานเมื่อมีการยกเลิกการปฏิบัติงาน

๑๑. การใช้งานอินเทอร์เน็ต (Use of the Internet)

๑๑.๑. ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ตผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้ตามสิทธิ์ที่ได้รับ

๑๑.๒. ห้ามใช้อินเทอร์เน็ตของสถาบันเพื่อหาผลประโยชน์เชิงพาณิชย์เป็นการส่วนบุคคล

๑๑.๓. ผู้ใช้งานต้องไม่เข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงของชาติ ศาสนา และพระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ์ของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสถาบัน เป็นต้น

๑๑.๔. ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการปรับปรุงโปรแกรมต่าง ๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

๑๑.๕. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่างๆ ของไฟร์วอลล์

๑๑.๖. ไม่ควรใช้บริการบนอินเทอร์เน็ตที่มีการครอบครองแบนด์วิดท์จำนวนมากหรือเป็นเวลานาน

๑๒. การใช้งานและการควบคุมการใช้จดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒.๑. ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (E-Mail) ต้องทำการกรอกข้อมูลขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ (E-Mail) โดยยื่นคำขอกับหน่วยเทคโนโลยีสารสนเทศ

๑๒.๒. รหัสจดหมายอิเล็กทรอนิกส์เวลาใส่รหัสผ่านต้องไม่ปรากฏหรือแสดงรหัสผ่านออกมาแต่ต้องแสดงออกมาในรูปของสัญลักษณ์แทนตัวอักษรนั้น เช่น “x” หรือ “O” ในการพิมพ์แต่ละตัวอักษร

๑๒.๓. เมื่อได้รับรหัสผ่าน (Password) ครั้งแรกในการเข้าระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นให้เปลี่ยนรหัสผ่าน (Password) โดยทันที

๑๒.๔. ผู้ดูแลระบบต้องกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดได้ เช่น ไม่เกิน ๓ ครั้ง

๑๒.๕. ไม่บันทึกหรือเก็บรหัสผ่าน (Password) ไว้ในระบบคอมพิวเตอร์

๑๒.๖. เปลี่ยนรหัสผ่าน (Password) ทุก ๓ – ๖ เดือน

๑๒.๗. ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-Mail Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความยกเว้นแต่จะได้รับการยินยอมจากเจ้าของผู้ใช้งานและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ (E-Mail) เป็นผู้รับผิดชอบต่อการใช้งานในจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตน

๑๒.๘. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-Mail) เสร็จสิ้นต้องลงบันทึกออก (Logout) ทุกครั้ง

๑๒.๙. การส่งข้อมูลที่เป็นความลับไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์ (E-Mail) เว้นเสียแต่ว่าจะใช้วิธีการเข้ารหัสข้อมูลอีเมล์ที่หน่วยงานกำหนดไว้ให้ใช้ความระมัดระวังในการระบุชื่อที่อยู่ E-Mail ของผู้รับให้ถูกต้องเพื่อป้องกันการส่งผิดตัวผู้รับ

๑๒.๑๐. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายขยะ (Spam Mail)

๑๒.๑๑. ห้ามส่งอีเมล์ที่มีลักษณะเป็นจดหมายลูกโซ่ (Chain Letter)

๑๒.๑๒. ห้ามส่งอีเมล์ที่มีลักษณะเป็นการละเมิดต่อกฎหมายหรือสิทธิของบุคคลอื่น

๑๒.๑๓. ห้ามส่งอีเมล์ที่มีไวรัสไปให้กับบุคคลอื่นโดยเจตนา

๑๒.๑๔. ให้ระบุชื่อของผู้ส่งในอีเมล์ทุกฉบับที่ส่งไป

๑๒.๑๕. ให้ทำการสำรองข้อมูลอีเมล์ตามความจำเป็นอย่างสม่ำเสมอ (แม้ว่าหน่วยงานจะทำการสำรองข้อมูล E-Mail ไว้ให้แต่ก็เพียงช่วงระยะเวลาหนึ่งเท่านั้น ดังนั้น อีเมล์ที่เก่ามากๆ และจำเป็นต้องใช้งานจึงมีความจำเป็นต้องสำรองเก็บไว้ด้วยตนเอง)

๑๒.๑๖. ผู้ใช้งานต้องทำการตรวจสอบเอกสารแนบจากจดหมายอิเล็กทรอนิกส์ (E-Mail) ก่อนการเปิดเพื่อตรวจสอบไฟล์โดยใช้โปรแกรมป้องกันไวรัสเป็นการป้องกันในการเปิดไฟล์ที่เป็น Executable file เช่น .exe .com เป็นต้น

๑๒.๑๗. ผู้ใช้งานต้องไม่เปิดหรือส่งต่อจดหมายอิเล็กทรอนิกส์ (E-Mail) หรือข้อความที่ได้รับจาก ผู้ส่งที่ไม่รู้จัก

๑๒.๑๘. ผู้ใช้งานต้องไม่ใช้ข้อความที่ไม่สุภาพหรือรับส่งจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่เหมาะสมข้อมูลอันอาจทำให้เสียชื่อเสียงของหน่วยงานทำให้เกิดความแตกแยกระหว่างหน่วยงานผ่านทางจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒.๑๙. ผู้ใช้งานต้องตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตนเองทุกวันและควรจัดเก็บแฟ้มข้อมูลและจดหมายอิเล็กทรอนิกส์ (E-Mail) ของตนให้เหลือจำนวนน้อยที่สุดและควรลบจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่ต้องการออกจากระบบเพื่อลดปริมาณการใช้เนื้อที่ระบบจดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒.๒๐. ข้อควรระวัง ผู้ใช้งานควรโอนย้ายจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่จะใช้อ้างอิงภายหลังมายังเครื่องคอมพิวเตอร์ของตนเพื่อเป็นการป้องกันผู้อื่นแอบอ่านจดหมายได้ ดังนั้น ไม่ควรจัดเก็บข้อมูลหรือจดหมายอิเล็กทรอนิกส์ (E-Mail) ที่ไม่ได้ใช้แล้วไว้ในตู้จดหมายอิเล็กทรอนิกส์ (E-Mail)

๑๒.๒๑. ผู้ใช้งานต้องใช้จดหมายอิเล็กทรอนิกส์ (E-Mail) ของสถาบันสำหรับใช้รับ-ส่งข้อมูล ติดต่อกับหน่วยงานภายในสถาบัน หรือหน่วยงานอื่น ๆ ภายนอก

๑๓. การบริหารจัดการคอมพิวเตอร์แม่ข่าย (Server Management)

๑๓.๑. กำหนดผู้ดูแลระบบสำหรับเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องอย่างเป็นลายลักษณ์อักษร

๑๓.๒. มีขั้นตอน/กระบวนการในการตรวจสอบคอมพิวเตอร์แม่ข่าย และในกรณีที่พบว่ามีการใช้งานหรือเปลี่ยนแปลงค่าที่ผิดปกติ จะต้องดำเนินการแก้ไขและบันทึกรายงานการแก้ไขโดยทันที

๑๓.๓. ตั้งนาฬิกาของเครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่อง และอุปกรณ์คอมพิวเตอร์ที่ให้บริการทุกชนิดให้ตรงกับเวลาอ้างอิงมาตรฐาน (๑.ntp.redcross.or.th และ ๒.ntp.redcross.or.th) ที่สถาบันใช้อ้างอิง

๑๓.๔. เปิดใช้บริการเท่าที่จำเป็นเท่านั้น โดยต้องมีมาตรการป้องกันเพิ่มเติมสำหรับบริการที่มีความเสี่ยงต่อระบบรักษาความปลอดภัย

๑๓.๕. ต้องปรับปรุงซอฟต์แวร์ให้เป็นปัจจุบันอยู่เสมอ เพื่ออุดช่องโหว่ต่าง ๆ

๑๓.๖. ต้องทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัยและประสิทธิภาพการใช้งานโดยทั่วไปก่อนติดตั้งและหลังจากการแก้ไขหรือบำรุงรักษา

๑๓.๗. การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะต้องดำเนินการโดยผู้ดูแลระบบของหน่วยงาน

๑๔. การควบคุมการใช้งานอุปกรณ์ป้องกันเครือข่าย (Firewall Control)

๑๔.๑. หน่วยงานที่มีหน้าที่ในการบริหารจัดการ การติดตั้ง และกำหนดค่าของไฟร์วอลล์ทั้งหมด

๑๔.๒. การกำหนดค่าเริ่มต้นของไฟร์วอลล์ต้องกำหนดเป็นปฏิเสธทั้งหมด (Deny)

๑๔.๓. ทุกบริการ (Services) และเส้นทางเชื่อมต่ออินเทอร์เน็ตที่ไม่อนุญาตตาม Policy จะต้องถูกบล็อก (Block) โดยไฟร์วอลล์

๑๔.๔. ผู้ใช้งานอินเทอร์เน็ตจะต้องทำการลงบันทึกเข้าใช้งาน (Login) ก่อนการใช้งานทุกครั้ง

๑๔.๕. การกำหนดค่าบริการและการเชื่อมต่อที่อนุญาตจะต้องมีการบันทึกการเปลี่ยนแปลงทุกครั้งหากมีการเปลี่ยนแปลงค่าต่างๆของไฟร์วอลล์

๑๔.๖. การเข้าถึงตัวอุปกรณ์ไฟร์วอลล์ จะต้องสามารถเข้าถึงได้เฉพาะผู้ที่ได้รับมอบหมายให้ดูแลจัดการเท่านั้น

๑๔.๗. ข้อมูลจราจรทางคอมพิวเตอร์ที่เข้าออกอุปกรณ์ไฟร์วอลล์ จะต้องส่งค่าไปจัดเก็บยังอุปกรณ์จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Centralized log) โดยจะต้องจัดเก็บตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐

๑๔.๘. การกำหนดนโยบายในการให้บริการอินเทอร์เน็ตกับเครื่องคอมพิวเตอร์ลูกข่ายจะเปิดพอร์ตการเชื่อมต่อพื้นฐานของโปรแกรมทั่วไปที่อนุญาตให้ใช้งานซึ่งหากมีความจำเป็นที่จะใช้งานพอร์ตการเชื่อมต่อนอกเหนือที่กำหนดจะต้องได้รับความยินยอมจากผู้บังคับบัญชาก่อน

๑๔.๙. การกำหนดค่าการให้บริการของเครื่องคอมพิวเตอร์แม่ข่ายในแต่ละส่วนของเครือข่ายจะต้องกำหนดค่าอนุญาตเฉพาะพอร์ตการเชื่อมต่อที่จำเป็นต่อการให้บริการเท่านั้น

๑๔.๑๐. จะต้องมีการสำรองข้อมูลการกำหนดค่าต่างๆ ของอุปกรณ์ไฟร์วอลล์เป็นประจำทุกสัปดาห์หรือทุกครั้งก่อนที่จะมีการเปลี่ยนแปลงค่า

๑๔.๑๑. เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบงานสารสนเทศต่างๆ ภายในหน่วยงานที่มีลักษณะที่เป็นอินทราเน็ตจะต้องไม่อนุญาตให้มีการเชื่อมต่อเพื่อใช้งานอินเทอร์เน็ต เว้นแต่มีความจำเป็นโดยจะต้องกำหนดเป็นกรณีไป

๑๔.๑๒. หน่วยงานมีสิทธิ์ที่จะระงับหรือบล็อกการใช้งานของเครื่องคอมพิวเตอร์ลูกข่ายที่มีพฤติกรรมการใช้งานที่ผิดนโยบายหรือเกิดจากการทำงานของโปรแกรมที่มีความเสี่ยงต่อความปลอดภัยจนกว่าจะได้รับการแก้ไข

๑๔.๑๓. การเชื่อมต่อในลักษณะของการ Remote Login จากภายนอกมายังเครื่องคอมพิวเตอร์แม่ข่ายหรืออุปกรณ์เครือข่ายภายในจะต้องบันทึกรายการของการดำเนินการตามแบบการขออนุญาตดำเนินการเกี่ยวกับเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย และจะต้องได้รับความเห็นชอบจากผู้บังคับบัญชาก่อน

๑๔.๑๔. ผู้ละเมิดนโยบายด้านความปลอดภัยของไฟร์วอลล์ จะถูกระงับการใช้งานอินเทอร์เน็ตโดยทันที

๑๕. การตรวจจับการบุกรุก (Intrusion Detection System / Intrusion Prevention System Policy: IDS/IPS)

๑๕.๑. IDS/IPS Policy เป็นนโยบายการติดตั้งระบบตรวจสอบการบุกรุกและตรวจสอบความปลอดภัยของเครือข่ายเพื่อป้องกันทรัพยากรระบบสารสนเทศและข้อมูลบนเครือข่ายภายในสถาบันให้มีความมั่นคงปลอดภัยเป็นแนวทางการปฏิบัติเกี่ยวกับการตรวจสอบการบุกรุกเครือข่ายพร้อมกับบทบาทและความรับผิดชอบที่เกี่ยวข้อง

๑๕.๒. IDS/IPS Policy ครอบคลุมทุกโฮสต์ (Host) ในเครือข่ายของสถาบันและเครือข่ายข้อมูลทั้งหมดรวมถึงเส้นทางที่ข้อมูลอาจเดินทางซึ่งไม่อยู่ในเครือข่ายอินเทอร์เน็ตทุกเส้นทาง

๑๕.๓. ระบบทั้งหมดที่สามารถเข้าถึงได้จากอินเทอร์เน็ตหรือที่สาธารณะจะต้องผ่านการตรวจสอบจากระบบ IDS/IPS

๑๕.๔. ระบบทั้งหมดใน DMZ (Demilitarized zone) จะต้องได้รับการตรวจสอบรูปแบบการให้บริการก่อนการติดตั้งและเปิดให้บริการ

๑๕.๕. โฮสต์ (Host) และเครือข่ายทั้งหมดที่มีการส่งผ่านข้อมูลผ่าน IDS/IPS จะต้องมีการบันทึกผลการตรวจสอบ

๑๕.๖. ระบบ IDS/IPS จะต้องมีการตรวจสอบและ Update Patch/Signature เป็นประจำ

๑๕.๗. ต้องมีการตรวจสอบเหตุการณ์ข้อมูลจราจรพฤติกรรมการใช้งานกิจกรรมและบันทึกปริมาณข้อมูลเข้าใช้งานเครือข่ายเป็นประจำทุกวันโดยผู้ดูแลระบบ

๑๕.๘. IDS/IPS จะทำงานภายใต้กฎควบคุมพื้นฐานของไฟร์วอลล์ที่ใช้ในการเข้าถึงเครือข่ายของระบบสารสนเทศตามปกติ

๑๕.๙. เครื่องแม่ข่ายที่มีการติดตั้ง host-based IDS จะต้องมีการตรวจสอบข้อมูลประจำวัน

๑๕.๑๐. พฤติกรรมการใช้งานกิจกรรมหรือเหตุการณ์ทั้งหมดที่มีความเสี่ยงต่อการบุกรุกการโจมตีระบบพฤติกรรมที่น่าสงสัยหรือการพยายามเข้าระบบทั้งที่ประสบความสำเร็จและไม่ประสบความสำเร็จจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบทันทีที่ตรวจพบ

๑๕.๑๑. พฤติกรรมกิจกรรมที่น่าสงสัยหรือระบบการทำงานที่ผิดปกติที่ถูกค้นพบจะต้องมีการรายงานให้ผู้บังคับบัญชาทราบภายใน ๑ ชั่วโมงที่ตรวจพบ

๑๕.๑๒. การตรวจสอบการบุกรุกทั้งหมดจะต้องเก็บบันทึกข้อมูลไว้ไม่น้อยกว่า ๙๐ วัน

๑๕.๑๓. ระบบ IDS/IPS มีรูปแบบการตอบสนองต่อเหตุการณ์ที่เกิดขึ้น ได้แก่ รายงานผลการตรวจพบของเหตุการณ์ต่างๆ ดำเนินการตามขั้นตอนเพื่อลดความเสียหาย ลบซอฟต์แวร์มุ่งร้ายที่ตรวจพบป้องกันเหตุการณ์ที่อาจเกิดอีกในอนาคตและดำเนินการตามแผน เป็นต้น

๑๕.๑๔. หน่วยงานมีสิทธิ์ในการยุติการเชื่อมต่อเครือข่ายของเครื่องคอมพิวเตอร์ที่มีพฤติกรรมเสี่ยงต่อการบุกรุกระบบโดยไม่ต้องมีการแจ้งแก่ผู้ใช้งานล่วงหน้า

๑๕.๑๕. ผู้ที่ถูกตรวจสอบว่าพยายามกระทำการอันใดที่เป็นการละเมิดนโยบายของสถาบัน การพยายามเข้าถึงระบบโดยมิชอบ การโจมตีระบบหรือมีพฤติกรรมเสี่ยงต่อการทำงานของระบบสารสนเทศจะถูกระงับการใช้เครือข่ายทันที หากการกระทำดังกล่าวเป็นการกระทำความผิดที่สอดคล้องกับกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.๒๕๕๐ หรือเป็นการกระทำที่ส่งผลให้เกิดความเสียหายต่อข้อมูลและทรัพยากรระบบของหน่วยงานจะต้องถูกดำเนินคดีตามขั้นตอนของกฎหมาย

๑๖. การใช้งานเครื่องคอมพิวเตอร์แบบตั้งโต๊ะ (Computer Desktop Used)

๑๖.๑. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานของสถาบัน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์ของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์แบบตั้งโต๊ะหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์แบบตั้งโต๊ะของหน่วยงาน

(๔) การเคลื่อนย้ายหรือส่งเครื่องคอมพิวเตอร์แบบตั้งโต๊ะตรวจซ่อมจะต้องดำเนินการโดยเจ้าหน้าที่ของหน่วยงานหรือผู้รับจ้างเหมาบำรุงรักษาเครื่องคอมพิวเตอร์และอุปกรณ์ที่ได้ทำสัญญากับสถาบันเท่านั้น

(๕) ก่อนการใช้งานสื่อบันทึกพกพาต่างๆ ต้องมีการตรวจสอบเพื่อหาไวรัสโดยโปรแกรมป้องกันไวรัส

(๖) ผู้ใช้งานมีหน้าที่และรับผิดชอบต่อการดูแลรักษาความปลอดภัยของเครื่องคอมพิวเตอร์

(๗) ปิดเครื่องคอมพิวเตอร์แบบตั้งโต๊ะที่ตนเองครอบครองใช้งานอยู่ เมื่อใช้งานประจำวันเสร็จสิ้นหรือเมื่อมีการยุติการใช้งานเกินกว่า ๑ ชั่วโมง

(๘) ทำการตั้งค่า Screen Saver ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะที่ตนเองรับผิดชอบให้มีการล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเกินกว่า ๓๐ นาที เพื่อป้องกันบุคคลอื่นมาใช้งานที่เครื่องคอมพิวเตอร์

(๙) ห้ามนำเครื่องคอมพิวเตอร์ส่วนตัวที่เจ้าหน้าที่เป็นเจ้าของมาใช้กับระบบเครือข่ายของหน่วยงาน ยกเว้นจะได้รับการตรวจสอบจากผู้ดูแลระบบของสถาบันก่อนการใช้งาน

๑๖.๒. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

๑๖.๓. การป้องกันจากโปรแกรมชุดคำสั่งไม่พึงประสงค์ (Malware)

(๑) ผู้ใช้งานต้องตรวจสอบหาไวรัสจากสื่อต่างๆ เช่น Floppy Disk, Flash Drive และ Data Storage อื่นๆ เป็นต้น ก่อนนำมาใช้งานร่วมกับเครื่องคอมพิวเตอร์

(๒) ผู้ใช้งานต้องตรวจสอบไฟล์ที่แนบมากับจดหมายอิเล็กทรอนิกส์ (E-mail) หรือไฟล์ที่ดาวน์โหลดมาจากอินเทอร์เน็ตด้วยโปรแกรมป้องกันไวรัสก่อนใช้งาน

(๓) ผู้ใช้งานต้องตรวจสอบข้อมูลคอมพิวเตอร์ใดที่มีชุดคำสั่งไม่พึงประสงค์รวมอยู่ด้วย ซึ่งมีผลทำให้ข้อมูลคอมพิวเตอร์ หรือระบบคอมพิวเตอร์ หรือชุดคำสั่งอื่นเกิดความเสียหาย ถูกทำลาย ถูกแก้ไข เปลี่ยนแปลง หรือปฏิบัติงานไม่ตรงตามคำสั่งที่กำหนดไว้

๑๖.๔. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องรับผิดชอบในการสำรองข้อมูลจากเครื่องคอมพิวเตอร์ไว้บนสื่อบันทึกอื่นๆ เช่น CD, DVD, External Hard Disk เป็นต้น

(๒) ผู้ใช้งานมีหน้าที่เก็บรักษาสื่อข้อมูลสำรอง (Backup Media) ไว้ในสถานที่ที่เหมาะสม ไม่เสี่ยงต่อการรั่วไหลของข้อมูลและทดสอบการกู้คืนข้อมูลที่สำรองไว้อย่างสม่ำเสมอ

(๓) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๑๗. การใช้งานเครื่องคอมพิวเตอร์แบบพกพา (Computer Notebook Used)

๑๗.๑. แนวทางปฏิบัติการใช้งานทั่วไป

(๑) เครื่องคอมพิวเตอร์แบบพกพาที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในงานของสถาบัน

(๒) โปรแกรมที่ได้ถูกติดตั้งลงบนเครื่องคอมพิวเตอร์แบบพกพาของหน่วยงานต้องเป็นโปรแกรมที่หน่วยงานได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมาย ดังนั้น ห้ามผู้ใช้งานคัดลอกโปรแกรมต่างๆ และนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัวหรือแก้ไขหรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(๓) ผู้ใช้งานต้องศึกษาและปฏิบัติตามคู่มือการใช้งานอย่างละเอียดเพื่อการใช้งานอย่างปลอดภัยและมีประสิทธิภาพ

(๔) ไม่ดัดแปลงแก้ไขส่วนประกอบต่างๆ ของเครื่องคอมพิวเตอร์และรักษาสภาพของเครื่องคอมพิวเตอร์ให้มีสภาพเดิม

(๕) ในกรณีที่ต้องการเคลื่อนย้ายเครื่องคอมพิวเตอร์แบบพกพาควรใส่กระเป๋าสำหรับเครื่องคอมพิวเตอร์แบบพกพาเพื่อป้องกันอันตรายที่เกิดจากการกระทบกระเทือน เช่น การตกจากโต๊ะทำงานหรือหลุดมือ เป็นต้น

(๖) หลีกเลี่ยงการใช้นิ้วหรือของแข็ง เช่น ปลายปากกากดสัมผัสหน้าจอ LCD ให้เป็นรอยขีดข่วนหรือทำให้จอ LCD ของเครื่องคอมพิวเตอร์แบบพกพาแตกเสียหายได้ เป็นต้น

(๗) ไม่วางของทับบนหน้าจอและแป้นพิมพ์

(๘) การเช็ดทำความสะอาดหน้าจอภาพต้องเช็ดอย่างเบามือที่สุดและต้องเช็ดไปในแนวทางเดียวกัน ห้ามเช็ดแบบหมุนวนเพราะจะทำให้หน้าจอมีรอยขีดข่วนได้

(๙) การใช้เครื่องคอมพิวเตอร์แบบพกพาเป็นระยะเวลานานเกินไปในสภาพที่มีอากาศร้อนจัดต้องปิดเครื่องคอมพิวเตอร์เพื่อเป็นการพักเครื่องสักระยะหนึ่งก่อนเปิดใช้งานใหม่อีกครั้ง

(๑๐) การเคลื่อนย้ายเครื่องขณะที่เครื่องเปิดใช้งานอยู่ให้ทำการยกจากฐานภายใต้แป้นพิมพ์ ห้ามย้ายเครื่องโดยการดึงหน้าจอภาพขึ้น

๑๗.๒. ความปลอดภัยทางด้านกายภาพ

(๑) ผู้ใช้งานมีหน้าที่รับผิดชอบในการป้องกันการสูญหาย เช่น ควรล็อกเครื่องขณะที่ไม่ได้ใช้งาน ไม่วางเครื่องทิ้งไว้ในที่สาธารณะหรือในบริเวณที่มีความเสี่ยงต่อการสูญหาย เป็นต้น

(๒) ผู้ใช้งานไม่เก็บหรือใช้งานเครื่องคอมพิวเตอร์แบบพกพาในสถานที่ที่มีความร้อน/ความชื้น/ฝุ่นละอองสูง และต้องระวังป้องกันการตกกระทบ

๑๗.๓. การควบคุมการเข้าถึงระบบปฏิบัติการ

(๑) ผู้ใช้งานต้องกำหนดชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์แบบพกพา

(๒) ผู้ใช้งานต้องกำหนดรหัสผ่านให้มีคุณภาพดีอย่างน้อยตามที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

(๓) ผู้ใช้งานต้องตั้งการใช้งานโปรแกรมรักษาจอภาพ (Screen Saver) โดยตั้งเวลาประมาณ ๑๕ นาที ให้ทำการล็อกหน้าจอเมื่อไม่มีการใช้งาน หลังจากนั้นเมื่อต้องการใช้งานต้องใส่รหัสผ่าน

(๔) ผู้ใช้งานต้องทำการ Logout ออกจากระบบทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๑๗.๔. การใช้รหัสผ่านให้ผู้ใช้งานปฏิบัติตามแนวทางการบริหารจัดการรหัสผ่านที่ระบุไว้ในเอกสาร “การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน”

๑๗.๕. การสำรองข้อมูลและการกู้คืน

(๑) ผู้ใช้งานต้องทำการสำรองข้อมูลจากเครื่องคอมพิวเตอร์แบบพกพาโดยวิธีการและสื่อต่างๆ เพื่อป้องกันการสูญหายของข้อมูล

(๒) ผู้ใช้งานต้องจะเก็บรักษาสื่อสำรองข้อมูล (Backup media) ไว้ในสถานที่ที่เหมาะสมไม่เสี่ยงต่อการรั่วไหลของข้อมูล

(๓) แผ่นสื่อสำรองข้อมูลต่างๆ ที่เก็บข้อมูลไว้จะต้องทำการทดสอบการกู้คืนอย่างสม่ำเสมอ

(๔) แผ่นสื่อสำรองข้อมูลที่ไม่ใช้งานแล้วต้องทำลายไม่ให้สามารถนำไปใช้งานได้อีก

(๕) ผู้ใช้งานต้องประเมินความเสี่ยงว่าข้อมูลที่เก็บไว้บน Hard Disk ไม่ควรจะเป็นข้อมูลสำคัญเกี่ยวข้องกับการทำงาน เพราะหาก Hard Disk เสียไปก็ไม่กระทบต่อการดำเนินการของหน่วยงาน

๑๘. การติดตั้งและกำหนดค่าของระบบ (System Installation and Configuration)

๑๘.๑. การปรับปรุงระบบปฏิบัติการ (Operating System Update)

(๑) ตรวจสอบเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ระบบ

(๒) ติดตั้งระบบปฏิบัติการตรงตามความต้องการการใช้งาน

(๓) กำหนดชื่อและรหัสผ่านผู้ดูแลระบบและชื่อผู้ใช้งาน (User)

(๔) กำหนดค่าติดตั้งชื่อเครื่อง (Computer Name) / IP Address

(๕) ปรับปรุง/กำหนดค่าระดับความปลอดภัยของระบบปฏิบัติการ (กรณีที่ระบบปฏิบัติการที่มี ServicePatch Update)

(๖) ติดตั้งโปรแกรม Antivirus/ปรับปรุง Virus Definition และกำหนดค่าการตรวจสอบระบบการสแกนและปรับปรุงโปรแกรม

๑๘.๒. การบริหารบัญชีผู้ใช้งาน/สิทธิ์การเข้าถึงและการใช้งานระบบ (User Account Management)

(๑) กำหนดชื่อและรหัสผ่านผู้ดูแลระบบ (System Adminstrator)

(๒) กำหนดชื่อผู้ใช้งาน (User Name) และรหัสผ่าน (Password)

(๓) บันทึกบัญชีผู้ใช้งานและสิทธิ์การเข้าใช้ระบบ

๑๘.๓. การปรับปรุงการรักษาความปลอดภัย/Anti Virus (System Security & Antivirus Upadte)

(๑) ติดตามเฝ้าระวังระบบการทำงานของเครื่องคอมพิวเตอร์การเข้าใช้ระบบ

(๒) Performance ของระบบหรือตรวจสอบจากระบบรักษาความปลอดภัยที่ติดตั้ง

(๓) ปรับปรุง/กำหนดค่าระบบความปลอดภัยให้เหมาะสมกับปัญหา

(๔) ปรับปรุงโปรแกรม Antivirus และ Definition ให้ทันสมัยเป็นประจำทุกสัปดาห์

(๕) ดำเนินการ Scan ตรวจหาไวรัสคอมพิวเตอร์เป็นประจำ

๑๘.๔. ติดตั้ง/ปรับปรุงระบบจัดการฐานข้อูล (Database Management Operation)

(๑) ติดตั้งระบบจัดการฐานข้อมูลตามความต้องการของระบบงานที่หน่วยงานใช้

(๒) กำหนดค่าระบบหรือโปรแกรมฐานข้อมูลให้ทำงานร่วมกับระบบปฏิบัติการได้อย่างถูกต้องและมีประสิทธิภาพตามระบบฐานข้อมูลนั้นกำหนด

(๓) สร้างและกำหนดรายชื่อผู้จัดการฐานข้อมูล (Database Manager) ชื่อผู้ใช้งานอื่นและสิทธิ์การใช้

(๔) ปรับปรุง/กำหนดค่าระบบให้เหมาะสมทันสมัยหรือป้องกันการเกิดปัญหาอยู่เสมอ

๑๘.๕. ติดตั้งฐานข้อมูลโปรแกรมระบบงานต่างๆ /กำหนดค่าระบบของโปรแกรมและกำหนดผู้ใช้และสิทธิ์การเข้าใช้บริการหรือเข้าถึงฐานข้อมูล

(๑) ติดตั้งโปรแกรมระบบงานตามความต้องการหรือการพัฒนา

(๒) กำหนดค่าหรือโปรแกรมหรือบริการให้ทำงานร่วมกับระบบปฏิบัติการเป็นไปตามโปรแกรมหรือระบบงานนั้นอย่างถูกต้องและมีประสิทธิภาพ

(๓) ติดตั้งฐานข้อมูลและเชื่อมต่อระบบงาน และทำการทดสอบการให้บริการตามระบบงานนั้นกำหนด

(๔) แจ้งผู้ใช้งานหรือเจ้าของระบบงานให้สามารถเริ่มใช้งานได้ โดยแจ้งรายชื่อ รหัสผ่านและสิทธิ์การเข้าใช้ระบบและฐานข้อมูลตามที่กำหนดไว้

(๕) กำหนดเกณฑ์การสำรอง / สำเนา / ทดสอบกู้คืน (Restore Test)

(๖) บันทึกข้อกำหนดค่าติดตั้งและบัญชีชื่อผู้ใช้งานแต่ละระดับของระบบทุกครั้งที่มีการสร้างหรือปรับปรุง

๑๙. การจัดเก็บข้อมูลจราจรคอมพิวเตอร์ (Traffic Log)

๑๙.๑. จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริงระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้ และข้อมูลที่ใช้ในการจัดเก็บต้องกำหนดชั้นความลับในการเข้าถึง

๑๙.๒. กำหนดวิธีการในการนำส่งข้อมูลจราจรคอมพิวเตอร์จากสื่อที่ใช้เก็บไปยัง Centralized Log Server ของสถาบัน

๑๙.๓. ห้ามแก้ไขข้อมูลจราจรคอมพิวเตอร์ที่เก็บรักษาไว้

๑๙.๔. กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า–ออกระบบ บันทึกการพยายามเข้าสู่ระบบ เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกไว้อย่างน้อย ๙๐ วันนับตั้งแต่การใช้งานสิ้นสุดลงโดยปฏิบัติตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๖๐

๑๙.๕. ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิ์การเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๒๐. หน้าที่และความรับผิดชอบของผู้ดูแลระบบ (System Administrator Responsibilities)

๒๐.๑. ผู้ดูแลระบบ แบ่งออกเป็น ๓ กลุ่ม

(๑) ผู้ดูแลระบบเครือข่าย (Network Administrator)

(๒) ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย (System Administrator)

(๓) ผู้ดูแลระบบสารสนเทศ (Application Administrator)

๒๐.๒. ผู้ดูแลระบบเครือข่าย มีหน้าที่และความรับผิดชอบดังนี้

(๑) ดูแลรักษาและตรวจสอบอุปกรณ์เครือข่ายและช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(๒) เก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์เท่าที่จำเป็นเพื่อให้สามารถระบุตัวตนผู้ใช้งานนับตั้งแต่เริ่มใช้บริการ และต้องเก็บรักษาไว้เป็นเป็นระยะเวลาตามที่กฎหมายกำหนดนับตั้งแต่การใช้บริการสิ้นสุดลง และการเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังนี้

(๒.๑) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บและกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความครบถ้วนสมบูรณ์ถูกต้องและความน่าเชื่อถือของข้อมูลและไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บไว้ เว้นแต่ ได้มีการกำหนดผู้ที่สามารถเข้าถึงข้อมูลได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของหน่วยงาน หรือบุคคลที่หน่วยงานมอบหมาย

(๒.๒) ข้อมูลจราจรทางคอมพิวเตอร์ต้องระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

๒๐.๓. ผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย มีหน้าที่และความรับผิดชอบดังนี้

(๑) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายของหน่วยงานให้เป็นไปด้วยความเรียบร้อย และมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายให้รีบดำเนินการแก้ไข รวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ให้รีบแจ้งผู้ใช้งานนั้นให้ยุติการกระทำในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบพิจารณาระงับการใช้งานของผู้ใช้งานทันที

(๒) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์แม่ข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและทันสมัยอยู่เสมอ

(๓) ติดตั้งโปรแกรมสำหรับจัดการโปรแกรมไม่ประสงค์ดีต่าง ๆ ให้เหมาะสม

(๔) ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

(๕) ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้เครื่องคอมพิวเตอร์แม่ข่ายให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๒๐.๔. ผู้ดูแลระบบสารสนเทศ มีหน้าที่และความรับผิดชอบดังนี้

(๑) ดูแลรักษาและปรับปรุงระบบบัญชีผู้ใช้ระบบสารสนเทศให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

(๒) ปรับปรุงรายการระบบสารสนเทศและรายการอุปกรณ์ที่เกี่ยวข้องกับระบบสารสนเทศนั้นให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ

๒๐.๕. หลักธรรมาภิบาลของผู้ดูแลระบบ

(๑) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลผู้ใช้งานโดยไม่มีเหตุผลอันสมควร

(๒) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งานหรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(๓) ไม่เปิดเผยข้อมูลที่ได้จากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

๒๑. การใช้งานเครือข่ายสังคมออนไลน์ (Social Network)

๒๑.๑. การใช้งานหรือใช้บริการเว็บไซต์เครือข่ายสังคมออนไลน์ ต้องใช้งานเพื่อประโยชน์ของสถาบันเป็นสำคัญ

๒๑.๒. ในการใช้งานเครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของสถาบัน

๒๑.๓. ในการใช้เครือข่ายสังคมออนไลน์ ผู้ใช้งานต้องไม่เสนอความเห็น หรือใช้ข้อความยั่วยุ ให้ร้ายที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสถาบัน

๒๑.๔. หากผู้ใช้งานทราบและรู้สึกในภายหลังว่าการใช้งานเครือข่ายสังคมออนไลน์ของท่านอาจมีผลกระทบกับสถาบัน ผู้ใช้งานต้องแจ้งหน่วยเทคโนโลยีสารสนเทศโดยเร็วที่สุด เพื่อดำเนินการตามความเหมาะสม

๒๒. การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม (Physical and Environmental Security)

๒๒.๑. อาคารสถานที่และพื้นที่ใช้งานระบบสารสนเทศ หมายถึง ที่ซึ่งเป็นที่ตั้งของระบบคอมพิวเตอร์ ระบบเครือข่ายหรือระบบสารสนเทศอื่นๆ พื้นที่เตรียมข้อมูลจัดเก็บคอมพิวเตอร์และอุปกรณ์ พื้นที่ปฏิบัติงานของบุคลากรทางคอมพิวเตอร์รวมทั้งเครื่องคอมพิวเตอร์แบบตั้งโต๊ะและแบบพกพาและอุปกรณ์ประกอบที่ติดตั้งประจำโต๊ะทำงาน

๒๒.๒. ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ต้องมีลักษณะ ดังนี้

(๑) กำหนดเป็นเขตหวงห้ามเด็ดขาดหรือเขตหวงห้ามเฉพาะโดยพิจารณาตามความสำคัญแล้วแต่กรณี

(๒) ต้องเป็นพื้นที่ที่ไม่ตั้งอยู่ในบริเวณที่มีการผ่านเข้า–ออกของบุคคลเป็นจำนวนมาก

(๓) จะต้องไม่มีป้ายหรือสัญลักษณ์ที่บ่งบอกถึงการมีระบบสำคัญอยู่ภายในสถานที่ดังกล่าว

(๔) จะต้องปิดล็อกหรือใส่กุญแจประตูหน้าต่างหรือห้องเสมอเมื่อไม่มีเจ้าหน้าที่ประจำอยู่

(๕) หากจำเป็นต้องใช้เครื่องโทรสารหรือเครื่องถ่ายเอกสารให้ติดตั้งแยกออกมาจากบริเวณดังกล่าว

(๖) ไม่อนุญาตให้ถ่ายรูปหรือบันทึกภาพเคลื่อนไหวในบริเวณดังกล่าวเป็นอันขาด

(๗) จัดพื้นที่สำหรับการส่งมอบผลิตภัณฑ์โดยแยกจากบริเวณที่มีทรัพยากรสารสนเทศจัดตั้งไว้ เพื่อป้องกันการเข้าถึงระบบจากผู้ไม่ได้รับอนุญาต

๒๒.๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

(๑) มีการจำแนกและกำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ อย่างเหมาะสม เพื่อจุดประสงค์ในการเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัยจากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

(๒) กำหนดและแบ่งแยกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจนรวมทั้งจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวอาจแบ่งออกได้เป็น พื้นที่ทำงานทั่วไป (General Working Area) พื้นที่ทำงานของผู้ดูแลระบบ (System Administrator Area) พื้นที่ติดตั้งอุปกรณ์ระบบเทคโนโลยีสารสนเทศ (IT Equipment Area) พื้นที่จัดเก็บข้อมูลคอมพิวเตอร์ (Data Storage Area) และพื้นที่ใช้งานเครือข่ายไร้สาย (Wireless LAN Coverage Area) เป็นต้น

๒๒.๔. การควบคุมการเข้า-ออกอาคารสถานที่

(๑) กำหนดสิทธิ์ผู้ใช้งานที่มีสิทธิ์ผ่านเข้า-ออก และช่วงเวลาที่มีสิทธิ์ในการผ่านเข้าออกในแต่ละ “พื้นที่ใช้งานระบบ” อย่างชัดเจน

(๒) การเข้าถึงอาคารของหน่วยงานของบุคคลภายนอกหรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัยจะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประจำตัวประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

(๓) ให้มีการบันทึกวันและเวลาการเข้า-ออกพื้นที่สำคัญของผู้ที่มาติดต่อ (Visitor)

(๔) ผู้มาติดต่อต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาที่อยู่ภายในสถาบัน

(๕) หน่วยงานภายนอกที่ได้รับการว่าจ้างต้องติดบัตรให้เห็นเด่นชัดตลอดระยะเวลาการทำงาน

(๖) จัดเก็บบันทึกการเข้า-ออกสำหรับพื้นที่หรือบริเวณที่มีความสำคัญ เช่น (Data Center) เป็นต้น เพื่อใช้ในการตรวจสอบในภายหลังเมื่อมีความจำเป็น

(๗) ดูแลผู้ที่มาติดต่อในพื้นที่หรือบริเวณที่มีความสำคัญจนกระทั่งเสร็จสิ้นภารกิจและจากไป เพื่อป้องกันการสูญหายของทรัพย์สินหรือป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต

(๘) มีกลไกการอนุญาตการเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญของบุคคลภายนอกและต้องมีเหตุผลที่เพียงพอในการเข้าถึงบริเวณดังกล่าว

(๙) สร้างความตระหนักให้ผู้ที่มาติดต่อจากภายนอกเข้าใจในกฎเกณฑ์หรือข้อกำหนดต่างๆ ที่ต้องปฏิบัติระหว่างที่อยู่ในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๐) มีการควบคุมการเข้าถึงพื้นที่ที่มีข้อมูลสำคัญจัดเก็บหรือประมวลผลอยู่

(๑๑) ไม่อนุญาตให้ผู้ไม่มีกิจเข้าไปในพื้นที่หรือบริเวณที่มีความสำคัญ เว้นแต่ได้รับการอนุญาต

(๑๒) มีการพิสูจน์ตัวตน เช่น การใช้บัตรรูด การใช้รหัสผ่าน เป็นต้น เพื่อควบคุมการเข้า-ออกในพื้นที่หรือบริเวณที่มีความสำคัญ (Data Center)

(๑๓) จัดให้มีการดูแลและเฝ้าระวังการปฏิบัติงานของบุคคลภายนอกในขณะที่ปฏิบัติงานในพื้นที่หรือบริเวณที่มีความสำคัญ

(๑๔) จัดให้มีการทบทวนหรือยกเลิกสิทธิ์การเข้าถึงพื้นที่หรือบริเวณที่มีความสำคัญ อย่างน้อยปีละ ๑ ครั้ง

๒๒.๕. ระบบและอุปกรณ์สนับสนุนการทำงาน (Supporting Utilities)

(๑) มีระบบสนับสนุนการทำงานของระบบเทคโนโลยีสารสนเทศของหน่วยงานที่เพียงพอต่อความต้องการใช้งานโดยให้มีระบบ ดังต่อไปนี้

(๑.๑) ระบบสำรองกระแสไฟฟ้า (UPS)

(๑.๒) เครื่องกำเนิดกระแสไฟฟ้าสำรอง (Generator)

(๑.๓) ระบบระบายอากาศ

(๑.๔) ระบบปรับอากาศและควบคุมความชื้น

(๒) ให้มีการตรวจสอบหรือทดสอบระบบสนับสนุนเหล่านั้นอย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าระบบทำงานตามปกติและลดความเสี่ยงจากการล้มเหลวในการทำงานของระบบ

(๓) ติดตั้งระบบแจ้งเตือนเพื่อแจ้งเตือนกรณีที่ระบบสนับสนุนการทำงานภายในห้องคอมพิวเตอร์แม่ข่าย (Server) ทำงานผิดปกติหรือหยุดการทำงาน

๒๒.๖. การติดตั้งสายไฟสายสื่อสารและสายเคเบิ้ลอื่นๆ (Cabling Security)

(๑) หลีกเลี่ยงการติดตั้งสายสัญญาณเครือข่ายของสถาบันในลักษณะที่ต้องผ่านเข้าไปในบริเวณที่มีบุคคลภายนอกเข้าถึงได้

(๒) ให้มีการร้อยท่อสายสัญญาณต่างๆ เพื่อป้องกันการดักจับสัญญาณหรือการตัดสายสัญญาณเพื่อทำให้เกิดความเสียหาย

(๓) ให้ติดตั้งสายสัญญาณสื่อสารและสายไฟฟ้าแยกออกจากกันเพื่อป้องกันการแทรกแซงรบกวนของสัญญาณซึ่งกันและกัน

(๔) ต้องทำป้ายชื่อสำหรับสายสัญญาณและบนอุปกรณ์เพื่อป้องกันการตัดต่อสัญญาณ ผิดเส้น

(๕) จัดทำแผนผังสายสัญญาณสื่อสารต่างๆ ให้ครบถ้วนและถูกต้อง

(๖) ห้องที่มีสายสัญญาณสื่อสารต่างๆ ปิดใส่สลักให้สนิทเพื่อป้องกันการเข้าถึงของบุคคลภายนอก

(๗) พิจารณาใช้งานสายไฟเบอร์ออฟติกแทนสายสัญญาณสื่อสารแบบเดิม (เช่น สายสัญญาณแบบ coaxial cable เป็นต้น) สำหรับระบบสารสนเทศที่สำคัญ

(๘) ดำเนินการสำรวจระบบสายสัญญาณสื่อสารทั้งหมดเพื่อตรวจหาการติดตั้งอุปกรณ์ดักจับสัญญาณโดยผู้ไม่ประสงค์ดี

๒๒.๗. การบำรุงรักษาอุปกรณ์ (Equipment Maintenance)

(๑) ให้มีกำหนดการบำรุงรักษาอุปกรณ์ตามรอบระยะเวลาที่แนะนำโดยผู้ผลิต

(๒) ปฏิบัติตามคำแนะนำในการบำรุงรักษาตามที่ผู้ผลิตแนะนำ

(๓) จัดเก็บบันทึกกิจกรรมการบำรุงรักษาอุปกรณ์สำหรับการให้บริการทุกครั้งเพื่อใช้ในการตรวจสอบหรือประเมินในภายหลัง

(๔) จัดเก็บบันทึกปัญหาและข้อบกพร่องของอุปกรณ์ที่พบเพื่อใช้ในการประเมินและปรับปรุงอุปกรณ์ดังกล่าว

(๕) ควบคุมและสอดส่องดูแลการปฏิบัติงานของผู้ให้บริการภายนอกที่มาทำการบำรุงรักษาอุปกรณ์ภายในสถาบัน

(๖) จัดให้มีการอนุมัติสิทธิ์การเข้าถึงอุปกรณ์ที่มีข้อมูลสำคัญโดยผู้รับจ้างให้บริการจากภายนอก (ที่มาทำการบำรุงรักษาอุปกรณ์) เพื่อป้องกันการเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

๒๒.๘. การนำทรัพย์สินของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

(๑) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน

(๒) กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน

(๓) กำหนดระยะเวลาของการนำอุปกรณ์ออกไปใช้งานนอกหน่วยงาน

(๔) เมื่อมีการนำอุปกรณ์ส่งคืนให้ตรวจสอบว่าสอดคล้องกับระยะเวลาที่อนุญาตและตรวจสอบการชำรุดเสียหายของอุปกรณ์ด้วย

(๕) บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงานเพื่อเอาไว้เป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์ส่งคืน

๒๒.๙. การป้องกันอุปกรณ์ที่ใช้งานอยู่นอกหน่วยงาน (Security of Equipment off-premises)

(๑) กำหนดมาตรการความปลอดภัยเพื่อป้องกันความเสี่ยงจากการนำอุปกรณ์หรือทรัพย์สินของหน่วยงานออกไปใช้งาน เช่น การขนส่ง การเกิดอุบัติเหตุกับอุปกรณ์ เป็นต้น

(๒) ไม่ทิ้งอุปกรณ์หรือทรัพย์สินของหน่วยงานไว้โดยลำพังในที่สาธารณะ

(๓) เจ้าหน้าที่มีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตนเอง

๒๒.๑๐. การกำจัดอุปกรณ์หรือการนำอุปกรณ์กลับมาใช้งานอีกครั้ง (Secure Disposal or reuse of Equipment)

(๑) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

ส่วนที่ ๒

นโยบายการจัดทำระบบสำรองสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้ระบบสารสนเทศของสถาบันมีสภาพพร้อมใช้และสามารถให้บริการได้อย่างต่อเนื่อง

๒. เพื่อกำหนดแนวปฏิบัติการจัดทำระบบสำรอง การสำรองข้อมูล และการกู้คืนข้อมูล ให้ผู้ดูแลระบบเครือข่าย ผู้ดูแลเครื่องคอมพิวเตอร์แม่ข่ายและผู้ดูแลระบบสารสนเทศหน่วยงานถือปฏิบัติ เพื่อให้มั่นใจได้ว่ามีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ในกรณีที่ระบบหลักมีปัญหาต้องสำรองข้อมูลและสามารถกู้คืนข้อมูลได้ในกรณีที่จำเป็น

ผู้รับผิดชอบ

๑. หน่วยเทคโนโลยีสารสนเทศ

๒. ผู้ดูแลระบบที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์

แนวปฏิบัติ

๑. ระบบสำรอง (Disaster Recovery Site : DR Site)

๑.๑. จัดทำบัญชีระบบเครือข่ายและระบบสารสนเทศที่สำคัญและจำเป็นต้องมีระบบสำรองและทบทวนบัญชีอย่างน้อยปีละ ๑ ครั้ง เช่น ระบบบริการแปลงชื่อเป็นหมายเลขไอพีแอดเดรส ระบบสารสนเทศทางการเงิน การบัญชี และการพัสดุ ระบบบริหารงานทรัพยากรบุคคล ระบบทะเบียนและประมวลผลทางการศึกษา ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น

๑.๒. ระบบสำรองต้องอยู่ในห้องหรือพื้นที่ที่ต่างจากระบบหลัก และมีการควบคุม ดังนี้

(๑) มีระบบการควบคุมการเข้าถึงที่อนุญาตเฉพาะผู้มีหน้าที่เกี่ยวข้อง

(๒) มีระบบไฟฟ้าสำรอง

(๓) มีระบบปรับอากาศและความชื้นที่เหมาะสม

(๔) มีระบบป้องกันอัคคีภัย

(๕) มีระบบส่องสว่างที่เหมาะสม

(๖) มีระบบสื่อสารหรือระบบเครือข่ายสำรอง

(๗) มีระบบแจ้งเตือนกรณีที่ระบบสนับสนุนทำงานผิดปกติหรือหยุดการทำงาน

๑.๓. มีแผนบำรุงรักษาระบบสำรองทุกระบบอย่างต่อเนื่อง

๒. การสำรองข้อมูล (Data Backup)

๒.๑. จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงานที่จะทำการสำรองข้อมูล และทบทวนบัญชีปีละ ๑ ครั้ง เช่น ระบบบริการแปลงชื่อเป็นหมายเลขไอพีแอดเดรส ระบบสารสนเทศทางการเงิน การบัญชี และการพัสดุ ระบบบริหารงานทรัพยากรบุคคล ระบบทะเบียนและประมวลผลทางการศึกษา ระบบสารบรรณอิเล็กทรอนิกส์ เป็นต้น

๒.๒. กำหนดวิธีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ

๒.๓. กำหนดความถี่ในการสำรองข้อมูล ระบบที่มีความสำคัญสูง หรือระบบที่มีการเปลี่ยนแปลงบ่อย ต้องกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น

๒.๔. บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สถานการณ์ทำงานสำเร็จ/ไม่สำเร็จ เป็นต้น

๒.๕. ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่างๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลในฐานข้อมูล และข้อมูลการตั้งค่าระบบและอุปกรณ์ต่างๆ เป็นต้น

๒.๖. จัดเก็บข้อมูลสำรองไว้ในระบบสำรอง

๒.๗. ดำเนินการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรองที่ใช้จัดเก็บข้อมูลสำรอง

๒.๘. มีแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ ดังนี้

(๑) ต้องกำหนดหน้าที่และความรับผิดชอบของผู้ที่เกี่ยวข้องทั้งหมด

(๒) ต้องประเมินความเสี่ยงสำหรับระบบที่มีความสำคัญเหล่านั้น และกำหนดมาตรการเพื่อลดความเสี่ยงเหล่านั้น เช่น ไฟดับเป็นระยะเวลานาน ไฟไหม้ แผ่นดินไหว การชุมนุมประท้วงทำให้ไม่สามารถเข้ามาใช้ระบบงานได้ เป็นต้น

(๓) ต้องกำหนดขั้นตอนปฏิบัติในการกู้คืนระบบสารสนเทศ

(๔) ต้องกำหนดขั้นตอนปฏิบัติในการสำรองข้อมูล และทดสอบกู้คืนข้อมูลสำรองไว้

(๕) ต้องทบทวนเพื่อปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ อย่างน้อยปีละ ๑ ครั้ง

๓. การกู้คืนข้อมูล (Data Recovery)

๓.๑. จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูล และตรวจสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติอย่างสม่ำเสมอ

๓.๒. ตรวจสอบผลการบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

๓.๓. ให้ใช้ข้อมูลทันสมัยที่สุด (Last Update) ที่ได้สำรองไว้หรือตามความเหมาะสม เพื่อกู้คืนระบบ

๓.๔. ทดสอบการกู้คืนข้อมูลที่ได้ทำการสำรองไว้อย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง

๔. การทดสอบสภาพพร้อมใช้งาน

๔.๑. ต้องทดสอบสภาพพร้อมใช้ของระบบสารสนเทศ ระบบสำรอง ระบบสำรองข้อมูลและแผนเตรียมความพร้อมกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๓
นโยบายการตรวจสอบและประเมินความเสี่ยงสารสนเทศ

วัตถุประสงค์

๑. เพื่อให้มีการตรวจสอบและประเมินความเสี่ยงของระบบสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้
๒. เพื่อเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นได้กับระบบสารสนเทศ
๓. เพื่อเป็นแนวทางในการปฏิบัติหากเกิดความเสี่ยงที่เป็นอันตรายต่อระบบสารสนเทศ

ผู้รับผิดชอบ

๑. หน่วยเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

ประกาศคณะกรรมการธุรกรรมทางอิเล็คทรอนิกส์ เรื่อง มาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามวิธีการแบบปลอดภัย พ.ศ. ๒๕๕๕

แนวปฏิบัติ

๑. การตรวจสอบและประเมินความเสี่ยง

ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศหรือสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดได้ที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศ โดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ โดยมีแนวทางในการตรวจสอบและประเมินความเสี่ยงที่ต้องคำนึงถึง ดังนี้

๑.๑. จัดลำดับความสำคัญของความเสี่ยง
๑.๒. ค้นหาวิธีการดำเนินการเพื่อลดความเสี่ยง
๑.๓. ศึกษาข้อดีข้อเสียของวิธีการดำเนินการเพื่อลดความเสี่ยง
๑.๔. สรุปผลข้อเสนอแนะและแนวทางแก้ไขเพื่อลดความเสี่ยงที่ตรวจสอบได้
๑.๕. มีการตรวจสอบและประเมินความเสี่ยงและให้จัดทำรายงานพร้อมข้อเสนอแนะ
๑.๖. มีมาตรการในการตรวจประเมินระบบสารสนเทศอย่างน้อย ดังนี้
    (๑) กำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
    (๒) ในกรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้นเพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งต้องทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จหรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี
    (๓) กำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบระบบบริหารจัดการความมั่นคงปลอดภัย
    (๔) กำหนดให้มีการเฝ้าระวัง การเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลจราจรคอมพิวเตอร์แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

(๕) ในกรณีที่มีเครื่องมือสำหรับการตรวจประเมินระบบสารสนเทศ กำหนดให้แยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบให้บริการจริงหรือระบบที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

๒. ความเสี่ยงที่อาจเป็นอันตรายต่อระบบเทคโนโลยีสารสนเทศ

จากการติดตามตรวจสอบความเสี่ยงต่างๆ รวมถึงเหตุการณ์ด้านความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศสามารถแยกเป็นภัยต่างๆ ได้ ๔ ประเภท ดังนี้

๒.๑. ประเภทที่ ๑ ภัยที่เกิดจากเจ้าหน้าที่หรือบุคลากรของหน่วยงาน (Human Error) เช่น เจ้าหน้าที่หรือบุคลากรของหน่วยงานขาดความรู้ความเข้าใจในเครื่องมืออุปกรณ์คอมพิวเตอร์ทั้งด้าน Hardware และ Software ซึ่งอาจทำให้ระบบเทคโนโลยีสารสนเทศเสียหายใช้งานไม่ได้เกิดการชะงักงันหรือหยุดทำงาน และส่งผลให้ไม่สามารถใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างเต็มประสิทธิภาพ เป็นต้น ได้กำหนดแนวทางการดำเนินการเบื้องต้นเพื่อลดปัญหาความเสี่ยงที่จะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศไว้ ดังนี้

(๑) จัดหลักสูตรอบรมเจ้าหน้าที่ของหน่วยงานให้มีความรู้ความเข้าใจในด้าน Hardware และ Software เบื้องต้น เพื่อลดความเสี่ยงด้าน Human error ให้น้อยที่สุดทำให้เจ้าหน้าที่มีความรู้ความเข้าใจการใช้และบริหารจัดการเครื่องมืออุปกรณ์ทางด้านสารสนเทศทั้งทางด้าน Hardware และ Software ได้มีประสิทธิภาพยิ่งขึ้นทำให้ความเสี่ยงที่เกิดจาก Human error ลดน้อยลง

(๒) จัดทำหนังสือแจ้งเวียนทุกหน่วยงานเรื่องการใช้และการประหยัดพลังงานให้กับเครื่องคอมพิวเตอร์และอุปกรณ์เพื่อเป็นแนวทางปฏิบัติได้อย่างถูกต้อง

๒.๒. ประเภทที่ ๒ ภัยที่เกิดจาก Software ที่สร้างความเสียหายให้แก่เครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ประกอบด้วย ไวรัสคอมพิวเตอร์ (Computer Virus), หนอนอินเทอร์เน็ต (Internet Worm), ม้าโทรจัน (Trojan Horse), และข่าวไวรัสหลอกลวง (Hoax) พวก Software เหล่านี้อาจรบกวนการทำงานและก่อให้เกิดความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศถึงขั้นทำให้ระบบเครือข่ายคอมพิวเตอร์ใช้งานไม่ได้ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ภัยจาก Software ดังนี้

(๑) ติดตั้งไฟล์วอลล์ที่เครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่ในการกำหนดสิทธิ์การเข้าใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและป้องกันการบุกรุกจากภายนอก

(๒) ติดตั้งซอฟต์แวร์ Anti virus ดักจับไวรัสที่เข้ามาในระบบเครือข่ายและสามารถตรวจสอบได้ว่ามีไวรัสชนิดใดเข้ามาทำความเสียหายกับระบบเครือข่ายคอมพิวเตอร์

๒.๓. ประเภทที่ ๓ ภัยจากไฟไหม้หรือระบบไฟฟ้า จัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) ติดตั้งอุปกรณ์สำรองไฟฟ้า (UPS) เพื่อควบคุมการจ่ายกระแสไฟฟ้าให้กับระบบเครื่องคอมพิวเตอร์แม่ข่าย (Server) ในกรณีเกิดกระแสไฟฟ้าขัดข้องระบบเครือข่ายคอมพิวเตอร์จะสามารถให้บริการได้ในระยะเวลาที่สามารถจัดเก็บและสำรองข้อมูลไว้อย่างปลอดภัย

(๒) ติดตั้งอุปกรณ์ตรวจจับควันกรณีที่เกิดเหตุการณ์กระแสไฟฟ้าขัดข้องหรือมีควันไฟเกิดขึ้นภายในห้องควบคุมระบบเครือข่าย อุปกรณ์ดังกล่าวจะส่งสัญญาณแจ้งเตือนที่หน่วยรักษาความปลอดภัยเพื่อทราบและรีบเข้ามาระงับเหตุฉุกเฉินอย่างทันท่วงทีซึ่งมีการตรวจสอบความพร้อมของอุปกรณ์อย่างสม่ำเสมอ

(๓) ติดตั้งอุปกรณ์ดับเพลิงชนิดก๊าซที่ห้องควบคุมระบบคอมพิวเตอร์เพื่อไว้ใช้ในกรณีเหตุฉุกเฉิน (ไฟไหม้) โดยมีการตรวจสอบความพร้อมของอุปกรณ์และทดลองใช้งานโดยสม่ำเสมอ

๒.๔. ประเภทที่ ๔ ภัยจากน้ำท่วม (อุทกภัย) ความเสี่ยงต่อความเสียหายจากน้ำท่วมจัดเป็นภัยร้ายแรงที่ทำความเสียหายให้แก่ระบบเทคโนโลยีสารสนเทศ ได้กำหนดแนวทางปฏิบัติเพื่อเตรียมรับสถานการณ์ ดังนี้

(๑) เฝ้าระวังภัยอันเกิดจากน้ำท่วมโดยติดตามจากพยากรณ์อากาศของกรมอุตุนิยมวิทยาตลอดเวลา

(๒) ถอดเทป Back up ข้อมูลทั้งหมดไปเก็บไว้ในที่ปลอดภัย

(๓) ดำเนินการตัดระบบไฟฟ้าในห้องควบคุมโดยปิดเบรคเกอร์เครื่องปรับอากาศเพื่อป้องกันเครื่องควบคุมเสียหายและป้องกันภัยจากไฟฟ้า

(๔) เจ้าหน้าที่ช่วยกันเคลื่อนย้ายเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายไว้ในที่สูง

(๕) กรณีน้ำลดลงเรียบร้อยแล้วให้ช่างไฟฟ้าตรวจสอบระบบไฟฟ้าในห้องควบคุมเครือข่ายว่าสามารถใช้งานได้ปกติหรือไม่ และเตรียมความพร้อมห้องควบคุมระบบเครือข่ายสำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่าย

(๖) ทำการติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์เครือข่ายพร้อมทั้งทดสอบการใช้งานของเครื่องคอมพิวเตอร์แม่ข่ายแต่ละเครื่องว่าสามารถให้บริการได้ตามปกติหรือไม่ ตรวจสอบระบบ Network ว่าสามารถเชื่อมต่อและให้บริการกับเครื่องคอมพิวเตอร์ลูกข่ายได้หรือไม่

(๗) เมื่อตรวจสอบแล้วว่าเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายสามารถให้บริการข้อมูลได้เรียบร้อยแล้ว แจ้งให้หน่วยงานที่เกี่ยวข้องทราบเพื่อเข้ามาใช้บริการได้ตามปกติ

ส่วนที่ ๔
นโยบายการสร้างความตระหนักในเรื่องการรักษาความปลอดภัยด้านสารสนเทศ

วัตถุประสงค์

๑. เพื่อสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งาน
๒. เพื่อให้การใช้งานระบบสารสนเทศศและระบบคอมพิวเตอร์เกิดความมั่นคงปลอดภัย
๓. เพื่อป้องกันและลดการกระทำความผิดที่เกิดขึ้นจากการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์โดยไม่คาดคิด

ผู้รับผิดชอบ

๑. หน่วยเทคโนโลยีสารสนเทศ
๒. หน่วยงานที่ได้รับมอบหมายในการจัดฝึกอบรม
๓. ผู้ดูแลระบบที่ได้รับมอบหมาย
๔. เจ้าหน้าที่ของหน่วยงานที่ได้รับมอบหมาย

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมอิเล็คทรอนิกส์

แนวปฏิบัติ

๑. จัดให้มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอยู่เสมอ อย่างน้อยปีละ ๑ ครั้ง
๒. จัดฝึกอบรมแนวปฏิบัติตามนโยบายอย่างสม่ำเสมอโดยการจัดฝึกอบรม โดยใช้วิธีการเสริมเนื้อหาแนวปฏิบัติตามนโยบายเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน
๓. จัดสัมมนาเพื่อเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และสร้างความตระหนักถึงความสำคัญของการปฏิบัติให้กับบุคลากรโดยการจัดสัมมนา มีแผนการดำเนินงานปีละไม่น้อยกว่า ๑ ครั้ง โดยจะจัดร่วมกับการสัมมนาที่เกี่ยวข้องกับด้านเทคโนโลยีสารสนเทศ และมีการเชิญวิทยากรจากภายนอกที่มีประสบการณ์ด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมาถ่ายทอดความรู้
๔. ติดประกาศประชาสัมพันธ์ให้ความรู้เกี่ยวกับแนวปฏิบัติในลักษณะเกร็ดความรู้หรือข้อระวังในรูปแบบที่สามารถเข้าใจและนำไปปฏิบัติได้ง่าย โดยมีการปรับเปลี่ยนเกร็ดความรู้อยู่เสมอ
๕. ระดมการมีส่วนร่วมและลงสู่ภาคปฏิบัติด้วยการกำกับติดตามประเมินผลและสำรวจความต้องการของผู้ใช้งาน
๖. ให้มีการสร้างความตระหนักเกี่ยวกับโปรแกรมไม่ประสงค์ดีเพื่อให้เจ้าหน้าที่มีความรู้ความเข้าใจและสามารถป้องกันตนเองได้ และให้รับทราบขั้นตอนปฏิบัติเมื่อพบเหตุโปรแกรมไม่ประสงค์ดีว่าต้องดำเนินการอย่างไร
๗. สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานให้ตระหนักถึงเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดขึ้น และสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด เพื่อให้ผู้ใช้งานปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของหน่วยงาน
๘. ผู้ใช้งานต้องตระหนักและปฏิบัติตามกฎหมายใดๆ ที่ได้ประกาศใช้ในประเทศไทย รวมทั้งกฎระเบียบของสภากาชาดไทยและข้อตกลงระหว่างประเทศอย่างเคร่งครัด ทั้งนี้ หากผู้ใช้งานไม่ปฏิบัติตามกฎหมายดังกล่าว ถือว่าความผิดนั้นเป็นความผิดส่วนบุคคลซึ่งผู้ใช้งานจะต้องรับผิดชอบต่อความผิดที่เกิดขึ้นเอง

ส่วนที่ ๕

นโยบายการดำเนินการตอบสนองเหตุการณ์ความมั่นคงปลอดภัยทางระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการในการป้องกันการบุกรุกและการโจมตีหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้มีความมั่นคงปลอดภัย

ผู้รับผิดชอบ

๑. หน่วยเทคโนโลยีสารสนเทศ
๒. ผู้ดูแลระบบที่ได้รับมอบหมาย
๓. เจ้าหน้าที่ที่ได้รับมอบหมาย

แนวปฏิบัติ

๑. **ระบบป้องกันผู้บุกรุก (IPS/IDS Syatem)**
   (๑) ดำเนินการตรวจสอบ Log File หรือรายงานของระบบป้องกันการบุกรุกสิ่งที่ทำการตรวจสอบมีดังต่อไปนี้
      (๑.๑) มีการโจมตีมากน้อยเพียงใดและเป็นการโจมตีประเภทใดมากที่สุด
      (๑.๒) ลักษณะของการโจมตีที่เกิดขึ้นมีรูปแบบที่สามารถคาดเดาได้หรือไม่
      (๑.๓) ระดับความรุนแรงมากน้อยเพียงใด
      (๑.๔) หมายเลขไอพีของเครือข่ายที่เป็นผู้โจมตี

๒. **ระบบไฟร์วอลล์ (Firewall Syatem)**
   (๑) ดำเนินการตรวจระบบป้องกันการบุกรุก อย่างน้อยเดือนละ ๑ ครั้ง
   (๒) ดำเนินการตรวจสอบบันทึกของ Log File และรายงานของไฟร์วอลล์สิ่งที่ต้องตรวจสอบมีดังต่อไปนี้
      (๒.๑) Packet ที่ไฟร์วอลล์ได้ทำการ Block
      (๒.๒) ลักษณะของ Packet ที่ถูก Block
      (๒.๓) Packet ของหมายเลขไอพีของเครือข่ายใดถูก Block เป็นจำนวนมาก
   (๓) กรณีตรวจพบการโจมตีระบบหรือเหตุการณ์ละเมิดความปลอดภัยระบบสารสนเทศให้แจ้งผู้บังคับบัญชาเพื่อตัดสินใจดำเนินการแก้ไขปัญหา

๓. ระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต ภัยคุกคามทางอินเทอร์เน็ตหรือมัลแวร์ (Malware) ประกอบด้วย ไวรัสหนอนอินเทอร์เน็ต โทรจัน รวมถึงสปายแวร์
   (๑) ดำเนินการตรวจสอบ Log File และรายงานของอุปกรณ์ที่เกี่ยวข้องกับระบบป้องกันภัยคุกคามทางอินเทอร์เน็ต สิ่งที่ต้องตรวจสอบ มีดังนี้
      (๑.๑) มัลแวร์ประเภทใดถูกพบเป็นจำนวนมาก
      (๑.๒) มัลแวร์ถูกส่งมาจากเครือข่ายใดและถูกส่งไปยังที่ใด

(๑.๓) มีการส่งมัลแวร์จากเครือข่ายภายในสถาบันไปยังภายนอกหรือไม่

(๒) ศึกษาหาวิธีแก้ไขเครื่องคอมพิวเตอร์ที่ติดมัลแวร์ โดยเฉพาะมัลแวร์ประเภทที่ตรวจพบว่ากระจายอยู่ในเครือข่ายของสถาบัน

(๓) ตรวจสอบพบว่าเครื่องคอมพิวเตอร์ภายในเครือข่ายติดมัลแวร์หรือส่งมัลแวร์ออกไปข้างนอก ต้องระงับการเชื่อมต่อของเครื่องที่ติดมัลแวร์กับระบบเครือข่ายแล้วทำการแก้ไขเครื่องนั้นทันที

ส่วนที่ ๖

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ (IT Contingency Plan) สถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย

๑. หลักการและเหตุผล

ข้อมูลสารสนเทศซึ่งจัดเก็บไว้ที่ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ถือเป็นทรัพย์สินทางการบริหารสำคัญของสถาบันการพยาบาลศรีสวรินทิรา สภากาชาดไทย จำเป็นต้องได้รับการดูแลรักษาเพื่อให้เกิดความมั่นคงปลอดภัย สามารถนำไปใช้ประโยชน์ต่อการวางแผนด้านบริหาร การจัดการเรียนการสอน การวิจัย และการให้บริการประชาชน ดังนั้น เพื่อป้องกันปัจจัยจากภายนอกและปัจจัยภายในมากระทบ และทำให้ระบบเทคโนโลยีสารสนเทศ รวมทั้งอุปกรณ์ต่าง ๆ เกิดความเสียหายได้ สถาบันจึงได้จัดทำแผนป้องกันปัญหาระบบเทคโนโลยีสารสนเทศจากเหตุการณ์ฉุกเฉิน (IT Contingency Plan) เพื่อเป็นกรอบแนวทางในการดูแลรักษาป้องกันและแก้ไขปัญหาที่อาจกระทบต่อระบบเทคโนโลยีสารสนเทศของสถาบัน

๒. วัตถุประสงค์

๒.๑. เพื่อสร้างความเข้าใจร่วมกันระหว่างผู้บริหารและผู้ปฏิบัติงาน ในการดูแลระบบรักษาความปลอดภัยด้านเทคโนโลยีสารสนเทศ

๒.๒. เพื่อเป็นแนวทางในการดูแลรักษาระบบความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศของสถาบัน ให้มีเสถียรภาพและมีความพร้อมใช้งาน

๒.๓. เพื่อให้ระบบเทคโนโลยีสารสนเทศสามารถดำเนินการได้อย่างต่อเนื่อง และมีประสิทธิภาพ สามารถแก้ไขสถานการณ์ได้อย่างทันท่วงที

๒.๔. เพื่อเตรียมความพร้อมรับสถานการณ์ฉุกเฉินและลดความเสียหายที่อาจจะเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศของสถาบัน

๓. เหตุภัยพิบัติ

ภัยพิบัติเป็นภัยที่อาจก่อให้เกิดความเสียหายกับระบบเทคโนโลยีสารสนเทศของสถาบัน ซึ่งสามารถจำแนกประเภทของภัยได้ดังนี้

๓.๑. ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ได้แก่ อัคคีภัย อุทกภัย การป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

๓.๒. การโจรกรรมอุปกรณ์คอมพิวเตอร์ที่เป็นส่วนของการจัดเก็บและรวบรวมข้อมูล

๓.๓. ระบบสื่อสารของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

๓.๔. กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

๓.๕. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายข้อมูล

๓.๖. ไวรัสคอมพิวเตอร์

๓.๗. ระบบเสียหายจากภัยสงคราม เหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

๓.๘. ระบบเทคโนโลยีสารสนเทศหลักเสียหาย หรือข้อมูลถูกทำลาย

๔. แนวทางการป้องกันและแก้ไขความเสียหายจากภัยพิบัติ

๔.๑. ภัยธรรมชาติ

ภัยธรรมชาติที่กระทำต่ออาคารสถานที่ตั้งของศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) ได้แก่ อัคคีภัย อุทกภัย และการป้องกันความชื้นและอุณหภูมิที่ไม่เหมาะสม เป็นต้น

(๔.๑.๑.) การป้องกันอัคคีภัย

(๑) กำหนดเขตพื้นที่ควบคุมการเกิดอัคคีภัย และจัดทำป้ายเตือนให้มองเห็นชัดเจน

(๒) จัดอบรมแผนป้องกันและระงับอัคคีภัย ซ้อมดับเพลิงและการหนีไฟขั้นต้นให้แก่บุคลากรทุกคนอย่างน้อยปีละ ๑ ครั้ง

(๓) จัดทำระบบดับเพลิงอัตโนมัติสำหรับศูนย์ข้อมูลคอมพิวเตอร์

(๔.๑.๒.) การป้องกันอุทกภัย ความชื้น และอุณหภูมิที่ไม่เหมาะสม

(๑) เปิดเครื่องปรับอากาศและเครื่องควบคุมความชื้น และติดตั้งระบบอัตโนมัติตรวจสอบการทำงาน ๒๔ ชั่วโมง

(๒) ตรวจสอบการรั่วซึมของหลังคาอาคารเพื่อป้องกันการรั่วซึมของน้ำฝนที่ค้างสะสม

๔.๒. การโจรกรรมอุปกรณ์ส่วนของการจัดเก็บและให้บริการข้อมูล

(๔.๒.๑.) ควบคุมการเข้าออกศูนย์ข้อมูลคอมพิวเตอร์ โดยห้ามบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้องเข้าไปในห้อง หากจำเป็นให้มีเจ้าหน้าที่ผู้รับผิดชอบเป็นผู้รับผิดชอบนำเข้าไป

(๔.๒.๒.) จัดให้มีระบบรักษาความปลอดภัยในการเข้าถึงอุปกรณ์คอมพิวเตอร์แม่ข่าย เช่น ระบบยืนยันตัวตนด้วยรหัสเฉพาะผู้รับผิดชอบ

(๔.๒.๓.) มีเวรเฝ้าระวังและตรวจสอบการทำงานของระบบให้ใช้งานได้อยู่เสมอ

(๔.๒.๔.) ติดตั้งกล้องวงจรปิด และส่งสัญญาณภาพมาไว้ที่จอภาพส่วนกลาง

๔.๓. ระบบสื่อสารที่เชื่อมต่อกับระบบเครือข่ายภายนอกขัดข้อง

(๔.๓.๑.) ตรวจสอบและเฝ้าระวังระบบเครือข่ายทั้งภายในและภายนอกให้สามารถใช้งานได้ตลอดเวลา

(๔.๓.๒.) ต้องจัดให้มีเครือข่ายสำรอง กำหนดให้ใช้งานได้ในกรณีที่ระบบสื่อสารเส้นทางหลักไม่สามารถใช้งานได้

๔.๔. กระแสไฟฟ้าขัดข้องหรือไฟฟ้าดับ

(๔.๔.๑.) มีระบบสำรองไฟฟ้าและปรับแรงดันอัตโนมัติ เพื่อป้องกันความเสียหายที่อาจเกิดขึ้นกับอุปกรณ์คอมพิวเตอร์ทั้งในส่วนของเครื่องคอมพิวเตอร์แม่ข่าย ระบบเครือข่าย และเครื่องคอมพิวเตอร์ส่วนบุคคล ซึ่งต้องมีระยะเวลาในการสำรองไฟฟ้าได้ไม่น้อยกว่า ๓๐ นาที

(๔.๔.๒.) เปิดเครื่องสำรองไฟฟ้าตลอดระยะเวลาให้บริการ ตรวจสอบการทำงานของระบบทุกวัน และบำรุงรักษาเครื่องสำรองไฟฟ้าให้อยู่ในสภาพพร้อมใช้งานอย่างน้อยเดือนละ ๑ ครั้ง

๔.๕. การบุกรุกหรือโจมตีจากภายนอก เพื่อเข้าถึงหรือควบคุมระบบเทคโนโลยีสารสนเทศ รวมทั้งสร้างความเสียหายหรือทำลายระบบข้อมูล

(๔.๕.๑.) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อตรวจสอบและป้องกันผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตและอินทราเน็ต สามารถเข้าสู่ระบบตลอดเวลา

(๔.๕.๒.) จัดเวรเฝ้าระวังระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเทอร์เน็ตและอินทราเน็ต เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติ หรือมีความถี่ในการเรียกใช้งานผิดปกติ เพื่อจะได้สรุปหาสาเหตุและป้องกัน

(๔.๕.๓.) ติดตั้งระบบป้องกันไวรัสคอมพิวเตอร์ให้ทันสมัย และปรับปรุงอย่างสม่ำเสมอ และปิดพอร์ตที่ไม่ใช้งาน

(๔.๕.๔.) กำหนดรหัสผ่านเพื่อป้องกันการเข้าถึงระบบไม่ได้รับอนุญาต

(๔.๕.๕.) ป้องกันการปลอมแปลงหมายเลขไอพีแอดเดรส (IP address) โดยการกรองแพ็คเกทที่มาจากภายนอก

๔.๖. ไวรัสคอมพิวเตอร์

(๔.๖.๑.) ติดตั้งโปรแกรมป้องกันไวรัสและอัพเดทข้อมูลไวรัสอยู่เสมอ และต้องใช้โปรแกรมเพื่อตรวจหาไวรัสอย่างน้อยสัปดาห์ละ ๑ ครั้ง

(๔.๖.๒.) ระวังภัยจากการเปิดไฟล์จากสื่อบันทึกข้อมูลต่างๆ

(๔.๖.๓.) ใช้ความระมัดระวังในการเปิดจดหมายอีเล็กทรอนิกส์ เช่น ไม่เปิดจดหมายอีเล็กทรอนิกส์ ที่ไม่ทราบแหล่งที่มา หรือลบจดหมายอีเล็กทรอนิกส์ทิ้งทันทีถ้าไม่ทราบแหล่งที่มา

(๔.๖.๔.) ระมัดระวังการดาวน์โหลดไฟล์ต่างๆ จากอินเทอร์เน็ต

๔.๗. ระบบเสียหายจากภัยสงครามหรือเหตุจลาจล และการเกิดสถานการณ์ความไม่สงบ

เนื่องจากภัยดังกล่าวเป็นภัยจากปัจจัยภายนอกที่ไม่สามารถยับยั้งได้ สามารถป้องกันได้โดยการจัดทำศูนย์ข้อมูลคอมพิวเตอร์สำรองนอกอาคารศูนย์ข้อมูลคอมพิวเตอร์ และมีระบบสำรองข้อมูลโดยแยกสถานที่จัดเก็บอย่างน้อย ๑ ที่ หากเกิดความเสียหายกับข้อมูลก็จะสามารถนำข้อมูลที่มีในศูนย์ข้อมูลคอมพิวเตอร์สำรองหรือข้อมูลในระบบสำรองที่จัดเก็บไว้มาใช้แทนที่ได้ทันที

๔.๘. ระบบบริการหลัก ระบบฐานข้อมูลหลักเสียหาย หรือข้อมูลถูกทำลาย

(๔.๘.๑.) สำรองข้อมูลอัตโนมัติ โดยเครื่องคอมพิวเตอร์แม่ข่ายจะสำรองข้อมูลไว้ในเครื่องคอมพิวเตอร์แม่ข่ายซึ่งทำหน้าที่สำรองข้อมูลกลางทุกวัน และเครื่องดังกล่าวจะกระจายข้อมูลที่สำรองไว้ไปยังฮาร์ดดิสก์ภายนอก (External Harddisk)

(๔.๘.๒.) สำรองข้อมูลอัตโนมัติ โดยเครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์ข้อมูลคอมพิวเตอร์หลักไว้ในเครื่องคอมพิวเตอร์แม่ข่ายที่ศูนย์ข้อมูลคอมพิวเตอร์สำรอง (DR Site) ทุก ๑ ชั่วโมง

(๔.๘.๓.) ทดสอบการกู้คืนข้อมูลและฐานข้อมูล ที่ได้สำรองไว้อย่างสม่ำเสมอทุกระบบอย่างน้อยปีละ ๑ ครั้ง

(๔.๘.๔.) บำรุงรักษาข้อมูลและระบบสำรอง เพื่อลดความเสี่ยงของข้อมูล

๔.๙. การบุกรุก และภัยคุกคามทางคอมพิวเตอร์ โจมตีระบบเครือข่าย

เพื่อเป็นการเสริมสร้างความปลอดภัยให้กับระบบสารสนเทศและระบบเครือข่าย มีแนวทางดังนี้

(๔.๙.๑.) มีระบบยืนยันตัวตน เพื่อตรวจสอบสิทธิ์ก่อนเข้าใช้อินเตอร์เน็ตหรือใช้งานระบบเครือข่าย ตามอำนาจหน้าที่และความรับผิดชอบ

(๔.๙.๒.) กำหนดมาตรการควบคุมการเข้า-ออกห้องควบคุมระบบเครือข่ายและการป้องกันความเสียหาย

(๔.๙.๓.) หากบุคคลที่ไม่มีอำนาจหน้าที่เกี่ยวข้อง จำเป็นต้องเข้าไปในศูนย์ข้อมูลคอมพิวเตอร์ จะต้องให้เจ้าหน้าที่ผู้ดูแลศูนย์ข้อมูลคอมพิวเตอร์เป็นผู้รับผิดชอบนำเข้าไป และคอยกำกับดูแลตลอดการปฏิบัติงาน สำหรับประตูเข้าออกต้องติดตั้งระบบตรวจสอบและติดตั้งกล้องวงจรปิดเพื่อป้องกันการโจรกรรม

(๔.๙.๔.) ติดตั้งระบบป้องกันการบุกรุกเครือข่าย เพื่อป้องกันไม่ให้ผู้ที่ไม่ได้รับอนุญาตจากระบบเครือข่ายอินเตอร์เน็ตสามารถเข้าสู่ระบบสารสนเทศและระบบเครือข่ายคอมพิวเตอร์ได้ โดยเปิดใช้งานตลอดเวลา

(๔.๙.๕.) มีเจ้าหน้าที่ดูแลระบบเครือข่าย ตรวจสอบปริมาณข้อมูลบนเครือข่ายอินเตอร์เน็ตขององค์กร เพื่อสังเกตปริมาณข้อมูลบนเครือข่ายว่ามีปริมาณมากผิดปกติหรือการเรียกใช้ระบบสารสนเทศมีความถี่ในการเรียกใช้ผิดปกติ

๕. การกู้คืนระบบคอมพิวเตอร์กลับสู่สภาวะปกติ

การกู้คืนระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย โดยปกติระบบเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายต้องอยู่ในสภาพพร้อมให้บริการตลอดเวลา ๒๔ ชั่วโมง หากไม่สามารถให้บริการได้ต้องรีบกู้ระบบคืนให้ได้เร็วที่สุด เพื่อทำให้ระบบการทำงานของเครื่องคอมพิวเตอร์และข้อมูลกลับสู่สภาพเดิม เมื่อระบบเกิดความเสียหายหรือหยุดทำงาน ต้องดำเนินการ ดังนี้

๕.๑. ตรวจสอบระบบปฏิบัติการ ระบบฐานข้อมูล ตรวจสอบความถูกต้องของข้อมูลและระบบอื่นๆ ที่เกี่ยวข้อง

๕.๒ จัดหาอุปกรณ์หรือชิ้นส่วน เพื่อทดแทน

๕.๓ ซ่อมบำรุงวัสดุอุปกรณ์ที่เสียหาย ให้เสร็จภายใน ๔๘ ชั่วโมง

๕.๔ นำข้อมูลจากสื่อบันทึกข้อมูลสำรองหรือจากระบบสำรองข้อมูลกลับมาใช้งานโดยเร็วภายใน ๔๘ ชั่วโมง

๖. ผู้รับผิดชอบเมื่อเกิดสถานการณ์ฉุกเฉิน

หน่วยงานต้องจัดเตรียมทีมงาน และมอบหมายหน้าที่ความรับผิดชอบอย่างชัดเจน เพื่อรองรับกับภัยฉุกเฉินที่อาจจะเกิดขึ้น ดังนี้

๖.๑. ระดับนโยบาย

รับผิดชอบในการกำหนดนโยบาย ให้ข้อเสนอแนะ คำปรึกษา ตลอดจนติดตาม กำกับ ดูแล ควบคุม ตรวจสอบ เจ้าหน้าที่ในระดับปฏิบัติ ผู้รับผิดชอบ ได้แก่

(๖.๑.๑.) ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Office : CEO)

(๖.๑.๒.) หัวหน้าหน่วยเทคโนโลยีสารสนเทศ

๖.๒. ระดับปฏิบัติ

(๖.๒.๑.) ทีมบริการเครื่องคอมพิวเตอร์แม่ข่าย ทำหน้าที่

(๑) บริหารจัดการและบำรุงรักษาเครื่องคอมพิวเตอร์แม่ข่ายให้อยู่ในสภาพพร้อมใช้งานและกู้คืนเมื่อเครื่องไม่ทำงาน

(๒) เฝ้าระวังการทำงานของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการระบบเทคโนโลยีสารสนเทศขององค์กร

(๓) ดูแลการสำรองและกู้คืนข้อมูลและฐานข้อมูลจากความเสียหายให้กลับมาใช้งานตามปกติ

(๔) ทดสอบการกู้คืนข้อมูลในระบบสำรองข้อมูล เพื่อทดสอบว่าข้อมูลที่สำรองไว้สามารถนำกลับมาใช้งานได้เมื่อจำเป็น

(๕) บำรุงรักษาและทดสอบการกู้คืนระบบสำรองข้อมูล เพื่อให้ระบบมีความพร้อมใช้อยู่เสมอ

(๖) ประเมินผลกระทบจากภาวะฉุกเฉินต่อระบบสารสนเทศในส่วนเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์คอมพิวเตอร์

(๖.๒.๒.) ทีมบริการระบบเครือข่ายและสื่อสาร

(๑) อยู่เวรเฝ้าระวังการทำงานของระบบเครือข่ายและสื่อสารให้ทำงานได้ตลอดเวลาที่เปิดบริการ

(๒) บำรุงรักษาและกู้คืนระบบเครือข่ายและสื่อสารให้ทำงานได้ปกติ

(๓) ค้นหาสาเหตุและอุดช่องโหว่ระบบเครือข่าย เพื่อป้องกันภัยคุกคามทางคอมพิวเตอร์

(๔) จัดเตรียมสถานที่สำหรับไซต์สำรอง รวมถึงระบบไฟฟ้า ระบบสื่อสาร ระบบปรับอากาศ ให้พร้อมใช้งาน

(๕) บำรุงรักษาศูนย์ข้อมูลคอมพิวเตอร์เป็นประจำทุกเดือน เพื่อให้ศูนย์ข้อมูลคอมพิวเตอร์ (Data Center) อยู่ในสภาพพร้อมใช้อยู่เสมอ

(๖) ดูแลและบำรุงรักษาระบบไฟฟ้า ระบบปรับอากาศ การควบคุมความชื้นห้องศูนย์ข้อมูลคอมพิวเตอร์ (Data Center)

(๗) ประเมินผลกระทบจากภาวะฉุกเฉินต่อระบบสารสนเทศในส่วนระบบเครือข่ายและสื่อสาร

(๖.๒.๓.) ทีมบริการระบบสารสนเทศ

(๑) บริหารจัดการและเฝ้าระวังระบบสารสนเทศให้สามารถดำเนินงานต่อได้

(๒) จัดเตรียมการย้ายส่วนประมวลผลของระบบสารสนเทศหลักให้สามารถดำเนินงานต่อได้

(๓) รับผิดชอบในการกอบกู้ระบบงานหลักที่สำคัญ

(๔) ประเมินผลกระทบจากภาวะฉุกเฉินต่อระบบสารสนเทศในส่วนระบบงาน

๗. การทบทวนและปรับปรุงแผน

แผนรองรับสถานการณ์ฉุกเฉินด้านเทคโนโลยีสารสนเทศ ต้องได้รับการปรับปรุงให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ ตามที่ระบุอย่างน้อยปีละ ๑ ครั้ง

๘. การติดตามและรายงานผล

กำหนดให้เจ้าหน้าที่ผู้รับผิดชอบรายงานผลการดำเนินการ หรือการตรวจสอบ ให้หัวหน้าหน่วยเทคโนโลยีสารสนเทศทราบเป็นประจำทุกเดือน เพื่อรายงานสรุปให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) ทราบ และหากมีเหตุฉุกเฉินร้ายแรงต้องรายงานให้ผู้บริหารระดับสูงสุดของหน่วยงานทราบ

ที่ปรึกษานโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

- ผศ.ดร. สุชาติ คุ้มมะณี หัวหน้าภาควิชาวิทยาการคอมพิวเตอร์/อาจารย์ประจำคณะวิทยาการสารสนเทศมหาวิทยาลัยมหาสารคาม
- ผศ. พงษ์ศนัญ ชาญชัยชิณวรฒ์ อาจารย์ประจำสาขาวิชาคอมพิวเตอร์ธุรกิจ คณะวิทยาศาสตร์และสังคมศาสตร์ มหาวิทยาลัยบูรพา
- อ. ธวัชวงศ์ ลาวัลย์ อาจารย์ประจำคณะวิทยาการสารสนเทศ มหาวิทยาลัยมหาสารคาม

คณะผู้จัดทำ

- นางศรัณยา จันทรตรี หัวหน้าฝ่ายบริการการศึกษา
- นายวิโชค มณีสงค์ หัวหน่วยเทคโนโลยีสารสนเทศ
- นายอำนาจ บุญอริยะ นักวิชาการคอมพิวเตอร์
- นายเจษฎา เลอวิทย์วรพงศ์ นักวิชาการคอมพิวเตอร์
- นายปวริศ กิตตินัทพันธุ์ นักวิชาการคอมพิวเตอร์
- นางสาวพิชญ์สนี เชียงเครือ นายช่างคอมพิวเตอร์