ระเบียบสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) ว่าด้วยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2556

โดยที่เป็นการสมควรกำหนดมาตรการรักษาความปลอดภัยด้านสารสนเทศของสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) และเพื่อให้เป็นไปตามที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินธุรกรรมด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ อาศัยอำนาจตามพระราชกฤษฎีกาจัดตั้งสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) พ.ศ. 2551 มาตรา 27 (3) จึงวางระเบียบไว้ดังต่อไปนี้

ข้อ 1 ระเบียบนี้เรียกว่า "ระเบียบสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) ว่าด้วยนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. 2556"

ข้อ 2 ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ 3 ให้ยกเลิกระเบียบสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน) ว่าด้วยการใช้งานและความมั่นคงปลอดภัยของระบบคอมพิวเตอร์และเครือข่าย พ.ศ. 2554

ข้อ 4 ในระเบียบนี้

"สถาบัน" หมายความว่า สถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน)

"ผู้อำนวยการ" หมายความว่า ผู้อำนวยการสถาบันสารสนเทศทรัพยากรน้ำและการเกษตร (องค์การมหาชน)

"ผู้บังคับบัญชา" หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของสถาบัน

"ผู้ใช้งาน" หมายความว่า เจ้าหน้าที่และลูกจ้างของสถาบัน รวมถึงบุคคลอื่นที่สถาบันมอบหมายหรือว่าจ้างให้ปฏิบัติงานให้แก่สถาบันด้วย หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบัน

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิเฉพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสถาบัน

"สินทรัพย์" หมายความว่า ข้อมูล ระบบข้อมูล และสินทรัพย์ด้านเทคโนโลยีสารสนเทศและการสื่อสารของสถาบัน และสิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่าย หรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security" หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted / Unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ผู้ดูแลระบบ (System Administrator)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบดูแลรักษาหรือจัดการระบบคอมพิวเตอร์และระบบเครือข่ายไม่ว่าส่วนหนึ่งส่วนใด

"หน่วยงานภายนอก" หมายความว่า องค์กร หรือหน่วยงานภายนอกที่ได้รับอนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของสถาบัน โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล"ผู้ตรวจสอบระบบสารสนเทศของสถาบัน (IT Auditor)" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้บังคับบัญชา ให้มีหน้าที่ตรวจสอบข้อมูลจราจรทางคอมพิวเตอร์ (Log) และรับผิดชอบให้สามารถเข้าถึงข้อมูลจราจรทางคอมพิวเตอร์ (Log)

"ระบบเทคโนโลยีสารสนเทศ (Information Technology System)" หมายความว่า ระบบงานของสถาบันที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการ

สร้างสารสนเทศที่สถาบันสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ เช่น ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ เป็นต้น

"ระบบคอมพิวเตอร์" หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกันโดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย" หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบเทคโนโลยีสารสนเทศต่างๆ ของสถาบันได้ เช่น ระบบแลน (LAN) ระบบอินทราเน็ต (Intranet) ระบบอินเทอร์เน็ต (Internet) เป็นต้น

"ระบบแลน (Local Area Network)" และ "ระบบอินทราเน็ต (Intranet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในสถาบันเข้าด้วยกัน เป็นระบบเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในสถาบัน

"ระบบอินเตอร์เน็ต (Internet)" หมายความว่า ระบบเครือข่ายอิเล็กทรอนิกส์ที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของสถาบันเข้ากับเครือข่ายอินเทอร์เน็ตสากล "จดหมายอิเล็กทรอนิกส์ (e-mail)" หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกัน โดยผ่านเครื่องคอมพิวเตอร์และระบบเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งอาจเป็นได้ทั้ง ตัวอักษร ภาพถ่าย ภาพกราฟิก ภาพเคลื่อนไหว และเสียง ที่ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP3 และ IMAP เป็นต้น

"ชื่อผู้ใช้ (Username)" หมายความว่า ชุดของตัวอักษรหรือตัวเลขที่ถูกกำหนดขึ้นเพื่อใช้ในการลงบันทึกเข้า (Login) เพื่อใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่มีการกำหนดสิทธิการใช้งานไว้

"บัญชีผู้ใช้งาน (Account)" หมายความว่า รายชื่อผู้มีสิทธิใช้งานเครื่องคอมพิวเตอร์และบริการในระบบเครือข่ายของสถาบัน ซึ่งมีการเข้าถึงระบบได้ตามการใช้งานที่กำหนด

"รหัสผ่าน (Password)" หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงข้อมูลและระบบข้อมูลในการรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศ

"ลงบันทึกเข้า (Login)" หมายความว่า กระบวนการที่ผู้ใช้งานต้องทำให้เสร็จสิ้นตามขั้นตอนที่ตั้งไว้เพื่อเข้าใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย ซึ่งปกติแล้วจะอยู่ในรูปแบบของการกรอกชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ให้ถูกต้อง เพื่อเป็นการพิสูจน์ยืนยันตัวตน

"ออกจากระบบ (Logout)" หมายความว่า กระบวนการที่ผู้ใช้งานทำเพื่อสิ้นสุดการใช้งานระบบคอมพิวเตอร์และระบบเครือข่าย

"เครื่องคอมพิวเตอร์" หมายความว่า เครื่องคอมพิวเตอร์แบบตั้งโต๊ะและเครื่องคอมพิวเตอร์แบบพกพา

"ชื่อเครื่องคอมพิวเตอร์ (Computer Name)" หมายความว่า ชื่อที่กำหนดเฉพาะให้กับเครื่องคอมพิวเตอร์บนระบบเครือข่ายโดยจะมีชื่อที่ไม่ซ้ำกัน ทำให้บ่งบอกได้ว่าเป็นเครื่องคอมพิวเตอร์ใดในระบบเครือข่าย

"สื่อบันทึกพกพา" หมายความว่า สื่ออิเล็กทรอนิกส์ที่ใช้ในการบันทึกหรือจัดเก็บข้อมูล ได้แก่ Flash Drive หรือ Handy Drive หรือ Thumb Drive หรือ External Hard disk หรือ Floppy disk เป็นต้น

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์

"สารสนเทศ (Information)" หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจ และอื่นๆ

"พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ" หมายความว่า พื้นที่ที่สถาบันอนุญาตให้มีการใช้งานระบบเทคโนโลยีสารสนเทศ โดยแบ่งเป็น

(1) พื้นที่ทำงาน หมายความว่า พื้นที่ติดตั้งเครื่องคอมพิวเตอร์ส่วนบุคคล และคอมพิวเตอร์แบบพกพาที่ประจำโต๊ะทำงาน รวมถึงพื้นที่ทำงานของผู้ดูแลระบบ

(2) พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย หมายความว่า พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย และให้หมายความรวมถึงพื้นที่จัดเก็บข้อมูลคอมพิวเตอร์

(3) พื้นที่ใช้งานระบบเครือข่ายไร้สาย หมายความว่า พื้นที่ในการให้บริการระบบเครือข่ายไร้สาย

"แผนผังระบบเครือข่าย (Network Diagram)" หมายความว่า แผนผังซึ่งแสดงถึงการเชื่อมต่อของระบบเครือข่ายของสถาบัน

"อุปกรณ์จัดเส้นทาง (Router)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่จัดเส้นทางและค้นหาเส้นทางเพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

"อุปกรณ์กระจายสัญญาณข้อมูล (Switch)" หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ที่ทำหน้าที่รับ-ส่งข้อมูล

"อุปกรณ์กระจายสัญญาณ (Access Point)" หมายความว่า อุปกรณ์ที่ทำหน้าที่กระจายสัญญาณในเครือข่ายไร้สาย

"SSID (Service Set Identifier)" หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน

"WEP (Wired Equivalent Privacy)" หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายโดยอาศัยชุดตัวเลขมาใช้เข้ารหัสข้อมูล ดังนั้นทุกเครื่องในเครือข่ายที่รับส่งข้อมูลถึงกันจึงต้องรู้ค่าชุดตัวเลขนี้

"WPA (Wi-Fi Protected Access)" หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สายที่พัฒนาขึ้นมาใหม่ให้มีความปลอดภัยมากกว่าวิธีเดิมอย่าง WEP (Wired Equivalent Privacy)

"Wireless LAN Client" หมายความว่า เครื่องคอมพิวเตอร์ลูกข่ายที่ต่ออยู่ในระบบแลน โดยใช้คลื่นวิทยุในการสื่อสารข้อมูลตามการใช้สายสัญญาณ โดยเครื่องคอมพิวเตอร์แต่ละเครื่องจะต้องมีการ์ดรับและส่งสัญญาณ ซึ่งมีมาตรฐานที่นิยมใช้เรียกว่า IEEE 802.11

"MAC Address (Media Access Control Address)" หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกัน ตัวเลขจะอยู่ในรูปของ เลขฐาน 16 จำนวน 6 คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง

"VPN (Virtual Private Network)" หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนที่สร้างขึ้นมาเป็นของส่วนตัว โดยในการรับส่งข้อมูลจริง จะทำโดยการเข้ารหัสแพคเกตแล้วรับ – ส่งผ่านเครือข่ายอินเทอร์เน็ต ทำให้บุคคลอื่นไม่สามารถอ่านได้ และจะไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง

"Web Server" หมายความว่า เครื่องคอมพิวเตอร์ที่ติดตั้งโปรแกรมบริการเว็บและมีหน้าที่ให้บริการเว็บแก่ต่างๆ

"ซับโดเมนเนม (Sub Domain Name)" หมายความว่า ส่วนย่อยที่จะช่วยขยายให้ทราบถึงกลุ่มต่างๆ ภายในโดเมนนั้น ซึ่งเป็นชื่อที่ระบุให้กับผู้ใช้เพื่อเข้ามายังเว็บไซต์ของตน หรืออาจจะใช้ 'ที่อยู่เว็บไซต์' แทนก็ได้

"โปรแกรมประสงค์ร้าย (Malware)" หมายความว่า โปรแกรมคอมพิวเตอร์ชุดคำสั่งและ/หรือข้อมูลอิเล็กทรอนิกส์ที่ได้รับการออกแบบขึ้นมาที่มีวัตถุประสงค์เพื่อก่อกวนหรือสร้างความ

เสียหายไม่ว่าโดยตรงหรือโดยอ้อมแก่ระบบคอมพิวเตอร์หรือระบบเครือข่าย เช่น ไวรัสคอมพิวเตอร์ (Computer Virus) หรือสปายแวร์ (Spyware) หรือหนอน (Worm) หรือม้าโทรจัน (Trojan horse) หรือ ฟิชชิง (Phishing) หรือจดหมายลูกโซ่ (Mass Mailing) เป็นต้น

"ไบออส (BIOS)" หมายความว่า ซอฟต์แวร์ขนาดเล็กซึ่งเก็บอยู่ในหน่วยความจำบนแผงวงจรของเครื่องคอมพิวเตอร์ ทำหน้าที่ควบคุมขั้นตอนการบู๊ตและการทำงานของอุปกรณ์พื้นฐานต่างๆ ที่ติดตั้งอยู่บนแผงวงจร

"การตั้งค่าระบบ (Configuration)" หมายความว่า ค่าที่ใช้กำหนดการทำงานของโปรแกรมหรือองค์ประกอบของเครื่องคอมพิวเตอร์ทั้งทางด้านฮาร์ดแวร์และซอฟต์แวร์

"โดยปริยาย (Default)" หมายความว่า ค่าที่เครื่องคอมพิวเตอร์หรือโปรแกรมได้กำหนดไว้ล่วงหน้า และนำไปใช้ได้โดยปริยายหากไม่มีการเปลี่ยนแปลงจากผู้ใช้งาน

"เลขที่อยู่ไอพี (IP Address)" หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขนี้ของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข 4 ส่วนหรือ 6 ส่วน ที่คั่นด้วยเครื่องหมายมหัพภาค (.)

"เลขที่อยู่ไอพีสาธารณะ (Public IP Address)" หมายความว่า เลขที่อยู่ไอพีที่มีไว้สำหรับให้แต่ละหน่วยงาน หรือแต่ละบุคคลสามารถเชื่อมต่อเข้าหากัน หรือรับส่งข้อมูลระหว่างกันผ่านเครือข่ายสาธารณะได้

"แบนด์วิดท์ (Bandwidth)" หมายความว่า ปริมาณข้อมูลที่ไหลเข้าหรือออกจากจุดใดจุดหนึ่งของระบบ เป็นการแสดงให้เห็นถึงปริมาณข้อมูลที่สามารถส่งโอนได้ในช่วงเวลาหนึ่ง และเป็นการบอกถึงความเร็วในการรับส่งข้อมูล

"ลำดับชั้นข้อมูลความลับ" หมายความว่า ชั้นความลับของข้อมูลข่าวสารที่อยู่ในความดูแลของสถาบัน ทั้งนี้ การกำหนดชั้นความลับให้เป็นไปตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544 (ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ พ.ศ. 2526 และ ระเบียบสำนักนายกรัฐมนตรีว่าด้วยงานสารบรรณ ฉบับที่ 2 พ.ศ. 2548)

"การเข้ารหัส (Encryption)" หมายความว่า การนำข้อมูลมาเข้ารหัสเพื่อป้องกันการลักลอบเข้ามาใช้ข้อมูล ผู้ที่สามารถเปิดไฟล์ข้อมูลที่เข้ารหัสไว้จะต้องมีโปรแกรมถอดรหัสเพื่อให้ข้อมูลกลับมาใช้งานได้ตามปกติ

"การพิสูจน์ยืนยันตัวตน (Authentication)" หมายความว่า ขั้นตอนการรักษาความปลอดภัยในการเข้าใช้ระบบ เป็นขั้นตอนในการพิสูจน์ตัวตนของผู้ใช้งานระบบ ทั่วไปแล้วจะเป็นการพิสูจน์โดยใช้ชื่อผู้ใช้ (Username) และรหัสผ่าน (Password)

"ไฟร์วอลล์ (Firewall)" หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย

"Firewall Log" หมายความว่า การบันทึกการสื่อสารทั้งหมดที่เกิดขึ้นไม่ว่าไฟร์วอลล์ (Firewall) จะอนุญาตให้เกิดการสื่อสารนั้นได้หรือไม่ก็ตาม ซึ่งสามารถนำมาใช้ในการวิเคราะห์ เพื่อตรวจสอบปริมาณการของการสื่อสาร ปริมาณการสื่อสาร นอกจากนั้นแล้วยังอาจจะสะท้อนให้เห็นจำนวนครั้งที่พยายามจะบุกรุกเข้ามาภายในสถาบัน

"ข้อมูลจราจรทางคอมพิวเตอร์ (Log)" หมายความว่า ข้อมูลที่เกี่ยวกับการติดต่อสื่อสารของระบบคอมพิวเตอร์ ซึ่งแสดงถึงแหล่งกำเนิด ต้นทาง ปลายทาง เส้นทาง วันที่ ปริมาณ ระยะเวลา และชนิดของบริการอื่นๆ ที่เกี่ยวข้องในการติดต่อสื่อสารของระบบคอมพิวเตอร์นั้น

"เวลาอ้างอิงสากล (Stratum 0)" หมายความว่า การเปรียบเทียบเวลาของเครื่องคอมพิวเตอร์แม่ข่ายที่ใช้ในการเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) กับเวลามาตรฐานสากล ในประเทศไทยอ้างอิงกับหน่วยงานมาตรฐาน (เช่น กรมอุทกศาสตร์กองทัพเรือ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ) เพื่อให้สอดคล้องกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

"อัพเดท (Update)" หมายความว่า ปรับให้เป็นปัจจุบัน การปรับปรุงข้อมูลด้านต่างๆ ของสารสนเทศให้ทันสมัยอยู่เสมอ

"ช่องโหว่ (Vulnerability)" หมายความว่า ความอ่อนแอในโปรแกรมคอมพิวเตอร์ซึ่งยอมให้เกิดการกระทำที่ไม่ได้รับอนุญาตได้ โดยเกิดจากข้อบกพร่องจากการออกแบบโปรแกรม ทำให้มีการอาศัยข้อบกพร่องดังกล่าวเพื่อเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต

"Command Line" หมายความว่า บรรทัดที่ให้ผู้ใช้งานป้อนคำสั่งแบบข้อความเพื่อสั่งให้เครื่องคอมพิวเตอร์ทำงานตามต้องการ

"ไฟล์ที่สามารถประมวลผลได้ (Executable file)" หมายความว่า ไฟล์โปรแกรมที่สามารถเรียกใช้งานได้ทันที เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe .xls.exe ในขณะที่ไฟล์ข้อมูลอื่นๆ จะเป็นไฟล์ข้อมูลประกอบ

ข้อ 5 ให้ผู้อำนวยการเป็นผู้ดูแลและดำเนินการให้เป็นไปตามระเบียบนี้

ข้อ 6 ให้ผู้อำนวยการฝ่ายวิจัยและพัฒนาเป็นผู้กำหนดรหัสและสิทธิของผู้ใช้ที่จะสามารถเข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ โดยความเห็นชอบของผู้อำนวยการ

ให้ผู้อำนวยการฝ่ายบริหารในฐานะนายทะเบียนเอกสารลับ กำหนดสิทธิการเข้าถึงชั้นข้อมูลความลับ โดยความเห็นชอบของผู้อำนวยการ

ข้อ 7 ผู้อำนวยการฝ่ายวิจัยและพัฒนามีอำนาจแต่งตั้ง "ผู้ดูแลระบบ (System Administrator)" เพื่อทำหน้าที่ตามที่ได้รับมอบหมายได้ โดยความเห็นชอบของผู้อำนวยการ

ข้อ 8 ในการมีข้อบกพร่องหรือข้อบกพร่องสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่สถาบัน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายความมั่นคงปลอดภัยด้านสารสนเทศ ผู้อำนวยการต้องเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยมีอำนาจจัดตั้งคณะกรรมการเพื่อสอบสวนข้อเท็จจริงที่เกิดขึ้น

หมวด 1
วัตถุประสงค์

ข้อ 9 สถาบันจัดทำนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อวัตถุประสงค์ ดังต่อไปนี้

(1) ส่งเสริมและสนับสนุนการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องต่อหน้าที่และกิจกรรมของสถาบัน

(2) มุ่งกำหนดแนวปฏิบัติ แนวทางแก้ไข หรือบทลงโทษตามความเหมาะสมหากมีการละเมิดหรือ ฝ่าฝืนแนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามและตรวจสอบการดำเนินงานอย่างสม่ำเสมอ เพื่อให้เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

(3) เน้นกำกับดูแลการดำเนินงานเพื่อบริหารจัดการให้ระบบเทคโนโลยีสารสนเทศมีความถูกต้องสมบูรณ์ และพร้อมใช้งานอยู่เสมอ

(4) เผยแพร่ความรู้ ความเข้าใจเพื่อสร้างความตระหนักให้กับบุคลากรที่เกี่ยวข้องทั้งของสถาบันและของหน่วยงานที่เกี่ยวข้อง ตลอดจนส่งเสริมให้มีการศึกษาอย่างต่อเนื่อง

(5) ติดตาม ตรวจสอบการดำเนินงาน และปรับปรุงแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องตามการเปลี่ยนแปลงของเทคโนโลยี

หมวด 2
นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ 10 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสถาบัน แบ่งเป็น 9 ด้าน ดังต่อไปนี้

นโยบายการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์

นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

นโยบายการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย (ผู้ใช้งานทั่วไป)

นโยบายในการจัดการระบบสารสนเทศของสถาบัน (ผู้ดูแลระบบ)

นโยบายการจัดการระบบสำรองและการเตรียมความพร้อมกรณีฉุกเฉิน

นโยบายการจัดการประเมินความเสี่ยง

นโยบายการสร้างความตระหนักในเรื่องการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ

หมวด 3

นโยบายการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่าย

ส่วนที่ 1
วัตถุประสงค์

ข้อ 11 เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศและระบบเครือข่ายของหน่วยงาน และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากโปรแกรมประสงค์ร้าย (Malware) ที่จะสร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบสารสนเทศและระบบเครือข่ายให้หยุดชะงัก รวมทั้งให้สามารถตรวจสอบติดตามหลักฐานตัวบุคคลที่เข้าใช้งานระบบสารสนเทศและระบบเครือข่ายของหน่วยงานได้อย่างถูกต้อง

ส่วนที่ 2
แนวปฏิบัติการควบคุมการเข้าถึงระบบสารสนเทศ

ข้อ 12 ให้ผู้อำนวยการฝ่ายวิจัยและพัฒนาเป็นผู้กำหนดระดับและสิทธิของผู้ใช้ที่จะสามารถเข้าใช้งานระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ ให้เหมาะสมกับการปฏิบัติงาน รวมทั้งมีการทบทวนสิทธิการเข้าถึงอย่างน้อยปีละ 1 ครั้ง

ข้อ 13 ให้ผู้ดูแลระบบกำหนดมาตรการควบคุมการเข้าใช้งานระบบสารสนเทศของสถาบัน เพื่อดูแลรักษาความปลอดภัย โดยที่บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบสารสนเทศของสถาบันจะต้องขออนุญาตเป็นลายลักษณ์อักษรต่อผู้ดูแลระบบ

ข้อ 14 ผู้ดูแลระบบควรจัดให้มีการติดตั้งระบบบันทึกและติดตามการใช้งานระบบสารสนเทศของสถาบัน และตรวจสอบการละเมิดความปลอดภัย ที่มีต่อระบบข้อมูล

ข้อ 15 ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบการแก้ไขเปลี่ยนแปลงสิทธิต่างๆ และการผ่านเข้า-ออกสถานที่ตั้งของระบบ ของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐาน ในการตรวจสอบ

ส่วนที่ 3
การบริหารรหัสผ่าน

ข้อ 16 ผู้ดูแลระบบต้องบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่านของบุคลากร ดังต่อไปนี้

(1) เจ้าหน้าที่และลูกจ้างของสถาบันที่เข้าทำงานใหม่ ต้องลงทะเบียนผู้ใช้งานใหม่ โดยการกรอกแบบฟอร์มเพื่อขอใช้งานระบบสารสนเทศและเครือข่ายของสถาบัน พร้อมกับลงชื่อรับทราบระเบียบนี้ ยื่นต่อผู้ดูแลระบบ เพื่อสร้างชื่อผู้ใช้และรหัสผ่านสำหรับเริ่มใช้งาน พร้อมทั้งกำหนดสิทธิการเข้าถึงตามหน้าที่การปฏิบัติงานให้สอดคล้องตาม ข้อ 40

(2) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการฝ่ายวิจัยและพัฒนา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการจำกัดสิทธิพิเศษในการเข้าถึง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

(3) การจัดเก็บรหัสผ่านในฐานข้อมูลต้องเก็บในรูปแบบที่มีการเข้ารหัส เพื่อป้องกันการรั่วไหลของข้อมูล และรหัสผ่านจะถูกกำหนดให้เปลี่ยนใหม่ทุก 3 เดือน และมีระบบที่ป้องกันการนำรหัสที่เคยใช้ไปแล้วกลับมาใช้ซ้ำ

(4) กำหนดการเปลี่ยนแปลงและการยกเลิกชื่อผู้ใช้และรหัสผ่าน เมื่อผู้ใช้งานระบบลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

(5) ส่งมอบรหัสผ่านชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย ควรหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการป้องกันในการส่งรหัสผ่าน

(6) กำหนดให้ผู้ใช้งานลงนามยืนยันการได้รับรหัสผ่าน

(7) กำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

(8) กำหนดชื่อผู้ใช้หรือรหัสผ่านต้องไม่ซ้ำกัน

ข้อ 17 ผู้ดูแลระบบต้องบริหารจัดการการเข้าถึงข้อมูลตามประเภทชั้นความลับ ในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ ดังต่อไปนี้

(1) ต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน

(2) ต้องกำหนดรายชื่อผู้ใช้และรหัสผ่าน เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(3) ควรกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าว

(4) การยกเลิกชั้นความลับประกาศโดยนายทะเบียนเอกสารลับ และแจ้งผู้ดูแลระบบดำเนินการตามความเหมาะสม

(5) การรับส่งข้อมูลสำคัญผ่านระบบเครือข่ายสาธารณะ ควรได้รับการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล เช่น SSL VPN หรือ XML Encryption เป็นต้น

(6) ควรกำหนดการเปลี่ยนรหัสผ่าน ตามระยะเวลาที่กำหนดตามระดับความสำคัญของข้อมูล

(7) ควรกำหนดมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ออกนอกพื้นที่ของสถาบัน เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อมควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

ส่วนที่ 4
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ข้อ 18 ผู้ดูแลระบบต้องควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) ให้รั่วไหลออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด

ข้อ 19 ผู้ดูแลระบบควรทำการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณมาใช้งาน

ข้อ 20 ผู้ดูแลระบบต้องกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่างผู้ใช้งานระบบเครือข่ายแบบไร้สายและอุปกรณ์กระจายสัญญาณ และกำหนดค่าให้ไม่แสดงชื่อระบบเครือข่ายไร้สาย

ข้อ 21 ผู้ดูแลระบบต้องเลือกใช้วิธีการควบคุม MAC Address (Media Access Control Address) และชื่อผู้ใช้ รวมทั้งรหัสผ่านของผู้ใช้งานที่มีสิทธิในการเข้าใช้งานระบบเครือข่ายไร้สาย โดยระบุอนุญาตเฉพาะอุปกรณ์ที่มี MAC address (Media Access Control Address) และชื่อผู้ใช้และรหัสผ่านตามที่กำหนดไว้เท่านั้นให้เข้าใช้ระบบเครือข่ายไร้สายได้อย่างถูกต้อง

(1) เจ้าหน้าที่และลูกจ้างของสถาบันที่ประสงค์จะนำคอมพิวเตอร์โน้ตบุ๊คส่วนตัวมาใช้ในการปฏิบัติงานภายในสถาบันต้องนำมาลงทะเบียน MAC Address ของเครื่องไว้เพื่อเป็นการพิสูจน์ตัวตนอุปกรณ์ในเครือข่ายของสถาบัน

(2) บุคคลภายนอกที่มาติดต่องาน มาประชุมหากมีความต้องการใช้งานเครือข่ายไร้สายของสถาบัน ติดต่อผู้ดูแลระบบเพื่อขอใช้ชื่อผู้ใช้และรหัสผ่านชั่วคราว พร้อมทั้งลงชื่อบันทึกเป็นหลักฐานการใช้งาน โดยถือเป็นความรับผิดชอบหากมีการนำชื่อผู้ใช้และรหัสผ่านนั้นไปก่อให้เกิดความเสียหายต่อสถาบันหรือบุคคลที่สาม

ข้อ 22 ผู้ดูแลระบบควรมีการติดตั้งไฟร์วอลล์ (Firewall) ระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในสถาบัน

ข้อ 23 ผู้ดูแลระบบควรใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของระบบเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์ที่น่าสงสัยเกิดขึ้นในระบบเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก 3 เดือน และในกรณีที่ตรวจสอบพบการใช้งานระบบเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานต่อผู้อำนวยการฝ่ายวิจัยและพัฒนาทราบทันที

ข้อ 24 ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของสถาบัน

ข้อ 25 ห้ามบุคคลใดติดตั้งหรือรื้อถอนอุปกรณ์กระจายสัญญาณไร้สายภายในสถาบัน เว้นแต่เพื่อการซ่อมบำรุง หากมีความจำเป็นต้องติดตั้งต้องขออนุญาตจากผู้ดูแลระบบ และให้ดำเนินตามมาตรการเพื่อความมั่นคงปลอดภัยการควบคุมการเข้าถึงระบบเครือข่ายไร้สาย

ส่วนที่ 5
แนวปฏิบัติการควบคุมการเข้าถึงระบบเครือข่าย

ข้อ 26 ให้ผู้ดูแลระบบกำหนดมาตรการควบคุมการเข้า-ออกห้องที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย

ข้อ 27 ผู้ใช้งานที่ประสงค์จะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบัน ต้องได้รับอนุญาตจากผู้อำนวยการฝ่ายวิจัยและพัฒนาหรือผู้ดูแลระบบ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

ข้อ 28 การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่สถาบันรับผิดชอบอยู่ จะต้องขออนุญาตต่อผู้อำนวยการฝ่ายวิจัยและพัฒนาหรือผู้ดูแลระบบและจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อระบบและการใช้งานผู้ใช้อื่นๆ

ข้อ 29 ห้ามผู้ใดกระทำการเคลื่อนย้าย ติดตั้งเพิ่มเติมหรือทำการใดๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 30 ผู้ดูแลระบบต้องควบคุมการเข้าถึงระบบเครือข่าย เพื่อบริหารจัดการระบบเครือข่ายได้อย่างมีประสิทธิภาพ ดังต่อไปนี้

(1) ต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้งานเฉพาะระบบเครือข่ายที่ได้รับอนุญาตเท่านั้น

(2) ต้องมีวิธีการจำกัดเส้นทางการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกัน โดยแบ่งแยกเครือข่ายเป็น 3 กลุ่มตามลักษณะการให้บริการ คือ LAN สำหรับงานภายใน และ DMZ สำหรับบริการสาธารณะภายในสถาบัน DMZ สำหรับบริการสาธารณะแก่ผู้ใช้บริการภายนอกสถาบัน

(3) ต้องกำหนดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่ายจากเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์ในเน่าย่าย เพื่อไม่ให้ผู้ใช้งานสามารถใช้เส้นทางอื่นๆ ได้

(4) ระบบเครือข่ายทั้งหมดของสถาบันที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่นๆ ภายนอกสถาบันควรเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก รวมทั้งต้องมีความสามารถในการตรวจจับโปรแกรมประสงค์ร้ายด้วย

(5) ระบบเครือข่ายต้องติดตั้งระบบตรวจจับการบุกรุก (Intrusion Prevention System/ Intrusion Detection System) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสถาบันในลักษณะที่ผิดปกติ

(6) การเข้าสู่ระบบเครือข่ายภายในสถาบัน โดยผ่านทางระบบอินเทอร์เน็ตจำเป็นต้องมีการลงบันทึกเข้า และต้องมีการพิสูจน์ยืนยันตัวตน (Authentication) เพื่อตรวจสอบความถูกต้องของผู้ใช้งาน

(7) เลขที่อยู่ไอพี (IP Address) ภายในของระบบเครือข่ายภายในของสถาบันจำเป็นต้องมีการป้องกันมิให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้

(8) ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

(9) การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

(10) ต้องจำกัดระยะเวลาการเชื่อมต่อระบบ (Limitation of Connection Time) สำหรับระบบที่มีความเสี่ยงหรือความสำคัญสูง การตั้งเวลาให้พิจารณาตามลักษณะการทำงานของระบบงาน

การเชื่อมต่อเข้าเครื่อง Server ของสถาบันทำผ่านโปรโตคอล Secure Socket Layer กำหนดช่วงเวลาที่อนุญาตให้เชื่อมต่อติดต่อและมีการทำงานติดต่อกัน 4 ชั่วโมงต่อการเชื่อมต่อ 1 ครั้ง

(11) กำหนด Session time-out ของเครื่องแม่ข่ายไว้ 5 นาที เมื่อไม่มีการใช้งานจะตัดการเชื่อมต่อโดยอัตโนมัติ

ข้อ 31 ผู้ดูแลระบบต้องบริหารควบคุมเครื่องคอมพิวเตอร์แม่ข่าย และรับผิดชอบในการดูแลระบบคอมพิวเตอร์แม่ข่ายในการกำหนดแก้ไข หรือเปลี่ยนแปลงค่าต่างๆ ของซอฟต์แวร์ระบบ (Systems Software)

ข้อ 32 ให้ผู้ดูแลระบบกำหนดมาตรการควบคุมการจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Log) เพื่อให้ข้อมูลจราจรทางคอมพิวเตอร์มีความถูกต้องและสามารถระบุถึงตัวบุคคลได้ตามแนวทางดังต่อไปนี้

(1) จัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ไว้ในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วน ถูกต้อง แท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้และข้อมูลที่ใช้ในการจัดเก็บ ต้องกำหนดชั้นความลับในการเข้าถึงเพื่อมิให้ผู้ดูแลระบบในมีสิทธิ์หรือได้รับอนุญาตในการแก้ไขข้อมูลที่เก็บรักษาไว้ ยกเว้นผู้ตรวจสอบระบบสารสนเทศของสถาบัน (IT Auditor) หรือบุคคลที่สถาบันมอบหมาย

(2) กำหนดให้มีการบันทึกการทำงานของระบบบันทึกการปฏิบัติงานของผู้ใช้งาน (Application Logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้า-ออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command Line และ Firewall Log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย 90 วัน นับตั้งแต่การใช้บริการสิ้นสุดลง

(3) ตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานระบบอย่างสม่ำเสมอ

(4) ต้องมีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

ข้อ 33 ให้ผู้ดูแลระบบกำหนดมาตรการควบคุมการใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่าย เพื่อดูแลรักษาความปลอดภัยของระบบจากภายนอกตามแนวทาง ดังต่อไปนี้

(1) บุคคลจากหน่วยงานภายนอกที่ต้องการสิทธิในการเข้าใช้งานระบบเครือข่ายและเครื่องคอมพิวเตอร์แม่ข่ายของสถาบันจะต้องทำเรื่องขออนุญาตเป็นลายลักษณ์อักษร เพื่อขออนุญาตจากผู้อำนวยการฝ่ายวิจัยและพัฒนา หากต้องเข้าสู่ระบบสารสนเทศของสถาบันได้ขอรับชื่อผู้ใช้และรหัสผ่านสำหรับบุคคลภายนอก เพื่อใช้ยืนยันตัวในการเข้าระบบสารสนเทศของสถาบันจากผู้ดูแลระบบ

(2) หากผู้ใช้งานมีความจำเป็นต้องปรับปรุงหรือเปลี่ยนการตั้งค่าของระบบปฏิบัติการของเครื่องแม่ข่ายต้องแจ้งผู้ดูแลระบบเพื่อตรวจสอบผลที่อาจกระทบต่อระบบอื่นที่อยู่บนเครื่องแม่ข่ายเดียวกัน

(3) สำหรับเจ้าหน้าที่ที่ได้รับมอบหมายให้ดูแลโครงการที่ใช้งานเครื่องแม่ข่ายต้องแจ้งแบบการขอแบบฟอร์มขอใช้บริการกับผู้ดูแลระบบ เพื่อสร้างชื่อผู้ใช้และรหัสผ่าน พร้อมกำหนดชั้นการเข้าถึงข้อมูลในเครื่องแม่ข่ายนั้นๆ เมื่อเสร็จสิ้นโครงการต้องแจ้งผู้ดูแลระบบเพื่อลบหรือจำกัดข้อมูลไว้ต่อไป

(4) มีการควบคุมช่องทาง (Port) ที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม กำหนดรายการพอร์ตมาตรฐานที่ใช้งาน สำหรับการเปิดพอร์ตพิเศษนอกเหนือจากการใช้งานในระบบปกติของสถาบัน ให้แจ้งขอเปิดพอร์ตกับผู้ดูแลระบบ สำหรับพอร์ตที่ต้องเปิดแก่บุคคลภายนอกเพื่อการเข้าถึงระบบเครือข่ายต้องขออนุญาตผู้ดูแลระบบ เพื่อการตรวจสอบและควบคุมการใช้งาน เมื่อใช้งานแล้วเสร็จให้ปิดพอร์ตดังกล่าว

(5) วิธีการใดๆ ที่สามารถเข้าสู่ข้อมูลหรือระบบข้อมูลได้จากระยะไกลต้องได้รับการ

อนุญาตจากผู้ช่วยการฝ่ายวิจัยและพัฒนา การเชื่อมต่อเข้าระบบจากภายนอกต้องขอเปิดพอร์ตสำหรับ
การใช้งาน VPN ที่ผู้ดูแลระบบ

หมวด 4

นโยบายการควบคุมการเข้าถึงระบบปฏิบัติการ

ส่วนที่ 1

วัตถุประสงค์

ข้อ 34 เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบปฏิบัติการ ซึ่งผู้ใช้งานจะได้รับการติดตั้งระบบปฏิบัติการตามหน้าที่ ซึ่งพิจารณาและอนุมัติโดยผู้บังคับบัญชาเป็นลายลักษณ์อักษร ซึ่งมาตรการดังกล่าวนี้จะช่วยให้ผู้ใช้งานสามารถปฏิบัติตนภายใต้หลักการของความมั่นคงปลอดภัย

ส่วนที่ 2

แนวปฏิบัติการควบคุมการเข้าถึงระบบปฏิบัติการ

ข้อ 35 ผู้ใช้งานจะได้รับการติดตั้งระบบปฏิบัติการตามลักษณะการใช้งาน โดยการอนุมัติจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร

ข้อ 36 ผู้ใช้งานต้องกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ในการเข้าใช้งานระบบปฏิบัติการของเครื่องคอมพิวเตอร์ของสถาบัน ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้และรหัสผ่านของตนในการเข้าใช้งานเครื่องคอมพิวเตอร์ของสถาบันร่วมกัน

ข้อ 37 ผู้ใช้งานต้องตั้งค่าคุณสมบัติการใช้งานสำหรับระบบสารสนเทศ (Session Timeout) เพื่อป้องกันการเข้าถึงสารสนเทศเมื่อผู้ใช้งานว่างเว้นจากการใช้งานเป็นระยะเวลาหนึ่ง หรือการใช้งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งาน กำหนดให้มีการล็อคหน้าจอเมื่อไม่มีการใช้งานเกิน 5 นาที

ข้อ 38 ให้ผู้ดูแลระบบกำหนดจำนวนครั้งในการป้อนรหัสผ่านผิด หากป้อนผิดเกิน 3 ครั้ง ระบบจะทำการล็อคสิทธิการเข้าใช้ ให้ผู้ใช้งานติดต่อผู้ดูแลระบบเพื่อปลดล็อคให้

หมวด 5

นโยบายการควบคุมการเข้าถึงโปรแกรมประยุกต์

ส่วนที่ 1

วัตถุประสงค์

ข้อ 39 เพื่อเป็นมาตรการในการควบคุมการเข้าถึงและการใช้งานโปรแกรมประยุกต์ ที่สถาบันจัดหาหรือพัฒนาขึ้นเพื่อใช้ในการปฏิบัติงานตามหน้าที่ของผู้ใช้งานในแต่ละส่วนงาน ให้มีสิทธิการใช้โปรแกรมงานฟังก์ชั่นต่างๆ ภายใต้หลักการของความมั่นคงปลอดภัย

ส่วนที่ 2

แนวปฏิบัติการบริหารจัดการการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

ข้อ 40 ให้ผู้ดูแลระบบร่วมกับผู้ปฏิบัติงานที่เกี่ยวข้องจัดทำข้อกำหนดการใช้งานตามการกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control)

(1) จัดทำบัญชีรายชื่อโปรแกรมประยุกต์หรือระบบงาน พร้อมรายชื่อผู้ใช้และกำหนดสิทธิการเข้าถึง และระดับในการใช้งานสำหรับโปรแกรมต่างๆ ตามหน้าที่ปฏิบัติงาน

(2) ผู้ใช้งานที่ต้องการเข้าใช้ระบบงานนั้น นอกจากส่วนที่เกี่ยวข้องกับงานของตนแล้วให้แจ้งขอสิทธิต่อผู้ดูแลระบบงานนั้นๆ โดยมีรายละเอียดอย่างน้อย ชื่อผู้ขอใช้บริการ เหตุผลในการขอใช้และระยะเวลาในการขอใช้บริการ

(3) ผู้ดูแลระบบงานอนุญาตให้ผู้ใช้งานเข้าสู่ระบบได้เฉพาะในส่วนที่จำเป็นตามหน้าที่งานเท่านั้น

(4) ผู้ดูแลระบบงานต้องทำการตรวจสอบสิทธิที่มอบให้ผู้ใช้งานตาม (2) เพื่อติดตามการใช้งานและระยะเวลาที่อนุญาตให้ใช้

ข้อ 41 ผู้ดูแลระบบต้องควบคุมการเข้าถึงและการใช้งานโปรแกรมประยุกต์ (Application) และฟังก์ชั่นต่างๆ ของโปรแกรมประยุกต์ โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

(1) สำหรับระบบคอมพิวเตอร์โปรแกรมประยุกต์ที่ซื้อหรือจ้างพัฒนาขึ้น เมื่อส่งมอบแล้วควรเปลี่ยนบัญชีผู้ใช้และรหัสผ่านที่ใช้ในการเข้าถึงของบุคคลภายนอกทันที หากมีความจำเป็นต้องใช้งานกำหนดให้ตามโอกาสการใช้งานนั้นๆ

(2) ให้ผู้ดูแลระบบจัดทำทะเบียนผู้ใช้งาน เพื่อจำกัดสิทธิการใช้งานให้สอดคล้องกับการปฏิบัติงานของผู้ใช้งาน

(3) ให้ผู้ดูแลระบบทำการทบทวนสิทธิการเข้าถึงของผู้ใช้งานเป็นการทั่วไปอย่างน้อย

ปีละ 1 ครั้ง และปรับปรุงทะเบียนผู้ใช้งานให้เป็นปัจจุบันอยู่เสมอ หากได้รับการแจ้งการสิ้นสุดการเป็น
พนักงานให้ผู้ดูแลระบบเพิกถอนสิทธิทันที พร้อมด้วยเหตุผลในการพิจารณาของผู้บังคับบัญชา

หมวด 6
นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ส่วนที่ 1
วัตถุประสงค์

ข้อ 42 เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นสินทรัพย์ที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

ส่วนที่ 2
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

ข้อ 43 ให้ผู้ดูแลระบบเป็นผู้กำหนดพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าว แบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

ห้ามผู้ดูแลระบบและผู้ใช้งาน เปิดเผยที่ตั้งของระบบสารสนเทศต่อบุคคลภายนอก เว้นแต่การมีการซ่อมบำรุง หรือเป็นกิจกรรมของสถาบัน

ข้อ 44 ให้ผู้ดูแลระบบเป็นผู้กำหนดสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ และกำหนดมาตรการควบคุมการเข้า-ออก พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

ข้อ 45 หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในสถาบัน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์เพื่อรับชื่อผู้ใช้และรหัสผ่านสำหรับบุคคลภายนอก เพื่อใช้ยืนยันตัวในการเข้าระบบสารสนเทศของสถาบัน และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาคอยดูแลระหว่างปฏิบัติงาน

ข้อ 46 ผู้ดูแลระบบและผู้ใช้งานในกรณีที่ต้องการนำทรัพย์สินต่างๆ ออกจากหน่วยงานต้องได้รับอนุมัติจากผู้บังคับบัญชาก่อนทุกครั้ง

ข้อ 47 กำหนดให้ผู้ใช้งานต้องตั้งค่าพักการใช้งานสำหรับระบบสารสนเทศ (Session Timeout) เพื่อป้องกันการเข้าถึงสารสนเทศเมื่อผู้ใช้งานว่างเว้นจากการใช้งานเป็นระยะเวลาหนึ่ง หรือการใช้

งานโปรแกรมถนอมหน้าจอ (Screen saver) เพื่อทำการล็อคหน้าจอภาพเมื่อไม่มีการใช้งาน และต้องใส่รหัสผ่าน (Password) เพื่อกลับเข้าใช้งาน กำหนดให้มีการล็อคหน้าจอเมื่อไม่มีการใช้งานเกิน 5 นาที

ส่วนที่ 3
แนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลซึ่งเป็นสินทรัพย์ของสถาบัน

ข้อ 48 แบ่งข้อมูลออกเป็น 3 ประเภท ประกอบด้วย ข้อมูลแบบแพร่หลายทั่วไป ข้อมูลตามหน้าที่การปฏิบัติงาน และข้อมูลที่เป็นความลับ โดยจัดเก็บและกำหนดการเข้าถึงตามความเหมาะสม

(1) ข้อมูลแบบแพร่หลายทั่วไป หมายถึง ข้อมูลที่เปิดเผยต่อสาธารณะ และใช้งานโดยทั่วไปภายในสถาบัน สามารถเข้าถึงได้ตลอดเวลาผ่านระบบสารสนเทศของสถาบัน

(2) ข้อมูลตามหน้าที่การปฏิบัติงาน หมายถึง ข้อมูลที่มีการควบคุมการเข้าถึงตามหน้าที่การปฏิบัติงาน สามารถเข้าถึงได้ตลอดเวลาตามช่องทางที่กำหนดโดยผู้ดูแลระบบ

(3) ข้อมูลที่เป็นความลับ หมายถึง ข้อมูลที่อยู่ในลำดับชั้นข้อมูลความลับ ตามระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. 2544

ข้อ 49 จัดชั้นความลับเป็น 3 ลำดับคือ ลับที่สุด ลับมาก และลับ โดยมอบหมายให้ผู้อำนวยการฝ่ายบริหารเป็นนายทะเบียนเอกสารลับและแต่งตั้งผู้ช่วยนายทะเบียนเพื่อดำเนินการจัดการเอกสาร

(1) เอกสารลับในรูปแบบเอกสารกระดาษให้เก็บในตู้ที่มีการป้องกันการเข้าถึง เช่นตู้ที่มีกุญแจล็อค ในรูปแบบสื่อบันทึกพกพาเก็บในพื้นที่มีรหัสผ่านป้องกันการเข้าถึง และเข้ารหัสเอกสารข้อมูลที่เป็นความลับ

(2) การเข้าถึงข้อมูลลับสามารถทำได้ในช่วงเวลาการปฏิบัติงานปกติของสถาบัน เว้นแต่ได้รับอนุมัติจากผู้อำนวยการสถาบัน

(3) ผู้เข้าถึงข้อมูลชั้นความลับ คือ ผู้อำนวยการสถาบัน นายทะเบียนเอกสารลับ ผู้ช่วยนายทะเบียน หรือผู้ที่เกี่ยวข้องที่ได้รับมอบหมายเป็นลายลักษณ์อักษรจาก ผู้อำนวยการสถาบันหรือนายทะเบียนเอกสารลับ

(4) คงระดับความลับของเอกสารไว้จนกว่าจะมีประกาศยกเลิกความลับ

(5) ห้ามมิให้พิมพ์ข้อมูลลับด้วยเครื่องพิมพ์ที่ตั้งอยู่ในบริเวณเปิด เว้นแต่มีความจำเป็น ให้ผู้ใช้งานรอรับเอกสารที่เครื่องพิมพ์ทุกครั้ง

(6) ต้องไม่ทิ้งเอกสาร สื่อบันทึก วัสดุหรืออุปกรณ์ที่จัดเก็บข้อมูลลับ หากไม่ได้รับการทำลายด้วยวิธีที่เหมาะสม เช่นการบดเอกสารกระดาษในเครื่องทำลายเอกสาร หรือล้างแม่เหล็กหรือเขียนทับก่อนทิ้ง

(7) การลบข้อมูลที่เป็นความลับจากสื่อบันทึกข้อมูลให้ใช้วิธี DOD 5220.22 M

ข้อ 50 ผู้ดูแลระบบต้องมีวิธีการทำลายข้อมูลแบบถาวรในอุปกรณ์ที่ส่งออกไปภายนอกสถาบัน เช่น เครื่องคอมพิวเตอร์ที่ส่งคืนผู้ให้เช่า เครื่องคอมพิวเตอร์ของสำนักงานที่จำหน่ายซ่อม โดยใช้วิธีการลบข้อมูลแบบถาวรตาม 49 (7) ส่วนเครื่องคอมพิวเตอร์ที่ส่งออกไปซ่อมภายนอกสถาบันให้ลบฮาร์ดิสก์ออกก่อนหรือดำเนินการสำรองข้อมูลที่สำคัญ พร้อมทั้งทำลายข้อมูลแบบถาวรบนสื่อบันทึกข้อมูลที่มีความเสี่ยงต่อข้อมูลรั่วไหล

ข้อ 51 ผู้ใช้งานต้องเก็บเอกสาร ข้อมูลในการทำงานหรือสื่อบันทึกข้อมูลไว้ในที่ปลอดภัย เช่น ใส่ตู้หรือโต๊ะที่สามารถล็อคกุญแจได้

ข้อ 52 ผู้ใช้งานจะต้องไม่นำข้อมูลของสถาบัน และข้อมูลซึ่งได้มาจากการปฏิบัติงานให้แก่สถาบัน ไม่ว่าจะเป็นข้อมูลของสถาบัน หรือของหน่วยงานหรือผู้ยื่นก็ตาม ออกเผยแพร่ โดยไม่ได้รับอนุญาต และโดยมีวัตถุประสงค์ดังต่อไปนี้

(1) เพื่อหาประโยชน์ในเชิงธุรกิจ เป็นการส่วนตัว หรือการค้าเมียง เว้นแต่เป็นไปเพื่อประโยชน์ของทางราชการ

(2) เพื่อกระทำการอันมีลักษณะเป็นการละเมิดทรัพย์สินทางปัญญาของสถาบัน และของหน่วยงานและบุคคลผู้เป็นเจ้าของข้อมูล

ข้อมูลที่เก็บอยู่ในระบบคอมพิวเตอร์ของสถาบัน ถือเป็นสินทรัพย์ของสถาบัน สถาบันมีสิทธิดำการตรวจสอบในกรณีที่เกิดข้อสงสัยว่าอาจมีการกระทำใดๆ อันไม่พึงประสงค์ขึ้นได้ และสามารถเปิดเผยหรือใช้งานข้อมูลเหล่านี้เป็นหลักฐานในการสืบสวนความผิดต่างๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า ข้อมูลข้างต้นไม่รวมข้อมูลที่เป็นทรัพย์สินของลูกค้า หรือบุคคลภายนอก ซอฟต์แวร์หรือวัตถุอื่นๆ ที่ได้รับการคุ้มครองสิทธิบัตร หรือสิทธิอื่นของบุคคลภายนอก

หมวด 7
นโยบายการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย (ผู้ใช้งานทั่วไป)

ส่วนที่ 1
วัตถุประสงค์

ข้อ 53 เพื่อช่วยให้ผู้ใช้งาน ได้รับทราบถึงหน้าที่และความรับผิดชอบในการใช้ระบบคอมพิวเตอร์และระบบเครือข่าย รวมทั้งทำความเข้าใจและปฏิบัติตามอย่างเคร่งครัด อันจะเป็นการป้องกันทรัพย์สินและข้อมูลของหน่วยงานให้มีความลับ ความถูกต้องและมีความพร้อมใช้งานอยู่เสมอ

ส่วนที่ 2
แนวปฏิบัติการใช้เครื่องคอมพิวเตอร์และระบบเครือข่าย

ข้อ 54 ผู้ใช้งานจะต้องไม่ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายโดยมีวัตถุประสงค์ดังต่อไปนี้

(1) ทำให้เผยแพร่หรือซึ่งข้อมูลคอมพิวเตอร์ที่ขายกระทบกระเทือนต่อความมั่นคงแห่งราชอาณาจักร หรือที่มีลักษณะขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

(2) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ปลอมไม่ว่าทั้งหมดหรือบางส่วนหรือข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(3) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์อันเป็นเท็จ โดยประการที่น่าจะเกิดความเสียหายต่อความมั่นคงของประเทศหรือก่อให้เกิดความตื่นตระหนกแก่ประชาชน

(4) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ อันเป็นความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักรหรือความผิดเกี่ยวกับการก่อการร้ายตามประมวลกฎหมายอาญา

(5) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ใดๆ ที่มีลักษณะลามกอนาจาร

(6) นำเข้าสู่ระบบคอมพิวเตอร์ซึ่งข้อมูลคอมพิวเตอร์ที่ปรากฏเป็นภาพของผู้อื่น และภาพนั้นเป็นภาพที่เกิดจากการสร้างขึ้น ดัดต่อเติมหรือดัดแปลงด้วยวิธีการทางอิเล็กทรอนิกส์หรือวิธีการอื่นใด ทั้งนี้โดยประการที่น่าจะทำให้ผู้อื่นนั้นเสียชื่อเสียง ถูกดูหมิ่น ถูกเกลียดชังหรือได้รับความอับอาย

(7) เผยแพร่หรือส่งต่อซึ่งข้อมูลคอมพิวเตอร์โดยรู้อยู่แล้วว่าเป็นข้อมูลคอมพิวเตอร์ตาม (1) (2) (3) (4) (5) หรือ (6)

ข้อ 55 ผู้ใช้งานจะต้องไม่สนับสนุนหรือยินยอมให้มีการกระทำความผิดตาม ข้อ 54 ในระบบคอมพิวเตอร์ที่อยู่ในความควบคุมของตน

ข้อ 56 ผู้ใช้งานจะต้องไม่กระทำการดังต่อไปนี้

(1) เข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะ และมาตรการนั้นมิได้มีไว้สำหรับตน

(2) นำมาตรการป้องกันการเข้าถึงระบบคอมพิวเตอร์ที่ผู้อื่นจัดทำขึ้นเป็นการเฉพาะไปเปิดเผย โดยมิชอบในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่น

(3) กระทำด้วยประการใดโดยมิชอบด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อดักรับไว้ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ และข้อมูลคอมพิวเตอร์นั้นมิได้มีไว้เพื่อประโยชน์สาธารณะหรือเพื่อให้บุคคลทั่วไปใช้ประโยชน์ได้

(4) ทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

(5) กระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

(6) ส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์ (e-mail) แก่บุคคลอื่นโดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่งข้อมูลดังกล่าว อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

(7) กระทำโดยประการที่น่าจะเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศ หรือการบริการสาธารณะ หรือเป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่มีไว้เพื่อประโยชน์สาธารณะ

(8) จำหน่ายหรือเผยแพร่โปรแกรมที่จัดทำขึ้นโดยเฉพาะเพื่อนำไปใช้เป็นเครื่องมือในการกระทำความผิดตาม (1) (2) (3) (4) (5) (6) หรือ (7)

(9) ห้ามผู้ใช้งานติดตั้งโปรแกรมคอมพิวเตอร์ หรือซอฟต์แวร์ใดๆ เพิ่มเติมนอกเหนือจากที่ผู้ดูแลระบบได้กำหนดสิทธิการใช้งานมาให้ในเครื่องคอมพิวเตอร์ส่วนบุคคล ยกเว้นที่เป็นการอัพเดตของโปรแกรมที่ติดตั้งไว้ หากมีความจำเป็นต้องต่อผู้ดูแลระบบเป็นการชั่วคราว

(10) ห้ามติดตั้งซอฟต์แวร์ละเมิดลิขสิทธิ์ในเครื่องคอมพิวเตอร์ของสถาบัน การละเมิดลิขสิทธิ์ซอฟต์แวร์หากมีการตรวจพบและมีการดำเนินคดี ถือเป็นความผิดทางวินัย และเป็นความผิดตามกฎหมายของผู้ใช้งานโดยตรง

ข้อ 57 การใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่าย ผู้ใช้งานต้องปฏิบัติดังต่อไปนี้

(1) ใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบันอย่างมีประสิทธิภาพและเกิดประโยชน์สูงสุดแก่ทางราชการ

(2) ไม่ติดตั้งโปรแกรมต่างๆ ที่สถาบันไม่ได้ซื้อลิขสิทธิ์มาอย่างถูกต้องตามกฎหมายนำไปติดตั้งบนเครื่องคอมพิวเตอร์ส่วนตัว หรือแก้ไข หรือนำไปให้ผู้อื่นใช้งานโดยผิดกฎหมาย

(3) การตั้งชื่อเครื่องคอมพิวเตอร์ (Computer Name) ของสถาบัน จะต้องตั้งตามรูปแบบที่กำหนดโดยผู้ดูแลระบบเท่านั้น

(4) ไม่ทำการปรับแต่งไบออส (BIOS) หรือการตั้งค่าระบบ (Configuration) อื่นใดที่อาจส่งผลกระทบต่อระบบการทำงานของคอมพิวเตอร์ อันเป็นเหตุให้ไม่สามารถเปิดเครื่องใช้งานได้เป็นปกติ

(5) ไม่ทำการเปลี่ยนแปลงแก้ไขหมายเลขที่อยู่ไอพี (IP Address) ของเครื่องคอมพิวเตอร์แบบตั้งโต๊ะภายในสถาบัน

(6) หากผู้ใช้งานที่มีความประสงค์จะขอใช้งานที่อยู่ไอพีสาธารณะ (Public IP Address) จะต้องทำหนังสือขออนุญาตเป็นลายลักษณ์อักษรต่อผู้อำนวยการฝ่ายวิจัยและพัฒนา

(7) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์ที่สามารถใช้ในการตรวจสอบข้อมูลบนระบบเครือข่ายได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการฝ่ายวิจัยและพัฒนา

(8) ไม่ติดตั้งโปรแกรมคอมพิวเตอร์หรืออุปกรณ์คอมพิวเตอร์อื่นใดเพิ่มเติมในเครื่องคอมพิวเตอร์ และเครื่องคอมพิวเตอร์แม่ข่าย (Server) ของสถาบัน เพื่อให้บุคคลอื่นสามารถใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบันได้ เว้นแต่จะได้รับอนุญาตจากผู้อำนวยการฝ่ายวิจัยและพัฒนา

(9) ไม่ใช้บริการบนระบบอินเทอร์เน็ต (Internet) ที่มีการควบคุมปริมาณแบนด์วิดท์ (Bandwidth) จำนวนมากหรือเป็นเวลานานในระหว่างเวลาทำงานโดยเด็ดขาด ยกเว้นเป็นงานส่วนที่ได้รับการอนุมัติจากผู้บังคับบัญชา

(10) ห้ามผู้ใช้งานติดตั้งหรือรื้อถอนฮาร์ดแวร์หรือซอฟต์แวร์ใดๆ ที่เกี่ยวข้องกับการให้บริการระบบเครือข่าย เช่น อุปกรณ์ Router อุปกรณ์ Switch อุปกรณ์ Hub อุปกรณ์ Wireless Access Point เป็นต้น

ในกรณีที่ติดตั้งเพื่อวัตถุประสงค์ในการดำเนินงานตามหน้าที่ ผู้ที่ประสงค์จะติดตั้งต้องขออนุมัติจากผู้ดูแลระบบ เพื่อพิจารณาว่าการดำเนินการดังกล่าวส่งผลกระทบต่อการให้บริการของสถาบันหรือไม่

ส่วนที่ 3
แนวปฏิบัติการใช้ชื่อผู้ใช้และรหัสผ่าน

ข้อ 58 ผู้ใช้งานที่เป็นเจ้าของชื่อผู้ใช้ต้องเป็นผู้รับผิดชอบในผลต่างๆ อันอาจเกิดขึ้นจากการใช้ชื่อผู้ใช้นั้น เว้นแต่จะพิสูจน์ได้ว่าผลเสียหายนั้นเกิดจากการกระทำของผู้อื่น

ข้อ 59 ผู้ใช้งานจะต้องเก็บรักษาชื่อผู้ใช้ไว้เป็นความลับและห้ามเปิดเผยต่อบุคคลอื่น ห้ามโอน จำหน่าย หรือจ่ายแจกให้ผู้อื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ข้อ 60 ผู้ใช้งานจะต้องลงชื่อเข้าใช้งานด้วยชื่อผู้ใช้ของตนเอง และทำการลงชื่อออกทุกครั้ง เมื่อสิ้นสุดการใช้งานหรือหยุดการใช้งานชั่วคราว

ข้อ 61 รหัสผ่านต้องมีความยาวไม่น้อยกว่า 8 ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ

ข้อ 62 ไม่กำหนดรหัสผ่านจากชื่อ หรือชื่อสกุลของผู้ใช้งาน ชื่อบุคคลในครอบครัวบุคคลที่มีความสัมพันธ์กับตนหรือคำศัพท์ที่ใช้ในพจนานุกรม หรือจากหมายเลขโทรศัพท์ทำการเปลี่ยนรหัสผ่านเพื่อใช้งานเครื่องคอมพิวเตอร์ของตนทุก 3 เดือน หรือเปลี่ยนรหัสผ่านทุกครั้งที่มีสัญญาณบอกเหตุว่าอาจรั่วไหล

ข้อ 63 ผู้ใช้งานจะต้องเก็บรักษารหัสผ่าน สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มา โดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

ส่วนที่ 4
แนวปฏิบัติการป้องกันจากโปรแกรมประสงค์ร้าย (Malware)

ข้อ 64 ผู้ดูแลระบบต้องติดตั้งโปรแกรมกำจัดโปรแกรมประสงค์ร้ายทั้งในเครื่องคอมพิวเตอร์ทั้งโดย คอมพิวเตอร์พกพาของสำนักงาน รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ 65 ผู้ใช้งานควรทำการอัพเดท ระบบปฏิบัติการ เว็บบราวเซอร์ และโปรแกรมการใช้งานต่างๆ อย่างสม่ำเสมอเพื่อปิดช่องโหว่ (Vulnerability) ที่เกิดขึ้นจากซอฟต์แวร์ เป็นการป้องกันการโจมตีจากภัยคุกคามต่างๆ

ข้อ 66 ห้ามมิให้ผู้ใช้งานทำการปิดหรือยกเลิกหรือเปลี่ยนระบบการป้องกันโปรแกรมประสงค์ร้ายที่ติดตั้งอยู่บนเครื่องคอมพิวเตอร์โดยมิได้รับอนุญาตจากผู้ดูแลระบบ

ข้อ 67 หากผู้ใช้งานพบหรือสงสัยว่าเครื่องคอมพิวเตอร์ติดโปรแกรมประสงค์ร้าย ห้ามมิให้ผู้ใช้งานเชื่อมต่อเครื่องคอมพิวเตอร์เข้ากับระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของโปรแกรมประสงค์ร้ายไปยังเครื่องคอมพิวเตอร์อื่นๆ และรีบแจ้งผู้ดูแลระบบเพื่อดำเนินการตรวจสอบและแก้ไขปัญหาทันที

ข้อ 68 ก่อนการใช้งานสื่อบันทึกพกพา ควรมีการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้าย

ข้อ 69 ในการรับส่งข้อมูลคอมพิวเตอร์หรือการสนทนาผ่านทางระบบเครือข่าย ผู้ใช้งานต้องทำการตรวจสอบ เพื่อป้องกันและกำจัดโปรแกรมประสงค์ร้ายก่อนการรับส่งทุกครั้ง

ข้อ 70 ผู้ใช้งานควรทำการตรวจสอบไฟล์ก่อนทำการเปิด โดยใช้โปรแกรมป้องกันโปรแกรมประสงค์ร้าย เป็นการป้องกันในการเปิดไฟล์ที่สามารถประมวลผลได้ (Executable File) เช่น .exe .com .bat .vbs .scr .pif .hta .txt.exe .doc.exe xls.exe เป็นต้น

ส่วนที่ 5
แนวปฏิบัติการใช้งานระบบอินเทอร์เน็ต (Internet)

ข้อ 71 ผู้ใช้งานต้องเชื่อมต่อระบบคอมพิวเตอร์เพื่อการเข้าใช้งานระบบอินเทอร์เน็ต (Internet) ผ่านระบบรักษาความปลอดภัยที่สถาบันจัดสรรไว้เท่านั้น (Firewall Authentication) โดยใช้ชื่อผู้ใช้และรหัสผ่านที่ได้รับจากการลงทะเบียนตามข้อ 16 (1)

ข้อ 72 ผู้ใช้งานต้องเข้าถึงแหล่งข้อมูลและบริการตามสิทธิที่ได้รับตามหน้าที่ความรับผิดชอบเพื่อประสิทธิภาพของระบบเครือข่ายและความปลอดภัยทางข้อมูลของสถาบัน และต้องไม่ใช้ระบบอินเทอร์เน็ต (Internet) ของสถาบัน เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหายั่วยุกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อรัฐ ต่อศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อความเสียหายให้กับสถาบัน เป็นต้น

(1) ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ผู้ดูแลระบบอนุญาตให้เข้าถึงเท่านั้น

(2) ผู้ใช้งานที่ต้องการใช้บริการนอกเหนือจากที่ผู้ดูแลระบบกำหนดไว้ ให้ติดต่อผู้ดูแลระบบเพื่อพิจารณาเป็นกรณี

(3) การใช้งานอินเทอร์เน็ตในทางที่ผิดอาจถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมายทั้งทางแพ่งและอาญา

ข้อ 73 ห้ามผู้ใช้งานเปิดเผยข้อมูลสำคัญที่เป็นความลับเกี่ยวกับงานของสถาบัน ที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านระบบอินเทอร์เน็ต

ข้อ 74 ผู้ใช้งานต้องระมัดระวังการดาวน์โหลดโปรแกรมใช้งานจากระบบอินเทอร์เน็ต ซึ่งรวมถึงการดาวน์โหลดการอัพเดท (Update) โปรแกรมต่างๆ ต้องเป็นไปโดยไม่ละเมิดลิขสิทธิ์หรือทรัพย์สินทางปัญญา

ข้อ 75 หากประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ของผู้ใช้งานลดลงหลังจาก การเข้าสู่เว็บไซต์ใดๆ ผู้ใช้งานต้องรีบแจ้งผู้ดูแลระบบทราบทันทีเพื่อดำเนินการตรวจสอบและแก้ไข

ข้อ 76 ในการใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่แสดงความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่ทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของสถาบัน หรือเป็นการทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

ข้อ 77 หลังจากใช้งานระบบอินเทอร์เน็ตเสร็จสิ้น ให้ผู้ใช้งานทำการปิดเว็บเบราเซอร์เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่นๆ

ส่วนที่ 6
แนวปฏิบัติการใช้งานและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (e-mail)

ข้อ 78 แนวปฏิบัติการใช้งานสำหรับผู้ใช้งาน

(1) ผู้ใช้งานที่ต้องการขอลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ของสถาบัน ยื่นคำขอกับเจ้าหน้าที่เพื่อดำเนินการกำหนดสิทธิบัญชีผู้ใช้งานรายใหม่และรหัสผ่าน

(2) ผู้ใช้งานที่ได้รับรหัสผ่านครั้งแรกในการผ่านเข้าระบบจดหมายอิเล็กทรอนิกส์และเมื่อมีการเข้าสู่ระบบในครั้งแรกนั้นจะต้องเปลี่ยนรหัสผ่านโดยทันที

(3) ผู้ใช้งานไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ในรูปแบบ ที่ไม่ได้ป้องกันการเข้าถึง

(4) ผู้ใช้งานควรมีการเปลี่ยนรหัสผ่านทุก 3-6 เดือน

(5) ผู้ใช้งานไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (e-mail address) ของผู้อื่นเพื่ออ่าน รับส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าและให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์ เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ ในจดหมายอิเล็กทรอนิกส์ของตน

(6) หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้นผู้ใช้งานควรทำการลงบันทึกออกทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

(7) ในกรณีที่ต้องการส่งข้อมูลที่เป็นความลับ ผู้ใช้งานไม่ควรระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

(8) ผู้ใช้งานมีหน้าที่จะต้องรักษาชื่อผู้ใช้และรหัสผ่าน เป็นความลับไม่ให้รั่วไหลไปยังบุคคลที่ไม่เกี่ยวข้อง

(9) ผู้ใช้งานมีหน้าที่ต้องบริหารจัดการกล่องรับจดหมายอิเล็กทรอนิกส์ (Mailbox) ของตนเองที่สถาบันจัดสรรให้ เพื่อให้สามารถรับ-ส่ง ใช้งานได้ตามปกติอยู่เสมอ และพึงตระหนักว่ามีพื้นที่ให้บริการกล่องรับจดหมายอิเล็กทรอนิกส์มีขนาดจำกัดและเครื่องบริการ (Server) จะไม่สามารถรับ-ส่งจดหมายอิเล็กทรอนิกส์ได้หากจดหมายอิเล็กทรอนิกส์ทั้งหมดมีขนาดเกินจากที่กำหนดไว้

(10) ผู้ใช้งานต้องบริหารจัดการขนาดของจดหมายอิเล็กทรอนิกส์แต่ละฉบับของตนเพื่อให้สามารถรับ-ส่งจดหมายอิเล็กทรอนิกส์ได้ตามปกติ

(11) ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่คนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีโปรแกรมประสงค์ร้าย ให้ดูการดำเนินการตามข้อ 71 และหากโปรแกรมป้องกันมีการแจ้งเตือนผู้ใช้งานต้องระงับการใช้งานและรีบแจ้งผู้ดูแลระบบทันทีเพื่อดำเนินการตรวจสอบและแก้ไข

ข้อ 79 แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

(1) ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานใช้รหัสผ่านในการเข้าถึงบัญชีจดหมายอิเล็กทรอนิกส์ และกำหนดให้การติดต่อระหว่างผู้ใช้งานกับเครื่องบริการจดหมายอิเล็กทรอนิกส์ผ่านช่องทางการสื่อสารที่มีความปลอดภัย ด้วยเทคโนโลยีเข้ารหัส เช่น SSL หรือ TSL เป็นอย่างน้อย เพื่อป้องกันการถูกล่วงละเมิดการดักและดักจับรหัสผ่านไปใช้ในทางที่ผิด

(2) ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์ (e-mail) ของแต่ละบัญชีให้เหมาะสมกับการเข้าใช้บริการของผู้ใช้ระบบและหน้าที่ความรับผิดชอบของผู้ใช้งานรวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การโอนย้าย เป็นต้น

(3) ผู้ดูแลระบบควรกำหนดจำนวนครั้งที่ยอมให้ผู้ใช้งานใส่รหัสผ่านผิดพลาดได้ไม่เกิน 3 ครั้ง

(4) สงวนสิทธิในการเข้าถึงและตรวจสอบจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า การตรวจสอบจะดำเนินการเมื่อมีความจำเป็นเท่านั้น และผู้ดำเนินการจะไม่เปิดเผยข้อมูลใดของผู้ใช้งานที่ได้รับจากการตรวจสอบ เว้นแต่เป็นการเปิดเผยตามคำสั่งศาล ตามบทบัญญัติของกฎหมาย หรือความยินยอมจากผู้ใช้งานเท่านั้น

ส่วนที่ 7

การใช้สื่อสังคมออนไลน์

ข้อ 80 ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ที่สถาบันจัดให้ในการลงทะเบียนหรือประกาศข้อมูลใดๆ ในสื่อสังคมออนไลน์ เช่น เว็บบอร์ด บล็อก และกรุ๊ปสนทนาข่าว เป็นต้น เว้นแต่การลงทะเบียนหรือประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายจากสถาบัน

ข้อ 81 ผู้ใช้งานที่ต้องสื่อสารกับบุคคลภายนอกในการปฏิบัติงานของสถาบันผ่านสื่อสังคมออนไลน์ เช่น twitter, facebook ให้ใช้แนวปฏิบัติดังนี้

(1) การนำเสนอข่าวสารของสถาบัน โดยการใช้สื่อสังคมออนไลน์ ควรมีหลักในการอ้างอิงถึงสถาบัน ด้วยชื่อ รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงความเป็นสถาบัน หรือตัวแทนจากการ

ถึงที่ยืนยันสถานะและความมีตัวตนของสถาบัน

(2) การนำเสนอข้อมูลข่าวสารของสถาบัน ต้องไม่เป็นการสร้างความแตกแยกทางความคิดระหว่างคนในสังคม และไม่ยุยงให้เกิดความรุนแรงจนนำไปสู่ความขัดแย้งหรือเสื่อมเสียในสังคม

(3) ผู้ใช้งานต้องใช้ความระมัดระวังในการเผยแพร่ข้อมูลข่าวสาร โดยไม่ละเมิดลิขสิทธิ์ของข้อมูล ข่าวสาร ภาพ หรืออื่นๆ ที่ผลิตโดยบุคคลอื่น

(4) การคัดลอกข้อความใดๆ จากเรื่องสังคมออนไลน์ ควรทำต่อเมื่อได้รับอนุญาตจากเจ้าของข้อความนั้นๆ ในกรณีที่จำเป็นต้องคัดลอกข้อความจากเรื่องสังคมออนไลน์เพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสาร ผู้ใช้งานต้องอ้างอิงแหล่งที่มาของข้อความและข่าวสารเหล่านั้น โดยรับรู้ถึงสิทธิหรือลิขสิทธิ์ของบุคคล หรือองค์กรผู้เป็นเจ้าของข้อมูลดังกล่าวเสมอ

(5) ผู้ใช้งานใช้ความระมัดระวังในการนำเสนอข้อมูลข่าวสารของสำนักงาน โดยเน้นหลักความถูกต้องและใช้ภาษาที่เหมาะสม หลีกเลี่ยงการแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของสถาบัน ในลักษณะที่อาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

ข้อ 82 ผู้ใช้งานควรหลีกเลี่ยงการใช้งานสื่อสังคมออนไลน์ผ่านทางระบบสารสนเทศของสถาบัน เพื่อไม่ให้สถาบันตกอยู่ในความเสี่ยงเกินความจำเป็น

หมวด 8

นโยบายในการจัดการระบบสารสนเทศของสถาบัน (ผู้ดูแลระบบ)

ส่วนที่ 1

วัตถุประสงค์

ข้อ 83 เพื่อกำหนดหน้าที่และแนวปฏิบัติของผู้ดูแลระบบในการบริหารจัดการ กำกับ ดูแลเครื่องคอมพิวเตอร์และระบบเครือข่ายให้สามารถใช้งานได้ดีอยู่เสมอ รวมทั้งการสอดส่องดูแลการใช้งานของผู้ใช้งานให้เป็นไปตามแนวนโยบาย

ส่วนที่ 2

แนวปฏิบัติของผู้ดูแลระบบ (System Administrator)

ข้อ 84 ผู้ดูแลระบบมีหน้าที่ ดังต่อไปนี้

(1) ตรวจสอบดูแลรักษาการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายของสถาบันให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายให้รีบดำเนินการแก้ไขรวมทั้งป้องกันและบรรเทาความเสียหายที่อาจจะเกิดขึ้นในทันที ในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานที่ไม่เป็นไปตามนโยบายนี้ ให้รีบแจ้งผู้ใช้งานนั้นให้ยุติการกระทำดังกล่าวในทันที และในกรณีจำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่สถาบัน ให้ผู้ดูแลระบบมีอำนาจสั่งระงับการใช้ระบบเครือข่ายของผู้ใช้งานดังกล่าวได้ทันที

(2) ติดตั้งและปรับปรุงโปรแกรมคอมพิวเตอร์สำหรับแก้ไขข้อบกพร่องของเครื่องคอมพิวเตอร์และระบบเครือข่าย ให้มีความมั่นคงปลอดภัยในการใช้งานและพร้อมใช้งานอยู่เสมอ

(3) ตรวจสอบความมั่นคงปลอดภัยในการใช้งานเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

(4) ดูแลรักษาและตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นต้องใช้งานในทันที

(5) ดูแลรักษาและปรับปรุงบัญชีจดหมายอิเล็กทรอนิกส์ (e-mail) ให้ถูกต้องและเป็นปัจจุบันอยู่เสมอ โดยให้ยกเลิกสิทธิการใช้งานของผู้ใช้งานที่พ้นสภาพการเป็นผู้ใช้งาน

(6) ตรวจสอบเครื่องคอมพิวเตอร์ของผู้ใช้งานให้มีการกำหนดรหัสผ่าน รวมทั้งการเก็บรักษารหัสผ่าน

(7) ไม่ใช้อำนาจหน้าที่ของตนในการเข้าถึงข้อมูลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์โดยไม่มีเหตุผลอันสมควร

(8) ไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิหรือข้อมูลส่วนบุคคลของผู้ใช้งานที่ใช้งานระบบคอมพิวเตอร์หรือมีข้อมูลส่วนบุคคลจัดเก็บไว้ในระบบคอมพิวเตอร์ โดยไม่มีเหตุผลอันสมควร

(9) ไม่เปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่เปิดเผยให้บุคคลอื่นบุคคลใดทราบ โดยไม่มีเหตุผลอันสมควร

(10) ผู้ดูแลระบบมีหน้าที่ปรับปรุงนโยบายและข้อปฏิบัติให้มีความทันสมัยสอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยีและกฎหมาย โดยทำการปรับปรุงและสื่อสารต่อผู้ปฏิบัติงานอย่างน้อยปีละ 1 ครั้ง

(11) เมื่อผู้ดูแลระบบพ้นจากหน้าที่จะต้องคืนสินทรัพย์ของสถาบันที่เกี่ยวข้องกับการปฏิบัติหน้าที่ของตนในทันทีที่พ้นจากหน้าที่ และให้ผู้อำนวยการฝ่ายวิจัยและพัฒนา หรือผู้ที่ได้รับมอบหมายตรวจสอบการคืนสินทรัพย์

ข้อ 65 ผู้ดูแลระบบจะต้องเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) โดยจะต้องเก็บรักษาข้อมูลของผู้ใช้งานเท่าที่จำเป็นเพื่อให้สามารถระบุตัวผู้ใช้งานนับตั้งแต่เริ่มใช้บริการและต้องเก็บรักษาไว้เป็นเวลาไม่น้อยกว่าเก้าสิบวันนับตั้งแต่การใช้บริการสิ้นสุดลง การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ต้องใช้วิธีการที่มั่นคงปลอดภัย ดังต่อไปนี้

(1) เก็บในสื่อเก็บข้อมูลที่สามารถรักษาความครบถ้วนถูกต้องแท้จริง และระบุตัวบุคคลที่เข้าถึงสื่อดังกล่าวได้

(2) มีระบบการเก็บรักษาความลับของข้อมูลที่จัดเก็บ และกำหนดชั้นความลับในการเข้าถึงข้อมูลดังกล่าว เพื่อรักษาความน่าเชื่อถือของข้อมูล และไม่ให้ผู้ดูแลระบบสามารถแก้ไขข้อมูลที่เก็บรักษาไว้ เว้นแต่ ผู้ที่กำหนดให้สามารถเข้าถึงข้อมูลดังกล่าวได้ เช่น ผู้ตรวจสอบระบบสารสนเทศของสถาบัน (IT Auditor) หรือบุคคลที่สถาบันมอบหมาย

(3) ในการเก็บข้อมูลจราจรนั้น ต้องสามารถระบุรายละเอียดผู้ใช้งานเป็นรายบุคคลได้

(4) เพื่อให้ข้อมูลจราจรมีความถูกต้องและนำมาใช้ประโยชน์ได้จริงผู้ให้บริการต้องตั้งนาฬิกาของอุปกรณ์บริการทุกชนิดให้ตรงกับเวลาอ้างอิงสากล (Stratum 0) โดยมีคลาดไม่เกิน 10 มิลลิวินาที

หมวด 9

นโยบายการจัดการระบบสำรองและการเตรียมความพร้อมกรณีฉุกเฉิน

ส่วนที่ 1

วัตถุประสงค์

ข้อ 86 เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลักที่ทำหน้าที่เชื่อมโยงระบบเครือข่าย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

ส่วนที่ 2

แนวปฏิบัติการสำรองข้อมูลและการเตรียมความพร้อมกรณีฉุกเฉิน

ข้อ 87 กำหนดแผนการจัดทำสำเนาข้อมูลและซอฟต์แวร์เก็บไว้ โดยจัดเรียงตามลำดับความจำเป็นของการสำรองข้อมูลระบบสารสนเทศของสถาบันจากจำเป็นมากไปหาน้อย และให้มีการทบทวนรายการลำดับความสำคัญแต่ละรายการอย่างน้อยปีละ 1 ครั้ง

ข้อ 88 มีขั้นตอนการปฏิบัติการจัดทำสำรองข้อมูลและการกู้คืนข้อมูลอย่างถูกต้อง ทั้งระบบซอฟต์แวร์และข้อมูลในระบบสารสนเทศ โดยขั้นตอนปฏิบัติแยกตามระบบสารสนเทศแต่ละระบบ

ทั้งนี้การคัดเลือกระบบสำคัญที่ต้องมีการจัดทำระบบสำรองเป็นดุลยพินิจของผู้อำนวยการฝ่ายวิจัยและพัฒนา โดยพิจารณาจากความสำคัญในการให้บริการและความสามารถในการดำเนินงานภายใน

ข้อ 89 จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูลและผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน ข้อมูลที่สำรองควรจัดเก็บไว้ในสถานที่เก็บข้อมูลสำรองซึ่งตั้งอยู่ที่สถานที่อื่น และต้องมีการทดสอบสื่อเก็บข้อมูลสำรองอย่างสม่ำเสมอ

ข้อ 90 ต้องมีการจัดทำแผนเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉินเพื่อให้สามารถปฏิบัติงานต่อภายในระยะเวลาที่เหมาะสม

ข้อ 91 สำหรับระบบที่มีความสำคัญในการให้บริการของสถาบันต้องจัดทำระบบสำรอง เพื่อเตรียมความพร้อมกรณีฉุกเฉินไม่สามารถใช้ระบบหลักได้

สำหรับรายละเอียดของการสำรองข้อมูล รายการระบบสำคัญที่มีการจัดทำระบบสำรอง ขั้นตอนการปฏิบัติในการะฉุกเฉิน ดูเอกสารแนบท้ายประกาศ

หมวด 10

นโยบายการจัดการประเมินความเสี่ยง

ส่วนที่ 1

วัตถุประสงค์

ข้อ 92 เพื่อให้มีมาตรการในการควบคุมความเสี่ยงและป้องกันผลกระทบที่อาจมีต่อความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งให้สามารถกำหนดวิธีการประเมินความเสี่ยงได้อย่างถูกต้อง ส่งผลให้ระบุความเสี่ยงได้อย่างชัดเจน และสามารถควบคุมความเสี่ยงได้อย่างมีประสิทธิภาพ

ส่วนที่ 2

แนวปฏิบัติการประเมินความเสี่ยง

ข้อ 93 ระบุความเสี่ยงและผลกระทบของความเสี่ยงให้สอดคล้องตามแผนบริหารความเสี่ยงของหน่วยงานเพื่อการประเมินความเสี่ยงนั้น ดังต่อไปนี้

(1) ความเสี่ยงที่เกิดจากการลอบเข้าทางระบบปฏิบัติการเพื่อยึดครองเครื่องคอมพิวเตอร์แม่ข่ายผ่านระบบอินเทอร์เน็ต

(2) ความเสี่ยงที่เกิดจากการลักลอบเข้าเชื่อมโยงกับระบบเครือข่ายไร้สายโดยไม่ได้รับอนุญาต

(3) ความเสี่ยงที่เกิดจากเครื่องมือด้านเทคโนโลยีสารสนเทศ หรือระบบเครือข่ายเกิดการขัดข้องระหว่างการใช้งาน

(4) ความเสี่ยงที่เกิดจากการลงบันทึกเข้าใช้สารสนเทศที่สำคัญผ่านระบบเครือข่ายของผู้ใช้งานคนเดียวกันมากกว่าหนึ่งจุด

(5) ความเสี่ยงที่เกิดจากการลักลอบใช้รหัสผ่านของผู้อื่นโดยไม่ได้รับอนุญาต

ข้อ 94 กำหนดวิธีการในการประเมินความเสี่ยงและความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงนั้น

ข้อ 95 การประเมินความเสี่ยงให้คำนึงถึงองค์ประกอบดังต่อไปนี้

(1) ความรุนแรงของผลกระทบที่เกิดจากความเสี่ยงที่ระบุ

(2) ภัยคุกคามหรือสิ่งที่อาจก่อให้เกิดเหตุการณ์ที่ระบุรวมถึงความเป็นไปได้ที่จะเกิดขึ้น

(3) จุดอ่อนหรือช่องโหว่ที่อาจถูกใช้ในการก่อให้เกิดเหตุการณ์ที่ระบุ

ข้อ 96 ผลการประเมินภาพรวมของความเสี่ยงที่ระบุ ต้องจัดทำเป็นคะแนนโดยมีคะแนนเต็มเป็น 100 คะแนน และกำหนดให้มีเกณฑ์ในการพิจารณาว่า ความเสี่ยงที่ระบุนั้นต้องมีการบริหารจัดการลดความเสี่ยงนั้นหรือไม่ โดยให้มีเกณฑ์เป็น 80 คะแนนขึ้นไป กำหนดให้ทำการประเมินความเสี่ยงอย่างน้อยปีละ 1 ครั้ง โดยแต่งตั้งให้ผู้ตรวจสอบภายในเป็นผู้รับผิดชอบการดำเนินการประเมินความเสี่ยง

หมวด 11

[illegible]

ส่วนที่ 1

วัตถุประสงค์

ข้อ ๘๘ [illegible]

ส่วนที่ 2

[illegible]

ข้อ ๘๙ [illegible]

ข้อ ๙๐ [illegible]

ข้อ ๙๑ [illegible]

ประกาศ ณ วันที่ 1 [illegible] 2558

[illegible]

ผู้อำนวยการ

[illegible] (องค์การมหาชน)