องค์การคลังสินค้า

ประกาศองค์การคลังสินค้า
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การคลังสินค้า

.....

๑. หลักการและเหตุผล

ตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ ในมาตรา ๕ "หน่วยงานของรัฐต้องจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือ โดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้" และตามประกาศคณะกรรมการธรกรรม ทางอิเล็กทรอนิกส์ เรื่องนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเป็นลายลักษณ์อักษร นั้น

เพื่อให้ระบบสารสนเทศขององค์การคลังสินค้า หรือต่อไปนี้เรียกว่า "อคส." เป็นไปอย่างเหมาะสม มีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่างๆ อคส. จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับพระราชกฤษฎีกาฯ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ฯ

๒. วัตถุประสงค์

๒.๑ เพื่อให้ผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กรตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๒.๒ เพื่อใช้เป็นแนวทางในการจัดทำแนวปฏิบัติของผู้บริหาร เจ้าหน้าที่ ผู้ดูแลระบบ และบุคคลภายนอกที่ปฏิบัติงานให้กับองค์กร

๒.๓ เพื่อให้ผู้ใช้งานเกิดความเชื่อมั่น และมีความมั่นคงปลอดภัยในการใช้งานระบบสารสนเทศขององค์กร

๒.๔ เพื่อให้การบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศขององค์กรมีประสิทธิภาพ

๓. องค์ประกอบของนโยบาย

๓.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์ และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์ขององค์การคลังสินค้า

(๓) กำหนดผู้รับผิดชอบตามแนวนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายอย่างน้อยปีละ ๑ ครั้ง

๓.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

มีนโยบายที่จะให้บริการเทคโนโลยีสารสนเทศแก่ผู้ใช้งาน และประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานและประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวก และรวดเร็วรวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย ดังนี้

๑.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบ สารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๑.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบ ทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผล

๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๑.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๑.๕ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่น และสารสนเทศ (application and information access control) โดยต้องมีการควบคุมการจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือ ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

๑.๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) การควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

(๒) มีระบบสารสนเทศและระบบสำรองของสารสนเทศ

มีนโยบายในการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองระบบสารสนเทศ และระบบคอมพิวเตอร์ที่สมบูรณ์พร้อมใช้งานรวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

มีนโยบายในการตรวจสอบและประเมินความเสี่ยง รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศและระบบคอมพิวเตอร์

มีนโยบายในการสร้างความรู้ความเข้าใจโดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศและระบบคอมพิวเตอร์ให้แก่ผู้ใช้งานทั้งภายในและภายนอก

๔. ข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามที่กำหนดในเอกสารแนบท้ายประกาศองค์การคลังสินค้า เรื่อง"นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การคลังสินค้า"

๕. อำนาจหน้าที่

ต้องกำหนดความรับผิดชอบที่ชัดเจนกรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่หน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่องละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยกำหนดให้ผู้บริหารระดับสูงสุดขององค์การคลังสินค้า (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น โดยให้สำนักเทคโนโลยีสารสนเทศ องค์การคลังสินค้าเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง เมื่อนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศมีการเปลี่ยนแปลงให้ประกาศใหม่ โดยให้เจ้าหน้าที่อคส. และหน่วยงานภายนอกทราบและถือปฏิบัติอย่างเคร่งครัดต่อไป

ประกาศฉบับนี้มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๑ มีนาคม พ.ศ. ๒๕๕๘

(นางสาวจีระวัฒน์ วัฒนฐานะ)
รองผู้อำนวยการ รักษาการแทน
ผู้อำนวยการองค์การคลังสินค้า

เอกสารแนบท้ายประกาศองค์การคลังสินค้า

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ องค์การคลังสินค้า

ส่วนที่ ๑

บทที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

๑.๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๑.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) เพื่อควบคุมการเข้าถึงระบบ สารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว และผ่านการฝึกอบรมหลักสูตรการสร้างความตระหนักเรื่องความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

(๒) การลงทะเบียนผู้ใช้งาน (user registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๓) การบริหารจัดการสิทธิของผู้ใช้งาน (user management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง

(๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (user password management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

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

๑.๑.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (user responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

(๑) การใช้งานรหัสผ่าน (password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

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

(๓) การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์ บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

(๔) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

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

(๖) การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

(๗) การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

๑.๑.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

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

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

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

(๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

(๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๑.๑.๕ มีการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (application and information access control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

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

(๓) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

(๔) การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) ต้องกำหนดแนวปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

๑.๑.๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (access control) อย่างน้อยดังนี้

(๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งาน และ ความมั่นคงปลอดภัย

(๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจขององค์กร

(๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๒ นโยบายการจัดทำระบบสำรองของสารสนเทศ

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองและระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

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

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์การคลังสินค้า (internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (external auditor) เพื่อให้องค์การคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๔ นโยบายการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

(๑) องค์การคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ โดยเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ

(๒) จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับแนวปฏิบัติขององค์การคลังสินค้า

บทที่ ๒ คำนิยาม

ประกอบด้วย

"ผู้บริหารระดับสูงสุด" (CEO) หมายถึง ผู้อำนวยการองค์การคลังสินค้า ทำหน้าที่รับผิดชอบความเสี่ยง ความเสียหาย ตามประกาศคณะกรรมการฉบับที่ ๒

"ผู้บังคับบัญชา" หมายถึง ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ อคส.

"ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง" (CIO) หมายถึง ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของ อคส. ซึ่งมีบทบาทหน้าที่และความรับผิดชอบในส่วนของการกำหนดนโยบายมาตรฐานการควบคุมดูแลการใช้งานระบบสารสนเทศ

"สำนักเทคโนโลยีสารสนเทศ" หมายถึง หน่วยงานที่ให้บริการด้านเทคโนโลยีสารสนเทศ ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบงาน ระบบคอมพิวเตอร์และเครือข่ายภายใน อคส.

"ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ" หมายถึง ผู้บังคับบัญชาสูงสุดในการบริหารจัดการ และมีอำนาจตัดสินใจเกี่ยวกับระบบสารสนเทศภายใน อคส.

"การรักษาความมั่นคงปลอดภัย" หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของ อคส.

"แนวทางปฏิบัติ (Guideline)" หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

"ผู้ใช้งาน" หมายถึง บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role) ซึ่ง อคส.กำหนดไว้ดังนี้

"ผู้บริหาร" หมายถึง ผู้มีอำนาจบริหารในระดับสูงของ อคส. เช่น ผู้อำนวยการสำนัก/ส่วนงาน เป็นต้น

"ผู้ดูแลระบบ (System Administrator)" หมายถึง เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลระบบงาน ระบบฐานข้อมูล ระบบคอมพิวเตอร์และเครือข่ายคอมพิวเตอร์ซึ่งสามารถเข้าถึงโปรแกรมคอมพิวเตอร์หรือข้อมูลอื่นเพื่อการจัดการเครือข่ายคอมพิวเตอร์ได้ เช่น บัญชีผู้ใช้ระบบคอมพิวเตอร์ (User Account) หรือบัญชีไปรษณีย์อิเล็กทรอนิกส์ (Email Account) เป็นต้น

"เจ้าหน้าที่" หมายถึง พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างโครงการต่างๆ พนักงานจ้างเหมา ของ อคส.

"หน่วยงานภายนอก" หมายถึง องค์กรหรือหน่วยงานภายนอกที่ อคส. อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือทรัพย์สินต่างๆ ของ อคส. โดยจะได้รับสิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับข้อมูลของ อคส.

"ข้อมูล" หมายถึง สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือวิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"สารสนเทศ (Information)" หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และสามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

"ระบบคอมพิวเตอร์" หมายถึง อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ

"ระบบเครือข่าย(Network System)" หมายถึง ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและสารสนเทศระหว่างระบบสารสนเทศต่างๆ ขององค์กรได้

"แลน (Lan) และอินทราเน็ต (intranet)" หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายในหน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสารแลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

"อินเทอร์เน็ต (Internet)" หมายถึง ระบบเครือข่ายที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงานเข้ากับเครือข่ายคอมพิวเตอร์ทั่วโลก

"ระบบสารสนเทศ (Information System)" หมายถึง ระบบงานของหน่วยงานที่นำเอาระบบคอมพิวเตอร์และระบบการสื่อสารมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการดำเนินการต่างๆ ของหน่วยงาน

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบสารสนเทศโดยเจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของหน่วยงาน ตามที่กำหนดในภารกิจของผู้ใช้งาน (User Role)

"สินทรัพย์" หมายถึง ข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน หรือบุคคลภายนอก เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)" หมายถึง กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายถึง สถานการณ์ ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

"จดหมายอิเล็กทรอนิกส์ (Email)" หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP

"ระบบจดหมายอิเล็กทรอนิกส์ของ อคส." หมายถึง ระบบจดหมายอิเล็กทรอนิกส์ของ สำนักงานปลัด กระทรวงพาณิชย์ หรือ กระทรวง ICT ซึ่งอนุญาตให้ผู้ใช้งาน ใช้เพื่อการดำเนินงานของ อคส.

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงและรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"ซอฟต์แวร์ประสงค์ร้าย (Malware)" หมายถึง ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อทำลาย หรือสร้างความเสียหายให้กับระบบสารสนเทศ การโจรกรรมข้อมูล หรือการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"ผู้บุกรุก " หมายถึง บุคคลที่เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"สำนักงานปลัดกระทรวงพาณิชย์ " หมายถึง ชื่อหน่วยงาน สำนักงานปลัด สังกัด กระทรวงพาณิชย์ ตั้งอยู่เลขที่ ๔๔/๑๐๐ ถนนนนทบุรี ๑ อำเภอเมือง จังหวัดนนทบุรี ๑๑๐๐๐

ส่วนที่ ๒
แนวปฏิบัติการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุก หรือจากซอฟต์แวร์ประสงค์ร้าย รวมทั้งกำหนดประเภทของข้อมูล ลำดับชั้นความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒.๕)

แนวปฏิบัติ

๒.๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติในการลงทะเบียนเจ้าหน้าที่ใหม่ การให้สิทธิต่างๆ ในการใช้งานตามความจำเป็น และการยกเลิกสิทธิการใช้งาน เช่น การลาออก หรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึง และใช้งานระบบสารสนเทศที่สำคัญ เช่น ซอฟต์แวร์ประยุกต์ จดหมายอิเล็กทรอนิกส์ เครือข่ายไร้สาย และอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงและใช้งานระบบสารสนเทศของบุคลากรดังต่อไปนี้

๒.๑.๓.๑ การลงทะเบียนของผู้ใช้งาน (User Registration) ให้ผู้ดูแลระบบงานหรือผู้ที่ได้รับมอบหมายจัดทำแบบฟอร์มสำหรับลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัว แรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/ หรือความต้องการทางธุรกิจ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออก จากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒.๑.๓.๒ การบริหารจัดการสิทธิของผู้ใช้งาน (user management) โดยแสดงรายละเอียดที่เกี่ยวกับการ ควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ใช้งานต้องลงทะเบียนผู้ใช้งานเพื่อนำข้อมูลไปตรวจสอบสิทธิก่อนการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความ รับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๑.๓.๓ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการเดา และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน โดย จัดส่งบัญชีและรหัสผ่านใส่ซองปิดผนึกและประทับตรา “ลับ” และแนบเอกสารอื่นๆ ที่เกี่ยวข้องกับการปฏิบัติงานของผู้ใช้งาน ส่งมอบให้ผู้ใช้งาน และให้ผู้ใช้งานลงนามรับเอกสารนั้น รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดยเคร่งครัด

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง

๒.๑.๓.๔ กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านเมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน

๒.๑.๓.๕ หลีกเลี่ยงการส่งรหัสผ่านให้ผู้ใช้งาน โดยใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการรักษาความปลอดภัย

๒.๑.๓.๖ ต้องกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๑.๓.๗ ต้องทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งาน (Review Of User Access Rights) อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

๒.๑.๓.๘ ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนดระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

๒.๒.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (password use) สำหรับผู้ใช้งาน เพื่อให้สามารถกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้

(๑) เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก

(๒) ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา

(๓) ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน

(๔) ต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม

(๕) ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์

(๖) เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ

(๗) ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่น หรือเก็บไว้ในระบบคอมพิวเตอร์

(๘) กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๒.๒.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

(๑) ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

(๒) ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้

(๓) มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต

(๔) มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว

(๕) สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน

๒.๒.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้

(๑) กำหนดวิธีป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่าง ๆ

- ใกล้สิ้นปีงบประมาณต้องสำรวจทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ว่ายังสามารถใช้งานได้หรือไม่ จำนวนครบหรือไม่ ถ้าเกิดกรณีชำรุด/เสียหาย จะทำเรื่องส่งซ่อม/ส่งคืนพัสดุ
- จัดห้องสำหรับรวบรวมเครื่องคอมพิวเตอร์และอุปกรณ์ที่จะส่งซ่อม/ส่งคืน และปิดล็อคห้องทุกครั้งหลังเข้า-ออก เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย
- การควบคุมการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ โดยการใช้การ์ดหรือสแกนนิ้วมือ ก่อนและหลังเข้าออกทุกครั้ง
- การจัดทำทะเบียนยืม-คืน อุปกรณ์คอมพิวเตอร์ โดยแบบฟอร์มขอใช้อุปกรณ์คอมพิวเตอร์ เพื่อใช้งานภายในและภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
- การจัดทำทะเบียนยืม-คืน โน้ตบุ๊ค โดยใช้แบบฟอร์มยืมโน้ตบุ๊ค เพื่อใช้งานภายในและภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย

- การวางอุปกรณ์ มีการจัดที่เฉพาะและเหมาะสมสำหรับวางเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ (Data Center)
- การจัดทำระบบเอกสารคุณภาพ (ISO ๙๐๐๑ : ๒๐๐๘) ใช้ในองค์กร

(๒) การนำเครื่องคอมพิวเตอร์ โน้ตบุ๊ค และอุปกรณ์ เข้า-ออก องค์การคลังสินค้าต้องได้รับการตรวจเช็คจากเจ้าหน้าที่ฝ่ายอาคาร อย่างเคร่งครัด

(๓) ต้องป้องกันการเข้าใช้งานเครื่องคอมพิวเตอร์ โดยใช้รหัสผู้ใช้งาน (username) รหัสผ่าน (password) เป็นการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และมีการตั้งค่าพักหน้าจออัตโนมัติ เมื่อไม่ได้ใช้งาน

(๔) การป้องกันการใช้ทรัพย์สินอย่างมีประสิทธิภาพและปลอดภัย ดังนี้
- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- Log out ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

(๕) การทำลายข้อมูลอิเล็กทรอนิกส์และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ดังนี้

(๕.๑) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลาย CD/DVD
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แม็ต (Format) ตามมาตรฐานการทำลายข้อมูลบนฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกาDOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

(๕.๒) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

(๑) จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับและป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว

(๒) การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล

(๓) ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับขององค์การคลังสินค้าไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น

(๔) ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน

(๕) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใช้รหัสผ่านที่มีความมั่นคงปลอดภัย

(๖) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายขององค์การคลังสินค้า เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)

(๗) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่

(๘) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามีการติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่

(๙) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

(๑๐) ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

๒.๒.๔ ผู้ใช้งานได้ใช้งานระบบงานสารบรรณอิเล็กทรอนิกส์ที่นำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

(๑) องค์การคลังสินค้ามีระบบงานสารบรรณอิเล็กทรอนิกส์สำหรับควบคุมการจัดเก็บและนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ดังนี้

(๑.๑) ลงทะเบียนผู้ใช้งานระบบสารบรรณอิเล็กทรอนิกส์ มีการกำหนดสิทธิ์การเข้าตามหน่วยงาน หรือตามผู้ใช้งาน

(๑.๒) เข้าสู่ระบบงานสารบรรณอิเล็กทรอนิกส์ โดยระบบจะทำการตรวจสอบสิทธิ์ของผู้ใช้งานก่อนเข้าสู่ระบบ

(๑.๓) กรณีผู้ใช้งานได้รับเอกสารลับ /ลับมาก /ลับที่สุด ให้นายทะเบียนลับ ลงรับเอกสาร โดยบันทึกข้อมูลและกำหนดชั้นความลับของเอกสารตามที่ปรากฏบนหน้าซอง พร้อมทั้งนำเลขทะเบียนรับที่ระบบออกให้ เขียนบนหน้าซอง ก่อนนำเสนอผู้มีอำนาจพิจารณาดำเนินการต่อไป

(๑.๔) เมื่อผู้ใช้งาน เช่น เลขานุการผู้บริหาร เจ้าหน้าที่สารบรรณ เป็นต้น กำหนดชั้นความลับของเอกสารแล้ว จะไม่สามารถดำเนินการใดๆ กับเรื่องดังกล่าวในระบบได้อีก ยกเว้นเป็นผู้ที่ได้รับสิทธิ์ ให้เข้าถึงเอกสารประเภท ลับ ลับมาก ลับที่สุด ได้เท่านั้น

(๑.๕) ต้องนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับของหน่วยงาน

๒.๓ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๓.๑ ตรวจสอบการใช้งานเครือข่าย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจพบสิ่งผิดปกติเกี่ยวกับการใช้งานเครือข่ายให้รีบดำเนินการแก้ไขรวมทั้งป้องกันและบรรเทาความเสียหาย ที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการใช้งานของผู้ใช้งานและให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและในกรณีที่จำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงาน ให้ผู้ดูแลระบบเครือข่ายพิจารณาระงับใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานดังกล่าวได้ทันที

๒.๓.๒ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๒.๓.๓ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๒.๓.๔ ห้ามผู้ใดกระทำการเคลื่อนย้ายติดตั้งเพิ่มเติมหรือทำการใด ๆ ต่ออุปกรณ์ส่วนกลาง ได้แก่ อุปกรณ์จัดเส้นทาง (Router) อุปกรณ์กระจายสัญญาณข้อมูล (Switch) อุปกรณ์ที่เชื่อมต่อกับระบบเครือข่ายหลัก โดยไม่ได้รับอนุญาตจากผู้ดูแลระบบ

๒.๓.๕ ระบบยืนยันตัวบุคคลต้องสามารถกำหนดสิทธิการใช้งานระบบสารสนเทศต่างๆ ผ่านเครือข่าย ตามบทบาทหน้าที่ของผู้ใช้ (user role) แต่ละคนได้

๒.๓.๖ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (user authentication for external connections) ให้มีการยืนยันตัวบุคคล (authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password)

๒.๓.๗ การระบุอุปกรณ์บนเครือข่าย (equipment identification in networks) เพื่อใช้สำหรับการยืนยันการเข้าถึง ดังนี้

(๑) กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลขไอพีแบบคงที่ (Static IP address) ให้จัดทำฐานข้อมูลเพื่อจัดเก็บหมายเลข MAC ของอุปกรณ์ดังกล่าว

(๒) กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลขไอพีแบบไดนามิค (Dynamic IP address) ให้จัดเก็บ Log ใน DHCP server โดยมีข้อมูลซึ่งอ้างอิงกับหมายเลขไอพีอย่างน้อยดังนี้

- หมายเลข MAC ของอุปกรณ์
- ชื่ออุปกรณ์ (Hostname)
- วัน เวลาในการเข้าใช้งาน

๒.๓.๘ ให้ทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (remote diagnostic and configuration port protection) ดังนี้

(๑) กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งไม่จำเป็นต้องใช้งาน ให้ปิดพอร์ตดังกล่าว

(๒) กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งมีการใช้งานบางช่วงเวลา ให้กำหนดระยะเวลาการเปิดใช้งานเท่าที่จำเป็นและต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร โดยต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล

(๓) กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งจำเป็นต้องใช้งานเป็นประจำ ต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล

(๔) สำหรับการป้องกันการเข้าถึงทางกายภาพ ให้ใช้แนวปฏิบัติในการควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์

๒.๓.๙ การแบ่งแยกเครือข่าย (segregation in networks) ให้จัดทำ VLAN โดยพิจารณาตามลักษณะการใช้งาน การรักษาความปลอดภัย และนโยบายของหน่วยงาน

(๑) องค์การคลังสินค้าได้มีการจัดแบ่งแยกเครือข่ายตามหน่วยงานระดับสำนักและตามหน้าที่เฉพาะ

(๒) กำหนดรหัสวงเครือข่าย (VLAN) ชื่อวงเครือข่าย IP Addresss และค่าอื่นๆ ที่ใช้ในการกำหนดในอุปกรณ์สวิทต์และอุปกรณ์ต่างๆที่เกี่ยวข้อง

(๓) มีการติดตั้งค่าอุปกรณ์ต่างๆ แล้วทำการทดสอบการใช้งานเครือข่ายแต่ละวง

(๔) จัดทำทะเบียนวงเครือข่ายและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง

(๕) ผู้ดูแลระบบทำการบำรุงรักษา ตรวจเช็คการใช้งานเครือข่าย(monitoring)

(๖) เมื่อมีการเปลี่ยนหน่วยงานจะมีการทบทวนและจัดการแบ่งแยกเครือข่ายตามโครงสร้างหน่วยงานใหม่

๒.๓.๑๐ การควบคุมการเชื่อมต่อทางเครือข่าย (network connection control) ให้ควบคุมการเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ดังนี้

(๑) ต้องตรวจสอบการเชื่อมต่อเครือข่ายของอุปกรณ์ต่างๆ ในศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) อย่างน้อยเดือนละ ๑ ครั้ง

(๒) ต้องติดตั้งอุปกรณ์ ไฟร์วอลล์ เพื่อควบคุมการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน

(๓) ต้องตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์ แม่ข่าย

๒.๓.๑๑ การควบคุมการจัดเส้นทางบนเครือข่าย (network routing control) ให้ทำการควบคุมการจัดเส้นทางบนเครือข่าย ดังนี้

(๑) ต้องกำหนดค่าโปรโตคอลสำหรับการหาเส้นทาง (routing protocol) ที่สอดคล้องกับเครือข่ายหลักที่หน่วยงานเชื่อมต่อ

(๒) ต้องบันทึกข้อมูลแผนผังการจัดเส้นทางบนเครือข่ายและข้อมูลการตั้งค่าอุปกรณ์หาเส้นทาง

(๓) เมื่อมีความจำเป็นต้องเปลี่ยนการหาเส้นทางบนเครือข่าย ให้ผู้ดูแลทำการปรับปรุงข้อมูลที่บันทึกไว้และแจ้งผู้บังคับบัญชาทราบ

(๔) กำหนดให้มีการแปลงหมายเลขเครือข่าย (NAT) เพื่อแยกเครือข่ายย่อย

๒.๓.๑๒ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๑) กำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้ใช้งานได้

(๒) กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) กำหนดการใช้งานระบบสารสนเทศที่สำคัญ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (wireless LAN) ระบบอินเทอร์เน็ต (internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง ซึ่งองค์การคลังสินค้ามีแบบฟอร์มการขอใช้บริการดังกล่าว โดยมีขั้นตอนการปฏิบัติดังนี้

- ผู้ใช้งานกรอกแบบฟอร์มขอใช้บริการ/แจ้งปัญหา และได้รับอนุมัติตามสายงานผู้แจ้ง และส่งแบบฟอร์มมายังหน่วยงานผู้ดูแลระบบแล้ว
- ผู้ดูแลระบบดำเนินการวิเคราะห์และกำหนดสิทธิการใช้งาน พร้อมทั้งทำการทดสอบการใช้งานตามสิทธิ์ เมื่อสามารถใช้งานได้แล้ว จึงแจ้งรหัสผู้ใช้งาน (username) และ รหัสผ่าน (password) ปิดซองอย่างมิดชิด ส่งให้ผู้ขอใช้บริการ และให้ลงลายมือชื่อการใช้บริการ
- ผู้ดูแลระบบจัดทำรายงานสรุปการขอใช้บริการ/รับแจ้งปัญหารายไตรมาส
- สิ้นปีจะทำการทบทวนสิทธิ์การใช้งานตามรายชื่อผู้ใช้งานเทียบกับรายชื่อพนักงานที่ปฏิบัติงานอยู่ และรายชื่อบุคคลภายนอกหรือ Out Source ที่ขอใช้บริการ

๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๔.๑ ให้มีการกำหนดชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันตัวตนในการเข้าใช้งานระบบปฏิบัติการ

๒.๔.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่าน ของตนในการเข้าใช้งานระบบปฏิบัติการร่วมกัน

๒.๔.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ แบบที่มีการสอบถามรหัสผ่านในการกลับเข้าใช้งานระบบปฏิบัติการ

๒.๔.๔ ผู้ใช้งานต้องทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน

๒.๔.๕ ติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้าย รวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ

๒.๔.๖ องค์การคลังสินค้าใช้การบริหารจัดการรหัสผ่านที่ทำงานแบบ Interactive ซึ่งรองรับโปรโตคอลมาตรฐาน LDAP หรือ Active directory

๒.๔.๗ การใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบ (use of system utilities) ให้มีการจำกัดและควบคุมการใช้งานดังนี้

(๑) จำกัดสิทธิการติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบตามสิทธิของผู้ใช้งาน

(๒) หากผู้ใช้งานมีความจำเป็นต้องติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบให้ขออนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร

(๓) กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์สำหรับระบบที่ไม่จำเป็นออกจากระบบปฏิบัติการ

(๔) ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น

๒.๔.๘ กำหนดมาตรการกรณีมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งดังนี้

(๑) กรณีระบบสารสนเทศทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๑๕ นาที

(๒) กรณีระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๕ นาที

๒.๔.๙ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ให้ดำเนินการดังนี้

(๑) ให้กำหนดระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง แต่ละครั้งได้ไม่เกิน ๓ ช.ม.เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น

(๒) กรณีระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ซึ่งจำเป็นต้องเชื่อมต่อเกินระยะเวลาหรือช่วงเวลาที่กำหนด ให้ผู้ใช้งานแจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษร

๒.๔.๑๐ ระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตน ที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง โดยมีแนวปฏิบัติดังนี้

(๑) ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) สำหรับเข้าใช้งานระบบ สารสนเทศของหน่วยงาน

(๒) หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (username) และรหัสผ่าน (password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๒.๕.๑ การจำกัดการเข้าถึงสารสนเทศ (information access restriction) ให้จำกัดสิทธิการใช้งานโปรแกรมประยุกต์และสารสนเทศตามสิทธิของผู้ใช้งานหรือผู้รับจ้าง (Out Source) ที่ได้รับอนุญาตเท่านั้น

๒.๕.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน โดยกำหนดรายชื่อผู้ใช้ (username) และรหัสผ่าน (password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

๒.๕.๓ ตรวจสอบการใช้งานโปรแกรมประยุกต์ ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับโปรแกรมที่ใช้ หรือการทำงานของโปรแกรมผิดพลาดให้รีบดำเนินการแก้ไขในทันที

๒.๕.๔ สำรองโปรแกรมระบบงานประยุกต์ (File Program Backup) อย่างน้อยปีละ ๑ - ๒ ครั้ง

๒.๕.๕ ทำการแยกระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน จะต้องดำเนินการดังนี้

(๑) แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ระบบสารสนเทศที่ใช้เฉพาะภายในหน่วยงานให้ติดตั้งในเครือข่ายภายใน ส่วนระบบสารสนเทศที่สามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ตต้องติดตั้งอยู่หลังไฟร์วอลล์

(๒) ติดตั้งระบบสารสนเทศแต่ละระบบ บนสภาพแวดล้อมการประมวลผล (Computing environment) ที่แยกจากกัน เพื่อควบคุมสภาพแวดล้อมของระบบ

๒.๕.๖ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ดำเนินการดังนี้

(๑) ผู้ใช้งานที่ต้องการนำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ต้องลงทะเบียนอุปกรณ์ดังกล่าวจึงจะสามารถใช้งานระบบเครือข่ายของหน่วยงานได้

(๒) บุคคลภายนอกหรือผู้รับจ้าง (Out Source) ที่ต้องการนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ให้สามารถใช้งานได้เฉพาะอินเทอร์เน็ต โดยให้ติดต่อผู้ดูแลระบบเพื่อขอชื่อผู้ใช้และรหัสผ่าน

๒.๕.๗ การปฏิบัติงานจากภายนอกหน่วยงาน (teleworking) มีข้อกำหนดในการปฏิบัติงานดังนี้

(๑) ไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

(๒) ไม่ใช้งานระบบสารสนเทศของหน่วยงานผ่านเครือข่ายที่ไม่น่าเชื่อถือ เครือข่ายในร้านอินเทอร์เน็ต เครือข่ายไร้สายที่ไม่ได้ให้บริการโดยผู้ให้บริการอินเทอร์เน็ต หรือหน่วยงานภาครัฐ เป็นต้น

(๓) การนำเครื่องคอมพิวเตอร์ของหน่วยงานออกไปใช้ภายนอกหน่วยงานต้องมีการเข้ารหัสข้อมูลที่สำคัญในสื่อบันทึกข้อมูลต่างๆ

๒.๖ การควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

๒.๖.๑ มีการควบคุมดูแลการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ของ อคส. ๒ ชั้น

๒.๖.๑.๑ ประตูชั้นนอก ใช้คีย์การ์ด หรือการแสกนลายนิ้วมือที่ให้เฉพาะเจ้าหน้าที่ที่ดูแลระบบของแต่ละหน่วยงานในกระทรวงพาณิชย์เท่านั้น

๒.๖.๑.๒ ประตูชั้นใน เป็นประตูเหล็กที่มีระบบแสกนนิ้วมือให้เจ้าหน้าที่แต่ละหน่วยงานเพื่อเข้า-ออกในห้องควบคุมของหน่วยงานตนเอง

๒.๖.๑.๓ มีกล้องวงจรปิดบันทึกผู้เข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ เพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้งป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

๒.๖.๒ มีการกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อคส. เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย

๒.๖.๒.๑ เจ้าหน้าที่ส่วนงานบริหารฐานข้อมูลที่ดูแลห้องควบคุมระบบคอมพิวเตอร์ อคส. ต้องได้รับการแสกนลายนิ้วมือจากสำนักงานปลัด กระทรวงพาณิชย์ เพื่อเข้า-ออกห้องควบคุมเท่านั้น

๒.๖.๒.๒ มีการจัดทำ "ตารางเวรของเจ้าหน้าที่ดูแลห้องควบคุมฯ " เพื่อปฏิบัติหน้าที่ตามสิทธิและหน้าที่ที่ได้รับเท่านั้น

๒.๖.๒.๓ เจ้าหน้าที่องค์การคลังสินค้า หรือบุคคลภายนอก(Out Source) ที่เข้ามาติดต่อขอเข้าห้องควบคุมระบบคอมพิวเตอร์ต้องได้รับอนุญาต และต้องลงชื่อในสมุดบันทึกการเข้า-ออกในแบบฟอร์มและจะต้องมีเจ้าหน้าที่ที่ดูแลห้องควบคุมอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๒.๗ การควบคุมการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย

๒.๗.๑ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด

๒.๗.๒ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งาน

๒.๘ การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless Network Access Control)

๒.๘.๑ การติดตั้ง Access Point, Wireless Router หรืออุปกรณ์อื่นๆ ที่มีการทำงานในลักษณะเดียวกัน ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และต้องกำหนดรหัสการเข้าใช้งาน เพื่อเป็นการรักษาความมั่นคงปลอดภัยในการใช้งานอุปกรณ์ดังกล่าว กรณีได้รับอนุญาต ให้ผู้ดูแลระบบดำเนินการ ดังนี้

๒.๘.๑.๑ ต้องวางอุปกรณ์ในตำแหน่งที่เหมาะสม และ ต้องเพิ่มการรับรองการเข้ารหัสด้วย (Authentication)

๒.๘.๑.๒ ให้กำหนดรายการ MAC Address ที่สามารถเข้าใช้อุปกรณ์ได้เฉพาะเครื่องคอมพิวเตอร์ที่อนุญาตเท่านั้น หรือตามชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้น

๒.๘.๑.๓ ให้เปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่า Default มาจาก โรงงานผลิตทันทีที่นำอุปกรณ์มาใช้งาน และต้องปิดคุณสมบัติการ Auto Broadcast SSID ของตัวอุปกรณ์ด้วย

๒.๘.๑.๔ ต้องเขียนคู่มือการติดตั้งอุปกรณ์อย่างถูกวิธีและกำหนดค่า Configuration ให้เหมาะสม รวมทั้งทำ Check List เกี่ยวกับ Security Configuration

๒.๘.๑.๕ ต้องกำหนดรูปแบบการรักษาความปลอดภัย แบบ WPA๒ (Wi-Fi Protected Access) หรือรูปแบบที่ดีกว่า

๒.๘.๒ ห้ามผู้ใช้งาน ใช้งานเครือข่ายแบบ Ad-Hoc หรือ Peer-To-Peer

๒.๘.๓ ผู้ดูแลระบบต้องควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาต ใช้งานเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๒.๘.๔ ผู้ดูแลระบบใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของเครือข่ายไร้สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในเครือข่ายไร้สาย และจัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งานเครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบทันที

๒.๙ การใช้จดหมายอิเล็กทรอนิกส์ (Email)

๒.๙.๑ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Email) ต้องทำการกรอกข้อมูลคำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงานลงในแบบฟอร์ม โดยยื่นแบบฟอร์มกับเจ้าหน้าที่ ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส.

๒.๙.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่านโดยทันที

๒.๙.๓ ห้ามบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๙.๔ ทำการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๒.๙.๕ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่งข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานที่อยู่จดหมายอิเล็กทรอนิกส์ดังกล่าว

๒.๙.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของ อคส. ผู้ใช้งานจะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมายอิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. ขัดข้องและได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๒.๙.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๒.๙.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุกปั่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็นส่วนบุคคล โดยอ้างว่าเป็นความเห็นของ อคส. หรือก่อให้เกิดความเสียหายต่อ อคส.

๒.๙.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือสิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อการดำเนินงานของ อคส. ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของ อคส.

๒.๙.๑๐ การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์

๒.๙.๑๑ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เสร็จสิ้นต้องออกจากระบบ (Log out) ทุกครั้ง

๒.๑๐ การใช้เครือข่ายอินเทอร์เน็ต (Internet)

๒.๑๐.๑ ผู้ใช้งานที่ต้องการใช้เครือข่ายอินเทอร์เน็ต ต้องลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต โดยยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส. สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ที่ได้รับมอบหมาย

๒.๑๐.๒ ไม่ใช้เครือข่ายคอมพิวเตอร์ของหน่วยงานที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความมั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๑๐.๓ ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องแม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๑๐.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตนั้นต้องเป็นผู้รับผิดชอบ

๒.๑๐.๕ ห้ามเปิดเผยข้อมูลของหน่วยงานที่เป็นความลับ หรือข้อมูลสำคัญที่ยังไม่ได้ประกาศอย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต

๒.๑๐.๖ การดาวน์โหลดข้อมูลและโปรแกรมต่างๆ จากเครือข่ายอินเทอร์เน็ต ต้องกระทำด้วยความระมัดระวัง และหากมีความจำเป็นต้องดาวน์โหลดไฟล์ขนาดใหญ่ ให้ดำเนินการนอกเวลาปฏิบัติงาน

๒.๑๐.๗ ห้ามดาวน์โหลดข้อมูลและโปรแกรมต่างๆ ที่ละเมิดลิขสิทธิ์ จากเครือข่ายอินเทอร์เน็ต

๒.๑๐.๘ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรของหน่วยงานอื่นๆ

๒.๑๐.๙ หลังจากใช้งานเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ Log out จากระบบการพิสูจน์ตัวจริงเพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๑๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (access control)

๒.๑๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๑๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

(๑) กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข

- อนุมัติ
- ไม่มีสิทธิ

(๒) กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (user access management) ที่ได้กำหนดไว้

(๓) ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๑๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

(๑) จัดแบ่งประเภทของข้อมูลออกเป็น

- ข้อมูลสารสนเทศด้านการบริหาร ข้อมูลนโยบาย ข้อมูลยุทธศาสตร์ ข้อมูลบุคลากร ข้อมูลงบประมาณการเงินและบัญชี เป็นต้น
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ ข้อมูลรับจำนำโครงการต่างๆ ข้อมูลซื้อ-ขายสินค้า ข้อมูลคลังสินค้า เป็นต้น

(๒) จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

(๓) จัดแบ่งลำดับชั้นความลับของข้อมูล

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

(๔) จัดแบ่งระดับชั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

(๕) การกำหนดเวลาที่ได้เข้าถึง

- ข้อมูลสารสนเทศด้านการบริหาร (Back Office) สำหรับผู้ใช้งานภายในสามารถเข้าถึงระบบสารสนเทศได้ตลอด ๒๔ ชั่วโมง (ต้องเข้ามาที่สำนักงานเท่านั้น)
- ข้อมูลสารสนเทศด้านการพาณิชย์ที่ให้บริการ (Front Office) สำหรับผู้ใช้งานภายนอกสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง

(๖) การกำหนดช่องทางที่สามารถเข้าถึง

- ผ่านระบบสารสนเทศที่ให้บริการ
- ผ่านทางจดหมายอิเล็กทรอนิกส์
- ผ่านทาง teleworking

- ผ่านเครื่องมือ (tools) การเข้าถึง

๒.๑๒ อำนาจหน้าที่

ให้ผู้บริหารระดับสูงสุดขององค์การคลังสินค้า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และผู้ดูแลระบบสารสนเทศมีอำนาจหน้าที่ในการรักษาความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ดังนี้

๒.๑๒.๑ ให้ผู้บริหารระดับสูงสุดขององค์การคลังสินค้า (Chief Executive Officer : CEO) มีอำนาจหน้าที่ดังต่อไปนี้

รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่เกิดขึ้นกับหน่วยงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๒.๑๒.๒ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer : CIO) มีอำนาจหน้าที่ดังต่อไปนี้

(๑) รับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

(๒) รับผิดชอบกำกับดูแล การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

(๓) จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ

(๔) มีอำนาจในการจัดสรรทรัพยากรในการดำเนินโครงการเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

(๕) ดำเนินการเรื่องอื่นตามที่ได้รับมอบหมาย

๒.๑๒.๓ ให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ มีอำนาจหน้าที่ดังต่อไปนี้

(๑) ให้คำแนะนำ และข้อเสนอแนะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง/หรือคณะกรรมการฯ ในการกำหนดนโยบาย ประกาศและมาตรการด้านสารสนเทศ

(๒) กำกับ ดูแล และควบคุมการให้บริการด้านระบบสารสนเทศ และการปฏิบัติตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

(๓) ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจาหน่ายอุปกรณ์ดังกล่าว (ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล ในส่วนที่ ๒ ข้อ ๒.๒.๓ (๕.๑)

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สาหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๒.๑๒.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่ดังต่อไปนี้

(๑) ดูแลรักษาและปรับปรุงระบบสารสนเทศให้สามารถใช้งานได้ดีอยู่เสมอ

(๒) ควบคุมดูแลผู้ใช้บริการให้ปฏิบัติตามกฎระเบียบการใช้งานระบบสารสนเทศขององค์การคลังสินค้า

(๓) กรณีพบว่าผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้งานระบบสารสนเทศขององค์การคลังสินค้า ผู้ดูแลระบบสารสนเทศจะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น ผู้ดูแลระบบสารสนเทศมีอำนาจในการระงับการใช้งานของผู้ใช้บริการดังกล่าวได้ทันที

(๔) ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการเสนอความเห็นต่อผู้อำนวยการสำนัก เพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารจัดการระบบสารสนเทศ

(๕) ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัสข้อมูลอัตโนมัติ (Encryption) หรือระบบอื่นใดที่เกี่ยวข้องกับระบบเครือข่ายสารสนเทศ และอุปกรณ์คอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ

(๖) ผู้ดูแลระบบสารสนเทศมีหน้าที่รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนการสำรองข้อมูล แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

ส่วนที่ ๓

แนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลัก และไฟล์โปรแกรมระบบงานที่สำคัญ ที่ทำหน้าที่ให้บริการข้อมูลที่ถูกต้องและทันสมัย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้กลับคืนได้ภายในระยะเวลาที่เหมาะสม

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๐๕ (Information Security Management System : ISMS)

แนวปฏิบัติ

๓.๑ การสำรองสารสนเทศ

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งาน ตามแนวทางต่อไปนี้

๓.๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๑.๒ กำหนดให้มีการสำรองข้อมูลของระบบสารสนเทศแต่ละระบบ และกำหนดความถี่ในการสำรองข้อมูล หากระบบใดที่มีการเปลี่ยนแปลงบ่อย ควรกำหนดให้มีความถี่ในการสำรองข้อมูลมากขึ้น โดยให้มีวิธีการสำรองข้อมูล ดังนี้

- กำหนดประเภทของข้อมูลที่ต้องทำการสำรองเก็บไว้ และความถี่ในการสำรอง
- กำหนดรูปแบบการสำรองข้อมูลให้เหมาะสมกับข้อมูลที่จะทำการสำรอง เช่น การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)
- บันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลาชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
- ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ ข้อมูลคอนฟิกกูเรชัน ข้อมูลในฐานข้อมูล เป็นต้น
- จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการสำรองข้อมูลไว้อย่างชัดเจน
- จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น

- ทดสอบบันทึกข้อมูลสำรองอย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๓.๒ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน

๓.๒.๑ ต้องจัดทำระบบสำรองของระบบสารสนเทศหลักที่สำคัญของหน่วยงาน และต้องมีการทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ

๓.๒.๒ ต้องจัดทำแผนการกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๒.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๓.๒.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒.๕ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๖ ต้องทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

กำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของหน่วยงาน เพื่อให้ระบบสารสนเทศของ อคส. มีความปลอดภัยและเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิดขึ้นกับระบบสารสนเทศของ อคส.ได้

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

COBIT ๕

แนวปฏิบัติ

๔.๑ การตรวจสอบและประเมินความเสี่ยง

๔.๑.๑ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit And Assessment) โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) และให้จัดทำรายงานพร้อมข้อเสนอแนะอย่างน้อยปีละ ๑ ครั้ง

๔.๑.๒ มีการทบทวนกระบวนการบริหารจัดการความเสี่ยง อย่างน้อยปีละ ๑ ครั้ง

๔.๑.๓ มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

๔.๑.๔ ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๔.๑.๕ ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๔.๑.๖ กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้โดยมีการป้องกันเป็นอย่างดี

๔.๑.๗ ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ โดยแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบออกจากระบบสารสนเทศที่ให้บริการจริงหรือที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกันเครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕

แนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับ ความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า

วัตถุประสงค์

เพื่อสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร โดยการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวปฏิบัติขององค์กร

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๐๕ (Information Security Management System : ISMS)

แนวปฏิบัติ

๕.๑ การสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย

๑. จัดฝึกอบรมแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับภาระงานของบุคลากร อย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน

๒. ประชาสัมพันธ์ความรู้เกี่ยวกับแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่เข้าใจง่าย โดยมีการปรับปรุงความรู้อย่างสม่ำเสมอ