

ประกาศองค์การคลังสินค้า
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
องค์การคลังสินค้า (ฉบับทบทวน)

ตามประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานภาครัฐ เพื่อให้การดำเนินการต่างๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ของหน่วยงาน โดยอาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

เพื่อให้การปฏิบัติงานและการบริหารงานมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากลองค์การคลังสินค้าจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้า โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศองค์การคลังสินค้า เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า (ฉบับทบทวน)”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓ องค์การคลังสินค้าได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า เป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ ประกอบด้วยเนื้อหาอย่างน้อยครอบคลุมตามประกาศ ดังนี้

๓.๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๓.๑.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต

๓.๑.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึง โดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ และการ ลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๓.๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการ ทางเครือข่ายโดยไม่ได้รับอนุญาต

๓.๑.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๓.๑.๕ มีการควบคุมการเข้าถึงระบบสารสนเทศ โปรแกรมประยุกต์หรือแอปพลิเคชัน และสารสนเทศ (System and Application Access Control) โดยต้องมีการควบคุม

๓.๑.๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control)

๓.๒ นโยบายการจัดทำระบบสำรองของสารสนเทศ

๓.๒.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๓.๒.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผน เตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้ งานตามภารกิจ

๓.๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบ สำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์

๓.๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน และทดสอบข้อมูลสำรองที่บันทึกไว้ อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๓.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๓.๑ องค์การคลังสินค้าต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับ ระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๓.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์การ คลังสินค้า (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้องค์การคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓.๔ นโยบายการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๓.๔.๑ องค์การคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยเผยแพร่ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ

๓.๔๒ จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวปฏิบัติขององค์การคลังสินค้า

ข้อ ๔ ข้อปฏิบัติการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปตามข้อกำหนดในเอกสารแนบท้ายประกาศองค์การคลังสินค้า เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ องค์การคลังสินค้า (ฉบับทบทวน)”

ข้อ ๕ องค์ประกอบของนโยบาย จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ “แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า (ฉบับทบทวน)” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของหน่วยงานภายในและหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศฉบับนี้มีผลบังคับใช้ตั้งแต่วันที่ถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๗ ธันวาคม พ.ศ. ๒๕๖๐



(นางอินทิรา โภคบุญยารักษ์)

ผู้อำนวยการองค์การคลังสินค้า

เอกสารแนบท้ายประกาศองค์การคลังสินค้า

เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย

ด้านสารสนเทศ องค์การคลังสินค้า

ส่วนที่ ๑

บทที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ

๑.๑. นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๑.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาตอย่างน้อยดังนี้

- (๑) การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการถอดถอนสิทธิ์ผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว
- (๒) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท ทุกระบบในองค์กร
- (๓) การบริหารจัดการสิทธิ์ของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิ์เพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิ์จำเพาะ สิทธิพิเศษ และสิทธิ์อื่นๆ ที่เกี่ยวข้องกับการเข้าถึง
- (๔) การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม
- (๕) การทบทวนสิทธิ์การเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

๑.๑.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการ ลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

- (๑) การใช้งานรหัสผ่าน (Password use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ
- (๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิ์สามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล
- (๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์ และต้อง กำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน
- (๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการ รักษาความลับทางราชการ พ.ศ. ๒๕๔๔

- ๑.๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการ ทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้
- (๑) ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ
 - (๒) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
 - (๓) การยืนยันตัวตนบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวตนบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้
 - (๔) การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์ บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน
 - (๕) ระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสม เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลสารสนเทศและระบบเทคโนโลยีสารสนเทศและการสื่อสาร
 - (๖) การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย
 - (๗) การแบ่งแยกเครือข่าย (Segregation in networks) ต้องทำการแบ่งแยกเครือข่ายตามกลุ่มของบริการสารสนเทศ กลุ่มผู้ใช้งาน และกลุ่มของระบบสารสนเทศ
 - (๘) การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง
 - (๙) การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และการส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ
 - (๑๐) ระบบเครือข่ายต้องได้รับการออกแบบหรือตั้งค่าให้ทำงานได้อย่างมีประสิทธิภาพ (Reliable) มีความยืดหยุ่น (Flexible) รวมถึงสามารถรองรับการขยายตัวและความต้องการใช้งานในอนาคต (Scalable)
- ๑.๑.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating system access control) เพื่อป้องกันการเข้าถึง ระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้
- (๑) กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการจะต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย
 - (๒) ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้มีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง
 - (๓) การบริหารจัดการรหัสผ่าน (Password management system) ต้องจัดทำหรือจัดให้มี ระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานใน ลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสผ่านที่มีคุณภาพ

- (๔) การใช้งานโปรแกรมอรรถประโยชน์ (Use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว
- (๕) เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (Session time-out)
- (๖) การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Limitation of connection time) ต้องจำกัดระยะเวลาในการเชื่อมต่อเพื่อให้มีความมั่นคงปลอดภัยมากยิ่งขึ้นสำหรับระบบสารสนเทศหรือโปรแกรมที่มีความเสี่ยงหรือมีความสำคัญสูง

๑.๑.๕ มีการควบคุมการเข้าถึงระบบสารสนเทศ โปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (System and Application Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

- (๑) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือ ควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานใน การเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือ แอปพลิเคชัน ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้
- (๒) การกำหนดขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกินจำนวนครั้งที่กำหนด
- (๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการ แยก ออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการ ควบคุม อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอก หน่วยงาน (Mobile computing and teleworking)
- (๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการ ที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่
- (๕) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงาน และ ขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน
- (๖) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบ ต้องมีการ จำกัดและควบคุมการใช้อย่างใกล้ชิด
- (๗) การควบคุมการเข้าถึงซอร์สโค้ดสำหรับระบบ (Access Control to Program Source Code) ต้องจัดให้มีการควบคุมการเข้าถึง Source Code ของระบบที่ให้บริการ

๑.๑.๖ มีข้อกำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access control) อย่างน้อย ดังนี้

- (๑) มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย
- (๒) ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจขององค์กร
- (๓) ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๒ นโยบายการจัดทำระบบสำรองของสารสนเทศ

- (๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม
- (๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผน เตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้ งานตามภารกิจ
- (๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์
- (๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองระบบแผนเตรียมพร้อมกรณีฉุกเฉิน และทดสอบข้อมูลสำรองที่บันทึกไว้ อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง
- (๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๑.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

- (๑) องค์กรคลังสินค้าต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information security audit and assessment) อย่างน้อยปีละ ๑ ครั้ง
- (๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์กรคลังสินค้า (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้องค์กรคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๔ นโยบายการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

- (๑) องค์กรคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ
- (๒) จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับแนวปฏิบัติขององค์กรคลังสินค้า

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 พัฒนาปรับปรุง 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 สิ่งที่สามารถทำให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าจะการสื่อความหมายนั้นจะทำได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผ่นผัง แผนที่ ภาพวาด ภาพถ่าย फिल्म การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือ วิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

"**สารสนเทศ (Information)**" หมายถึง ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบ ให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟิก 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 ระบบงานของหน่วยงานที่นำเอาระบบคอมพิวเตอร์ และระบบการสื่อสารมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการดำเนินการต่างๆ ของหน่วยงาน

"เจ้าของข้อมูล" หมายถึง ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบสารสนเทศโดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้นๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

"สิทธิของผู้ใช้งาน" หมายถึง สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ของหน่วยงาน ตามที่กำหนดในภารกิจของผู้ใช้งาน (User Role)

"สินทรัพย์" หมายถึง ข้อมูล และทรัพย์สินด้านเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายถึง การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน หรือบุคคลภายนอก เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายถึง การดำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้าน ความ ถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิดชอบ (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event)" หมายถึง กรณีที่ระบุการเกิด เหตุการณ์สภาพของการบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความ มั่นคงปลอดภัย หรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคง ปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident)" หมายถึง สถานการณ์ ซึ่งอาจทำให้ระบบขององค์กรถูกรบกวนหรือโจมตีและความมั่นคงปลอดภัยถูก คุกคาม

"จดหมายอิเล็กทรอนิกส์ (Email)" หมายถึง ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่องคอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่ง ข้อมูลชนิดนี้ได้แก่ SMTP, POP^๓ และ IMAP

"ระบบจดหมายอิเล็กทรอนิกส์ของ อคส." หมายถึง ระบบจดหมายอิเล็กทรอนิกส์ของ สำนักงานปลัด กระทรวงพาณิชย์หรือกระทรวง ICT ซึ่งอนุญาตให้ผู้ใช้งานใช้เพื่อการดำเนินงานของ อคส.

"รหัสผ่าน (Password)" หมายถึง ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงและรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

"ซอฟต์แวร์ประสงค์ร้าย (Malware)" หมายถึง ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อทำลาย หรือสร้างความเสียหายให้กับระบบสารสนเทศ การโจรกรรมข้อมูล หรือการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"ผู้บุกรุก " หมายถึง บุคคลที่เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

"สำนักงานปลัดกระทรวงพาณิชย์ " หมายถึง ชื่อหน่วยงาน สำนักงานปลัด สังกัดกระทรวงพาณิชย์ ตั้งอยู่เลขที่ ๕๖๓ ถนนนนทบุรี ๑ อำเภอเมือง จังหวัดนนทบุรี ๑๑๐๐๐

บทที่ ๓ อำนาจหน้าที่

ให้ผู้บริหารระดับสูงสุดขององค์กรคลังสินค้า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และผู้ดูแลระบบสารสนเทศมีอำนาจหน้าที่ในการรักษาความปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ดังนี้

- ๓.๑ ให้ผู้บริหารระดับสูงสุดขององค์กรคลังสินค้า (Chief Executive Officer: CEO) มีอำนาจหน้าที่ดังต่อไปนี้
รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่เกิดขึ้นกับหน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
- ๓.๒ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) มี อำนาจหน้าที่ดังต่อไปนี้
 - ๓.๒.๑ รับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์กรคลังสินค้า
 - ๓.๒.๒ รับผิดชอบกำกับดูแล การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์กรคลังสินค้า
 - ๓.๒.๓ จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ
 - ๓.๒.๔ มีอำนาจในการจัดสรรทรัพยากรในการดำเนินโครงการเทคโนโลยีสารสนเทศขององค์กรคลังสินค้า
 - ๓.๒.๕ ดำเนินการเรื่องอื่นตามที่ได้รับมอบหมาย
- ๓.๓ ให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ มีอำนาจหน้าที่ดังต่อไปนี้
 - ๓.๓.๑ ให้คำแนะนำ และข้อเสนอแนะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง/หรือคณะกรรมการฯ ในการกำหนดนโยบาย ประกาศและมาตรการด้านสารสนเทศ
 - ๓.๓.๒ กำกับ ดูแล และควบคุมการให้บริการด้านระบบสารสนเทศ และการปฏิบัติตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
 - ๓.๓.๓ ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้
 - (๑) ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแท่งจำหน่ายอุปกรณ์ดังกล่าว (ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล
 - (๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญใน อุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้เกิดการเข้าถึงข้อมูลสำคัญนั้นได้
- ๓.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่ดังต่อไปนี้
 - ๓.๔.๑ ดูแลรักษาและปรับปรุงระบบสารสนเทศให้สามารถใช้งานได้ดีอยู่เสมอ
 - ๓.๔.๒ ควบคุมดูแลผู้ใช้บริการให้ปฏิบัติตามกฎระเบียบการใช้งานระบบสารสนเทศของ องค์กรคลังสินค้า
 - ๓.๔.๓ กรณีพบว่าผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้งานระบบสารสนเทศขององค์กร คลังสินค้า ผู้ดูแลระบบสารสนเทศจะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น ผู้ดูแลระบบสารสนเทศมีอำนาจในการระงับการใช้งานของผู้ใช้บริการ ดังกล่าวได้ทันที
 - ๓.๔.๔ ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการเสนอความเห็นต่อผู้อำนวยการสำนัก เพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารจัดการระบบสารสนเทศ

- ๓.๔.๕ ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัส ข้อมูลอัตโนมัติ (Encryption) หรือระบบอื่นใดที่เกี่ยวข้องกับระบบเครือข่าย สารสนเทศ และอุปกรณ์ คอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้งานได้ดีอยู่เสมอ
- ๓.๔.๖ ผู้ดูแลระบบสารสนเทศมีหน้าที่รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการ จัดทำแผนการ สำรองข้อมูล แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถ ดำเนินการด้วยวิธีการทาง อิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูล และการ ทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

ส่วนที่ ๒

แนวปฏิบัติการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบ เครือข่าย จากผู้บุกรุก หรือจากซอฟต์แวร์ประสงค์ร้าย รวมทั้งกำหนดประเภทของข้อมูล ลำดับชั้น ความลับของข้อมูล 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 การโยกย้ายหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น
- ๒.๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึง และใช้งานระบบสารสนเทศที่สำคัญ เช่น ซอฟต์แวร์ประยุกต์ จดหมายอิเล็กทรอนิกส์ เครือข่ายไร้สาย และอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ
- ๒.๑.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงและใช้งานระบบสารสนเทศของบุคลากรดังต่อไปนี้
 - ๒.๑.๓.๑ การลงทะเบียนและการถอดถอนสิทธิผู้ใช้งาน (User Registration and De-Registration) ให้ผู้ดูแลระบบงานหรือผู้ที่ได้รับมอบหมายจัดทำแบบฟอร์มสำหรับลงทะเบียนผู้ใช้งานใหม่ ดังนี้
 - (๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน
 - (๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน
 - (๓) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัว แรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะไม่ซ้ำกับชื่อผู้ใช้งานคนอื่น
 - (๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น
 - (๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือ ความต้องการทางธุรกิจ
 - (๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

- (๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ
- (๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย
- (๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออก จากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอนย้าย หรือสิ้นสุดการจ้าง เป็นต้น
- (๑๐) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้น ต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนด ระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือ พ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

๒.๑.๓.๒ การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับ ผู้ใช้งานทุกประเภท เช่น ผู้ใช้งาน ผู้ดูแลระบบ รวมถึงทุกระบบในองค์กร

๒.๑.๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียดที่ เกี่ยวกับการ ควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศ แต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นๆ ที่ เกี่ยวข้องกับการเข้าถึง ดังนี้

- (๑) ผู้ใช้งานต้องลงทะเบียนผู้ใช้งานเพื่อนำข้อมูลไปตรวจสอบสิทธิก่อนการ มอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน
- (๒) ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตาม หน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน
- (๓) การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง
- (๔) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๑.๓.๔ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

- (๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคง ปลอดภัย
- (๒) การตั้งรหัสผ่านชั่วคราว ต้องยากต่อการสุ่ม และต้องมีความแตกต่างกัน
- (๓) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมาย อิเล็กทรอนิกส์ (e-mail) ในการ จัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับทันที หลังจากได้รับรหัสผ่าน โดย จัดส่งบัญชีและรหัสผ่านใส่ซองปิดผนึก และประทับตรา "ลับ" และแนบ เอกสารอื่นๆ ที่เกี่ยวข้องกับการ ปฏิบัติงานของผู้ใช้งาน ส่งมอบให้ผู้ใช้งาน และให้ผู้ใช้งานลงนามรับ เอกสารนั้น รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตาม เอกสารแนบดังกล่าวโดยเคร่งครัด
- (๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควร เปลี่ยนให้รหัสผ่านยากต่อการเดา
- (๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว
- (๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

- (๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่
- (๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งาน นั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนัก เทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง และมีการ กำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใดได้บ้าง
- (๙) กำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านเมื่อผู้ใช้งานลาออก หรือพ้นจากตำแหน่ง หรือยกเลิกการใช้งาน
- (๑๐) หลีกเลี่ยงการส่งรหัสผ่านให้ผู้ใช้งาน โดยใช้บุคคลอื่นหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ไม่มีการรักษาความปลอดภัย
- (๑๑) ต้องกำหนดให้ผู้ใช้งานไม่บันทึกหรือเก็บรหัสผ่าน ไว้ในระบบคอมพิวเตอร์ในรูปแบบที่ไม่ได้ป้องกันการเข้าถึง

๒.๑.๓.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Rights) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

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

๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลสารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

- ๒.๒.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน เพื่อให้สามารถ กำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ ดังนี้
 - ๒.๒.๑.๑ เปลี่ยนรหัสผ่านชั่วคราวทันทีเมื่อล็อกอินเข้าใช้งานระบบครั้งแรก
 - ๒.๒.๑.๒ ผู้ใช้งานต้องตั้งรหัสผ่านที่ยากต่อการคาดเดา
 - ๒.๒.๑.๓ ผู้ใช้งานต้องกำหนดรหัสผ่าน ให้มีตัวอักษรจำนวนมากกว่าหรือเท่ากับ ๘ ตัวอักษร โดยมีการผสมกันระหว่างตัวอักษรที่เป็นตัวพิมพ์ปกติ ตัวเลข และสัญลักษณ์เข้าด้วยกัน
 - ๒.๒.๑.๔ ต้องไม่กำหนดรหัสผ่านส่วนบุคคลจากชื่อหรือนามสกุลของตนเองหรือบุคคลในครอบครัวหรือบุคคลที่มีความสัมพันธ์ใกล้ชิดกับตน หรือจากคำศัพท์ที่ใช้ในพจนานุกรม
 - ๒.๒.๑.๕ ไม่ใช้รหัสผ่านส่วนบุคคลสำหรับการใช้แฟ้มข้อมูลร่วมกับบุคคลอื่นผ่านเครือข่ายคอมพิวเตอร์
 - ๒.๒.๑.๖ เก็บรักษารหัสผ่านทั้งของตนเองและของกลุ่มไว้เป็นความลับ
 - ๒.๒.๑.๗ ไม่จดหรือบันทึกรหัสผ่านส่วนบุคคลไว้ในสถานที่ที่ง่ายต่อการสังเกตเห็นของบุคคลอื่นหรือเก็บไว้ในระบบคอมพิวเตอร์
 - ๒.๒.๑.๘ กรณีที่มีความจำเป็นต้องบอกรหัสผ่านแก่ผู้อื่นเนื่องจากงาน หลังจากดำเนินการเรียบร้อยแล้วให้ทำการเปลี่ยนรหัสผ่านโดยทันที

- ๒.๒.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้
- ๒.๒.๒.๑ ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน
- ๒.๒.๒.๒ ตั้งให้เครื่องคอมพิวเตอร์ล็อกหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา ๔๕ นาที และต้องใส่รหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอได้
- ๒.๒.๒.๓ มีการกำหนดข้อปฏิบัติให้ป้องกันอุปกรณ์คอมพิวเตอร์ที่ใช้งาน เพื่อป้องกันการสูญหายหรือการเข้าถึงโดยไม่ได้รับอนุญาต
- ๒.๒.๒.๔ มีมาตรการป้องกันอุปกรณ์ที่ไม่มีผู้ใช้งาน หรือต้องปล่อยทิ้งไว้โดยไม่มีผู้ดูแลชั่วคราว
- ๒.๒.๒.๕ สร้างความตระหนักให้เกิดความเข้าใจในมาตรการป้องกัน
- ๒.๒.๓ การควบคุมทรัพย์สินสารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อบันทึก ข้อมูลคอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน ดังนี้
- ๒.๒.๓.๑ กำหนดวิธีป้องกันทรัพย์สินขององค์กร และควบคุมไม่ให้มีการทิ้งหรือปล่อยทรัพย์สินสารสนเทศที่สำคัญให้อยู่ในสถานที่ที่ไม่ปลอดภัย ให้ครอบคลุมเรื่องต่างๆ
- ใกล้เคียงปีงบประมาณต้องสำรวจทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ว่ายังสามารถใช้งานได้หรือไม่ จำนวนครบหรือไม่ ถ้าเกิดกรณีชำรุด/เสียหาย จะทำ เรื่องส่งซ่อม/ส่งคืนพัสดุ
 - จัดห้องสำหรับรวบรวมเครื่องคอมพิวเตอร์และอุปกรณ์ที่จะส่งซ่อม/ส่งคืน และปิดล็อกห้องทุกครั้งหลังเข้า-ออก เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย
 - การควบคุมการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ โดยการใช้การ์ดหรือสแกนนิ้วมือ ก่อนและหลังเข้า-ออกทุกครั้ง
 - การจัดทำทะเบียนยืม-คืน อุปกรณ์คอมพิวเตอร์ โดยแบบฟอร์มขอใช้อุปกรณ์คอมพิวเตอร์ เพื่อใช้งานภายในและภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
 - การจัดทำทะเบียนยืม-คืน โน้ตบุ๊ก โดยใช้แบบฟอร์มยืมโน้ตบุ๊ก เพื่อใช้งานภายใน และภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
 - การวางอุปกรณ์ มีการจัดที่เฉพาะและเหมาะสมสำหรับวางเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ (Data Center)
 - การจัดทำระบบเอกสารคุณภาพ (ISO ๙๐๐๑ : ๒๐๐๘) ใช้ในองค์กร
- ๒.๒.๓.๒ การนำเครื่องคอมพิวเตอร์ โน้ตบุ๊ก และอุปกรณ์ เข้า-ออก องค์กรคลังสินค้าต้องได้รับการตรวจเช็คจากเจ้าหน้าที่ฝ่ายอาคาร อย่างเคร่งครัด
- ๒.๒.๓.๓ ต้องป้องกันการเข้าใช้งานเครื่องคอมพิวเตอร์ โดยใช้รหัสผู้ใช้งาน (Username) รหัสผ่าน (Password) เป็นการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และมีการตั้งค่าพิกหน้าจออัตโนมัติ เมื่อไม่ได้ใช้งาน
- ๒.๒.๓.๔ การป้องกันการใช้ทรัพย์สินอย่างมีประสิทธิภาพและปลอดภัย ดังนี้
- ทุกคนต้องตระหนักและปฏิบัติตามการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
 - Log out ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
 - จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย

- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิทัล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๒.๓.๕ การทำลายข้อมูลอิเล็กทรอนิกส์และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ดังนี้

(๑) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

<u>ประเภทสื่อบันทึกข้อมูล</u>	<u>วิธีการทำลาย</u>
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลาย CD/DVD
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบน ฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

(๒) ในการจัดการกับไฟล์ข้อมูลลับ ให้ปฏิบัติดังนี้

- (๑) จัดหมวดหมู่ข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับและป้องกันให้มีความปลอดภัยอย่างพอเพียงต่อการเข้าถึงและควรแสดงชั้นความลับบนไฟล์ข้อมูลลับ เช่น การแสดงชั้นความลับกับทุกหน้าของไฟล์ดังกล่าว
- (๒) การสำเนาข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับ หรือเอกสารที่มีระดับความสำคัญสูงต้องได้รับอนุญาตจากผู้เป็นเจ้าของข้อมูล
- (๓) ระมัดระวังการกระจาย หรือแจกจ่ายข้อมูลอิเล็กทรอนิกส์ที่เป็นความลับขององค์การคลังสินค้าไปยังกลุ่มผู้รับที่มีความจำเป็นต้องรับรู้เท่านั้น
- (๔) ผู้เป็นเจ้าของข้อมูลอิเล็กทรอนิกส์ต้องตรวจสอบความถูกต้องของข้อมูลอิเล็กทรอนิกส์ก่อนนำไปใช้งาน
- (๕) ป้องกันไฟล์ข้อมูลลับที่จัดเก็บไว้ในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานโดยการใส่รหัสผ่านที่มีความมั่นคงปลอดภัย
- (๖) ห้าม Share ไฟล์ข้อมูลลับบนเครือข่ายขององค์การคลังสินค้า เพื่ออนุญาตให้ผู้อื่นเข้าถึงได้ (ไม่ว่าบุคคลผู้นั้นจะได้รับอนุญาตให้เข้าถึงข้อมูลได้หรือไม่ก็ตาม เนื่องจากในระหว่างที่มีการ Share ผู้อื่นอาจเข้าถึงไฟล์ข้อมูลลับนั้นได้)
- (๗) ตรวจสอบการทำงานของระบบป้องกันไวรัสอย่างสม่ำเสมอในเครื่องคอมพิวเตอร์ที่ใช้ในการจัดเตรียมไฟล์ข้อมูลลับว่ามีการทำงานป้องกันไวรัสตามปกติหรือไม่
- (๘) ตรวจสอบการทำงานของเครื่องคอมพิวเตอร์ที่ตนเองใช้งานว่ามี การติดตั้งโปรแกรมแก้ไขช่องโหว่เพื่อแก้ไขช่องโหว่ของซอฟต์แวร์ในเครื่องตามปกติหรือไม่
- (๙) ดำเนินการสำรองไฟล์ข้อมูลลับในเครื่องคอมพิวเตอร์ที่ตนเองใช้งานอย่างสม่ำเสมอหรือตามความจำเป็น

(๑๐) ต้องทำลายข้อมูลอิเล็กทรอนิกส์บนฮาร์ดดิสก์ของเครื่องคอมพิวเตอร์ที่ถูกยกเลิกการใช้งาน

(๑๑) ต้องมีการพิจารณาเพื่อทำลายข้อมูลส่วนบุคคล ซึ่งรอบความถี่ในการทำลายข้อมูลส่วนบุคคลอย่างน้อยปีละ ๑ โดยเจ้าหน้าที่ที่รับผิดชอบข้อมูล จะต้องมีการตรวจสอบและพิจารณาการทำลายข้อมูลส่วนบุคคล

๒.๒.๔ ผู้ใช้งานได้ใช้งานระบบงานสารบรรณอิเล็กทรอนิกส์ที่นำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ ดังนี้

๒.๒.๔.๑ องค์การคลังสินค้ามีระบบงานสารบรรณอิเล็กทรอนิกส์สำหรับควบคุมการจัดเก็บและนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ดังนี้

(๑) ลงทะเบียนผู้ใช้งานระบบสารบรรณอิเล็กทรอนิกส์ มีการกำหนดสิทธิ์การเข้าตามหน่วยงาน หรือตามผู้ใช้งาน

(๒) เข้าสู่ระบบงานสารบรรณอิเล็กทรอนิกส์ โดยระบบจะทำการตรวจสอบสิทธิ์ของผู้ใช้งานก่อนเข้าสู่ระบบ

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

(๔) เมื่อผู้ใช้งาน เช่น เลขานุการผู้บริหาร เจ้าหน้าที่สารบรรณ เป็นต้น กำหนดชั้นความลับของเอกสารแล้ว จะไม่สามารถดำเนินการใดๆ กับเรื่องดังกล่าวในระบบได้อีก ยกเว้นเป็นผู้ที่ได้รับสิทธิ์ ให้เข้าถึงเอกสารประเภท ลับ ลับมาก ลับที่สุดได้เท่านั้น

(๕) ต้องนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับของหน่วยงาน

๒.๒.๕ ผู้ดูแลระบบต้องมีวิธีการรับส่ง ประมวลผล และจัดเก็บข้อมูลส่วนบุคคลที่เป็นความลับตามระดับความสำคัญ

๒.๓ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)

๒.๓.๑ ตรวจสอบการใช้งานเครือข่าย ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพหากตรวจ พบสิ่งผิดปกติเกี่ยวกับการใช้งานเครือข่ายให้รีบดำเนินการแก้ไขรวมทั้งป้องกันและ บรรเทาความเสียหาย ที่อาจจะเกิดขึ้นในทันทีในกรณีที่สิ่งผิดปกติดังกล่าวเกิดขึ้นจากการ ใช้งานของผู้ใช้งาน และให้รีบแจ้งผู้ใช้งานผู้นั้นให้ยุติการกระทำดังกล่าวในทันทีและใน กรณีที่จำเป็นเพื่อป้องกันหรือบรรเทาความเสียหายที่จะเกิดขึ้นแก่หน่วยงานให้ผู้ดูแลระบบเครือข่ายพิจารณาระงับใช้งานเครือข่ายคอมพิวเตอร์ของผู้ใช้งานดังกล่าวได้ทันที

๒.๓.๒ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขต ของระบบเครือข่ายภายในและเครือข่ายภายนอก และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้ เป็นปัจจุบันอยู่เสมอ

๒.๓.๓ การใช้เครื่องมือต่างๆ เพื่อการตรวจสอบระบบเครือข่าย ควรได้รับการอนุมัติจากผู้ดูแลระบบ และจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

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

- ๒.๓.๕ ระบบยืนยันตัวตนบุคคลต้องสามารถกำหนดสิทธิการใช้งานระบบสารสนเทศต่างๆ ผ่านเครือข่ายตามบทบาทหน้าที่ของผู้ใช้ (User role) แต่ละคนได้
- ๒.๓.๖ การยืนยันตัวตนบุคคล สำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ให้มีการยืนยันตัวตนบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งานตัวจริง โดยการใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password)
- ๒.๓.๗ การระบุอุปกรณ์บนเครือข่าย (Equipment identification in networks) เพื่อใช้สำหรับการยืนยันการเข้าถึง ดังนี้
- ๒.๓.๗.๑ กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลข IP แบบคงที่ (Static IP address) ให้จัดทำฐานข้อมูลเพื่อจัดเก็บหมายเลข MAC ของอุปกรณ์ดังกล่าว
- ๒.๓.๗.๒ กรณีอุปกรณ์บนเครือข่ายทุกตัวที่มีหมายเลข IP แบบไดนามิก (Dynamic IP address) ให้จัดเก็บ Log ใน DHCP server โดยมีข้อมูลซึ่งอ้างอิงกับหมายเลข IP อย่างน้อยดังนี้
- หมายเลข MAC ของอุปกรณ์
 - ชื่ออุปกรณ์ (Hostname)
 - วัน เวลาในการเข้าใช้งาน
- ๒.๓.๘ ให้ทำการป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote diagnostic and configuration port protection) ดังนี้
- ๒.๓.๘.๑ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งไม่จำเป็นต้องใช้งาน ให้ปิดพอร์ตดังกล่าว
- ๒.๓.๘.๒ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งมีการใช้งานบางช่วงเวลา ให้กำหนดระยะเวลาการเปิดใช้งานเท่าที่จำเป็นและต้องได้รับการอนุญาตจากผู้รับผิดชอบเป็นลายลักษณ์อักษร โดยต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล
- ๒.๓.๘.๓ กรณีพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบซึ่งจำเป็นต้องใช้งานเป็นประจำ ต้องมีการยืนยันตัวตนก่อนการเข้าใช้งานและต้องเชื่อมต่อผ่านโปรโตคอลที่มีการเข้ารหัสข้อมูล
- ๒.๓.๘.๔ สำหรับการป้องกันการเข้าถึงทางกายภาพ ให้ใช้แนวปฏิบัติในการควบคุมการเข้าออก ศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์
- ๒.๓.๙ การแบ่งแยกเครือข่าย (Segregation in networks) ให้จัดทำ VLAN โดยพิจารณาตามลักษณะการใช้งาน การรักษาความปลอดภัย และนโยบายของหน่วยงาน
- ๒.๓.๙.๑ องค์กรคลังสินค้าได้มีการจัดแบ่งแยกเครือข่ายตามหน่วยงานระดับสำนักและตามหน้าที่เฉพาะ
- ๒.๓.๙.๒ กำหนดรหัสวงเครือข่าย (VLAN) ชื่อวงเครือข่าย IP Address และค่าอื่นๆ ที่ใช้ในการกำหนดในอุปกรณ์สวิตช์และอุปกรณ์ต่างๆที่เกี่ยวข้อง
- ๒.๓.๙.๓ มีการติดตั้งค่าอุปกรณ์ต่างๆ แล้วทำการทดสอบการใช้งานเครือข่ายแต่ละวง
- ๒.๓.๙.๔ จัดทำทะเบียนวงเครือข่ายและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง
- ๒.๓.๙.๕ ผู้ดูแลระบบทำการบำรุงรักษา ตรวจสอบเช็คการใช้งานเครือข่าย (Monitoring)
- ๒.๓.๙.๖ เมื่อมีการเปลี่ยนหน่วยงานจะมีการทบทวนและจัดการแบ่งแยกเครือข่ายตามโครงสร้างหน่วยงานใหม่

- ๒.๓.๑๐ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ให้ควบคุม การเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ดังนี้
- ๒.๓.๑๐.๑ ต้องตรวจสอบการเชื่อมต่อเครือข่ายของอุปกรณ์ต่างๆ ในศูนย์ข้อมูลและเครือข่าย คอมพิวเตอร์ (Data Center) อย่างน้อยเดือนละ ๑ ครั้ง
- ๒.๓.๑๐.๒ ต้องติดตั้งอุปกรณ์ ไฟร์วอลล์ เพื่อควบคุมการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน
- ๒.๓.๑๐.๓ ต้องตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย
- ๒.๓.๑๑ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ให้ทำการควบคุมการ จัดเส้นทางบนเครือข่าย ดังนี้
- ๒.๓.๑๑.๑ ต้องกำหนดค่าโปรโตคอลสำหรับการหาเส้นทาง (Routing protocol) ที่สอดคล้อง กับเครือข่ายหลักที่หน่วยงานเชื่อมต่อ
- ๒.๓.๑๑.๒ ต้องบันทึกข้อมูลแผนผังการจัดเส้นทางบนเครือข่ายและข้อมูลการตั้งค่าอุปกรณ์หา เส้นทาง
- ๒.๓.๑๑.๓ เมื่อมีความจำเป็นต้องเปลี่ยนการหาเส้นทางบนเครือข่าย ให้ผู้ดูแลทำการปรับปรุง ข้อมูลที่บันทึกไว้และแจ้งผู้บังคับบัญชาทราบ
- ๒.๓.๑๑.๔ กำหนดให้มีการแปลงหมายเลขเครือข่าย (NAT) เพื่อแยกเครือข่ายย่อย
- ๒.๓.๑๒ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่ เพียง บริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- ๒.๓.๑๒.๑ กำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่ อนุญาตให้ใช้งานได้
- ๒.๓.๑๒.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียง บริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น
- ๒.๓.๑๒.๓ กำหนดการใช้งานระบบสารสนเทศที่สำคัญ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงาน ในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง ซึ่งองค์การคลังสินค้ามี แบบฟอร์มการขอใช้บริการดังกล่าว โดยมีขั้นตอนการปฏิบัติดังนี้
- ผู้ใช้งานกรอกแบบฟอร์มขอใช้บริการ/แจ้งปัญหา และได้รับอนุมัติตามสาย งานผู้ แจ้ง และส่งแบบฟอร์มมายังหน่วยงานผู้ดูแลระบบแล้ว
 - ผู้ดูแลระบบดำเนินการวิเคราะห์และกำหนดสิทธิการใช้งาน พร้อมทั้งทำการ ทดสอบการใช้งานตามสิทธิ์ เมื่อสามารถใช้งานได้แล้ว จึงแจ้งรหัสผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ปิดช่องอย่างมิดชิด ส่งให้ผู้ขอใช้ บริการ และให้ลงลายมือชื่อการใช้งานบริการ
 - ผู้ดูแลระบบจัดทำรายงานสรุปการขอใช้บริการ/รับแจ้งปัญหาทราบไตรมาส
 - สิ้นปีจะทำการทบทวนสิทธิการใช้งานตามรายชื่อผู้ใช้งานเทียบกับรายชื่อ พนักงานที่ปฏิบัติงานอยู่ และรายชื่อบุคคลภายนอกหรือ Out Source ที่ขอ ใช้ บริการ

๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

- ๒.๔.๑ ให้มีการกำหนดชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันตัวตนในการเข้าใช้งานระบบปฏิบัติการ
- ๒.๔.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตนในการเข้าใช้งาน ระบบปฏิบัติการ ร่วมกัน
- ๒.๔.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถอนหน้าจอ แบบที่มีการสอบถามรหัสผ่านในการกลับเข้าใช้งานระบบปฏิบัติการ
- ๒.๔.๔ ผู้ใช้งานต้องทำการ Logout ทันทีเมื่อเลิกใช้งานหรือไม่อยู่ที่หน้าจอเป็นเวลานาน
- ๒.๔.๕ ติดตั้งและใช้งานโปรแกรมคอมพิวเตอร์สำหรับป้องกันและกำจัดซอฟต์แวร์ประสงค์ร้ายรวมทั้งทำการปรับปรุงให้ทันสมัยอยู่เสมอ
- ๒.๔.๖ องค์การคลังสินค้าใช้การบริหารจัดการรหัสผ่านที่ทำงานแบบ Interactive ซึ่งรองรับโปรโตคอลมาตรฐาน LDAP หรือ Active directory
- ๒.๔.๗ การใช้งานโปรแกรมอรรถประโยชน์สำหรับระบบ (Use of system utilities) ให้มีการจำกัดและควบคุมการใช้งานดังนี้
 - ๒.๔.๗.๑ จำกัดสิทธิการติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบตามสิทธิของผู้ใช้งาน
 - ๒.๔.๗.๒ หากผู้ใช้งานมีความจำเป็นต้องติดตั้งโปรแกรมอรรถประโยชน์สำหรับระบบให้ขออนุญาตจากผู้ดูแลระบบเป็นลายลักษณ์อักษร
 - ๒.๔.๗.๓ กำหนดให้มีการถอดถอนโปรแกรมอรรถประโยชน์สำหรับระบบที่ไม่จำเป็นออกจากระบบปฏิบัติการ
 - ๒.๔.๗.๔ ห้ามติดตั้งโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นการละเมิดสิทธิในทรัพย์สินทางปัญญาของบุคคลอื่น
- ๒.๔.๘ กำหนดมาตรการกรณีมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งดังนี้
 - ๒.๔.๘.๑ กรณีระบบสารสนเทศทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๑๕ นาที
 - ๒.๔.๘.๒ กรณีระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญทั่วไป ให้ยุติการใช้งานระบบสารสนเทศ (Session time out) หลังจากไม่มีการใช้งานเป็นเวลา ๕ นาที
- ๒.๔.๙ การจำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (limitation of connection time) ให้ดำเนินการดังนี้
 - ๒.๔.๙.๑ ให้กำหนดระยะเวลาการเชื่อมต่อสำหรับการใช้งานระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง แต่ครั้งใดไม่เกิน ๓ ชม.เฉพาะในช่วงเวลาการทำงานของหน่วยงานตามปกติเท่านั้น
 - ๒.๔.๙.๒ กรณีระบบสารสนเทศที่มีความเสี่ยงหรือมีความสำคัญสูง ซึ่งจำเป็นต้องเชื่อมต่อเกินระยะเวลาหรือช่วงเวลาที่กำหนด ให้ผู้ใช้งานแจ้งผู้ดูแลระบบเป็นลายลักษณ์อักษร
- ๒.๔.๑๐ ระบุและยืนยันตัวตนของผู้ใช้งาน (User identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ ขั้นตอนทางเทคนิคในการยืนยันตัวตน ที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งาน ที่ระบุถึง โดยมีแนวปฏิบัติดังนี้
 - ๒.๔.๑๐.๑ ผู้ใช้งานต้องมีชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบ สารสนเทศของหน่วยงาน
 - ๒.๔.๑๐.๒ หากอนุญาตให้ใช้ชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) ร่วมกัน ต้องขึ้นอยู่กับความจำเป็นทางด้านธุรกิจหรือด้านเทคนิค

๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ (Application and Information Access Control)

- ๒.๕.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ให้จำกัดสิทธิการใช้งาน โปรแกรมประยุกต์และสารสนเทศตามสิทธิของผู้ใช้งานหรือผู้รับจ้าง (Out Source) ที่ได้รับอนุญาตเท่านั้น
- ๒.๕.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน โดยกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละชั้นความลับของ ข้อมูล
- ๒.๕.๓ ตรวจสอบการใช้งานโปรแกรมประยุกต์ ให้เป็นไปด้วยความเรียบร้อยและมีประสิทธิภาพ หากตรวจพบสิ่งผิดปกติเกี่ยวกับโปรแกรมที่ใช้ หรือการทำงานของโปรแกรมผิดพลาดให้ รีบดำเนินการแก้ไขในทันที
- ๒.๕.๔ สำรองโปรแกรมระบบงานประยุกต์ (File Program Backup) อย่างน้อยปีละ ๑- ๒ ครั้ง
- ๒.๕.๕ ทำการแยกระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน เช่นระบบที่มีข้อมูลส่วนบุคคล จะต้องดำเนินการดังนี้
 - ๒.๕.๕.๑ แยกระบบซึ่งไวต่อการรบกวนดังกล่าวออกจากระบบอื่น ๆ ให้ระบบสารสนเทศที่ใช้ เฉพาะภายในหน่วยงานให้ติดตั้งในเครือข่ายภายใน ส่วนระบบสารสนเทศที่สามารถ ใช้งานผ่านเครือข่ายอินเทอร์เน็ตต้องติดตั้งอยู่หลังไฟร์วอลล์
 - ๒.๕.๕.๒ ติดตั้งระบบสารสนเทศแต่ละระบบ บนสภาพแวดล้อมการประมวลผล (Computing environment) ที่แยกจากกัน เพื่อควบคุมสภาพแวดล้อมของระบบ
- ๒.๕.๖ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ดำเนินการดังนี้
 - ๒.๕.๖.๑ ผู้ใช้งานที่ต้องการนำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ส่วนตัว มาใช้ใน หน่วยงาน ต้องลงทะเบียนอุปกรณ์ดังกล่าวจึงจะสามารถใช้งานระบบเครือข่ายของ หน่วยงานได้
 - ๒.๕.๖.๒ บุคคลภายนอกหรือผู้รับจ้าง (Out Source) ที่ต้องการนำอุปกรณ์คอมพิวเตอร์และ อุปกรณ์สื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ให้สามารถใช้งานได้เฉพาะ อินเทอร์เน็ต โดยให้ติดต่อผู้ดูแลระบบเพื่อขอชื่อผู้ใช้และรหัสผ่าน
- ๒.๕.๗ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) มีข้อกำหนดในการปฏิบัติงานดังนี้
 - ๒.๕.๗.๑ ไม่ใช่เครื่องคอมพิวเตอร์สาธารณะในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน
 - ๒.๕.๗.๒ ไม่ใช้งานระบบสารสนเทศของหน่วยงานผ่านเครือข่ายที่ไม่น่าเชื่อถือ เครือข่ายในร้าน อินเทอร์เน็ต เครือข่ายไร้สายที่ไม่ได้ให้บริการโดยผู้ให้บริการอินเทอร์เน็ต หรือ หน่วยงานภาครัฐ เป็นต้น
 - ๒.๕.๗.๓ การนำเครื่องคอมพิวเตอร์ของหน่วยงานออกไปใช้ภายนอกหน่วยงานต้องมีการ เข้ามหัสข้อมูลที่สำคัญในสื่อบันทึกข้อมูลต่างๆ

๒.๖ การควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)

- ๒.๖.๑ มีการควบคุมดูแลการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ของ อคส. ๒ ชั้น
 - ๒.๖.๑.๑. ประตูชั้นนอก ใช้คีย์การ์ด หรือการสแกนลายนิ้วมือที่ให้เฉพาะเจ้าหน้าที่ที่ดูแลระบบ ของแต่ละหน่วยงานในกระทรวงพาณิชย์เท่านั้น
 - ๒.๖.๑.๒ ประตูชั้นใน เป็นประตูเหล็กที่มีระบบสแกนนิ้วมือให้เจ้าหน้าที่แต่ละหน่วยงานเพื่อ เข้า-ออกในห้องควบคุมของหน่วยงานตนเอง

- ๒.๖.๑.๓ มีกล้องวงจรปิดบันทึกผู้เข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ เพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้ง ป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้
- ๒.๖.๒ มีการกำหนดสิทธิให้กับเจ้าหน้าที่ให้สามารถเข้าถึงห้องควบคุมระบบคอมพิวเตอร์ อกส. เพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมายประกอบด้วย
 - ๒.๖.๒.๑ เจ้าหน้าที่ส่วนงานบริหารฐานข้อมูลที่อยู่ดูแลห้องควบคุมระบบคอมพิวเตอร์ อกส.ต้องได้รับการสแกนลายนิ้วมือจากสำนักงานปลัด 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 ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และต้องปฏิบัติตามนโยบายนี้โดยเคร่งครัด
- ๒.๗.๒ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ และจะต้องไม่ติดตั้งโปรแกรมใดๆ ที่ส่งผลกระทบต่อการทำงานของระบบและผู้ใช้งาน

๒.๘ การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless Network Access Control)

- ๒.๘.๑ การติดตั้ง Access Point, Wireless Router หรืออุปกรณ์อื่นๆ ที่มีการทำงานในลักษณะเดียวกัน ต้องได้รับอนุญาตเป็นลายลักษณ์อักษรจากผู้บังคับบัญชาในแต่ละระดับ และ ต้องกำหนดรหัสการเข้าใช้งาน เพื่อเป็นการรักษาความมั่นคงปลอดภัยในการใช้งาน อุปกรณ์ดังกล่าวกรณีได้รับอนุญาต 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 มาจากโรงงานผลิตทันทีที่นำอุปกรณ์มาใช้งาน 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 และ จัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งาน เครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการสำนักเทคโนโลยีสารสนเทศทราบทันที

๒.๙ การใช้จดหมายอิเล็กทรอนิกส์ (Email)

- ๒.๙.๑ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Email) ต้องทำการกรอกข้อมูล คำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงานลงในแบบฟอร์ม โดยยื่น แบบฟอร์มกับเจ้าหน้าที่ ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส.
- ๒.๙.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่านโดยทันที
- ๒.๙.๓ ห้ามบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้
- ๒.๙.๔ ทำการเปลี่ยนรหัสผ่านทุก ๖ เดือน
- ๒.๙.๕ ไม่ใช่ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานที่อยู่จดหมาย อิเล็กทรอนิกส์ดังกล่าว
- ๒.๙.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของ อคส. ผู้ใช้งาน จะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมาย อิเล็กทรอนิกส์อื่น ยกเว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. ขัดข้องและ ได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น
- ๒.๙.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง
- ๒.๙.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุก ปิ่น ยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็น ส่วนบุคคล โดยอ้างว่าเป็นความเห็นของ อคส. หรือก่อให้เกิดความเสียหายต่อ อคส.
- ๒.๙.๙ ห้ามใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เพื่อเผยแพร่ ข้อมูลข้อความ รูปภาพ หรือ สิ่งอื่นใด ซึ่งมีลักษณะขัดต่อศีลธรรม ความมั่นคงของประเทศ กฎหมาย หรือกระทบต่อ การดำเนินงานของ อคส. ตลอดจนเป็นการรบกวนผู้ใช้งานอื่น รวมทั้งผู้รับบริการของ อคส.
- ๒.๙.๑๐ ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล หัวจดหมายอีเมล ลายเซ็นในอีเมล หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด
- ๒.๙.๑๑ ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมลโดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าจะบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม
- ๒.๙.๑๒ ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมลพร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล
- ๒.๙.๑๓ ผู้ใช้งานต้องทำการส่งอีเมลให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมลฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน
- ๒.๙.๑๔ ห้ามผู้ใช้งานส่งอีเมลที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมลขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น

- ๒.๙.๑๕ ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่ง อีเมลหลอกลวง หรือการส่งอีเมลในลักษณะ ถูกโซ่โดยเด็ดขาด
- ๒.๙.๑๖ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมลที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ช่มชู้ ลามกอนาจาร การยั่วยุทางเพศ หรือ อีเมลที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมลที่กระทบต่อความ มั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด
- ๒.๙.๑๗ การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย อีเล็กทรอนิกส์หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เสร็จสิ้นต้องออกจาก ระบบ (Log out) ทุกครั้ง

๒.๑๐ การใช้เครือข่ายอินเทอร์เน็ต (Internet)

- ๒.๑๐.๑ ผู้ใช้งานที่ต้องการใช้เครือข่ายอินเทอร์เน็ต ต้องลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต โดย ยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบ สำนักเทคโนโลยีสารสนเทศ อคส. สำหรับบุคคลภายนอก จะต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศ หรือผู้ที่ได้รับมอบหมาย
- ๒.๑๐.๒ ไม่ใช้เครือข่ายคอมพิวเตอร์ของหน่วยงานที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อหา ประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความ มั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ ของผู้อื่น หรือข้อมูลที อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน
- ๒.๑๐.๓ ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อมูลที่ดีที่สุด ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้อง รับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่อง แม่ข่าย หรือ ข้อมูลที่ส่งผ่านระบบเครือข่าย
- ๒.๑๐.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของตนโดยเด็ดขาด หากเกิด ปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ เครือข่าย อินเทอร์เน็ตนั้นต้องเป็นผู้รับผิดชอบ
- ๒.๑๐.๕ ห้ามเปิดเผยข้อมูลของหน่วยงานที่เป็นความลับ หรือข้อมูลสำคัญที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต
- ๒.๑๐.๖ การดาวน์โหลดข้อมูลและโปรแกรมต่างๆ จากเครือข่ายอินเทอร์เน็ต ต้องกระทำด้วย ความ ระมัดระวัง และหากมีความจำเป็นต้องดาวน์โหลดไฟล์ขนาดใหญ่ ให้ดำเนินการ นอกเวลา ปฏิบัติงาน
- ๒.๑๐.๗ ห้ามดาวน์โหลดข้อมูลและโปรแกรมต่างๆ ที่ละเมิดลิขสิทธิ์ จากเครือข่ายอินเทอร์เน็ต
- ๒.๑๐.๘ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความลับของ หน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้เกิดความเสื่อมเสียต่อ ชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรขอ หน่วยงานอื่นๆ
- ๒.๑๐.๙ ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้ สำนักงานฯ และบุคคลผู้ที่เกี่ยวข้องกับสำนักงานฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำ ที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูก ดำเนินคดีตามกฎหมาย
- ๒.๑๐.๑๐ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อปอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่อง คอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๒.๑๐.๑๑ หลังจากใช้งานเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ Log out จากระบบการพิสูจน์ตัวตนจริง เพื่อป้องกันการเข้าใช้งานโดยบุคคลอื่น

๒.๑๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access control)

๒.๑๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๑๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการกำหนดสิทธิ หรือการมอบอำนาจ ดังนี้

๒.๑๑.๒.๑ กำหนดสิทธิของผู้ใช้งานแต่ละกลุ่มที่เกี่ยวข้อง เช่น

- อ่านอย่างเดียว
- สร้างข้อมูล
- ป้อนข้อมูล
- แก้ไข
- อนุมัติ
- ไม่มีสิทธิ

๒.๑๑.๒.๒ กำหนดเกณฑ์การระงับสิทธิ มอบอำนาจ ให้เป็นไปตามการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) ที่ได้กำหนดไว้

๒.๑๑.๒.๓ ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีสารสนเทศหรือผู้ดูแลระบบที่ได้รับมอบหมาย

๒.๑๑.๓ ขั้นตอนปฏิบัติเพื่อการจัดเก็บข้อมูล

๒.๑๑.๓.๑ จัดแบ่งประเภทของข้อมูลออกเป็น

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

๒.๑๑.๓.๒ จัดแบ่งระดับความสำคัญของข้อมูล ออกเป็น ๓ ระดับ คือ

- ข้อมูลที่มีระดับความสำคัญมากที่สุด
- ข้อมูลที่มีระดับความสำคัญปานกลาง
- ข้อมูลที่มีระดับความสำคัญน้อย

๒.๑๑.๓.๓ จัดแบ่งลำดับชั้นความลับของข้อมูล

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

๒.๑๑.๓.๔ จัดแบ่งระดับขั้นการเข้าถึง

- ระดับขั้นสำหรับผู้บริหาร

- ระดับขั้นสำหรับผู้ใช้งานทั่วไป
- ระดับขั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

๒.๑๑.๓.๕ การกำหนดเวลาที่ได้เข้าถึง

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

๒.๑๑.๓.๖ การกำหนดช่องทางที่สามารถเข้าถึง

- ผ่านระบบสารสนเทศที่ให้บริการ
- ผ่านทางจดหมายอิเล็กทรอนิกส์
- ผ่านทาง Teleworking
- ผ่านเครื่องมือ (Tools) การเข้าถึง

๒.๑๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)

๒.๑๒.๑ เครื่องคอมพิวเตอร์ลูกข่าย และเครื่องคอมพิวเตอร์แบบพกพา ต้องได้รับการติดตั้งโปรแกรมป้องกันไวรัส รุ่นล่าสุดที่ได้รับการอนุมัติ และต้องเปิดใช้งานตลอดเวลาที่ใช้งานเครื่อง

๒.๑๒.๒ เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส ต้องมีการปรับปรุงข้อมูลล่าสุด (Update Latest Pattern) อยู่เสมอ เครื่องให้บริการ เครื่องตั้งโต๊ะ และโน้ตบุ๊กทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

๒.๑๒.๓ เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก ๖ เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

๒.๑๒.๔ ห้ามเจ้าหน้าที่ทำการดาวน์โหลด แชนแนล หรือพีวีวีโดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

๒.๑๒.๕ ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

๒.๑๒.๖ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมัลแวร์ใดๆ ตัวอย่าง เช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมลบอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ขององค์การ

๒.๑๒.๗ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๒.๑๒.๘ ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายขององค์การ ได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์การ ก่อนเปิดใช้งานเสมอ

๒.๑๒.๙ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชันการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่ต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

ส่วนที่ ๓

แนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลัก และไฟล์โปรแกรมระบบงานที่สำคัญ ที่ทำหน้าที่ให้บริการข้อมูลที่ต้องการและทันสมัย และเตรียมความพร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้ กลับคืนได้ ภายในระยะเวลาที่เหมาะสม

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Information Security Management System : ISMS)

แนวปฏิบัติ

๓.๑ การสำรองสารสนเทศ

ต้องพิจารณาคัดเลือกระบบสารสนเทศที่สำคัญและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพ พร้อมใช้งาน โดยต้องจัดให้มีการดูแลอุปกรณ์ หรือระบบสำรองข้อมูลให้มีประสิทธิภาพ และพร้อมใช้งานตามแนวทางต่อไปนี้

- ๓.๑.๑ จัดทำบัญชีระบบสารสนเทศที่มีความสำคัญทั้งหมดของหน่วยงาน พร้อมทั้งกำหนดระบบสารสนเทศที่จะจัดทำระบบสำรอง และจัดทำระบบแผนเตรียมพร้อมกรณีฉุกเฉิน อย่างน้อย ปีละ 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/เวลา ชื่อ ข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น
 - ตรวจสอบข้อมูลทั้งหมดของระบบว่ามีการสำรองข้อมูลไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ ต่าง ๆ ที่เกี่ยวข้องกับระบบสารสนเทศ การจัดการข้อมูลในฐานข้อมูล เป็นต้น
 - จัดเก็บข้อมูลที่สำรองนั้นในสื่อเก็บข้อมูล โดยมีการพิมพ์ชื่อบนสื่อเก็บข้อมูลนั้นให้ สามารถแสดงถึงระบบซอฟต์แวร์ วันที่ เวลาที่สำรองข้อมูล และผู้รับผิดชอบในการ สำรองข้อมูลไว้อย่างชัดเจน
 - จัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้เกิดผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
 - ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ

- ทดสอบข้อมูลสำรองที่บันทึกไว้อย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ
- ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๓.๒ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน

- ๓.๒.๑ ต้องจัดทำระบบสำรองของระบบสารสนเทศหลักที่สำคัญของหน่วยงานไว้อย่างเพียงพอและต้องมีการทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ
- ๓.๒.๒ ต้องจัดทำแผนการกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยมีรายละเอียดดังนี้
 - การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการทำงานของหน่วยงาน และการให้บริการด้านเทคโนโลยีสารสนเทศ
 - การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
 - การดำเนินการเพื่อให้สามารถดำเนินงานของหน่วยงาน เป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
 - การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงานหน่วยงาน กลับสู่ภาวะปกติ เช่น การกำหนดแนวทางการฟื้นฟูความเสียหายให้กลับเข้าสู่การปฏิบัติงานตามปกติ เป็นต้น
- ๓.๒.๓ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง
- ๓.๒.๔ ต้องกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการ ด้วยวิธีการทางอิเล็กทรอนิกส์
- ๓.๒.๕ ต้องทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉิน อย่างน้อยปีละ ๑ ครั้ง
- ๓.๒.๖ ต้องทบทวนระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉิน ที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

ส่วนที่ ๔

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

กำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของหน่วยงาน เพื่อให้ระบบสารสนเทศของ อคส. มีความปลอดภัยและเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิด ขึ้นกับระบบสารสนเทศของ อคส. ได้

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ อ่างอิง

มาตรฐาน

COBIT ๕ แนว

ปฏิบัติ

๔.๑ การตรวจสอบและประเมินความเสี่ยง

- ๔.๑.๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit And Assessment) โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) และให้จัดทำ รายงานพร้อมข้อเสนอแนะอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ
- ๔.๑.๒. มีการจัดทำและทบทวนกระบวนการบริหารจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยมีการวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านสารสนเทศอย่างเหมาะสม รวมถึงการควบคุมและลดความเสี่ยงเหล่านั้น
- ๔.๑.๓. มีการทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง
- ๔.๑.๔. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูลล็อกแสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ
- ๔.๑.๕. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่ต้องตรวจสอบได้แบบอ่านได้อย่างเดียว
- ๔.๑.๖. กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี
- ๔.๑.๗. ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบและ ประเมินความเสี่ยงด้านสารสนเทศ โดยแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบสารสนเทศที่ให้บริการจริงหรือที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกัน เครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕

แนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับ ความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า

วัตถุประสงค์

เพื่อสร้างความรู้ ความเข้าใจและความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์การ โดยการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดฝึกอบรมให้ความรู้ ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวปฏิบัติขององค์การ

ผู้รับผิดชอบ

สำนักเทคโนโลยีสารสนเทศ

อ้างอิงมาตรฐาน

ISO/IEC ๒๗๐๐๑ : ๒๐๑๓ (Information Security Management System : ISMS)

แนวปฏิบัติ

๕.๑ การสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย

- ๕.๑.๑. จัดฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับ ภาระงาน บทบาทหน้าที่ในการปฏิบัติงานของของบุคลากร อย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน เพื่อเป็นการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ
- ๕.๑.๒. เผยแพร่ หรือประชาสัมพันธ์ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะกระจัดความรู้ หรือข้อควรระวังในรูปแบบที่เข้าใจง่าย โดยมีการปรับปรุงความรู้อย่างสม่ำเสมอ
- ๕.๑.๓. บุคลากรใหม่ต้องได้รับการอบรมเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องอย่างน้อยภายใน ๙๐ วันนับจากเข้าปฏิบัติหน้าที่