องค์การคลังสินค้า กระทรวงพาณิชย์
563 ถนนนนทบุรี ตำบลบางกระสอ อำเภอเมืองนนทบุรี จังหวัดนนทบุรี 11000
โทร. 0-2507-5267 แฟกซ์ 0-2507-5268

ประกาศองค์การคลังสินค้า
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ขององค์การคลังสินค้า (ฉบับทบทวน) ประจำปี ๒๕๖๘

.....

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

เพื่อให้การปฏิบัติงานและการบริหารงานมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล องค์การคลังสินค้าจึงเห็นควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้า เพื่อเป็นเครื่องมือให้กับผู้ใช้บริการ ผู้ดูแลระบบงาน และผู้เกี่ยวข้องกับระบบเครือข่ายคอมพิวเตอร์ทุกคน ใช้เป็นแนวทางในการดูแลรักษาความมั่นคงปลอดภัยของข้อมูลและระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้า โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศองค์การคลังสินค้า เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้า (ฉบับทบทวน) ประจำปี ๒๕๖๘”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓ องค์การคลังสินค้าได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การการคลังสินค้า 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 หรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ

๓.๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต

๓.๑.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต

๓.๑.๕ มีการควบคุมการเข้าถึงระบบสารสนเทศ โปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (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 เตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๓.๒.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบ สำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๓.๒.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรอง ระบบแผนเตรียมพร้อมกรณีฉุกเฉิน และทดสอบข้อมูลสำรองที่บันทึกไว้อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๓.๒.๕ มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

๓.๓ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

๓.๓.๑ องค์การคลังสินค้าต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ (Information Security Audit and Assessment) อย่างน้อยปีละ ๑ ครั้ง

๓.๓.๒ ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์การคลังสินค้า (Internal Auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) เพื่อให้องค์การคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๓.๔ นโยบายการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร

๓.๔.๑ องค์การคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ

๓.๔.๒ จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับแนวปฏิบัติขององค์การคลังสินค้า

ข้อ ๔ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปอย่างมีประสิทธิภาพ จึงได้ข้อกำหนดให้สำนักเทคโนโลยีดิจิทัลและผู้เกี่ยวข้อง ดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้าให้ประกาศให้เจ้าหน้าที่ทุกระดับสำนักงานรับทราบทุกครั้ง

ข้อ ๕ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง จึงให้ใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสานสนเทศขององค์การคลังสินค้า ตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่และผู้เกี่ยวข้องจะต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศฉบับนี้มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๓๐ กันยายน พ.ศ. ๒๕๖๘

(นายกฤษณรักษ์ ใจดี)
ผู้ช่วยผู้อำนวยการองค์การคลังสินค้า
ปฏิบัติงานแทนผู้อำนวยการองค์การคลังสินค้า

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้า (ฉบับทบทวน) ประจำปี ๒๕๖๘

คำนำ

ระบบเทคโนโลยีสารสนเทศเป็นสิ่งสำคัญสำหรับสำนักงานในปัจจุบัน เพราะเข้ามาช่วยอำนวยความสะดวกในการดำเนินงาน ทำให้การเข้าถึงข้อมูลมีความรวดเร็ว การติดต่อสื่อสารมีประสิทธิภาพ และช่วยประหยัดต้นทุนในการดำเนินงานด้านต่างๆ ของสำนักงาน แต่ในขณะเดียวกันก็ทำให้สำนักงานมีความเสี่ยงเพิ่มขึ้นจากภัยคุกคามของระบบเทคโนโลยีสารสนเทศ ซึ่งอาจสร้างความเสียหายต่อการปฏิบัติงานขององค์กรได้เนื่องจากระบบเทคโนโลยีสารสนเทศมีการเชื่อมโยงข้อมูลไปยังสำนักงานต่างๆ ส่งผลให้ช่องทางในการถูกบุกรุกเปิดกว้างขึ้นและอาจก่อให้เกิดเหตุอาชญากรรมทางคอมพิวเตอร์กับสำนักงานได้หลายรูปแบบ เช่น โปรแกรมประสงค์ร้าย หรือการบุกรุกโจมตีผ่านระบบเครือข่ายอินเทอร์เน็ต เพื่อก่อกวนให้ระบบใช้การไม่ได้ รวมถึงการขโมยข้อมูลหรือความลับทางราชการ ส่งผลให้สำนักงานสูญเสียชื่อเสียงหรือภาพพจน์ได้ ดังนั้นผู้ใช้บริการและผู้ดูแลระบบงานด้านเทคโนโลยีสารสนเทศและการสื่อสาร จึงมีความจำเป็นจะต้องตระหนักถึงการดูแลบำรุงรักษา และการควบคุมรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นอย่างยิ่ง

ดังนั้น สำนักเทคโนโลยีดิจิทัล องค์การคลังสินค้า จึงจัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า เพื่อให้การดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์มีความมั่นคงปลอดภัยและเชื่อถือได้ และเพื่อให้มีมาตรการป้องกัน รับมือ และลดความเสี่ยงจากภัยคุกคามทางไซเบอร์ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล และให้การดำเนินการของหน่วยงานภายใน เป็นไปในทิศทางเดียวกัน สอดคล้องกับกฎหมายและระเบียบปฏิบัติที่เกี่ยวข้อง

ทั้งนี้ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า นั้นต้องได้รับความร่วมมือในการปฏิบัติตามอย่างเคร่งครัดและต้องทำอย่างต่อเนื่อง มีการตรวจสอบอย่างสม่ำเสมอ และปรับปรุงเพื่อให้สอดคล้องกับการพัฒนาของเทคโนโลยีที่เปลี่ยนแปลงไปอย่างรวดเร็วจึงหวังเป็นอย่างยิ่งว่านโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศฉบับนี้จะเป็นเครื่องมือให้กับผู้ใช้งาน ผู้ดูแลระบบ และผู้ที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้าทุกคน ในการดูแลรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้าต่อไป

สารบัญ

	หน้า
ส่วนที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ	
บทที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัย ด้านสารสนเทศ	๑
บทที่ ๒ คำนิยาม	๕
บทที่ ๓ อำนาจหน้าที่	๘
ส่วนที่ ๒ แนวปฏิบัติการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ	
๒.๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)	๑๐
๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)	๑๒
๒.๓ การควบคุมการเข้าถึงเครือข่าย (Network Access Control)	๑๕
๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)	๑๗
๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ	๑๘
๒.๖ การควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center)	๑๙
๒.๗ การควบคุมการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย (Server Access Control)	๒๐
๒.๘ การควบคุมการเข้าถึงเครือข่ายไร้สาย (Wireless Network Access Control)	๒๐
๒.๙ การใช้จดหมายอิเล็กทรอนิกส์ (Email)	๒๑
๒.๑๐ การใช้เครือข่ายอินเตอร์เน็ต (Internet)	๒๒
๒.๑๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ (Access Control)	๒๒
๒.๑๒ การป้องกันโปรแกรมไม่ประสงค์ดี (Control Against Malware)	๒๔
ส่วนที่ ๓ แนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ	๒๕
๓.๑ การสำรองสารสนเทศ	๒๕
๓.๒ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน	๒๖
ส่วนที่ ๔ แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๒๗
ส่วนที่ ๕ แนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย ด้านสารสนเทศขององค์การคลังสินค้า	๒๘
ส่วนที่ ๖ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านกายภาพ และสภาพแวดล้อม	๒๙
ส่วนที่ ๗ แนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก	๓๐
ส่วนที่ ๘ แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์ (Communications and Network Security)	๓๑
๘.๑ แนวทางปฏิบัติการควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer)	๓๑
๘.๒ แนวทางปฏิบัติการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)	๓๒
ส่วนที่ ๙ แนวปฏิบัติการบริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ (IT Asset, Data and Information Security Management)	๓๓
ส่วนที่ ๑๐ แนวปฏิบัติการใช้บริการคลาวด์	๓๕

เอกสารแนบท้ายประกาศองค์การคลังสินค้า

ส่วนที่ ๑

เรื่อง การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ องค์การคลังสินค้า

บทที่ ๑ การรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ

๑.๑ นโยบายการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๑.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน (User access management) เพื่อควบคุมการเข้าถึงข้อมูลและระบบสารสนเทศให้มีความมั่นคงปลอดภัย เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ต้องกำหนดให้มีขั้นตอนการปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการถอดถอนสิทธิ์ผู้ใช้งาน เมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

(๒) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน (User Access Provisioning) การจัดการสิทธิ์การเข้าถึงของผู้ใช้งาน ต้องกำหนดให้มีวิธีการในการบริหารจัดการสิทธิ์การเข้าถึงทั้งการให้สิทธิ์และการถอดถอนสิทธิ์ ต้องมีระเบียบวิธีการกำหนดไว้สำหรับผู้ใช้งานทุกประเภท ทุกระบบในองค์กร

(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) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่านการใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

(๒) การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล

(๓) การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear desk and clear screen policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เอกสาร สื่อบันทึกข้อมูลคอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

(๔) ผู้ใช้งานอาจนำการเข้ารหัส มาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

๑.๑.๓ มีการควบคุมการเข้าถึงเครือข่าย (Network access control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

(๑) ต้องควบคุมการเข้าถึงเครือข่ายและบริการบนเครือข่ายโดยเฉพาะ เพื่อรักษาความมั่นคงปลอดภัยให้แก่ข้อมูลและระบบเทคโนโลยีสารสนเทศ

(๒) การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

(๓) การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกหน่วยงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของหน่วยงานได้

(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) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

(๓) การบริหารจัดการรหัสผ่าน (Password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสผ่านที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงาน

ในลักษณะอัตโนมัติ 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 โปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (System and Application Access Control) โดยต้องมีการควบคุม อย่างน้อยดังนี้

(๑) การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงสารสนเทศและฟังก์ชัน (Functions) ต่างๆ ของโปรแกรมประยุกต์หรือแอพพลิเคชั่น ทั้งนี้โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงสารสนเทศที่ได้กำหนดไว้

(๒) การกำหนดขั้นตอนปฏิบัติสำหรับการเข้าสู่ระบบที่มีความมั่นคงปลอดภัย (Secure log-on Procedure) โดยกำหนดให้ระบบปฏิเสธการให้บริการ หากผู้ใช้งานพิมพ์รหัสผ่านผิดพลาดเกินจำนวนครั้งที่กำหนด

(๓) ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อหน่วยงาน ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกหน่วยงาน (Mobile computing and teleworking)

(๔) การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดแนวปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และ สื่อสารเคลื่อนที่

(๕) การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) ต้องกำหนดแนวปฏิบัติ แผนงานและขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานของหน่วยงานจากภายนอกหน่วยงาน

(๖) การใช้โปรแกรมอรรถประโยชน์ที่อาจละเมิดมาตรการความมั่นคงปลอดภัยของระบบต้องมีการจำกัดและควบคุมการใช้อย่างใกล้ชิด

(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 สำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูล รวมทั้งระดับขั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

๑.๒ นโยบายการจัดทำระบบสำรองของสารสนเทศ

(๑) ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

(๒) ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

(๓) ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และการจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

(๔) ต้องมีการทดสอบสภาพพร้อมใช้งานของระบบสารสนเทศ ระบบสำรองระบบแผนเตรียมพร้อมกรณีฉุกเฉิน และทดสอบข้อมูลสำรองที่บันทึกไว้ อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

(๕) มีการปฏิบัติและทบทวนแนวทางจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

(๖) มีแผนการรับมือภัยคุกคามทางไซเบอร์ ทั้งนี้ เพื่อประโยชน์ในการจัดทำประมวลแนวทางปฏิบัติด้านการรักษาความมั่นคงปลอดภัยไซเบอร์ ให้สำนักงานโดยความเห็นชอบของคณะกรรมการจัดทำประมวลแนวทางปฏิบัติและกรอบมาตรฐานสำหรับให้หน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศนำไปใช้เป็นแนวทางในการจัดทำหรือนำไปใช้เป็นประมวลแนวทางปฏิบัติของหน่วยงานของรัฐ หน่วยงานควบคุมหรือกำกับดูแล หรือหน่วยงานโครงสร้างพื้นฐานสำคัญทางสารสนเทศของตน และในกรณีที่หน่วยงานยังไม่มีหรือมีแต่ไม่ครบถ้วนหรือไม่สอดคล้องกับประมวลแนวทางปฏิบัติและกรอบมาตรฐาน ให้นำประมวลแนวทางปฏิบัติและกรอบมาตรฐานดังกล่าวไปใช้บังคับ

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) องค์การคลังสินค้าต้องจัดให้มีการสร้างความรู้และความเข้าใจ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมถึงกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม โดยเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และแจ้งให้เจ้าหน้าที่ทราบและถือปฏิบัติ

(๒) จัดอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับแนวปฏิบัติขององค์การคลังสินค้า

บทที่ ๒ คำนิยาม

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ประกอบด้วยคำนิยาม ดังนี้

ผู้บริหารระดับสูงสุด (CEO) หมายความว่า ผู้อำนวยการองค์การคลังสินค้า

ผู้บังคับบัญชา หมายความว่า ผู้มีอำนาจสั่งการตามโครงสร้างการบริหารของ อคส.

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) หมายความว่า ผู้มีอำนาจในด้านเทคโนโลยีสารสนเทศของ อคส.

สำนักเทคโนโลยีดิจิทัล หมายความว่า หน่วยงานที่ให้บริการด้านเทคโนโลยีดิจิทัล ให้คำปรึกษา พัฒนา ปรับปรุง บำรุงรักษาระบบงาน ระบบคอมพิวเตอร์และเครือข่ายภายใน อคส.

การรักษาความมั่นคงปลอดภัย หมายความว่า การรักษาความมั่นคงปลอดภัยสำหรับระบบสารสนเทศของ อคส. "แนวทางปฏิบัติ (Guideline)" หมายถึง แนวทางที่ไม่ได้บังคับให้ปฏิบัติ แต่แนะนำให้ปฏิบัติตามเพื่อให้สามารถบรรลุเป้าหมายได้ง่ายขึ้น

ผู้ใช้งาน หมายความว่า บุคคลที่ได้รับอนุญาต (Authorized User) ให้สามารถเข้าใช้งาน บริหาร หรือดูแลรักษาระบบสารสนเทศขององค์กร โดยมีสิทธิและหน้าที่ขึ้นอยู่กับบทบาท (Role)

ผู้บริหาร หมายความว่า ผู้มีอำนาจบริหารในระดับสูงของ อคส. เช่น ผู้อำนวยการสำนัก/ส่วนงาน เป็นต้น

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

เจ้าหน้าที่ หมายความว่า พนักงาน ลูกจ้างประจำ ลูกจ้างชั่วคราว ลูกจ้างโครงการต่างๆ พนักงานจ้างเหมาของ อคส.

หน่วยงานภายนอก หมายความว่า องค์กรหรือหน่วยงานภายนอกที่ อคส. อนุญาตให้มีสิทธิ์ในการเข้าถึงและใช้งาน ข้อมูลหรือทรัพย์สินต่างๆ ของ อคส. โดยจะได้รับสิทธิ์ในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการ รักษาความลับข้อมูลของ อคส.

ข้อมูล หมายความว่า สิ่งที่สื่อความหมายให้รู้เรื่องราว ข้อเท็จจริง หรือสิ่งใด ๆ ไม่ว่าการสื่อความหมายนั้นจะทำได้ โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และไม่ว่าจะได้จัดทำไว้ในรูปแบบของเอกสาร แฟ้ม รายงาน หนังสือ แผนผัง แผนที่ ภาพวาด ภาพถ่าย ฟิล์ม การบันทึกภาพหรือเสียง การบันทึกโดยเครื่องคอมพิวเตอร์ หรือ วิธีอื่นใดที่ทำให้สิ่งที่บันทึกไว้ปรากฏได้

สารสนเทศ (Information) หมายความว่า ข้อเท็จจริงที่ได้จากการนำข้อมูลมาผ่านการประมวลผล การจัดระเบียบ ให้ข้อมูลซึ่งอาจอยู่ในรูปของตัวเลข ข้อความ หรือภาพกราฟฟิก ให้เป็นระบบที่ผู้ใช้ สามารถเข้าใจได้ง่าย และ สามารถนำไปใช้ประโยชน์ในการบริหาร การวางแผน การตัดสินใจและอื่นๆ

ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยมีการ กำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูล โดยอัตโนมัติ

ระบบเครือข่าย (Network System) หมายความว่า ระบบที่สามารถใช้ในการติดต่อสื่อสารหรือการส่งข้อมูลและ สารสนเทศระหว่างระบบสารสนเทศต่างๆ ขององค์กรได้

- **ระบบแลน (LAN) และอินทราเน็ต (Intranet)** หมายความว่า ระบบเครือข่ายที่เชื่อมต่อระบบคอมพิวเตอร์ต่างๆ ภายใน หน่วยงานเข้าด้วยกัน เป็นเครือข่ายที่มีจุดประสงค์เพื่อการติดต่อสื่อสาร แลกเปลี่ยนข้อมูลและสารสนเทศภายในหน่วยงาน

- **ระบบอินเทอร์เน็ต (Internet)** หมายความว่า ระบบเครือข่ายที่เชื่อมต่อระบบเครือข่ายคอมพิวเตอร์ต่างๆ ของหน่วยงาน เข้ากับเครือข่ายคอมพิวเตอร์ทั่วโลก
- **SSID (Service Set Identifier)** หมายความว่า บริการที่ระบุชื่อของเครือข่ายไร้สายแต่ละเครือข่ายที่ไม่ซ้ำกัน โดยที่ทุกๆ เครื่องในระบบต้องตั้งค่า SSID ค่าเดียวกัน
- **WPA (Wi-Fi Protected Access)** หมายความว่า ระบบการเข้ารหัสเพื่อรักษาความปลอดภัยของข้อมูลในเครือข่ายไร้สาย
- **VPN (Virtual Private Network)** หมายความว่า เครือข่ายคอมพิวเตอร์เสมือนส่วนตัว โดยในการรับส่งข้อมูลจริงจะทำการเข้ารหัสเฉพาะแล้วรับส่งผ่านเครือข่ายอินเทอร์เน็ต ทำาให้บุคคลอื่นไม่สามารถอ่านได้และมองไม่เห็นข้อมูลนั้นไปจนถึงปลายทาง
- **ไฟร์วอลล์ (Firewall)** หมายความว่า เทคโนโลยีป้องกันการบุกรุกจากบุคคลภายนอก เพื่อไม่ให้ผู้ที่ไม่ได้รับอนุญาตเข้ามาใช้ข้อมูลและทรัพยากรในเครือข่าย โดยอาจใช้ทั้งฮาร์ดแวร์และซอฟต์แวร์ในการรักษาความปลอดภัย
- **MAC Address (Media Access Control Address)** หมายความว่า หมายเลขเฉพาะที่ใช้อ้างถึงอุปกรณ์ที่ต่อกับระบบเครือข่าย หมายเลขนี้จะมากับอีเทอร์เน็ตการ์ด โดยแต่ละการ์ดจะมีหมายเลขที่ไม่ซ้ำกันตัวเลขจะอยู่ในรูปของเลขฐาน ๑๖ จำนวน ๖ คู่ ตัวเลขเหล่านี้จะมีประโยชน์ไว้ใช้สำหรับการส่งผ่านข้อมูลไปยังต้นทางและปลายทางได้อย่างถูกต้อง
- **เลขที่อยู่ไอพี (IP Address)** หมายความว่า ตัวเลขประจำเครื่องคอมพิวเตอร์ที่ต่ออยู่ในระบบเครือข่าย ซึ่งเลขที่อยู่ไอพีของแต่ละเครื่องจะต้องไม่ซ้ำกัน โดยประกอบด้วยชุดของตัวเลข ๔ ส่วน หรือ ๖ ส่วน ที่คั่นด้วยเครื่องหมายจุด (.)
- **อุปกรณ์จัดเส้นทาง (Router)** หมายความว่า อุปกรณ์ที่ใช้ในระบบเครือข่ายคอมพิวเตอร์ทำหน้าที่จัดเส้นทางและค้นหาเส้นทาง เพื่อส่งข้อมูลต่อไปยังระบบเครือข่ายอื่น

ระบบสารสนเทศ (Information System) หมายความว่า ระบบงานของหน่วยงานที่นำเอาระบบคอมพิวเตอร์ และระบบการสื่อสารมาช่วยในการสร้างสารสนเทศที่สามารถนำมาใช้ประโยชน์ในการดำเนินการต่างๆ ของ หน่วยงาน

เจ้าของข้อมูล หมายความว่า ผู้ได้รับมอบอำนาจจากผู้บังคับบัญชาให้รับผิดชอบข้อมูลของระบบสารสนเทศ โดย เจ้าของข้อมูลเป็นผู้รับผิดชอบข้อมูลนั้น ๆ หรือ ได้รับผลกระทบโดยตรงหากข้อมูลเหล่านั้นเกิดสูญหาย

สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศ ของหน่วยงาน ตามที่กำหนดในภารกิจของผู้ใช้งาน (User Role)

สินทรัพย์ หมายความว่า ข้อมูล และทรัพย์สินด้านเทคโนโลยีดิจิทัลของหน่วยงาน

การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน หรือบุคคลภายนอก เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ

ความมั่นคงปลอดภัยด้านสารสนเทศ หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้อง ครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศ ทั้งนี้รวมถึงคุณสมบัติในด้านความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของการบริการหรือเครือข่าย ที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่านโยบายด้านความ มั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคง ปลอดภัย

สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตีและความมั่นคงปลอดภัยถูกคุกคาม

จดหมายอิเล็กทรอนิกส์ (Email) หมายความว่า ระบบที่บุคคลใช้ในการรับส่งข้อความระหว่างกันโดยผ่านเครื่อง คอมพิวเตอร์และเครือข่ายที่เชื่อมโยงถึงกัน ข้อมูลที่ส่งจะเป็นได้ทั้งตัวอักษร ภาพถ่าย ภาพกราฟฟิก ภาพเคลื่อนไหว และเสียง ผู้ส่งสามารถส่งข่าวสารไปยังผู้รับคนเดียวหรือหลายคนก็ได้ มาตรฐานที่ใช้ในการรับส่งข้อมูลชนิดนี้ได้แก่ SMTP, POP๓ และ IMAP

ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. หมายความว่า ระบบจดหมายอิเล็กทรอนิกส์ของ สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน) (สพร.) หรือสำนักงานปลัด กระทรวงพาณิชย์ ซึ่งอนุญาตให้ผู้ใช้งานใช้เพื่อการดำเนินงานของ อคส.

รหัสผ่าน (Password) หมายความว่า ตัวอักษรหรืออักขระหรือตัวเลข ที่ใช้เป็นเครื่องมือในการตรวจสอบยืนยันตัวบุคคล เพื่อควบคุมการเข้าถึงและรักษาความมั่นคงปลอดภัยของข้อมูลและระบบสารสนเทศ

ซอฟต์แวร์ประสงค์ร้าย (Malware) หมายความว่า ซอฟต์แวร์ที่ถูกสร้างขึ้นมาเพื่อทำลาย หรือสร้างความเสียหายให้กับระบบสารสนเทศ การโจรกรรมข้อมูล หรือการเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

ผู้บุกรุก หมายความว่า บุคคลที่เข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

บทที่ ๓ อำนาจหน้าที่

ให้ผู้บริหารระดับสูงสุดขององค์การคลังสินค้า ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลและผู้ดูแลระบบสารสนเทศมีอำนาจหน้าที่ในการรักษาความ ปลอดภัยของข้อมูลและเครือข่ายคอมพิวเตอร์ ดังนี้

๓.๑ ให้ผู้บริหารระดับสูงสุดขององค์การคลังสินค้า (Chief Executive Officer: CEO) มีอำนาจหน้าที่รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่เกิดขึ้นกับหน่วยงาน หรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๒ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (Chief Information Officer: CIO) มีอำนาจหน้าที่ดังต่อไปนี้

๓.๒.๑ รับผิดชอบงานด้านเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

๓.๒.๒ รับผิดชอบกำกับดูแล การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

๓.๒.๓ จัดทำแผนแม่บทเทคโนโลยีสารสนเทศ

๓.๒.๔ มีอำนาจในการจัดสรรทรัพยากรในการดำเนินโครงการเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

๓.๒.๕ ดำเนินการเรื่องอื่นตามที่ได้รับมอบหมาย

๓.๓ ให้ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล มีอำนาจหน้าที่ดังต่อไปนี้

๓.๓.๑ ให้คำแนะนำ และข้อเสนอแนะต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง/หรือคณะกรรมการฯ ในการกำหนดนโยบาย ประกาศและมาตรการด้านสารสนเทศ

๓.๓.๒ กำกับ ดูแล และควบคุมการให้บริการด้านระบบสารสนเทศ และการปฏิบัติตามแนวนโยบายและแนวปฏิบัติด้านการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๓.๓ ต้องควบคุมการจำหน่ายอุปกรณ์คอมพิวเตอร์หรือการนำสื่อบันทึกข้อมูลกลับมาใช้งานอีกครั้ง ดังนี้

(๑) ให้ทำลายข้อมูลสำคัญในสื่อบันทึกข้อมูลก่อนที่จะแทงจำหน่ายอุปกรณ์ดังกล่าว (ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูล

(๒) มีมาตรการหรือเทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญใน อุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญนั้นได้

๓.๔ ผู้ดูแลระบบสารสนเทศ มีหน้าที่ดังต่อไปนี้

๓.๔.๑ ดูแลรักษาและปรับปรุงระบบสารสนเทศให้สามารถใช้งานได้ดีอยู่เสมอ

๓.๔.๒ ควบคุมดูแลผู้ใช้บริการให้ปฏิบัติตามกฎระเบียบการใช้งานระบบสารสนเทศของ องค์การคลังสินค้า

๓.๔.๓ กรณีพบว่าผู้ใช้บริการไม่ปฏิบัติตามระเบียบการใช้งานระบบสารสนเทศขององค์การคลังสินค้า ผู้ดูแลระบบสารสนเทศจะต้องรายงานให้ผู้บริหารเทคโนโลยีสารสนเทศ ระดับสูงทราบโดยเร็วที่สุด และในกรณีจำเป็นเพื่อป้องกันความเสียหายที่อาจจะเกิดขึ้น ผู้ดูแลระบบสารสนเทศมีอำนาจในการระงับการใช้งานของผู้ใช้บริการ ดังกล่าวได้ทันที

๓.๔.๔ ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการเสนอความเห็นต่อผู้อำนวยการสำนัก เพื่อพิจารณาสั่งการเกี่ยวกับการปรับปรุงประสิทธิภาพและการบริหารจัดการระบบสารสนเทศ

๓.๔.๕ ผู้ดูแลระบบสารสนเทศมีหน้าที่ในการติดตั้งอุปกรณ์ ซอฟต์แวร์ ระบบการเข้ารหัส ข้อมูลอัตโนมัติ (Encryption) หรือระบบอื่นใดที่เกี่ยวข้องกับระบบเครือข่าย สารสนเทศ และอุปกรณ์คอมพิวเตอร์ ตลอดจนบำรุงรักษาสิ่งต่าง ๆ ดังกล่าวให้ใช้ งานได้ดีอยู่เสมอ

๓.๔.๖ ผู้ดูแลระบบสารสนเทศมีหน้าที่รับผิดชอบระบบสารสนเทศ ระบบสำรอง และการ จัดทำแผนการสำรองข้อมูล แผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถ ดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ และมีหน้าที่ในการทดสอบสภาพพร้อมใช้งาน การทำสำรองข้อมูล และการทดสอบการกู้คืนข้อมูลตามระยะเวลาที่เหมาะสม

ส่วนที่ ๒

แนวปฏิบัติในการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบ เครือข่ายจากผู้บุกรุก หรือจากซอฟต์แวร์ประสงค์ร้าย รวมทั้งกำหนดประเภทของข้อมูล ลำดับชั้น ความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

อ้างอิงมาตรฐาน

มาตรฐานการรักษาความมั่นคงปลอดภัยในการประกอบธุรกรรมทางอิเล็กทรอนิกส์ (เวอร์ชัน ๒. ๕)

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 การลงทะเบียนและการถอดถอนสิทธิ์ผู้ใช้งาน (User Registration and De-Registration) ให้ผู้ดูแลระบบงานหรือผู้ที่ ได้รับมอบหมายจัดทำแบบฟอร์มสำหรับลงทะเบียนผู้ใช้งานใหม่ ดังนี้

(๑) จัดทำแบบฟอร์มขอใช้ระบบงานสารสนเทศ และให้ผู้ใช้งานกรอกข้อมูลลงในแบบฟอร์ม เพื่อตรวจสอบสิทธิและดำเนินการตามขั้นตอนการลงทะเบียนผู้ใช้งาน

(๒) มีการระบุชื่อบัญชีผู้ใช้งานแยกกันเป็นรายบุคคล ไม่ซ้ำซ้อนกัน

(๓) การกำหนดชื่อผู้ใช้งาน (username) จะกำหนดจากชื่อภาษาอังกฤษและตามด้วยอักษรตัว แรกของนามสกุล หากซ้ำให้เพิ่มอักษรตัวที่สอง หรือจนกว่าจะ ไ ม่ซ้ำกับชื่อผู้ใช้งานคนอื่น

(๔) จำกัดการใช้งานบัญชีผู้ใช้งานแบบกลุ่มภายใต้บัญชีรายชื่อเดียวกันและอนุญาตให้ใช้เท่าที่จำเป็น

(๕) มีการตรวจสอบและมอบหมายสิทธิในการเข้าถึงที่เหมาะสมต่อหน้าที่ความรับผิดชอบ และ/หรือ ความต้องการทางธุรกิจ

(๖) จัดทำเอกสารแสดงถึงสิทธิและหน้าที่ความรับผิดชอบของผู้ใช้งานซึ่งต้องลงนามรับทราบด้วย

(๗) มีการทำบันทึกและจัดเก็บข้อมูลการขออนุมัติเข้าใช้ระบบสารสนเทศ

(๘) มีหลักเกณฑ์ในการอนุญาตให้เข้าถึงระบบสารสนเทศ และได้รับการพิจารณาอนุญาตจาก ผู้อำนวยการศูนย์หรือผู้ดูแลระบบที่ได้รับมอบหมาย

(๙) มีหลักเกณฑ์ในการยกเลิกเพิกถอนการอนุญาตให้เข้าถึงระบบสารสนเทศและการตัดออก จากทะเบียนของผู้ใช้งาน เมื่อมีการลาออก เปลี่ยนตำแหน่ง โอน

ย้าย หรือสิ้นสุดการจ้าง เป็นต้น

(๑๐) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งานนั้นต้องได้รับความเห็นชอบและอนุมัติจากผู้บังคับบัญชา โดยมีการกำหนด ระยะเวลาการใช้งานและระงับการใช้งานทันทีเมื่อพ้นระยะเวลาดังกล่าวหรือ พ้นจากตำแหน่ง และมีการกำหนดสิทธิพิเศษที่ได้รับว่าเข้าถึงได้ถึงระดับใด ได้บ้าง และต้องกำหนดให้รหัสผู้ใช้งานต่างจากรหัสผู้ใช้งานตามปกติ

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

๒.๑.๓.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) โดยแสดงรายละเอียด ที่เกี่ยวกับการ ควบคุมและจำกัดสิทธิเพื่อให้สามารถเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึง สิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่นๆ ที่เกี่ยวข้องกับการเข้าถึง ดังนี้

(๑) ผู้ใช้งานต้องลงทะเบียนผู้ใช้งานเพื่อนำข้อมูลไปตรวจสอบสิทธิก่อนการมอบหมายหรือกำหนดสิทธิการใช้งานให้แก่ผู้ใช้งาน

(๒) ต้องกำหนดระดับสิทธิในการเข้าถึงระบบสารสนเทศที่เหมาะสมตามหน้าที่ความรับผิดชอบ และตามความจำเป็นในการใช้งาน

(๓) การมอบหมายสิทธิต้องสอดคล้องกับนโยบายควบคุมการเข้าถึง

(๔) ต้องบันทึกและจัดเก็บข้อมูลการมอบหมายสิทธิให้แก่ผู้ใช้งาน

๒.๑.๓.๔ บริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management)

(๑) มีขั้นตอนปฏิบัติสำหรับการตั้งหรือเปลี่ยนรหัสผ่านที่มีความมั่นคงปลอดภัย

(๒) การตั้งรหัสผ่านชั่วคราวต้องยากต่อการสุ่ม และต้องมีความแตกต่างกัน

(๓) ส่งมอบรหัสผ่าน (password) ชั่วคราวให้กับผู้ใช้งานด้วยวิธีการที่ ปลอดภัย โดยหลีกเลี่ยงการใช้บุคคลอื่นหรือการส่งจดหมาย อิเล็กทรอนิกส์ (e-mail) ในการจัดส่งรหัสผ่าน และผู้ใช้งานควรตอบกลับ ทันที หลังจากได้รับรหัสผ่าน โดยจัดส่งบัญชีและรหัสผ่านใส่ซองปิดผนึก และประทับตรา "ลับ" และแนบเอกสารอื่นๆ ที่เกี่ยวข้องกับการ ปฏิบัติงานของผู้ใช้งาน ส่งมอบให้ผู้ใช้งาน และให้ผู้ใช้งานลงนามรับ เอกสารนั้น รวมทั้งแจ้งให้ผู้ใช้งานปฏิบัติตามเอกสารแนบดังกล่าวโดย เคร่งครัด

(๔) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านทันทีหลังจากได้รับรหัสผ่านชั่วคราว และควรเปลี่ยนให้รหัสผ่านยากต่อการเดา

(๕) เปลี่ยนรหัสผ่านทันทีหลังจากติดตั้งซอฟต์แวร์แล้ว

(๖) ต้องมีการลงนามเพื่อป้องกันการเปิดเผยข้อมูลรหัสผ่านของตน

(๗) การเปลี่ยนรหัสผ่านต้องตรวจสอบบัญชีชื่อผู้ใช้งานและรหัสผ่านปัจจุบันให้ถูกต้องก่อนที่จะอนุญาตให้เปลี่ยนรหัสใหม่

(๘) ในกรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งานที่มีสิทธิสูงสุด ผู้ใช้งาน นั้นจะต้องได้รับความเห็นชอบและอนุมัติจากผู้อำนวยการสำนัก เทคโนโลยีสารสนเทศ โดยมีการกำหนดระยะเวลาการใช้งานและระงับ การใช้งานทันที

เมื่อพ้นระยะเวลาดังกล่าวหรือพ้นจากตำแหน่ง 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 หรือการลักลอบทำสำเนาข้อมูล สารสนเทศ มีข้อปฏิบัติอย่างน้อย ดังนี้

๒.๒.๑ กำหนดวิธีปฏิบัติการใช้งานรหัสผ่าน (Password use) สำหรับผู้ใช้งาน เพื่อให้สามารถ กำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนหัสผ่านที่มีคุณภาพ 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 หลังจากดำเนินการเรียบร้อยให้ทำการเปลี่ยนรหัสผ่านโดยทันที

๒.๒.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานที่อุปกรณ์ ให้กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของหน่วยงานในขณะที่ไม่มีผู้ดูแล ดังนี้

๒.๒.๒.๑ ต้องออกจากระบบสารสนเทศทันทีที่เสร็จสิ้นการใช้งาน

๒.๒.๒.๒ ตั้งให้เครื่องคอมพิวเตอร์ล็อคหน้าจอหลังจากที่ไม่ได้ใช้งานเป็นเวลา 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

- ใกล้สิ้นปีงบประมาณต้องสำรวจทะเบียนครุภัณฑ์เครื่องคอมพิวเตอร์และอุปกรณ์ว่ายังสามารถใช้งานได้หรือไม่ จำนวนครบหรือไม่ ถ้าเกิดกรณีชำรุด/เสียหาย จะทำ เรื่องส่งซ่อม/ส่งคืนพัสดุ
- จัดห้องสำหรับรวบรวมเครื่องคอมพิวเตอร์และอุปกรณ์ที่จะส่งซ่อม/ส่งคืน และปิดล็อคห้องทุกครั้งหลังเข้า-ออก เพื่อป้องกันมิให้เครื่องคอมพิวเตอร์และอุปกรณ์สูญหาย
- การควบคุมการเข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ โดยการใช้การ์ดหรือสแกนนิ้วมือ ก่อนและหลังเข้า-ออกทุกครั้ง
- การจัดทำทะเบียนยืม-คืน อุปกรณ์คอมพิวเตอร์ โดยแบบฟอร์มขอใช้อุปกรณ์คอมพิวเตอร์ เพื่อใช้งานภายในและภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
- การจัดทำทะเบียนยืม-คืน โน้ตบุ๊ค โดยใช้แบบฟอร์มยืมโน้ตบุ๊ค เพื่อใช้งานภายใน และภายนอกองค์กร สำหรับควบคุมและป้องกันการสูญหาย
- การวางอุปกรณ์ มีการจัดที่เฉพาะและเหมาะสมสำหรับวางเครื่องคอมพิวเตอร์แม่ข่ายและอุปกรณ์ (Data Center)
- การจัดทำระบบเอกสารคุณภาพ (ISO ๙๐๐๑ : ๒๐๐๘) ใช้ในองค์กร

๒.๒.๓.๒ การนำเครื่องคอมพิวเตอร์ โน้ตบุ๊ค และอุปกรณ์ เข้า-ออก องค์การคลังสินค้าต้องได้รับการตรวจเช็คจากเจ้าหน้าที่ฝ่ายอาคาร อย่างเคร่งครัด

๒.๒.๓.๓ ต้องป้องกันการเข้าใช้งานเครื่องคอมพิวเตอร์ โดยใช้รหัสผู้ใช้งาน (Username) รหัสผ่าน (Password) เป็นการพิสูจน์ตัวตนที่เหมาะสมก่อนเข้าใช้งาน และมีการตั้งค่าพักหน้าจออัตโนมัติ เมื่อไม่ได้ใช้งาน

๒.๒.๓.๔ การป้องกันการใช้ทรัพย์สินอย่างมีประสิทธิภาพและปลอดภัย ดังนี้

- ทุกคนต้องตระหนักและปฏิบัติการใดๆ เพื่อป้องกันทรัพย์สินของหน่วยงาน
- Log out ออกจากระบบทันที เมื่อจำเป็นต้องปล่อยทิ้งโดยไม่มีผู้ดูแล
- จัดเก็บข้อมูลสำคัญในสถานที่ที่มีความปลอดภัย
- ล็อคเครื่องคอมพิวเตอร์ เมื่อไม่ได้ใช้งาน
- ป้องกันไม่ให้ผู้อื่นใช้อุปกรณ์ดังต่อไปนี้โดยไม่ได้รับอนุญาต ได้แก่ กล้องดิจิตอล เครื่องสำเนาเอกสาร เครื่องสแกนเอกสาร เป็นต้น
- นำเอกสารออกจากเครื่องพิมพ์ทันทีที่พิมพ์งานเสร็จ

๒.๒.๓.๕ การทำลายข้อมูลอิเล็กทรอนิกส์และสื่อบันทึกข้อมูลอิเล็กทรอนิกส์ ให้ปฏิบัติตามแนว

ทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ ดังนี้

(๑) ในการทำลายข้อมูลลับ ให้ปฏิบัติตามแนวทางการทำลายข้อมูลบนสื่อบันทึกข้อมูลประเภทต่างๆ

ประเภทสื่อบันทึกข้อมูล	วิธีการทำลาย
Flash Drive	ใช้วิธีการทุบหรือบดให้เสียหาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลาย CD/DVD
เทป	ใช้วิธีการทุบหรือบดให้เสียหายหรือเผาทำลาย
ฮาร์ดดิสก์	ใช้การทำลายข้อมูลบนฮาร์ดดิสก์ด้วยวิธีการฟอร์แมต (Format) ตามมาตรฐานการทำลายข้อมูลบน ฮาร์ดดิสก์ของกระทรวงกลาโหม สหรัฐอเมริกา DOD ๕๒๒๐.๓๓-M (ซึ่งมีการเขียนทับข้อมูลเดิมเป็นจำนวนหลายรอบ)

(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

(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 ลับที่สุด ได้เท่านั้น

(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 ควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

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

๒.๓.๕ ระบบยืนยันตัวบุคคลต้องสามารถกำหนดสิทธิการใช้งานระบบสารสนเทศต่างๆ ผ่านเครือข่ายตามบทบาทหน้าที่ของผู้ใช้ (User role) แต่ละคนได้

๒.๓.๖ การยืนยันตัวบุคคล สำหรับผู้ใช้งานที่อยู่ภายนอกหน่วยงาน (User authentication for external connections) ให้มีการยืนยันตัวบุคคล (Authentication) เพื่อแสดงว่าเป็นผู้ใช้งาน

ตัวจริง 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 แบบไดนามิค (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 องค์การคลังสินค้าได้มีการจัดแบ่งแยกเครือข่ายตามหน่วยงานระดับสำนักและตามหน้าที่เฉพาะ

๒.๓.๙.๒ กำหนดรหัสวงเครือข่าย (VLAN) ชื่อวงเครือข่าย IP Address และค่าอื่นๆ ที่ใช้ในการกำหนดในอุปกรณ์สวิทช์และอุปกรณ์ต่างๆที่เกี่ยวข้อง

๒.๓.๙.๓ มีการติดตั้งค่าอุปกรณ์ต่างๆ แล้วทำการทดสอบการใช้งานเครือข่ายแต่ละวง

๒.๓.๙.๔ จัดทำทะเบียนวงเครือข่ายและอุปกรณ์ต่างๆ ที่เกี่ยวข้อง

๒.๓.๙.๕ ผู้ดูแลระบบทำการบำรุงรักษา ตรวจเช็คการใช้งานเครือข่าย (Monitoring)

๒.๓.๙.๖ เมื่อมีการเปลี่ยนหน่วยงานจะมีการทบทวนและจัดการแบ่งแยกเครือข่ายตามโครงสร้างหน่วยงานใหม่

๒.๓.๑๐ การควบคุมการเชื่อมต่อทางเครือข่าย (Network connection control) ให้ควบคุม การเข้าถึง หรือใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือเชื่อมต่อระหว่างหน่วยงาน ดังนี้

๒.๓.๑๐.๑ ต้องตรวจสอบการเชื่อมต่อเครือข่ายของอุปกรณ์ต่างๆ ในศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์ (Data Center) อย่างน้อยเดือนละ ๑ ครั้ง

๒.๓.๑๐.๒ ต้องติดตั้งอุปกรณ์ ไฟร์วอลล์ เพื่อควบคุมการใช้งานเครือข่ายที่มีการใช้ร่วมกันหรือ

เชื่อมต่อระหว่างหน่วยงาน

๒.๓.๑๐.๓ ต้องตรวจจับผู้บุกรุกทั้งในระดับเครือข่าย และระดับเครื่องคอมพิวเตอร์แม่ข่าย

๒.๓.๑๑ การควบคุมการจัดเส้นทางบนเครือข่าย (Network routing control) ให้ทำการควบคุมการจัดเส้นทางบนเครือข่าย ดังนี้

๒.๓.๑๑.๑ ต้องกำหนดค่าโปรโตคอลสำหรับการหาเส้นทาง (Routing protocol) ที่สอดคล้องกับเครือข่ายหลักที่หน่วยงานเชื่อมต่อ

๒.๓.๑๑.๒ ต้องบันทึกข้อมูลแผนผังการจัดเส้นทางบนเครือข่ายและข้อมูลการตั้งค่าอุปกรณ์หาเส้นทาง

๒.๓.๑๑.๓ เมื่อมีความจำเป็นต้องเปลี่ยนการหาเส้นทางบนเครือข่าย ให้ผู้ดูแลทำการปรับปรุงข้อมูลที่บันทึกไว้และแจ้งผู้บังคับบัญชาทราบ

๒.๓.๑๑.๔ กำหนดให้มีการแปลงหมายเลขเครือข่าย (NAT) เพื่อแยกเครือข่ายย่อย

๒.๓.๑๒ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่ เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๓.๑๒.๑ กำหนดระบบสารสนเทศที่ต้องควบคุมการเข้าถึง โดยระบุเครือข่าย หรือบริการที่อนุญาตให้ใช้งานได้

๒.๓.๑๒.๒ กำหนดข้อปฏิบัติสำหรับผู้ใช้งานให้สามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๒.๓.๑๒.๓ กำหนดการใช้งานระบบสารสนเทศที่สำคัญ ระบบคอมพิวเตอร์โปรแกรมประยุกต์ (Application) จดหมายอิเล็กทรอนิกส์ (e-mail) ระบบเครือข่ายไร้สาย (Wireless LAN) ระบบอินเทอร์เน็ต (Internet) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจากผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิ ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง ซึ่งองค์การคลังสินค้ามีแบบฟอร์มการขอใช้บริการดังกล่าว โดยมีขั้นตอนการปฏิบัติดังนี้

- ผู้ใช้งานกรอกแบบฟอร์มขอใช้บริการ/แจ้งปัญหา และได้รับอนุมัติตามสาย งานผู้แจ้ง และส่งแบบฟอร์มมายังหน่วยงานผู้ดูแลระบบแล้ว
- ผู้ดูแลระบบดำเนินการวิเคราะห์และกำหนดสิทธิการใช้งาน พร้อมทั้งทำการทดสอบการใช้งานตามสิทธิ์ เมื่อสามารถใช้งานได้แล้ว จึงแจ้งรหัสผู้ใช้งาน (Username) และ รหัสผ่าน (Password) ปิดซองอย่างมิดชิด ส่งให้ผู้ขอใช้บริการ และให้ลงลายมือชื่อการใช้บริการ
- ผู้ดูแลระบบจัดทำรายงานสรุปการขอใช้บริการ/รับแจ้งปัญหารายไตรมาส
- สิ้นปีจะทำการทบทวนสิทธิ์การใช้งานตามรายชื่อผู้ใช้งานเทียบกับรายชื่อพนักงานที่ปฏิบัติงานอยู่ และรายชื่อบุคคลภายนอกหรือ Out Source ที่ขอ ใช้บริการ

๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control)

๒.๔.๑ ให้มีการกำหนดชื่อผู้ใช้ และรหัสผ่าน เพื่อยืนยันตัวตนในการเข้าใช้งานระบบปฏิบัติการ

๒.๔.๒ ผู้ใช้งานต้องไม่อนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ และรหัสผ่านของตนในการเข้าใช้งาน ระบบปฏิบัติการร่วมกัน

๒.๔.๓ ผู้ใช้งานต้องตั้งค่าการใช้งานโปรแกรมถนอมหน้าจอ 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 แต่ละครั้งไดไม่เกิน ๓ ช.ม.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 การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๒.๕.๑ การจำกัดการเข้าถึงสารสนเทศ (Information access restriction) ให้จำกัดสิทธิการใช้ งานโปรแกรมประยุกต์และสารสนเทศตามสิทธิของผู้ใช้งานหรือผู้รับจ้าง (Out Source) ที่ได้รับอนุญาตเท่านั้น

๒.๕.๒ ผู้ดูแลระบบต้องควบคุมการเข้าถึงข้อมูลแต่ละประเภทขั้นความลับทั้งการเข้าถึงโดยตรง และการเข้าถึงผ่านระบบงาน โดยกำหนดรายชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) เพื่อ

ใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ข้อมูลในแต่ละขั้นความลับของ 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 ให้ระบบสารสนเทศที่ใช้เฉพาะภายในหน่วยงานให้ติดตั้งในเครือข่ายภายใน ส่วนระบบสารสนเทศที่สามารถใช้งานผ่านเครือข่ายอินเทอร์เน็ตต้องติดตั้งอยู่หลังไฟร์วอลล์

๒.๕.๕.๒ ติดตั้งระบบสารสนเทศแต่ละระบบ บนสภาพแวดล้อมการประมวลผล (Computing environment) ที่แยกจากกัน เพื่อควบคุมสภาพแวดล้อมของระบบ

๒.๕.๖ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ให้ดำเนินการดังนี้

๒.๕.๖.๑ ผู้ใช้งานที่ต้องการนำอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงานต้องลงทะเบียนอุปกรณ์ดังกล่าวจึงจะสามารถใช้งานระบบเครือข่ายของหน่วยงานได้

๒.๕.๖.๒ บุคคลภายนอกหรือผู้รับจ้าง (Out Source) ที่ต้องการนำอุปกรณ์คอมพิวเตอร์และอุปกรณ์สื่อสารเคลื่อนที่ส่วนตัว มาใช้ในหน่วยงาน ให้สามารถใช้งานได้เฉพาะอินเทอร์เน็ต โดยให้ติดต่อผู้ดูแลระบบเพื่อขอชื่อผู้ใช้และรหัสผ่าน

๒.๕.๗ การปฏิบัติงานจากภายนอกหน่วยงาน (Teleworking) มีข้อกำหนดในการปฏิบัติงานดังนี้

๒.๕.๗.๑ ไม่ใช้เครื่องคอมพิวเตอร์สาธารณะในการเข้าใช้งานระบบสารสนเทศของหน่วยงาน

๒.๕.๗.๒ ไม่ใช้งานระบบสารสนเทศของหน่วยงานผ่านเครือข่ายที่ไม่น่าเชื่อถือ เครือข่ายในร้านอินเทอร์เน็ต เครือข่ายไร้สายที่ไม่ได้ให้บริการโดยผู้ให้บริการอินเทอร์เน็ต หรือหน่วยงานภาครัฐ เป็นต้น

๒.๕.๗.๓ 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-ออกในห้องควบคุมของหน่วยงานเท่านั้น

๒.๖.๑.๓ มีกล้องวงจรปิดบันทึกผู้เข้า-ออก ห้องควบคุมระบบคอมพิวเตอร์ เพื่อเฝ้าระวังควบคุมการรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาตรวมทั้ง ป้องกันความเสียหายอื่นๆที่อาจเกิดขึ้นได้

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 (Server Access Control)

๒.๗.๑ ผู้ใช้งานจะนำเครื่องคอมพิวเตอร์และอุปกรณ์มาเชื่อมต่อกับเครื่องคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายของหน่วยงาน ต้องได้รับอนุญาตจากผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล และต้องปฏิบัติตามนโยบายนี้โดย เคร่งครัด

๒.๗.๒ การขออนุญาตใช้งานพื้นที่ Web Server และชื่อโดเมนย่อย (Sub Domain Name) ที่หน่วยงานรับผิดชอบอยู่ จะต้องทำหนังสือขออนุญาตต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง หรือ ผู้อำนวยการสำนักเทคโนโลยีดิจิทัล 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 ผู้ดูแลระบบใช้ซอฟต์แวร์หรือฮาร์ดแวร์ตรวจสอบความมั่นคงปลอดภัยของเครือข่ายไร้ สายเพื่อคอยตรวจสอบและบันทึกเหตุการณ์น่าสงสัยที่เกิดขึ้นในเครือข่ายไร้สาย และ จัดส่งรายงานผลการตรวจสอบทุก ๓ เดือน และในกรณีที่ตรวจสอบพบการใช้งาน เครือข่ายไร้สายที่ผิดปกติ ให้ผู้ดูแลระบบรายงานให้ผู้อำนวยการสำนักเทคโนโลยีดิจิทัลทราบทันที

๒.๙ การใช้จดหมายอิเล็กทรอนิกส์ (Email)

๒.๙.๑ ในการลงทะเบียนบัญชีผู้ใช้งานจดหมายอิเล็กทรอนิกส์ (Email) ต้องทำการกรอกข้อมูล คำขอเข้าใช้บริการจดหมายอิเล็กทรอนิกส์ ของหน่วยงานลงในแบบฟอร์ม โดยยื่น แบบฟอร์มกับเจ้าหน้าที่ ผู้ดูแลระบบ สำนักเทคโนโลยีดิจิทัล อคส.

๒.๙.๒ เมื่อมีการเข้าสู่ระบบจดหมายอิเล็กทรอนิกส์ในครั้งแรกนั้น ต้องเปลี่ยนรหัสผ่านโดยทันที

๒.๙.๓ ห้ามบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์ หรือเก็บไว้ในที่ที่สังเกตได้

๒.๙.๔ ทำการเปลี่ยนรหัสผ่านทุก ๖ เดือน

๒.๙.๕ ไม่ใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (Email Address) ของผู้อื่นเพื่ออ่านหรือรับหรือส่ง ข้อความ ยกเว้นแต่จะได้รับการยินยอมจากเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์ และให้ ถือว่าเจ้าของที่อยู่จดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานที่อยู่จดหมาย อิเล็กทรอนิกส์ดังกล่าว

๒.๙.๖ การส่งจดหมายอิเล็กทรอนิกส์ให้กับผู้รับบริการ หรือตามภารกิจของ อคส. ผู้ใช้งาน จะต้องใช้ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เท่านั้น ห้ามไม่ให้ใช้ระบบจดหมาย อิเล็กทรอนิกส์อื่น เว้นแต่ในกรณีที่ระบบจดหมายอิเล็กทรอนิกส์ของ อคส. ขัดข้องและ ได้รับการอนุญาตจากผู้บังคับบัญชาแล้วเท่านั้น

๒.๙.๗ การใช้งานจดหมายอิเล็กทรอนิกส์ ผู้ใช้งานต้องไม่ปลอมแปลงชื่อบัญชีผู้ส่ง

๒.๙.๘ การใช้งานจดหมายอิเล็กทรอนิกส์ ต้องใช้ภาษาสุภาพ ไม่ขัดต่อจริยธรรม ไม่ทำการปลุก ปั่นยั่วยุ เสียดสี ส่อไปในทางผิดกฎหมาย และผู้ใช้งานต้องไม่ส่งข้อความที่เป็นความเห็น ส่วนบุคคลโดยอ้างว่าเป็นความเห็นของ 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 ห้ามผู้ใช้งานทำการปลอมแปลงข้อความในอีเมล์ หัวจดหมายอีเมล์ ลายเซ็นในอีเมล์ หรือ e-mail Account ของบุคคลอื่นโดยเด็ดขาด

๒.๙.๑๑ ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นทำการส่งอีเมล์โดยใช้ E-mail Account ของตนโดยเด็ดขาด ไม่ว่าบุคคลนั้นจะเป็นผู้บังคับบัญชา เลขานุการ ผู้ช่วย หรือบุคคลอื่นใดก็ตาม

๒.๙.๑๒ ผู้ใช้งานต้องหลีกเลี่ยงการใช้คำสั่ง “Reply with History” ซึ่งเป็นการตอบกลับอีเมล์พร้อมไฟล์แนบไปยังผู้รับ ยกเว้นในกรณีที่จำเป็นต้องใช้งานเท่านั้น อย่างไรก็ตาม เมื่อมีการใช้งานคำสั่ง “Reply with History” ผู้ใช้งานควรทำการลบไฟล์แนบทิ้งเสียก่อนที่จะทำการส่งอีเมล์

๒.๙.๑๓ ผู้ใช้งานต้องทำการส่งอีเมล์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบข้อมูลเท่านั้นและห้ามใช้คำสั่ง “Reply All” ถ้าหากอีเมล์ฉบับนั้นไม่ได้มีความจำเป็นต้องตอบกลับไปยังผู้รับทุกคน

๒.๙.๑๔ ห้ามผู้ใช้งานส่งอีเมล์ที่ผู้รับไม่ได้ต้องการ ตัวอย่างเช่น อีเมล์ขยะ (Junk Mail) หรือโฆษณาสินค้าต่างๆ (Spam Mail) เป็นต้น

๒.๙.๑๕ ห้ามผู้ใช้งานสร้างหรือมีส่วนร่วมใดๆ กับการส่ง อีเมล์หลอกลวง หรือการส่งอีเมล์ในลักษณะลูกโซ่โดยเด็ดขาด

๒.๙.๑๖ ห้ามผู้ใช้งานส่งหรือส่งต่ออีเมล์ที่มีเนื้อหา หรือรูปภาพที่เข้าข่ายการดูหมิ่น หมิ่นประมาท กล่าวร้าย ทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ ลามกอนาจาร การยั่วยุทางเพศ หรืออีเมล์ที่มีเนื้อหาสุ่มเสี่ยงต่อประเด็นทางวัฒนธรรม หรือศาสนา และอีเมล์ที่กระทบต่อความมั่นคงของชาติ หรือสถาบันพระมหากษัตริย์โดยเด็ดขาด

๒.๙.๑๗ การส่งข้อมูลที่เป็นความลับ ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมายอิเล็กทรอนิกส์หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ อคส. เสร็จสินต้องออกจากระบบ (Log out) ทุกครั้ง

๒.๑๐ การใช้เครือข่ายอินเทอร์เน็ต (Internet)

๒.๑๐.๑ ผู้ใช้งานที่ต้องการใช้เครือข่ายอินเทอร์เน็ต ต้องลงทะเบียนบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ต โดยยื่นคำขอกับเจ้าหน้าที่ผู้ดูแลระบบ สำนักเทคโนโลยีดิจิทัล อคส. สำหรับบุคคลภายนอกจะต้องได้รับอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีดิจิทัล หรือผู้ที่ได้รับมอบหมาย

๒.๑๐.๒ ไม่ใช้เครือข่ายคอมพิวเตอร์ของหน่วยงานที่เชื่อมต่อกับเครือข่ายอินเทอร์เน็ต เพื่อหาประโยชน์ในเชิงพาณิชย์เป็นการส่วนบุคคล และทำการเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เช่น เว็บไซต์ที่ขัดต่อศีลธรรม เว็บไซต์ที่มีเนื้อหาอันอาจกระทบกระเทือนหรือเป็นภัยต่อความ มั่นคงต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม หรือละเมิดสิทธิ ของผู้อื่น หรือข้อมูลที่อาจก่อให้เกิดความเสียหายให้กับหน่วยงาน

๒.๑๐.๓ ผู้ใช้งานอินเทอร์เน็ตพึงใช้ข้อความที่สุภาพ ตามธรรมเนียมปฏิบัติในการใช้บริการ และ ต้องรับผิดชอบต่อข้อมูลของตนเอง ทั้งที่เก็บไว้บนเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่อง แม่ข่าย หรือข้อมูลที่ส่งผ่านระบบเครือข่าย

๒.๑๐.๔ ผู้ใช้งานต้องไม่ให้ผู้อื่นใช้งานบัญชีผู้ใช้เครือข่ายอินเทอร์เน็ตของตนโดยเด็ดขาด หากเกิดปัญหา เช่น การละเมิดลิขสิทธิ์หรือการเก็บข้อมูลที่ผิดกฎหมาย เจ้าของบัญชีผู้ใช้ เครือข่ายอินเทอร์เน็ตนั้นต้องเป็นผู้รับผิดชอบ

๒.๑๐.๕ ห้ามเปิดเผยข้อมูลของหน่วยงานที่เป็นความสับ หรือข้อมูลสำคัญที่ยังไม่ได้ประกาศ อย่างเป็นทางการผ่านเครือข่ายอินเทอร์เน็ต

๒.๑๐.๖ การดาวน์โหลดข้อมูลและโปรแกรมต่างๆ จากเครือข่ายอินเทอร์เน็ต ต้องกระทำด้วย ความระมัดระวัง และหากมีความจำเป็นต้องดาวน์โหลดไฟล์ขนาดใหญ่ ให้ดำเนินการ นอกเวลาปฏิบัติงาน

๒.๑๐.๗ ห้ามดาวน์โหลดข้อมูลและโปรแกรมต่างๆ ที่ละเมิดลิขสิทธิ์ จากเครือข่ายอินเทอร์เน็ต

๒.๑๐.๘ การใช้งานกระดานสนทนาอิเล็กทรอนิกส์ ต้องไม่เปิดเผยข้อมูลที่สำคัญและเป็นความสับของหน่วยงาน ไม่เสนอความคิดเห็น หรือใช้ข้อความที่ยั่วยุ ให้ร้าย ที่จะทำให้ เกิดความเสื่อมเสียต่อชื่อเสียงของหน่วยงาน การทำลายความสัมพันธ์กับบุคลากรขอ หน่วยงานอื่นๆ

๒.๑๐.๙ ผู้ใช้งาน ต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และการใช้งานนั้นต้องไม่เป็นสาเหตุให้สำนักงานฯ และบุคคลผู้ที่เกี่ยวข้องกับสำนักงานฯ เสื่อมเสียชื่อเสียง หรือเกี่ยวพันกับการกระทำที่ผิดกฎหมาย ทั้งนี้การใช้งานอินเทอร์เน็ตในทางที่ผิดถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีตามกฎหมาย

๒.๑๐.๑๐ ห้ามผู้ใช้งานคลิกหน้าต่างโฆษณาแบบป๊อบอัพ หรือเข้าสู่เว็บไซต์ใดๆ ที่โฆษณาโดยสแปม เนื่องจากเว็บไซต์เหล่านี้อาจมีโปรแกรมมุ่งร้ายแฝงอยู่ หรืออาจโจรกรรมข้อมูลในเครื่องคอมพิวเตอร์ของผู้ใช้งานโดยที่ผู้ใช้งานไม่ได้รับทราบหรือไม่ได้อนุญาต

๒.๑๐.๑๑ หลังจากใช้งานเครือข่ายอินเทอร์เน็ตเสร็จแล้ว ให้ Log out จากระบบการพิสูจน์ตัวจริง 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 ผู้ใช้งานที่ต้องการเข้าใช้งานระบบสารสนเทศของหน่วยงานจะต้องขออนุญาตเป็นลายลักษณ์อักษรและได้รับการพิจารณาอนุญาตจากผู้อำนวยการสำนักเทคโนโลยีดิจิทัล หรือผู้ดูแลระบบที่ได้รับมอบหมาย

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 จัดแบ่งลำดับขั้นความลับของข้อมูล

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

๒.๑๑.๓.๔ จัดแบ่งระดับขั้นการเข้าถึง

- ระดับชั้นสำหรับผู้บริหาร
- ระดับชั้นสำหรับผู้ใช้งานทั่วไป
- ระดับชั้นสำหรับผู้ดูแลระบบหรือผู้ที่ได้มอบหมาย

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 และโน้ตบุ๊คทุกเครื่องต้องได้รับการปรับปรุงข้อมูลล่าสุดจากเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการการป้องกันไวรัส

๒.๑๒.๓ เอกสารการติดตั้งค่าของเครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการป้องกันไวรัส ต้องได้รับการตรวจสอบทุก ๖ เดือน และต้องจัดทำเอกสาร Checklist ประกอบการตรวจสอบด้วย

๒.๑๒.๔ ห้ามเจ้าหน้าที่ทำการดาวน์โหลด แชร์แวร์ หรือฟรีแวร์โดยตรงจากอินเทอร์เน็ต โดยปราศจากการอนุมัติ หลังจากการอนุมัติแล้ว เจ้าหน้าที่ต้องทำการสแกนซอฟต์แวร์ด้วยโปรแกรมตรวจหาไวรัส ก่อนการใช้งาน

๒.๑๒.๕ ไฟล์ทุกไฟล์ที่ดาวน์โหลดในหน่วยงานเป็นไฟล์แนบของอีเมล์ สำเนาจากแผ่นดิสก์ หรือไฟล์แชร์ต่าง ๆ ต้องได้รับการสแกนหาไวรัส

๒.๑๒.๖ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่โปรแกรมมุ่งร้ายใดๆ ตัวอย่าง เช่น ไวรัส หนอนอินเทอร์เน็ต โปรแกรมแฝง (ม้าโทรจัน) อีเมล์บอมบ์ ฯลฯ เข้าสู่ระบบคอมพิวเตอร์ขององค์การ

๒.๑๒.๗ ห้ามผู้ใช้งานขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันไวรัส

๒.๑๒.๘ ไฟล์ที่เกี่ยวข้องกับการทำงานเท่านั้น ที่ได้รับอนุญาตให้สามารถรับ-ส่งผ่านระบบเครือข่ายขององค์การ ได้ ทั้งนี้ผู้ใช้งานควรรับไฟล์เฉพาะจากบุคคลที่ตนรู้จัก และจากช่องทางการติดต่อสื่อสารที่น่าจะเป็นไปได้เท่านั้น นอกจากนี้ผู้ใช้งานต้องทำการสแกนไวรัสในไฟล์ที่ได้รับด้วยซอฟต์แวร์ป้องกันไวรัสขององค์การ ก่อนเปิดใช้งานเสมอ

๒.๑๒.๙ เครื่องคอมพิวเตอร์แม่ข่ายทุกเครื่องให้ปิดฟังก์ชั่นการทำงานเชื่อมต่อกับอินเทอร์เน็ตยกเว้นในกรณีที่จำเป็นต้องใช้เท่านั้น เพื่อเป็นการป้องกันไม่ให้โปรแกรมไม่ประสงค์ดีมีผลกระทบกับข้อมูลที่สำคัญบนเครื่องคอมพิวเตอร์แม่ข่ายเหล่านี้

ส่วนที่ ๓

แนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการสำรองข้อมูลเครื่องคอมพิวเตอร์แม่ข่าย (Server) อุปกรณ์หลัก และไฟล์โปรแกรมระบบงานที่สำคัญ ที่ทำหน้าที่ให้บริการข้อมูลที่ถูกต้องและทันสมัย และเตรียมความ พร้อมกรณีเกิดเหตุฉุกเฉิน หรือกรณีมีเหตุการณ์ที่ก่อให้เกิดความเสียหายต่อสารสนเทศ ให้สามารถกู้ กลับคืนได้ภายในระยะเวลาที่เหมาะสม

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 ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับหน่วยงานควรห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อข้อมูลที่จัดเก็บไว้นอกสถานที่นั้น ในกรณีที่เกิดภัยพิบัติกับหน่วยงาน เช่น ไฟไหม้ เป็นต้น
- ต้องมีการควบคุมการเข้าถึงทางกายภาพ (Physical Access Control) ของสถานที่ที่เก็บข้อมูลสำรอง สื่อเก็บข้อมูลต้องได้รับการป้องกันสอดคล้องกับระดับความสำคัญของระบบสารสนเทศ
- ทดสอบข้อมูลสำรองที่บันทึกไว้อย่างสม่ำเสมอ เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติ

- ต้องจัดให้มีทะเบียนการบันทึกข้อมูลการสำรองข้อมูล และการเรียกคืนข้อมูลในแต่ละครั้ง
- จัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้
- ตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างสม่ำเสมอ

๓.๒ ระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน

๓.๒.๑ ต้องจัดทำระบบสำรองของระบบสารสนเทศหลักที่สำคัญของหน่วยงานไว้อย่างเพียงพอและต้องมีการทดสอบการทำงานของระบบสำรองอย่างสม่ำเสมอ

๓.๒.๒ ต้องจัดทำแผนการกู้คืนระบบสารสนเทศได้ภายในระยะเวลาที่เหมาะสม เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยมีรายละเอียดดังนี้

- การเตรียมความพร้อมเพื่อป้องกันและลดโอกาสที่จะเกิดเหตุการณ์ที่ก่อให้เกิดความเสียหายและมีผลกระทบต่อการดำเนินงานของหน่วยงาน และการให้บริการด้านเทคโนโลยีสารสนเทศ
- การตอบสนองต่อสถานการณ์ฉุกเฉิน เพื่อควบคุมและจำกัดขอบเขตของความเสียหาย เช่น กำหนดแนวทางการควบคุม การแก้ไขสถานการณ์ฉุกเฉิน เป็นต้น
- การดำเนินการเพื่อให้สามารถดำเนินงานของหน่วยงาน เป็นไปได้อย่างต่อเนื่อง เช่น การสำรองข้อมูลและอุปกรณ์สำคัญ การกู้ระบบงานและข้อมูลที่เสียหาย เป็นต้น
- การกลับคืนสู่การทำงานปกติ เพื่อให้การดำเนินงานหน่วยงาน กลับสู่สภาวะปกติ 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 และระบบแผนเตรียมพร้อมกรณีฉุกเฉินที่เพียงพอต่อสภาพความเสี่ยงที่ยอมรับได้ของแต่ละหน่วยงาน อย่างน้อยปีละ ๑ ครั้ง เพื่อให้แผนนั้นมีความทันสมัย และเหมาะสมกับสถานการณ์ปัจจุบัน

ส่วนที่ ๔

แนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

วัตถุประสงค์

กำหนดมาตรการในการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศของหน่วยงาน เพื่อให้ ระบบสารสนเทศของ อคส. มีความปลอดภัยและเป็นการป้องกันและลดระดับความเสี่ยงที่อาจจะเกิด ขึ้นกับระบบสารสนเทศของ อคส. ได้

อ้างอิงมาตรฐาน

COBIT ๕

แนวปฏิบัติ

การตรวจสอบและประเมินความเสี่ยง

๔.๑. ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ (Information Security Audit And Assessment) โดยผู้ตรวจสอบภายในของหน่วยงาน (Internal Auditor) และให้จัดทำ รายงานพร้อมข้อเสนอแนะอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญ

๔.๒. มีการจัดทำและทบทวนกระบวนการบริหารจัดการความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง โดยมีการวิเคราะห์ ประเมินความเสี่ยงและบริหารจัดการความเสี่ยงด้านสารสนเทศอย่างเหมาะสม รวมถึงการควบคุมและลดความเสี่ยงเหล่านั้น

๔.๓. มีการทบทวนแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง

๔.๔. ควรกำหนดให้มีการเฝ้าระวังการเข้าถึงระบบโดยผู้ตรวจสอบ รวมทั้งบันทึกข้อมูล Log แสดงการเข้าถึงนั้น ซึ่งรวมถึงวันและเวลาที่เข้าถึงระบบงานที่สำคัญๆ

๔.๕. ควรกำหนดให้ผู้ตรวจสอบสามารถเข้าถึงข้อมูลที่จำเป็นต้องตรวจสอบได้แบบอ่านได้อย่างเดียว

๔.๖. กรณีที่จำเป็นต้องเข้าถึงข้อมูลในแบบอื่นๆ ให้สร้างสำเนาสำหรับข้อมูลนั้น เพื่อให้ผู้ตรวจสอบใช้งาน รวมทั้งควรทำลายหรือลบโดยทันทีที่ตรวจสอบเสร็จ หรือต้องจัดเก็บไว้ โดยมีการป้องกันเป็นอย่างดี

๔.๗. ควรกำหนดให้มีการระบุและจัดสรรทรัพยากรที่จำเป็นต้องใช้ในการตรวจสอบและ ประเมินความเสี่ยงด้านสารสนเทศ โดยแยกการติดตั้งเครื่องมือที่ใช้ในการตรวจสอบ ออกจากระบบสารสนเทศที่ให้บริการจริงหรือที่ใช้ในการพัฒนา และมีการจัดเก็บป้องกัน เครื่องมือนั้นจากการเข้าถึงโดยไม่ได้รับอนุญาต

ส่วนที่ ๕

แนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับ ความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า

วัตถุประสงค์

เพื่อสร้างความรู้ ความเข้าใจและความตระหนักเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศขององค์กร โดยการเผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ และจัดฝึกอบรมให้ความรู้ความเข้าใจในเรื่องการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้สอดคล้องกับแนวปฏิบัติขององค์กร

อ้างอิงมาตรฐาน

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

แนวปฏิบัติ

การสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัย

๕.๑. จัดฝึกอบรมนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับ ภาระงาน บทบาทหน้าที่ในการปฏิบัติงานของของบุคลากร อย่างสม่ำเสมอ โดยการจัดฝึกอบรมอาจใช้วิธีการเสริมเนื้อหาแนวปฏิบัติเข้ากับหลักสูตรอบรมต่างๆ ตามแผนการฝึกอบรมของหน่วยงาน เพื่อเป็นการสร้างความตระหนักด้านความมั่นคงปลอดภัยสารสนเทศ

๕.๒. เผยแพร่ หรือประชาสัมพันธ์ให้ความรู้เกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ในลักษณะเกร็ดความรู้ หรือข้อควรระวังในรูปแบบที่เข้าใจง่าย โดยมีการปรับปรุงความรู้อย่างสม่ำเสมอ

๕.๓. บุคลากรใหม่ต้องได้รับการอบรมเกี่ยวกับนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่เกี่ยวข้องอย่างน้อยภายใน ๙๐ วันนับจากเข้าปฏิบัติหน้าที่

ส่วนที่ ๖

แนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านกายภาพ และสภาพแวดล้อม

วัตถุประสงค์

เพื่อกำหนดเป็นมาตรการในการควบคุมและป้องกันการรักษาความมั่นคงปลอดภัยที่เกี่ยวข้องกับการเข้าใช้งานหรือการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ โดยพิจารณาตามความสำคัญของอุปกรณ์ ระบบเทคโนโลยีสารสนเทศและข้อมูล ซึ่งเป็นทรัพย์สินที่มีค่าและอาจจำเป็นต้องรักษาความลับ โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้บริการและหน่วยงานภายนอก ซึ่งมีส่วนเกี่ยวข้องกับการใช้งานระบบเทคโนโลยีสารสนเทศของหน่วยงาน

แนวปฏิบัติ

การรักษาความมั่นคงปลอดภัยด้านกายภาพ และสภาพแวดล้อม

๖.๑. ให้สำนักเทคโนโลยีดิจิทัลเป็นผู้กำหนดพื้นที่ผู้ใช้บริการ พื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศให้ชัดเจน และจัดทำแผนผังแสดงตำแหน่งของพื้นที่ใช้งานและประกาศให้รับทราบทั่วกัน โดยการกำหนดพื้นที่ดังกล่าวแบ่งออกได้เป็นพื้นที่ทำงาน พื้นที่ติดตั้งและจัดเก็บอุปกรณ์ระบบเทคโนโลยีสารสนเทศหรือระบบเครือข่าย พื้นที่ใช้งานระบบเครือข่ายไร้สาย เป็นต้น

๖.๒. ให้สำนักเทคโนโลยีดิจิทัลเป็นผู้กำหนดสิทธิ์ในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๖.๓. ให้สำนักเทคโนโลยีดิจิทัลกำหนดมาตรการควบคุมการเข้า-ออกพื้นที่ ที่ใช้งานระบบเทคโนโลยีสารสนเทศ

๖.๔. หน่วยงานภายนอกที่นำเครื่องคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้ในการปฏิบัติงานระบบเครือข่ายภายในหน่วยงาน จะต้องลงบันทึกในแบบฟอร์มการขออนุญาตใช้งานเครื่องคอมพิวเตอร์หรืออุปกรณ์ และต้องมีเจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาลงนาม

ส่วนที่ ๗
การบริหารจัดการผู้ให้บริการภายนอก

วัตถุประสงค์

เพื่อให้หน่วยงานภายนอก ได้ปฏิบัติตามนโยบายรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า ทำให้ระบบสารสนเทศดำเนินไปได้อย่างต่อเนื่องและมีประสิทธิภาพ

แนวปฏิบัติ

การบริหารจัดการผู้ให้บริการภายนอก

๗.๑. ต้องมีการประเมินความเสี่ยงจากการเข้าถึง ข้อมูล และระบบสารสนเทศ หรืออุปกรณ์ที่ใช้ในการประมวลผลโดยหน่วยงานภายนอก และกำหนดมาตรการควบคุมที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงข้อมูลและระบบสารสนเทศ หรืออุปกรณ์ดังกล่าวได้

๗.๒. การเข้าใช้งานระบบสารสนเทศ หรือเข้าถึงข้อมูลของหน่วยงานจากหน่วยงานภายนอกต้องมีการขออนุญาตอย่างเป็นทางการ และได้รับอนุญาตจากหัวหน้าหน่วยงานหรือผู้ดูแลระบบที่ได้รับมอบหมายก่อนเสมอ

๗.๓. การบริการ และการดำเนินงานจากหน่วยงานภายนอก จะต้องปฏิบัติตาม นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ แนวทางการปฏิบัติงาน มาตรฐาน และกฎข้อบังคับต่าง ๆ ขององค์การคลังสินค้า

๗.๔. ผู้ดูแลระบบต้องให้สิทธิ์การเข้าถึงข้อมูลต่อหน่วยงานภายนอกเท่าที่จำเป็นเท่านั้น

๗.๕. ต้องมีการทำสัญญาการรักษาความลับขององค์กร ระหว่างหน่วยงานและหน่วยงานภายนอกที่เข้ามาปฏิบัติงานก่อนเปิดให้ใช้บริการระบบเสมอ

๗.๖. ผู้ให้บริการหน่วยงานภายนอก ต้องจัดทำแผนการดาเนินงาน และวิธีการดำเนินงาน เป็นอย่างน้อยเพื่อควบคุมหรือตรวจสอบการให้บริการของผู้ให้บริการให้เป็นไปอย่างถูกต้อง มั่นคงปลอดภัย และเป็นไปตามขอบเขตที่ได้กำหนดไว้

๗.๗. สัญญาระหว่างหน่วยงานและหน่วยงานภายนอกในการให้บริการต้องระบุถึงหัวข้อต่าง ๆ ดังต่อไปนี้ เป็นอย่างน้อย

(๑) รายละเอียดการให้บริการ แผนการดำเนินงาน วิธีการดำเนินงาน และสิ่งที่ต้องส่งมอบ

(๒) ระดับการให้บริการ (Service Level)

(๓) หน้าที่และความรับผิดชอบขององค์กรและหน่วยงานภายนอก ในการให้บริการในครั้งนี้

(๔) ระยะเวลาในการให้บริการ และการตรวจรับงานบริการในครั้งนี้

(๕) ราคา และเงื่อนไขการชาระเงิน

(๖) ความเป็นเจ้าของและลิขสิทธิ์ของอุปกรณ์ ฮาร์ดแวร์ หรือซอฟต์แวร์ ที่ทำการจัดซื้อหรือพัฒนาขึ้น (ถ้ามี)

(๗) การรักษาความลับของข้อมูลที่ได้รับจากการให้บริการแก่องค์กร

ส่วนที่ ๘
การรักษาความมั่นคงปลอดภัยด้านการสื่อสารและระบบเครือข่ายคอมพิวเตอร์
(Communications and Network Security)

วัตถุประสงค์

เพื่อรักษาความมั่นคงปลอดภัยในการรับส่งข้อมูลสารสนเทศผ่านระบบเครือข่ายภายในองค์กร และระหว่างระบบเครือข่ายภายในองค์กรกับระบบเครือข่ายภายนอก และเพื่อป้องกันการกระทำที่มีความเสี่ยงต่อข้อมูลสารสนเทศในระบบเครือข่ายคอมพิวเตอร์ และป้องกันโครงสร้างพื้นฐานที่สนับสนุนระบบเครือข่ายคอมพิวเตอร์

แนวปฏิบัติ

๘.๑ แนวทางปฏิบัติการควบคุมการรับส่งข้อมูลสารสนเทศ (Information Transfer)

๘.๑.๑ มีการกำหนดนโยบายและหลักปฏิบัติเพื่อปกป้องข้อมูลสารสนเทศที่รับส่งผ่านระบบและอุปกรณ์ในการสื่อสารทุกประเภท โดยมีเนื้อหาขั้นต่ำครอบคลุมถึง

(๑) แนวปฏิบัติที่ดีในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารอิเล็กทรอนิกส์ประเภทต่าง ๆ

(๒) กระบวนการป้องกันการรับส่งข้อมูลสารสนเทศนอกเส้นทางที่ได้กำหนดไว้ การดักรับสัญญาณ การเปลี่ยนแปลงแก้ไขหรือทำความเสียหายกับข้อมูล และโปรแกรมไม่ประสงค์ดีที่ถูกส่งผ่านช่องทางการสื่อสาร

(๓) กระบวนการป้องกันข้อมูลที่เป็นความลับหรือมีความสำคัญที่รับส่งในรูปแบบของไฟล์แนบ (attachment files) และการส่งต่อจดหมายอิเล็กทรอนิกส์แบบอัตโนมัติออกสู่ภายนอกองค์กร

(๔) การนำเทคนิคการเข้ารหัสข้อมูลมาใช้ในการรับส่งข้อมูลสารสนเทศผ่านช่องทางการสื่อสารบางประเภทที่ต้องการการรักษาความมั่นคงปลอดภัย เช่น การใช้งานระบบ cloud computing เป็นต้น

๘.๑.๒ ในการใช้งานระบบรับส่งข้อความผ่านทางอิเล็กทรอนิกส์ (electronic messaging) ต้องคำนึงถึงความมั่นคงปลอดภัยของข้อมูลสารสนเทศที่รับส่งผ่านช่องทางดังกล่าว โดยต้องจัดให้มีมาตรการป้องกันการเปลี่ยนแปลงแก้ไข ทำความเสียหาย หรือเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต และมีกระบวนการตรวจสอบผู้ใช้งานอย่างเข้มงวดในกรณีที่ใช้งานผ่านเครือข่ายสาธารณะ รวมทั้งต้องจัดการ และควบคุมให้ระบบทำงานรับส่งข้อมูลได้อย่างถูกต้องและพร้อมใช้งานอยู่เสมอ ทั้งนี้ การใช้งานระบบส่งข้อความผ่านทางอิเล็กทรอนิกส์ที่ให้บริการโดยบุคคลภายนอก เช่น โปรแกรมสนทนาผ่านระบบ อิเล็กทรอนิกส์ (instant messaging) ระบบเครือข่ายสังคมออนไลน์ (social networking) หรือโปรแกรมเรียกใช้ แฟ้มข้อมูลร่วมกัน (file sharing) ต้องจัดให้มีการควบคุมดูแลอย่างเหมาะสมเพียงพอ เช่น มีการขออนุมัติก่อนการใช้งาน รวมทั้งต้องปฏิบัติตามกฎหมายและหลักเกณฑ์ของทางการอย่างเคร่งครัด

๘.๑.๓ ต้องจัดให้พนักงานและผู้ให้บริการภายนอก มีการทำสัญญารักษาความลับหรือไม่เปิดเผย ข้อมูลที่มีความสำคัญ โดยขั้นต่ำต้องมีเนื้อหาครอบคลุมถึง

(๑) การระบุความเป็นเจ้าของข้อมูลสำคัญทางธุรกิจ ทรัพย์สินทางปัญญา และวิธีป้องกันการรั่วไหล ของข้อมูล

(๒) การป้องกันการเปิดเผยข้อมูลโดยไม่ได้รับอนุญาต ต้องจัดให้มีการลงนามโดยผู้รับผิดชอบ

(๓) การกำหนดขั้นตอนการขออนุญาตเข้าถึงข้อมูลหรือกำหนดสิทธิการเข้าถึงข้อมูลตามที่ได้ลง

นาม

(๔) การกำหนดสิทธิการเข้าถึงข้อมูลเพื่อตรวจสอบหรือติดตามการใช้งานข้อมูลที่มีความสำคัญ

(๕) การกำหนดกระบวนการแจ้งเตือนและรายงานผู้เกี่ยวข้องหากพบการรั่วไหลหรือเปิดเผยข้อมูล โดยไม่ได้รับอนุญาต

(๖) การกำหนดมาตรการดำเนินการกรณีละเมิดหรือยกเลิกสัญญา รวมทั้งข้อกำหนดในการคืนหรือ ทำลายข้อมูลที่มีความสำคัญเมื่อสิ้นสุดสัญญา

๘.๒ แนวทางปฏิบัติการบริหารจัดการระบบเครือข่ายคอมพิวเตอร์ (Network Security Management)

๘.๒.๑ ต้องจัดให้มีการบริหารจัดการและควบคุมระบบเครือข่ายคอมพิวเตอร์อย่างมั่นคง ปลอดภัย โดยขั้นต่ำควรมีการดำเนินการ ดังนี้

(๑) แบ่งแยกหน้าที่ความรับผิดชอบระหว่าง network administrator และ computer administrator ออกจากกัน พร้อมทั้งกำหนดหน้าที่ความรับผิดชอบและขั้นตอนในการบริหารจัดการระบบ และอุปกรณ์เครือข่ายให้ชัดเจน

(๒) จำกัดการเชื่อมต่อระบบคอมพิวเตอร์ระหว่างเครือข่าย เช่น จำกัดการใช้งานจุดเชื่อมต่อระบบ เครือข่าย (port outlet)

(๓) เปิดใช้งาน service port ที่เชื่อมต่อตามความจำเป็น พร้อมทั้งมีวิธีการเพื่อระบุถึงอุปกรณ์ที่เชื่อมต่อ (authenticate) อย่างชัดเจน เช่น IP address และประเภทของอุปกรณ์ เป็นต้น

(๔) มีการควบคุมการเชื่อมต่อกับระบบเครือข่ายสาธารณะ (public network) และระบบเครือข่ายไร้สาย (wireless network) อย่างรัดกุม เพื่อป้องกันการรั่วไหลหรือเปลี่ยนแปลงแก้ไขข้อมูลที่ส่งผ่านระบบ เครือข่ายดังกล่าวรวมทั้งเพื่อป้องกันระบบที่เชื่อมต่อและแอพพลิเคชั่นที่ใช้งาน เช่น การเข้ารหัส เครือข่าย หรือการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ออกจากกัน เป็นต้น นอกจากนี้ จะต้องจัดให้ มีการควบคุมเป็นพิเศษเพื่อให้ระบบเครือข่ายดังกล่าวอยู่ในสภาพที่พร้อมใช้งานอยู่เสมอ เช่น จัดให้มีระบบเครือข่ายคอมพิวเตอร์ที่ใช้งานทดแทนกันได้ (network load balance) เป็นต้น

(๕) มีการบันทึกและจัดเก็บหลักฐาน (logs) เพื่อติดตามตรวจสอบการทำงานที่เกี่ยวข้อง หรืออาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์

๘.๒.๒ ต้องจัดทำข้อตกลงการใช้บริการระบบเครือข่ายคอมพิวเตอร์ (network services agreements) กับผู้ให้บริการภายนอกโดยมีเนื้อหาครอบคลุมถึงวิธีการบริหารจัดการ คุณภาพการให้บริการ รวมทั้งกระบวนการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายคอมพิวเตอร์ ทั้งนี้ ในกรณีการใช้บริการ จากผู้ให้บริการภายในองค์กร ให้ผู้ประกอบธุรกิจจัดให้เป็นไปตามนโยบายด้านระบบสารสนเทศขององค์กร

๘.๒.๓ ต้องจัดให้มีการแบ่งแยกระบบเครือข่ายคอมพิวเตอร์ตามความเหมาะสม โดยระบุขอบเขต (domain) ของระบบเครือข่ายย่อยอย่างชัดเจน และจัดให้มีกระบวนการควบคุมการเข้าถึงขอบเขต ดังกล่าวโดยสอดคล้องเหมาะสมกับระดับความต้องการด้านการรักษาความมั่นคงปลอดภัยของแต่ละขอบเขตที่ถูกจัดแบ่ง

ส่วนที่ ๙
การบริหารจัดการความมั่นคงปลอดภัยทรัพย์สินด้านเทคโนโลยีสารสนเทศและข้อมูลสารสนเทศ
(IT Asset, Data and Information Security Management)

วัตถุประสงค์

เพื่อให้ทรัพย์สินสารสนเทศที่มีความสำคัญได้รับการป้องกันอย่างเหมาะสม

แนวปฏิบัติ

การบริหารจัดการความมั่นคงปลอดภัยทรัพย์สิน

๙.๑. ผู้ใช้งานต้องไม่เข้าไปในศูนย์ปฏิบัติการข้อมูลอิเล็กทรอนิกส์ (Data Center หมายถึงสถานที่ที่ใช้สำหรับติดตั้งเครื่องคอมพิวเตอร์แม่ข่ายและ/หรืออุปกรณ์บริหารจัดการเครือข่าย) ที่เป็นเขตหวงห้ามโดยเด็ดขาด เว้นแต่ได้รับอนุญาตจากผู้ดูแลระบบ

๙.๒. ผู้ใช้งานต้องไม่นำอุปกรณ์หรือชิ้นส่วนใดออกจากห้องปฏิบัติการเครือข่ายคอมพิวเตอร์เว้นแต่จะได้รับอนุญาตจากผู้ดูแลระบบ

๙.๓. ผู้ใช้งานต้องไม่นาเครื่องมือ หรืออุปกรณ์อื่นใด เชื่อมเข้าเครือข่ายเพื่อการประกอบธุรกิจส่วนบุคคล

๙.๔. ผู้ใช้งานต้องไม่คัดลอกหรือทาสาเนาแฟ้มข้อมูลที่มีลิขสิทธิ์กากับการใช้งาน ก่อนได้รับอนุญาต และผู้ใช้งานต้องไม่ใช้ หรือลบแฟ้มข้อมูลของผู้อื่น ไม่ว่ากรณีใด ๆ

๙.๕. ผู้ใช้งานต้องทาลายข้อมูลสำคัญในอุปกรณ์สื่อบันทึกข้อมูล แฟ้มข้อมูล ก่อนที่จะกำจัดอุปกรณ์ดังกล่าว และใช้เทคนิคในการลบหรือเขียนข้อมูลทับบนข้อมูลที่มีความสำคัญในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์นั้นไปใช้งานต่อ เพื่อป้องกันไม่ให้มีการเข้าถึงข้อมูลสำคัญและข้อมูลอยู่ในภาวะซึ่งเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ์นั้นได้ และพิจารณาวิธีการทำลายข้อมูลบนสื่อบันทึกข้อมูลแต่ละประเภท ดังนี้

ประเภทสื่อบันทึกข้อมูล	วิธีทำลาย
กระดาษ	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
Flash Drive	- ให้การทำลายข้อมูลบน Flash Drive โดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย
แผ่น CD/DVD	ใช้การหั่นด้วยเครื่องหั่นทำลายเอกสาร
เทป	ใช้วิธีการทุบหรือบดให้เสียหาย หรือเผาทาลาย
ฮาร์ดดิสก์	- ให้การทำลายข้อมูลบน Flash Drive โดยการเขียนทับข้อมูลเดิมหลายรอบ - ใช้วิธีการทุบหรือบดให้เสียหาย

๙.๖. ผู้ใช้งานมีหน้าที่ต้องรับผิดชอบต่อสินทรัพย์ที่หน่วยงานมอบไว้ให้ใช้งานเสมือนหนึ่งเป็นสินทรัพย์ของผู้ใช้งานเอง โดยบรรดารายการสินทรัพย์ (Asset Lists) ที่ผู้ใช้งานต้องรับผิดชอบ การรับหรือคืนสินทรัพย์ จะถูกบันทึกและตรวจสอบทุกครั้งโดยเจ้าหน้าที่ที่หน่วยงานมอบหมาย

๙.๗. ผู้ใช้งานต้องไม่ให้ผู้อื่นยืมสินทรัพย์ ไม่ว่าในกรณีใด ๆ เว้นแต่การยืมนั้นได้รับการอนุมัติเป็นลายลักษณ์อักษรจากหัวหน้าหน่วยงาน

๙.๘. กรณีทำงานนอกสถานที่ผู้ใช้งานต้องดูแลและรับผิดชอบสินทรัพย์ของหน่วยงานที่ได้รับมอบหมาย

๙.๙. ผู้ใช้งานมีหน้าที่ต้องชดใช้ค่าเสียหายไม่ว่าทรัพย์สินนั้นจะชำรุด หรือสูญหายตามมูลค่าทรัพย์สิน

หากความเสียหายนั้นเกิดจากความประมาทของผู้ใช้งาน

๙.๑๐. ผู้ใช้งานมีสิทธิ์ใช้สินทรัพย์และระบบสารสนเทศต่าง ๆ ที่หน่วยงานจัดเตรียมไว้ให้ใช้งาน โดยมีวัตถุประสงค์เพื่อการใช้งานของหน่วยงานเท่านั้น ห้ามมิให้ผู้ใช้งานนำสินทรัพย์และระบบสารสนเทศต่าง ๆ ไปใช้ในกิจกรรมที่หน่วยงานไม่ได้กำหนด หรือทำให้เกิดความเสียหายต่อองค์การคลังสินค้า

๙.๑๑. ความเสียหายใด ๆ ที่เกิดจากการละเมิดตามข้อ ๙.๑.๑๐ ให้ถือเป็นความผิดส่วนบุคคล โดยผู้ใช้งานต้องรับผิดชอบต่อความเสียหายที่เกิดขึ้น

ส่วนที่ ๑๐

แนวปฏิบัติการใช้บริการคลาวด์

วัตถุประสงค์

เพื่อใช้อ้างอิงประกอบการพิจารณาบริการของผู้ให้บริการคลาวด์ โดยคำนึงถึงหลักเกณฑ์ขั้นพื้นฐาน ซึ่งเป็นมาตรการขั้นต่ำในการลดความเสี่ยงจากภัยคุกคาม โดยจะต้องตรวจสอบและประเมินความเสี่ยงอย่างสม่ำเสมอ รวมทั้งปรับปรุงมาตรการเพื่อรักษาความมั่นคงปลอดภัยตามความเหมาะสม

อ้างอิงมาตรฐาน

- ISO

ISO/ IEC ๒๐๐๐๐- ๑ (Information Technology Service Management System: ITSMS)
ISO/IEC ๒๗๐๐๑ (Information Security Management System)
ISO/ IEC ๒๗๐๑๗ (Information technology – Security techniques –Code of practice for information security controls based on
ISO/IEC ๒๗๐๐๒ for Cloud Service)
ISO/ IEC ๒๗๐๑๘ (Information technology – Security techniques –Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors)

- CSA STAR

CSA STAR Self-Assessment
CSA STAR Certification
CSA STAR Attestation

- NIST

SP ๘๐๐-๑๗๑ Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations

แนวปฏิบัติ

การใช้บริการคลาวด์

๑๐.๑ กระบวนการทำงาน

นโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ นโยบายการพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล นโยบายการจัดการสินทรัพย์ นโยบายการจัดการเปลี่ยนแปลง นโยบายการบริหารความเสี่ยง กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อสัญญาและการปฏิบัติอื่นใดตามที่กฎหมายกำหนด

๑๐.๒ มาตรการป้องกันทางกายภาพ

มาตรการป้องกันเพื่อรักษาความมั่นคงปลอดภัยแก่สินทรัพย์ทางกายภาพ เช่น การกำหนดควบคุมพื้นที่ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่

๑๐.๓ มาตรการป้องกันทางเทคนิค

มาตรการป้องกันสาหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค เช่น โครงสร้างระบบเสมือน (Virtual Infrastructure) และสภาพแวดล้อมของระบบ การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิ

ของผู้ใช้งาน ระบบความมั่นคงปลอดภัยเครือข่าย การคุ้มครองข้อมูลการเข้ารหัส การวิเคราะห์ ออกแบบและพัฒนาระบบตามวัฏจักรพัฒนาระบบงาน (System Development Life Cycle : SDLC) แนวทางการรักษาความปลอดภัยในการพัฒนาซอฟต์แวร์และ Application Programming Interface (API) และแนวทางในการรักษาความปลอดภัยในการจ้างบุคคลภายนอก (Outsourcing)

๑๐.๔ ประสิทธิภาพการให้บริการ

ผู้ใช้บริการควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับสภาพพร้อมใช้งาน ระยะเวลาการตอบสนอง ความสามารถรองรับปริมาณงาน บริการสนับสนุนและกระบวนการยุติสัญญา ซึ่งมีสาระสำคัญดังต่อไปนี้

๑๐.๔.๑ สภาพพร้อมใช้งาน (Availability) ความพร้อมใช้งานของบริการครอบคลุมร้อยละของเวลาที่พร้อมให้บริการต่อปี (Uptime) เช่น ไม่ต่ำกว่าร้อยละ ๙๙.๙ เป็นต้น

๑๐.๔.๒ ระยะเวลาการตอบสนอง (Response Time) ระยะเวลาการตอบสนองต่อเหตุการณ์ ซึ่งเป็นระยะเวลานับแต่ผู้ใช้บริการแจ้งความประสงค์ และผู้ให้บริการได้ดาเนินการต่อความประสงค์นั้น โดยระยะ เวลาการตอบสนองเป็นหลักการพิจารณาที่สำคัญ ของผู้ใช้บริการ การตอบสนองล่าช้ากว่ากำหนดอาจส่งผลให้เกิดความเสียหาย

๑๐.๔.๓ ความสามารถรองรับปริมาณงาน (Capacity) จำนวนปริมาณการเชื่อมต่อสูงสุดพร้อมกัน (Maximum Simultaneous Connections) ปริมาณการใช้งานของผู้ใช้บริการพร้อมกัน (Maximum Simultaneous Users) ปริมาณความจุของระบบที่รองรับการใช้งาน (Resource Capacity) และปริมาณงาน (Throughput)

๑๐.๔.๔ การบริการสนับสนุน ช่องทางและช่วงเวลาที่ผู้ใช้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการ เช่น การกำหนดให้ผู้ใช้บริการสามารถติดต่อผู้ให้บริการได้ตลอด ๒๔ ชั่วโมง และระยะเวลาในการแก้ไขปัญหาการใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด

๑๐.๔.๕ กระบวนการยุติสัญญา แนวทางกระบวนการยุติสัญญาล่วงหน้า กรณีผู้ใช้บริการ หรือผู้ให้บริการต้องการยุติสัญญา โดยควรกำหนดแนวทางการดาเนินการ เช่น ระยะเวลาสาหรับการเข้าถึงข้อมูลของผู้ใช้บริการ และระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการ และการกำหนดแผนการเลิกใช้บริการ (Exit Plan)

๑๐.๕ การรักษาความมั่นคงปลอดภัย

ควรพิจารณามาตรการ การรักษาความมั่นคงปลอดภัยในระบบสารสนเทศในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับความน่าเชื่อถือของบริการ การพิสูจน์ตัวตนและการอนุญาต การเข้ารหัส การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การตรวจสอบขั้นตอนกระบวนการทางานและความปลอดภัย

๑๐.๕.๑ การพิสูจน์ตัวตนและการอนุญาต กระบวนการพิสูจน์ตัวตนเพื่อเป็นการตรวจสอบความมีตัวตนของผู้มีสิทธิ์ในการเข้าใช้งาน ระยะเวลาเวลาในการดาเนินการเพิ่มหรือถอนสิทธิ์ผู้ใช้บริการที่เหมาะสม การป้องกันการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์ การกำหนดระดับการยืนยันตัวตน (Authentication Level) และการควบคุมการเข้าถึงการใช้งานจากบุคคลภายนอกที่สนับสนุนการให้บริการ (Outsourcing)

๑๐.๕.๒ การเข้ารหัส การเข้ารหัสในการแปลงข้อมูลเพื่อปกปิดข้อมูลป้องกันการเข้าถึง การแก้ไข และการใช้งาน โดยไม่ได้รับอนุญาต การกำหนดการเข้ารหัสให้สอดคล้องกับประเภทข้อมูล (Data Classification) และจัดให้มีนโยบายการควบคุมกุญแจสำหรับการเข้ารหัส (Key Access Control Policy) ตามความเหมาะสม

๑๐.๕.๓ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย การจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล เริ่มตั้งแต่กระบวนการตรวจพบเหตุการณ์ การรายงานเหตุการณ์ การประเมิน การตอบสนอง การแก้ปัญหา และการเรียนรู้จากเหตุการณ์ความปลอดภัยที่เกิดขึ้น

๑๐.๕.๔ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ การบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการและการใช้บริการเพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้

๑๐.๕.๕ การตรวจสอบขั้นตอนกระบวนการทางานและความปลอดภัย การตรวจสอบกระบวนการทางานและความปลอดภัยอย่างเป็นระบบอ้างอิงมาตรฐานสากล มีความเป็นอิสระ มีขั้นตอนการทางานที่มีเอกสารหลักฐาน และกำหนดสิทธิของผู้ตรวจสอบภายในผู้ตรวจสอบภายนอก เป็นประจำอย่างสม่ำเสมอ รวมถึงการกำหนดให้หน่วยงานของรัฐที่มีอำนาจตามกฎหมายสามารถเข้าตรวจสอบได้

๑๐.๕.๖ การจัดการช่องโหว่ การตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ หรือจุดเสี่ยงในระบบกระบวนการรักษาความปลอดภัยของระบบ มาตรการรักษาความมั่งคงปลอดภัยไซเบอร์ การควบคุมภายใน หรือการใช้งานที่อาจถูกนาไปใช้หรือถูกเรียกใช้โดยภัยคุกคาม กรณีบริการที่มีความสำคัญและมีความจาเป็นอาจมีการทดสอบระบบความปลอดภัย Vulnerability Assessments และ Penetration Testing โดยจะต้องดำเนินการตามมาตรการ และวิธีการที่เหมาะสมเพื่อลดความเสี่ยงในการเกิดความเสียหาย

๑๐.๕.๗ ธรรมาภิบาล การแจ้งให้ผู้ใช้บริการทราบล่วงหน้าในระยะเวลาที่เหมาะสม กรณีการเปลี่ยนแปลงการให้บริการอันเนื่องมาจากการปรับปรุง อัพเดตซอฟต์แวร์ ที่อาจส่งผลกระทบต่อกระบวนการทางาน ช่องทางการให้บริการหรือรายละเอียดในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๑๐.๖ การจัดการข้อมูล

ควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับการจัดประเภทข้อมูล การสารองข้อมูลและการเรียกคืนข้อมูล วงจรชีวิตของข้อมูล และการโอนย้ายข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๑๐.๖.๑ การจัดประเภทข้อมูล ประเภทความเป็นเจ้าของข้อมูล ได้แก่ ข้อมูลของผู้ใช้บริการ ข้อมูลของผู้ให้บริการ และ ข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ (Derived Data) ผู้ให้บริการควรจัดให้มีนโยบายที่เกี่ยวข้องกับการใช้ข้อมูลของผู้ใช้บริการ การกำหนดขอบเขตและแนวปฏิบัติรวมถึงกำหนดสิทธิ์ในการตรวจสอบข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการ

๑๐.๖.๒ การสารองข้อมูล และการเรียกคืนข้อมูล การสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน โดยกำหนดระยะเวลา ความถี่ในการดาเนินการวิธีการ และการเก็บรักษาที่เหมาะสม ในกรณีที่ข้อมูลปัจจุบันถูกทำลายหรือได้รับความเสียหายส่งผลทำให้ไม่สามารถใช้งานได้ ผู้ให้บริการควรดาเนินการเรียกคืนข้อมูลเพื่อให้เกิดความพร้อมในการใช้งานตามที่ระบุไว้ในข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA)

๑๐.๖.๓ วงจรชีวิตของข้อมูล นโยบายและแนวปฏิบัติที่เหมาะสมในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพครอบคลุม กระบวนการสร้าง การเก็บรักษา การใช้ การเปิดเผย และการทำลายข้อมูล

๑๐.๖.๔ การโอนย้ายข้อมูล นโยบายและแนวปฏิบัติในการส่งออกข้อมูล โดยกำหนดรูปแบบ หรือกระบวนการส่งออก ตามความเหมาะสมในกรณียุติข้อตกลงการให้บริการ

๑๐.๗ การคุ้มครองข้อมูลส่วนบุคคล

ควรพิจารณาข้อตกลงระดับการให้บริการ (Service Level Agreement : SLA) ที่เกี่ยวข้องกับแนวปฏิบัติตามมาตรฐานสากลในการคุ้มครองข้อมูลส่วนบุคคล การระบุวัตถุประสงค์การเก็บข้อมูล การเก็บรักษาข้อมูลเท่าที่จาเป็น การใช้ เก็บรักษาและการเปิดเผย ความโปร่งใสและการแจ้งเตือนความรับผิดชอบต่อข้อมูล สถานที่จัดเก็บข้อมูล และการอานวยความสะดวกในการเข้าถึงข้อมูล ซึ่งมีสาระสำคัญดังต่อไปนี้

๑๐.๗.๑ แนวปฏิบัติตามมาตรฐานสากล นโยบาย แนวทางปฏิบัติ มาตรการ หรือมาตรฐานที่สอดคล้องตามกฎหมายคุ้มครองข้อมูลส่วนบุคคล

๑๐.๗.๒ การระบุวัตถุประสงค์ ระบุวัตถุประสงค์และความยินยอมในการรวบรวม เก็บรักษา การใช้ และการเปิดเผยข้อมูลให้ชัดเจน ทั้งนี้ ผู้ให้บริการควรระมัดระวังในการดำเนินการกับข้อมูลส่วนบุคคล

๑๐.๗.๓ การเก็บรักษาข้อมูลเท่าที่จำเป็น ระยะเวลาในการเก็บรักษาข้อมูลที่เหมาะสม และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลหลังจากมีการแจ้งให้ทำลายข้อมูล

๑๐.๗.๔ การใช้ เก็บรักษา และการเปิดเผย การแจ้งผู้ใช้บริการทราบว่า ผู้ให้บริการจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บรวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ หรือเป็นกรณีที่กฎหมายกำหนด หรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล

๑๐.๗.๕ ความโปร่งใส และการแจ้งเตือน การแจ้งให้ผู้ใช้บริการทราบและให้ข้อมูลที่เพียงพอเกี่ยวกับความโปรงใส่ ในการดาเนินการกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด

๑๐.๗.๖ ความรับผิดชอบต่อข้อมูล นโยบายและแนวปฏิบัติในกรณีการละเมิดข้อมูล และควรมีกระบวนการเอกสารหลักฐานที่ได้ดำเนินการที่สอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล เนื่องจากความรับผิดชอบด้านสารสนเทศจะเป็นส่วนสำคัญในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล

๑๐.๗.๗ สถานที่จัดเก็บข้อมูล การแสดงให้ผู้ใช้บริการทราบสถานที่ในการจัดเก็บข้อมูล หรือกำหนดให้ผู้ใช้บริการสามารถเลือกสถานที่จัดเก็บข้อมูลได้ เพื่อเป็นการลดความเสี่ยงในการถูกละเมิด เนื่องจากการประมวลผลข้อมูลส่วนบุคคลอาจจะถูกโอนย้ายข้อมูลไปยังต่างประเทศ ซึ่งอาจจะมีกฎหมาย กฎระเบียบหรือระดับการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน

๑๐.๗.๘ การอำนวยความสะดวกในการเข้าถึงข้อมูล การอำนวยความสะดวกแก่ผู้ใช้บริการในระยะเวลาที่เหมาะสมและมีประสิทธิภาพ ทั้งนี้ห้ามมิให้ผู้ให้บริการใช้ข้อกำหนดทางเทคนิคหรือข้อกำหนดขององค์กรเป็นอุปสรรคในการ ปฏิเสธสิทธิ์ของเจ้าของข้อมูล