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

ประกาศองค์การคลังสินค้า
ที่ ๑๐๓ / ๒๕๖๙
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ขององค์การคลังสินค้า (ฉบับทบทวน) ประจำปี พ.ศ. ๒๕๖๙

.....

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 พ.ศ. ๒๕๖๙”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันออกประกาศ เป็นต้นไป

ข้อ ๓ องค์การคลังสินค้าได้จัดทำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การการคลังสินค้า เป็นลายลักษณ์อักษรตามเอกสารแนบท้ายประกาศ

ข้อ ๔ เพื่อให้การปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้เป็นไปอย่างมีประสิทธิภาพ จึงได้ข้อกำหนดให้สำนักเทคโนโลยีดิจิทัลและผู้เกี่ยวข้อง ดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวน ปรับปรุงนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้าให้เป็นปัจจุบันอยู่เสมออย่างน้อยปีละ ๑ ครั้ง และหากมีการเปลี่ยนแปลง ให้ประกาศให้เจ้าหน้าที่ทุกระดับขององค์การคลังสินค้ารับทราบทุกครั้ง

ข้อ ๕ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ จัดเป็นมาตรฐานด้านการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและการสื่อสารของหน่วยงาน เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีทางอิเล็กทรอนิกส์อย่างปลอดภัย เชื่อถือได้ เป็นไปตามกฎหมาย

และระเบียบที่เกี่ยวข้อง จึงให้ใช้แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศขององค์การคลังสินค้า ตามเอกสารแนบท้ายประกาศนี้ ซึ่งเจ้าหน้าที่และผู้เกี่ยวข้องจะต้องถือปฏิบัติตามอย่างเคร่งครัดต่อไป

ประกาศฉบับนี้มีผลบังคับใช้ตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๒๑ กันยายน พ.ศ. ๒๕๖๙

เรือโท

(วีระชัย โกสาแสง)

รองผู้อำนวยการองค์การคลังสินค้า

รักษาการแทนผู้อำนวยการองค์การคลังสินค้า

เอกสารแนบท้ายประกาศ

นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ขององค์การคลังสินค้า (ฉบับทบทวน) ประจำปี พ.ศ. ๒๕๖๙

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 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	
บทที่ ๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ	๑
บทที่ ๒ คำนิยาม	๘
บทที่ ๓ อำนาจหน้าที่	๑๑
ส่วนที่ ๒ แนวปฏิบัติการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ	
๒.๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน	๑๓
๒.๒ การกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน	๑๕
๒.๓ การควบคุมการเข้าถึงเครือข่าย	๑๘
๒.๔ การควบคุมการเข้าถึงระบบปฏิบัติการ	๒๐
๒.๕ การควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ	๒๑
๒.๖ การควบคุมการเข้าออกศูนย์ข้อมูลและเครือข่ายคอมพิวเตอร์	๒๒
๒.๗ การควบคุมการใช้งานเครื่องคอมพิวเตอร์แม่ข่าย	๒๓
๒.๘ การควบคุมการเข้าถึงเครือข่ายไร้สาย	๒๓
๒.๙ การใช้จดหมายอิเล็กทรอนิกส์	๒๔
๒.๑๐ การใช้เครือข่ายอินเตอร์เน็ต	๒๕
๒.๑๑ การควบคุมการเข้าถึงและใช้งานสารสนเทศ	๒๕
ส่วนที่ ๓ นโยบายและแนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ	๒๘
ส่วนที่ ๔ นโยบายและแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ	๓๓
ส่วนที่ ๕ นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ	๓๗
ส่วนที่ ๖ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ	๔๑
ส่วนที่ ๗ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม	๔๕
ส่วนที่ ๘ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร	๔๗
ส่วนที่ ๙ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ	๕๒
ส่วนที่ ๑๐ นโยบายและแนวปฏิบัติการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ	๕๗
ส่วนที่ ๑๑ นโยบายและแนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก	๖๒
ส่วนที่ ๑๒ นโยบายและแนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี	๖๗
ส่วนที่ ๑๓ นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต	๗๑
ส่วนที่ ๑๔ นโยบายและแนวปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน	๗๖
ส่วนที่ ๑๕ นโยบายและแนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศและการบริหารจัดการกุญแจ	๘๑

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

(๗) การกำหนดค่า Recovery Time Objective (RTO) และ Recovery Point Objective (RPO) องค์การคลังสินค้าต้องกำหนดค่าเป้าหมายในการกู้คืนระบบสารสนเทศ (Recovery Time Objective : RTO) และค่าเป้าหมายในการสูญเสียข้อมูลที่ยอมรับได้ (Recovery Point Objective : RPO) ให้เหมาะสมกับระดับความสำคัญของระบบสารสนเทศและภารกิจขององค์กร โดยมีแนวทางดังนี้

๑) ต้องจำแนกระดับความสำคัญของระบบสารสนเทศ (Criticality Classification) เพื่อใช้กำหนดค่า RTO และ RPO ของแต่ละระบบ

๒) ต้องกำหนดค่า RTO และ RPO สำหรับระบบสารสนเทศที่สำคัญทุกระบบ และได้รับความเห็นชอบจากเจ้าของระบบ (System Owner) หรือผู้บริหารที่เกี่ยวข้อง

๓) ต้องทบทวนค่า RTO และ RPO อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสารสนเทศ โครงสร้างพื้นฐาน หรือกระบวนการดำเนินงานที่สำคัญ

๔) ต้องจัดทำเอกสารแสดงค่า RTO และ RPO ของแต่ละระบบ และใช้เป็นข้อมูลอ้างอิงในการจัดทำแผนสำรองข้อมูล แผนกู้คืนระบบ และแผนบริหารความต่อเนื่องทางธุรกิจ (Business Continuity Plan : BCP)

๕) การกำหนดค่า RTO และ RPO ต้องคำนึงถึงผลกระทบต่อการดำเนินงาน ความเสียหายด้านข้อมูล การให้บริการประชาชน และข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

(๘) การทดสอบแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Test) องค์การคลังสินค้าต้องจัดให้มีการทดสอบแผนกู้คืนระบบสารสนเทศ (Disaster Recovery Plan : DRP) เพื่อให้มั่นใจว่าสามารถกู้คืนระบบและข้อมูลได้ภายในระยะเวลาที่กำหนด โดยมีแนวทาง ดังนี้

๑) ต้องจัดทำแผนการทดสอบ Disaster Recovery อย่างน้อยปีละ ๑ ครั้ง สำหรับระบบ

สารสนเทศที่สำคัญ

๒) การทดสอบต้องครอบคลุมอย่างน้อย

- การกู้คืนเครื่องแม่ข่าย (Server Recovery)
- การกู้คืนฐานข้อมูล (Database Recovery)
- การกู้คืนระบบเครือข่าย
- การกู้คืนข้อมูลจากระบบสำรอง (Backup Restoration)
- การทดสอบการเชื่อมโยงระบบงานที่เกี่ยวข้อง
- การตรวจสอบความครบถ้วนและความถูกต้องของข้อมูลหลังการกู้คืน

๓) ต้องมีการบันทึกผลการทดสอบ ระยะเวลาที่ใช้ในการกู้คืน ปัญหาที่พบ และข้อเสนอแนะในการปรับปรุง

๔) ผลการทดสอบต้องแสดงให้เห็นว่าระบบสามารถกู้คืนได้ภายในค่า RTO และข้อมูลสูญหายไม่เกินค่า RPO ที่กำหนด

๕) หากผลการทดสอบไม่เป็นไปตามเป้าหมาย ต้องจัดทำแผนแก้ไข (Corrective Action Plan) พร้อมกำหนดผู้รับผิดชอบและระยะเวลาดำเนินการ

๖) ให้สำนักเทคโนโลยีดิจิทัลรายงานผลการทดสอบ Disaster Recovery ต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) และคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ในการทบทวนและปรับปรุงแผนบริหารความต่อเนื่องขององค์กร

๑.๓ นโยบายการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management)

อคส. กำหนดให้มีกรอบการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management Framework) เพื่อให้สามารถบริหาร จัดการ ควบคุม และลดความเสี่ยงที่อาจส่งผลกระทบต่อข้อมูล ระบบสารสนเทศ และการดำเนินภารกิจขององค์กรอย่างเป็นระบบ โดยมีแนวทางดังต่อไปนี้

(๑) การกำหนดกรอบการบริหารความเสี่ยง

อคส. ต้องจัดให้มีกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่ครอบคลุม เช่น สินทรัพย์ด้านเทคโนโลยีสารสนเทศ ระบบสารสนเทศ ข้อมูลสารสนเทศ ระบบเครือข่าย ระบบ Cloud ระบบของผู้ให้บริการภายนอก อุปกรณ์ปลายทาง (Endpoint) บุคลากร กระบวนการดำเนินงาน

(๒) การระบุความเสี่ยง (Risk Identification)

ต้องมีการระบุความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศจากแหล่งต่าง ๆ อย่างสม่ำเสมอ เช่น Cyber Attack, Malware, Ransomware, Insider Threat, Human Error, Data Leakage, System Failure, Cloud Risk, Third Party Risk, Natural Disaster, Supply Chain Risk รวมถึงความเสี่ยงที่อาจเกิดจากการเปลี่ยนแปลงเทคโนโลยีและภัยคุกคามรูปแบบใหม่

(๓) การวิเคราะห์และประเมินความเสี่ยง (Risk Assessment)

อคส. ต้องดำเนินการประเมินความเสี่ยงโดยพิจารณาอย่างน้อย ดังนี้ โอกาสเกิด (Likelihood) ผลกระทบ (Impact) ระดับความเสี่ยง (Risk Level) มาตรการควบคุมที่มีอยู่ (Existing Controls) ความเสี่ยงคงเหลือ (Residual Risk) โดยใช้หลักเกณฑ์และระดับความเสี่ยงที่องค์กรกำหนดอย่างเป็นมาตรฐาน

(๔) การจัดทำทะเบียนความเสี่ยง (Risk Register)

ต้องจัดทำทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk

Register) อย่างเป็นระบบ โดยอย่างน้อยต้องประกอบด้วย รายการความเสี่ยง เจ้าของความเสี่ยง (Risk Owner) สินทรัพย์ที่ได้รับผลกระทบ ระดับความเสี่ยง มาตรการควบคุม แผนลดความเสี่ยง ระยะเวลาดำเนินการ สถานะการดำเนินงาน

(๕) การจัดการความเสี่ยง (Risk Treatment)

เมื่อประเมินความเสี่ยงแล้ว ต้องกำหนดแนวทางการจัดการความเสี่ยงอย่างเหมาะสม ได้แก่ การลดความเสี่ยง (Risk Mitigation) การหลีกเลี่ยงความเสี่ยง (Risk Avoidance) การโอนย้ายความเสี่ยง (Risk Transfer) การยอมรับความเสี่ยง (Risk Acceptance) ทั้งนี้ การยอมรับความเสี่ยงต้องได้รับความเห็นชอบจากผู้บริหารที่มีอำนาจตามระดับความเสี่ยงที่กำหนด

(๖) การติดตามและทบทวนความเสี่ยง (Risk Monitoring and Review)

ต้องติดตามและทบทวนความเสี่ยงอย่างต่อเนื่อง โดยอย่างน้อยทบทวนปีละ ๑ ครั้ง เมื่อเกิดเหตุการณ์ด้าน Cyber Security การเปลี่ยนแปลงระบบสำคัญ การนำระบบใหม่มาใช้งาน การเปลี่ยนแปลงกฎหมายหรือข้อกำหนด

(๗) การบริหารความเสี่ยงของโครงการด้านเทคโนโลยีสารสนเทศ

โครงการด้านเทคโนโลยีสารสนเทศทุกโครงการต้องดำเนินการประเมินความเสี่ยงก่อนเริ่มโครงการ ระหว่างดำเนินโครงการ และภายหลังเสร็จสิ้นโครงการ เพื่อให้สามารถบริหารจัดการความเสี่ยงได้ตลอดวงจรชีวิตของโครงการ

(๘) การบริหารความเสี่ยงของผู้ให้บริการภายนอก (Third Party Risk)

ต้องประเมินความเสี่ยงของผู้ให้บริการภายนอก ผู้รับจ้าง และผู้ให้บริการ Cloud ก่อนการว่าจ้าง และทบทวนเป็นประจำ โดยพิจารณาอย่างน้อย ดังนี้ ระดับความมั่นคงปลอดภัย การปฏิบัติตามกฎหมาย ความต่อเนื่องในการให้บริการ การคุ้มครองข้อมูล ผลการตรวจประเมินที่ผ่านมา

(๙) การรายงานความเสี่ยง

สำนักเทคโนโลยีดิจิทัลต้องจัดทำรายงานความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศเสนอต่อผู้บริหารเทคโนโลยีสารสนเทศระดับสูง (DCIO) และผู้บริหารที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อเกิดเหตุการณ์ที่มีผลกระทบในระดับสูงหรือวิกฤต

(๑๐) การปรับปรุงอย่างต่อเนื่อง

ผลการประเมินความเสี่ยง ผลการตรวจสอบภายใน ผลการตรวจสอบภายนอก ผลการทดสอบแผน Disaster Recovery และเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ ต้องนำมาใช้ในการทบทวนและปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศ แผนบริหารความเสี่ยง และแผนปฏิบัติการด้านเทคโนโลยีดิจิทัลขององค์การคลังสินค้าอย่างต่อเนื่อง

๑.๔ นโยบายการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ

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

(๒) ในการตรวจสอบและประเมินความเสี่ยงจะต้องดำเนินการโดยผู้ตรวจสอบภายในขององค์การคลังสินค้า (Internal auditor) หรือโดยผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External auditor) เพื่อให้องค์การคลังสินค้าได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศ

๑.๕ 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

๓.๒.๖ กำกับดูแลกรอบการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร

๓.๒.๗ พิจารณาอนุมัติการยอมรับความเสี่ยง (Risk Acceptance) ที่อยู่ในระดับสูงตามเกณฑ์ขององค์กร

๓.๒.๘ ติดตามผลการดำเนินงานด้านการบริหารความเสี่ยงและรายงานต่อผู้บริหารสูงสุด

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

๓.๓.๔ จัดทำและปรับปรุงทะเบียนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๓.๕ ดำเนินการประเมินความเสี่ยงของระบบสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

๓.๓.๖ ติดตามสถานะของมาตรการลดความเสี่ยงและรายงานผลต่อผู้บริหาร

๓.๓.๗ ให้คำปรึกษาและสนับสนุนหน่วยงานต่าง ๆ ในการบริหารความเสี่ยงด้านเทคโนโลยีสารสนเทศ

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
(Access control)

วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมการเข้าถึงระบบสารสนเทศ และป้องกันการบุกรุกผ่านระบบ เครือข่ายจากผู้บุกรุก หรือจากซอฟต์แวร์ประสงค์ร้าย รวมทั้งกำหนดประเภทของข้อมูล ลำดับชั้น ความลับของข้อมูล ระดับชั้นการเข้าถึง เวลาที่ได้เข้าถึง และช่องทางการเข้าถึง

แนวปฏิบัติ

๒.๑ การบริหารจัดการการเข้าถึงของผู้ใช้งาน (User Access Management)

๒.๑.๑ ผู้ดูแลระบบต้องกำหนดขั้นตอนปฏิบัติในการลงทะเบียนเจ้าหน้าที่ใหม่ การให้สิทธิต่างๆ ในการใช้งานตามความจำเป็น และการยกเลิกสิทธิการใช้งาน เช่น การลาออก การโยกย้ายหรือการเปลี่ยนตำแหน่งงานภายในหน่วยงาน เป็นต้น

๒.๑.๒ ผู้ดูแลระบบต้องกำหนดสิทธิการเข้าถึง และใช้งานระบบสารสนเทศที่สำคัญ เช่น ซอฟต์แวร์ประยุกต์ จดหมายอิเล็กทรอนิกส์ เครือข่ายไร้สาย และอินเทอร์เน็ต เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานในหน้าที่และต้องได้รับความเห็นชอบจาก ผู้บังคับบัญชาเป็นลายลักษณ์อักษร รวมทั้งต้องทบทวนสิทธิดังกล่าวอย่างสม่ำเสมอ

๒.๑.๓ ผู้ดูแลระบบต้องบริหารจัดการสิทธิการเข้าถึงและใช้งานระบบสารสนเทศของบุคลากรดังต่อไปนี้

๒.๑.๓.๑ 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 ๕๒๒๐.๒๒-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 ที่ใช้ในการกำหนดในอุปกรณ์สวิทซ์และอุปกรณ์ต่างๆที่เกี่ยวข้อง

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 ปีนยั่วยุ 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 ต้องไม่ระบุความสำคัญของข้อมูลลงในหัวข้อจดหมาย

อิเล็กทรอนิกส์หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์ของ 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

๒.๑๑.๑ จัดทำบัญชีทรัพย์สินหรือทะเบียนทรัพย์สิน การจำแนกกลุ่มทรัพยากรของระบบหรือการทำงานโดยให้กำหนดกลุ่มผู้ใช้งานและสิทธิของกลุ่มผู้ใช้งาน

๒.๑๑.๒ กำหนดเกณฑ์ในการอนุญาตให้เข้าถึงการใช้งานสารสนเทศ ที่เกี่ยวข้องกับการอนุญาตการ

กำหนดสิทธิ 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) สำหรับผู้ใช้งาน

ภายนอกสามารถเข้าถึงได้ตลอด ๒๔ ชั่วโมง

๒.๑๑.๓.๖ การกำหนดช่องทางที่สามารถเข้าถึง

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

ส่วนที่ ๓
นโยบายและแนวปฏิบัติการจัดทำระบบสำรองของสารสนเทศ
(Information Backup and Recovery)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดหลักเกณฑ์และแนวปฏิบัติในการสำรองข้อมูล ระบบสารสนเทศ ฐานข้อมูล ค่าการกำหนดระบบ และทรัพย์สินสารสนเทศที่สำคัญขององค์การคลังสินค้า

๑.๒ เพื่อป้องกันการสูญหาย ความเสียหาย การถูกทำลาย การแก้ไขโดยมิได้รับอนุญาต หรือการไม่สามารถเข้าถึงข้อมูลและระบบสารสนเทศ อันเกิดจากความผิดพลาดของบุคลากร ระบบขัดข้อง ภัยธรรมชาติ อัคคีภัย การโจมตีทางไซเบอร์ หรือโปรแกรมไม่ประสงค์ดี

๑.๓ เพื่อให้สามารถกู้คืนข้อมูลและระบบสารสนเทศที่สำคัญได้อย่างถูกต้อง ครบถ้วน ทันเวลา และสอดคล้องกับความจำเป็นในการดำเนินงานขององค์การ

๑.๔ เพื่อกำหนดให้มีระบบ อุปกรณ์ สถานที่ หรือบริการสำรองที่เหมาะสมสำหรับระบบสำคัญ เพื่อลดผลกระทบจากการหยุดชะงักของบริการและสนับสนุนแผนบริหารความต่อเนื่องทางธุรกิจ

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้มีกระบวนการสำรองและกู้คืนที่เป็นมาตรฐาน ทำซ้ำได้ มีหลักฐานการปฏิบัติงาน มีการทดสอบ และปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับข้อมูลสารสนเทศ ระบบสารสนเทศ ฐานข้อมูล เว็บไซต์ ระบบงานสำคัญ ระบบเครือข่าย ระบบคลาวด์ เครื่องแม่ข่าย อุปกรณ์จัดเก็บข้อมูล และอุปกรณ์รักษาความมั่นคงปลอดภัยสารสนเทศขององค์การคลังสินค้า

๒.๒ ครอบคลุมข้อมูลสำคัญทุกประเภท เช่น ข้อมูลการดำเนินงาน ข้อมูลการเงิน ข้อมูลสินค้าและคลังสินค้า ข้อมูลคู่ค้า ข้อมูลบุคลากร ข้อมูลส่วนบุคคล เอกสารอิเล็กทรอนิกส์ ข้อมูลบัญชีผู้ใช้งาน และข้อมูลที่มีผลกระทบต่อภารกิจขององค์การ

๒.๓ ครอบคลุมการสำรองข้อมูล การสำรองระบบ การสำรองค่าการกำหนดของอุปกรณ์และระบบ การจัดเก็บสื่อสำรอง การเข้ารหัส การกู้คืน การทดสอบการกู้คืน การใช้ระบบสำรอง และการทำลายสื่อสำรองเมื่อหมดอายุการใช้งาน

๒.๔ ใช้บังคับกับคณะกรรมการ ผู้บริหาร เจ้าของระบบ เจ้าของข้อมูล สำนักเทคโนโลยีดิจิทัล ผู้ดูแลระบบ ผู้ดูแลฐานข้อมูล ผู้ดูแลเครือข่าย พนักงาน ลูกจ้าง ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นที่เกี่ยวข้องกับการจัดเก็บหรือบริหารจัดการข้อมูลขององค์การ

๓. แนวปฏิบัติ

๓.๑ การกำหนดบทบาท หน้าที่ และความรับผิดชอบ

๑) ให้กำหนดเจ้าของข้อมูล (Data Owner) เจ้าของระบบ (System Owner) ผู้ดูแลระบบ ผู้ปฏิบัติงานสำรองข้อมูล และผู้รับผิดชอบการกู้คืนข้อมูลหรือระบบอย่างชัดเจน

๒) เจ้าของข้อมูลและเจ้าของระบบมีหน้าที่กำหนดระดับความสำคัญของข้อมูลและระบบ รวมถึงความจำเป็นในการสำรองข้อมูล ระยะเวลาการเก็บรักษา และลำดับความสำคัญในการกู้คืน

๓) สำนักเทคโนโลยีดิจิทัลมีหน้าที่จัดทำแผนสำรองข้อมูล ดำเนินการสำรอง ตรวจสอบผลการสำรอง จัดเก็บสื่อสำรอง ทดสอบการกู้คืน และรายงานผลการดำเนินงาน

๔) ผู้ใช้งานมีหน้าที่จัดเก็บข้อมูลการปฏิบัติงานไว้ในพื้นที่หรือระบบที่องค์การกำหนด เพื่อให้ข้อมูลอยู่ภายใต้กระบวนการสำรองข้อมูลขององค์การ

๓.๒ การจำแนกข้อมูลและระบบที่ต้องสำรอง

๑) ให้จัดทำบัญชีรายการข้อมูล ระบบ ฐานข้อมูล เครื่องแม่ข่าย อุปกรณ์เครือข่าย และค่าการกำหนดระบบที่ต้องสำรอง โดยระบุเจ้าของข้อมูลหรือระบบ ผู้รับผิดชอบ ระดับความสำคัญ และวิธีการสำรอง

๒) ข้อมูลและระบบสำคัญต้องได้รับการจัดลำดับความสำคัญในการกู้คืน โดยพิจารณาจากผลกระทบต่อภารกิจ ความต่อเนื่องในการให้บริการ ข้อกำหนดตามกฎหมาย และความเสียหายที่อาจเกิดขึ้นหากข้อมูลสูญหาย

๓) ให้กำหนดเป้าหมายระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) และเป้าหมายจุดกู้คืนข้อมูล (Recovery Point Objective: RPO) สำหรับระบบสำคัญตามความเหมาะสม

๔) ให้ทบทวนบัญชีรายการข้อมูลและระบบที่ต้องสำรองอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการจัดหา พัฒนา ปรับปรุง เปลี่ยนแปลง หรือยกเลิกระบบสารสนเทศ

๓.๓ การจัดทำแผนและตารางการสำรองข้อมูล

๑) ให้จัดทำแผนและตารางการสำรองข้อมูลเป็นลายลักษณ์อักษร โดยระบุอย่างน้อยประเภทข้อมูลหรือระบบ วิธีการสำรอง ความถี่ สถานที่จัดเก็บ ระยะเวลาการเก็บรักษา ผู้รับผิดชอบ และวิธีการกู้คืน

๒) การสำรองข้อมูลอาจดำเนินการในรูปแบบการสำรองข้อมูลทั้งหมด (Full Backup) การสำรองข้อมูลเฉพาะส่วนที่เปลี่ยนแปลง (Incremental Backup) หรือวิธีการอื่นที่เหมาะสมกับระบบและระดับความเสี่ยง

๓) ระบบและข้อมูลสำคัญต้องมีการสำรองข้อมูลตามรอบเวลาที่เหมาะสม และต้องสำรองข้อมูลก่อนดำเนินการเปลี่ยนแปลงสำคัญ เช่น การปรับปรุงระบบปฏิบัติการ ฐานข้อมูล ระบบแม่ข่าย อุปกรณ์เครือข่าย หรืออุปกรณ์รักษาความมั่นคงปลอดภัย

๔) ให้จัดเก็บข้อมูลสำรองอย่างน้อยในสื่อหรือสถานที่ที่แยกจากระบบหลักตามความเหมาะสม เพื่อลดความเสี่ยงจากเหตุการณ์ที่กระทบต่อระบบหลักและข้อมูลสำรองพร้อมกัน

๕) ข้อมูลสำรองของระบบสำคัญควรมีสำเนามากกว่าหนึ่งชุด และควรจัดเก็บอย่างน้อยหนึ่งชุดในสถานที่หรือระบบที่แยกออกจากสถานที่ปฏิบัติงานหลักตามความเสี่ยงและความจำเป็น

๓.๔ การคุ้มครองข้อมูลและสื่อสำรอง

๑) ข้อมูลสำรองต้องได้รับการคุ้มครองตามชั้นความลับและระดับความสำคัญของข้อมูล รวมถึงการควบคุมสิทธิ์เข้าถึง การเข้ารหัส และการจัดเก็บในพื้นที่ที่ปลอดภัย

๒) การเข้าถึงข้อมูลสำรอง สื่อสำรอง ระบบสำรอง และบัญชีผู้ดูแลระบบสำรอง ต้องจำกัดเฉพาะผู้ที่ได้รับอนุญาตตามหน้าที่และความจำเป็นในการปฏิบัติงาน

๓) ข้อมูลสำรองที่จัดเก็บในระบบคลาวด์หรืออยู่ภายใต้การดูแลของผู้ให้บริการภายนอก ต้องมีการกำหนดข้อกำหนดด้านการรักษาความลับ การเข้ารหัส การควบคุมสิทธิ์ การแจ้งเหตุการณ์ และการคืนหรือทำลายข้อมูลไว้ในสัญญาหรือข้อตกลง

๔) ให้มีการป้องกันข้อมูลสำรองจากการถูกแก้ไข ลบ หรือเข้ารหัสโดยมิได้รับอนุญาต โดยเฉพาะกรณีภัยคุกคามจากแรนซัมแวร์

๕) สื่อสำรองข้อมูลที่ไม่ใช้งานแล้ว หมดอายุ หรือไม่สามารถใช้งานได้ ต้องทำลายหรือลบข้อมูลด้วยวิธีที่ไม่สามารถกู้คืนได้ และจัดเก็บหลักฐานการดำเนินการไว้เพื่อการตรวจสอบ

๓.๕ การสำรองค่าการกำหนดระบบและอุปกรณ์

๑) ให้สำรองค่าการกำหนดของระบบและอุปกรณ์สำคัญ เช่น เครื่องแม่ข่าย ฐานข้อมูล Firewall Router Switch ระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล และระบบรักษาความมั่นคงปลอดภัยสารสนเทศ

๒) ต้องสำรองค่าการกำหนดก่อนและหลังการเปลี่ยนแปลงที่สำคัญ รวมถึงจัดเก็บข้อมูลการเปลี่ยนแปลงให้สามารถตรวจสอบและย้อนกลับได้

๓) ค่าการกำหนดที่สำรองไว้ต้องจัดเก็บในพื้นที่ที่มีการควบคุมสิทธิ์ และต้องมีการตรวจสอบว่าสามารถ

นำกลับมาใช้กู้คืนการทำงานของระบบได้

๓.๖ การตรวจสอบผลการสำรองข้อมูล

๑) ผู้รับผิดชอบต้องตรวจสอบผลการสำรองข้อมูลตามรอบเวลาที่กำหนด เพื่อยืนยันว่าการสำรองข้อมูลดำเนินการสำเร็จ ครบถ้วน และสามารถใช้งานได้

๒) ต้องจัดทำบันทึกการปฏิบัติงานสำรองข้อมูล เช่น วันและเวลา รายการที่สำรอง สถานะการสำรองข้อผิดพลาด ผู้รับผิดชอบ และแนวทางแก้ไข

๓) หากพบว่าการสำรองข้อมูลไม่สำเร็จ ไม่ครบถ้วน หรือเกิดข้อผิดพลาด ผู้รับผิดชอบต้องเร่งดำเนินการแก้ไข สำรองข้อมูลซ้ำตามความจำเป็น และรายงานผู้บังคับบัญชาหรือเจ้าของระบบเมื่อเกิดผลกระทบต่อข้อมูลหรือระบบสำคัญ

๔) ให้มีการวิเคราะห์สาเหตุของปัญหาการสำรองข้อมูลที่เกิดซ้ำ และกำหนดมาตรการป้องกันหรือปรับปรุงกระบวนการอย่างต่อเนื่อง

๓.๗ การทดสอบการกู้คืนข้อมูลและระบบ

๑) ต้องจัดให้มีการทดสอบการกู้คืนข้อมูลสำรองและระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง หรือตามระดับความสำคัญและความเสี่ยงของระบบ

๒) การทดสอบการกู้คืนต้องครอบคลุมอย่างน้อยการกู้คืนข้อมูล การกู้คืนฐานข้อมูล การกู้คืนค่าการกำหนดระบบ และการตรวจสอบความถูกต้องครบถ้วนของข้อมูลภายหลังการกู้คืน

๓) ระบบสำคัญควรได้รับการทดสอบตามค่า RTO และ RPO ที่กำหนด เพื่อประเมินว่าสามารถกู้คืนและกลับมาให้บริการได้ภายในระยะเวลาที่ยอมรับได้

๔) ให้บันทึกผลการทดสอบ ปัญหา อุปสรรค ระยะเวลาในการกู้คืน ผลการตรวจสอบข้อมูล และข้อเสนอแนะในการปรับปรุงไว้เป็นหลักฐาน

๕) หากผลการทดสอบไม่เป็นไปตามเป้าหมาย ต้องจัดทำแผนแก้ไขปรับปรุง กำหนดผู้รับผิดชอบ และติดตามผลจนกว่าจะสามารถกู้คืนข้อมูลหรือระบบได้ตามเกณฑ์ที่กำหนด

๓.๘ การจัดทำระบบและสถานที่สำรอง

๑) ให้ประเมินความจำเป็นในการจัดทำระบบ อุปกรณ์ เครือข่าย สถานที่ หรือบริการสำรองสำหรับระบบสารสนเทศที่สำคัญตามระดับความเสี่ยงและผลกระทบต่อภารกิจ

๒) ระบบสำรองต้องมีความสามารถในการรองรับการทำงานทดแทนระบบหลักได้ตามขอบเขตและระยะเวลาที่กำหนดในแผนบริหารความต่อเนื่องทางธุรกิจหรือแผนกู้คืนระบบเทคโนโลยีสารสนเทศ

๓) ต้องจัดทำเอกสารขั้นตอนการสลับการทำงานจากระบบหลักไปยังระบบสำรอง และขั้นตอนการกลับมาใช้ระบบหลักเมื่อสถานการณ์กลับสู่ภาวะปกติ

๔) ให้ทดสอบความพร้อมของระบบสำรอง อุปกรณ์สำรอง และสถานที่สำรองตามแผน เพื่อให้มั่นใจว่าสามารถใช้งานได้จริงเมื่อเกิดเหตุฉุกเฉิน

๓.๙ การกู้คืนและการจัดการเหตุการณ์

๑) เมื่อเกิดเหตุที่ส่งผลให้ข้อมูลหรือระบบไม่สามารถใช้งานได้ ให้สำนักเทคโนโลยีดิจิทัลประเมินผลกระทบ จัดลำดับความสำคัญ และดำเนินการกู้คืนตามแผนที่กำหนด

๒) การกู้คืนข้อมูลหรือระบบต้องได้รับอนุมัติจากผู้รับผิดชอบตามระดับความสำคัญของระบบ และให้บันทึกรายละเอียดการดำเนินการทุกครั้ง

๓) ในกรณีเกิดเหตุการณ์จากโปรแกรมไม่ประสงค์ดีหรือแรนซัมแวร์ ต้องตรวจสอบความปลอดภัยของระบบและข้อมูลสำรองก่อนดำเนินการกู้คืน เพื่อป้องกันการนำข้อมูลหรือโปรแกรมอันตรายกลับเข้าสู่ระบบ

๔) หลังการกู้คืน ให้ตรวจสอบความถูกต้อง ความครบถ้วน ความพร้อมใช้งาน และความมั่นคงปลอดภัย

ของระบบ ก่อนเปิดให้ผู้ใช้งานกลับมาใช้บริการ

๕) ภายหลังเหตุการณ์ ให้จัดทำรายงานสรุปสาเหตุ ผลกระทบ ระยะเวลาการกู้คืน บทเรียนที่ได้รับ และแผนปรับปรุงมาตรการสำรองหรือกู้คืนระบบ

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้สำนักเทคโนโลยีดิจิทัลจัดทำคู่มือ ขั้นตอนปฏิบัติงานมาตรฐาน แบบฟอร์ม และรายการตรวจสอบที่เกี่ยวข้อง เช่น แผนสำรองข้อมูล บันทึกผลการสำรองข้อมูล แบบทดสอบการกู้คืน และขั้นตอนการใช้งานระบบสำรอง

๔.๓ ให้ผู้บริหารและผู้บังคับบัญชาสื่อสารบทบาทหน้าที่ของเจ้าของข้อมูล เจ้าของระบบ และผู้ใช้งานในการจัดเก็บข้อมูลในพื้นที่ที่องค์การกำหนดและการสนับสนุนการสำรองข้อมูล

๔.๔ ให้จัดอบรมหรือถ่ายทอดความรู้แก่ผู้ดูแลระบบ ผู้ดูแลฐานข้อมูล ผู้ดูแลเครือข่าย และผู้ที่เกี่ยวข้องกับการกู้คืนระบบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบสำคัญ

๔.๕ ให้สื่อสารผลการทดสอบการกู้คืน ปัญหาที่ตรวจพบ และแนวทางปรับปรุงแก่เจ้าของระบบ ผู้บริหาร และผู้เกี่ยวข้องตามระดับความจำเป็น

๔.๖ ให้ผู้ให้บริการภายนอกที่มีหน้าที่เกี่ยวข้องกับการสำรองข้อมูล ระบบคลาวด์ หรือระบบสำรองรับทราบและปฏิบัติตามข้อกำหนดนี้ รวมถึงข้อกำหนดในสัญญาหรือข้อตกลงการให้บริการ

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
บัญชีรายการข้อมูลและระบบสำรอง	ร้อยละของข้อมูลและระบบสำคัญที่มีรายการกำหนดวิธีการสำรอง ผู้รับผิดชอบ และรอบการสำรองครบถ้วน	ร้อยละ ๑๐๐
ความสำเร็จของการสำรองข้อมูล	ร้อยละของรายการสำรองข้อมูลที่ดำเนินการสำเร็จตามแผน	ไม่น้อยกว่าร้อยละ ๙๘
การแก้ไขการสำรองข้อมูลล้มเหลว	ร้อยละของรายการสำรองข้อมูลที่ล้มเหลวและได้รับการแก้ไขหรือสำรองซ้ำภายในระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
การสำรองค่าการกำหนดระบบ	ร้อยละของระบบและอุปกรณ์สำคัญที่มีการสำรองค่าการกำหนดตามรอบและก่อนการเปลี่ยนแปลงสำคัญ	ร้อยละ ๑๐๐
การทดสอบการกู้คืน	ร้อยละของระบบสำคัญที่ผ่านการทดสอบกู้คืนข้อมูลหรือระบบตามแผน	ร้อยละ ๑๐๐ ต่อปี
ประสิทธิผลการกู้คืน	ร้อยละของการทดสอบกู้คืนที่สามารถดำเนินการได้ตามค่า RTO และ RPO ที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐
การคุ้มครองข้อมูลสำรอง	ร้อยละของข้อมูลสำรองสำคัญที่มีการควบคุมสิทธิ์และเข้ารหัสตามข้อกำหนด	ร้อยละ ๑๐๐
ความพร้อมของระบบสำรอง	ร้อยละของระบบหรืออุปกรณ์สำรองที่ผ่านการทดสอบและพร้อมใช้งานตามแผน	ร้อยละ ๑๐๐
การจัดการสื่อสำรอง	ร้อยละของสื่อสำรองที่หมดอายุหรือเลิกใช้งาน และมีหลักฐานการลบหรือทำลายข้อมูลอย่างปลอดภัย	ร้อยละ ๑๐๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการทดสอบกู้คืน การตรวจสอบ หรือเหตุการณ์จริงที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และรายงานผลการสำรองข้อมูล ผลการทดสอบกู้คืนข้อผิดพลาด และสถานะความพร้อมของระบบสำรองต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้ติดตามผลการสำรองข้อมูลที่ล้มเหลว สถานะข้อมูลสำรองของระบบสำคัญ และความพร้อมของระบบสำรองเป็นรายวัน รายสัปดาห์ หรือรายเดือนตามระดับความสำคัญของระบบ

๕.๓ ให้นำผลการทดสอบกู้คืน เหตุการณ์จริง ข้อค้นพบจากการตรวจสอบ และการเปลี่ยนแปลงของระบบหรือภัยคุกคาม มาใช้ทบทวนและปรับปรุงแผนสำรองข้อมูล แผนกู้คืนระบบ และแผนบริหารความต่อเนื่องทางธุรกิจอย่างน้อยปีละ ๑ ครั้ง

ส่วนที่ ๔
นโยบายและแนวปฏิบัติการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ
(Information Security Audit and Risk Assessment)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดแนวทางในการระบุ วิเคราะห์ ประเมิน จัดการ ติดตาม และทบทวนความเสี่ยงด้านสารสนเทศและความมั่นคงปลอดภัยไซเบอร์ขององค์การคลังสินค้าอย่างเป็นระบบ

๑.๒ เพื่อให้มีการตรวจสอบการปฏิบัติตามนโยบาย มาตรฐาน ระเบียบ ข้อกำหนด และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ รวมถึงการตรวจสอบประสิทธิผลของมาตรการควบคุมที่กำหนด

๑.๓ เพื่อป้องกันและลดผลกระทบจากภัยคุกคาม ช่องโหว่ ความผิดพลาดของบุคลากร ความล้มเหลวของระบบ การเข้าถึงโดยมิได้รับอนุญาต และเหตุการณ์ที่อาจกระทบต่อข้อมูล ระบบสารสนเทศ หรือภารกิจขององค์การ

๑.๔ เพื่อสนับสนุนให้ผู้บริหารสามารถตัดสินใจจัดลำดับความสำคัญในการบริหารความเสี่ยง จัดสรรทรัพยากร และกำหนดมาตรการควบคุมที่เหมาะสมตามระดับความเสี่ยง

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้มีการกำกับติดตาม ตรวจสอบ ประเมินผล รายงานผล และปรับปรุงการดำเนินงานด้านความมั่นคงปลอดภัยสารสนเทศอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับข้อมูลสารสนเทศ ระบบสารสนเทศ ระบบเครือข่าย เว็บไซต์ ฐานข้อมูล ศูนย์ข้อมูล บริการคลาวด์ อุปกรณ์เทคโนโลยีสารสนเทศ ผู้ให้บริการภายนอก และทรัพย์สินสารสนเทศทั้งหมดที่อยู่ภายใต้ความรับผิดชอบขององค์การคลังสินค้า

๒.๒ ครอบคลุมการประเมินความเสี่ยงก่อนเริ่มโครงการ การประเมินความเสี่ยงตามรอบระยะเวลา การประเมินเมื่อมีการเปลี่ยนแปลงสำคัญ และการประเมินภายหลังเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๓ ครอบคลุมการตรวจสอบภายใน การตรวจสอบการปฏิบัติตามนโยบาย การตรวจสอบช่องโหว่ การทดสอบความมั่นคงปลอดภัย การตรวจสอบผู้ให้บริการภายนอก และการติดตามผลการแก้ไขข้อค้นพบ

๒.๔ ใช้บังคับกับคณะกรรมการ ผู้บริหาร เจ้าของระบบ เจ้าของข้อมูล สำนักเทคโนโลยีดิจิทัล ส่วนงานบริหารความเสี่ยง หน่วยตรวจสอบภายใน พนักงาน ลูกจ้าง ผู้รับจ้าง ผู้ให้บริการภายนอก และผู้เกี่ยวข้องกับการใช้งานหรือบริหารจัดการทรัพย์สินสารสนเทศขององค์การ

๓. แนวปฏิบัติ

๓.๑ การกำหนดบทบาท หน้าที่ และความรับผิดชอบ

๑) ให้องค์การกำหนดบทบาท หน้าที่ และความรับผิดชอบของหน่วยงานและบุคลากรที่เกี่ยวข้องกับการบริหารความเสี่ยงและการตรวจสอบด้านสารสนเทศอย่างชัดเจน

๒) ให้สำนักเทคโนโลยีดิจิทัลรับผิดชอบในการระบุทรัพย์สินสารสนเทศ ภัยคุกคาม ช่องโหว่ มาตรการควบคุม และจัดทำข้อมูลประกอบการประเมินความเสี่ยง

๓) ให้เจ้าของระบบและเจ้าของข้อมูลรับผิดชอบในการประเมินผลกระทบ กำหนดระดับความสำคัญของระบบหรือข้อมูล และร่วมพิจารณามาตรการจัดการความเสี่ยง

๔) ให้ส่วนงานบริหารความเสี่ยงหรือหน่วยงานที่ได้รับมอบหมาย กำกับ ติดตาม และรวบรวมผลการประเมินความเสี่ยงด้านสารสนเทศเข้าสู่กระบวนการบริหารความเสี่ยงขององค์การ

๕) ให้หน่วยตรวจสอบภายในหรือผู้ตรวจสอบที่ได้รับมอบหมายดำเนินการตรวจสอบอย่างเป็นอิสระตามแผนการตรวจสอบ และรายงานผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง

๖) ผู้รับผิดชอบการตรวจสอบต้องไม่มีส่วนได้เสียโดยตรงกับกิจกรรม ระบบ หรือกระบวนการที่ตน

ตรวจสอบ หรือให้มีมาตรการทดแทนเพื่อรักษาความเป็นอิสระและความน่าเชื่อถือของผลการตรวจสอบ

๓.๒ การจัดทำทะเบียนทรัพย์สินและการระบุความเสี่ยง

๑) ให้จัดทำและทบทวนทะเบียนทรัพย์สินสารสนเทศที่สำคัญ เช่น ข้อมูล ระบบงาน ฐานข้อมูล อุปกรณ์เครือข่าย เว็บไซต์ บริการคลาวด์ และระบบของผู้ให้บริการภายนอก

๒) ทะเบียนทรัพย์สินสารสนเทศอย่างน้อยต้องระบุเจ้าของทรัพย์สิน ผู้รับผิดชอบ ระดับความสำคัญ สถานที่จัดเก็บหรือให้บริการ ระบบที่เชื่อมโยง และมาตรการควบคุมที่มีอยู่

๓) ให้ระบุภัยคุกคาม ช่องโหว่ เหตุการณ์ที่อาจเกิดขึ้น และปัจจัยเสี่ยงที่อาจส่งผลกระทบต่อความลับ ความถูกต้องครบถ้วน ความพร้อมใช้งาน และการปฏิบัติตามกฎหมายหรือข้อกำหนด

๔) ให้พิจารณาความเสี่ยงจากปัจจัยภายในและภายนอก เช่น บุคลากร กระบวนการทำงาน เทคโนโลยี ผู้ให้บริการภายนอก ภัยธรรมชาติ การโจมตีทางไซเบอร์ และการเปลี่ยนแปลงทางกฎหมาย

๕) ให้ใช้ข้อมูลจากเหตุการณ์จริง ผลการตรวจสอบ ข้อร้องเรียน ผลการทดสอบช่องโหว่ และข่าวสารภัยคุกคามที่เกี่ยวข้อง เป็นข้อมูลประกอบการระบุความเสี่ยง

๓.๓ การประเมินและจัดระดับความเสี่ยง

๑) ให้ประเมินความเสี่ยงโดยพิจารณาอย่างน้อยจากโอกาสที่จะเกิดเหตุการณ์ และระดับผลกระทบหากเหตุการณ์นั้นเกิดขึ้น

๒) ให้กำหนดหลักเกณฑ์การประเมินความเสี่ยงและระดับความเสี่ยงให้ชัดเจน เช่น ความเสี่ยงต่ำ ปานกลาง สูง และสูงมาก เพื่อให้ทุกหน่วยงานใช้เป็นมาตรฐานเดียวกัน

๓) การประเมินผลกระทบต้องพิจารณาอย่างน้อยในด้านการดำเนินงาน การเงิน กฎหมาย ชื่อเสียง ความเชื่อมั่นของผู้มีส่วนได้ส่วนเสีย ความปลอดภัยของข้อมูล และความต่อเนื่องของบริการ

๔) ระบบหรือข้อมูลที่มีความสำคัญสูง ข้อมูลลับ ข้อมูลส่วนบุคคล ระบบที่เชื่อมต่ออินเทอร์เน็ต หรือระบบที่ให้บริการแก่หน่วยงานภายนอก ต้องได้รับการประเมินความเสี่ยงในระดับที่เหมาะสมและมีมาตรการควบคุมเพิ่มเติม

๕) ให้จัดทำทะเบียนความเสี่ยงด้านสารสนเทศ (Information Security Risk Register) โดยระบุความเสี่ยง สาเหตุ ผลกระทบ ระดับความเสี่ยง มาตรการควบคุม ผู้รับผิดชอบ กำหนดเวลา และสถานะการดำเนินงาน

๓.๔ การจัดการและการยอมรับความเสี่ยง

๑) สำหรับความเสี่ยงที่อยู่ในระดับสูงหรือสูงมาก ต้องจัดทำแผนจัดการความเสี่ยงและดำเนินการลดความเสี่ยงโดยเร็ว

๒) แนวทางจัดการความเสี่ยงอาจประกอบด้วย การลดความเสี่ยง การหลีกเลี่ยงความเสี่ยง การถ่ายโอนความเสี่ยง หรือการยอมรับความเสี่ยง ตามความเหมาะสม

๓) แผนจัดการความเสี่ยงต้องระบุมาตรการควบคุม ผู้รับผิดชอบ ทรัพยากร ระยะเวลาดำเนินการ และตัวชี้วัดผลสำเร็จอย่างชัดเจน

๔) การยอมรับความเสี่ยงต้องได้รับอนุมัติจากผู้มีอำนาจตามระดับความเสี่ยงที่องค์การกำหนด และต้องระบุเหตุผล ระยะเวลาการยอมรับความเสี่ยง และมาตรการควบคุมทดแทน

๕) ให้ติดตามความคืบหน้าของแผนจัดการความเสี่ยงอย่างสม่ำเสมอ จนกว่าความเสี่ยงจะลดลงอยู่ในระดับที่องค์การยอมรับได้

๓.๕ การตรวจสอบการปฏิบัติตามและการตรวจสอบภายใน

๑) ให้จัดทำแผนตรวจสอบด้านความมั่นคงปลอดภัยสารสนเทศประจำปี โดยพิจารณาจากระดับความเสี่ยง ความสำคัญของระบบ ผลการตรวจสอบที่ผ่านมา และเหตุการณ์ที่เกิดขึ้น

๒) การตรวจสอบควรครอบคลุมอย่างน้อยเรื่องการควบคุมสิทธิ์เข้าถึง การจัดการบัญชีผู้ใช้ การสำรอง

และกู้คืนข้อมูล การจัดการช่องโหว่ การปรับปรุงแพตช์ การบันทึกเหตุการณ์ การบริหารผู้ให้บริการภายนอก และการปฏิบัติตามนโยบาย

๓) ให้ตรวจสอบหลักฐานการปฏิบัติงาน เช่น บันทึกเหตุการณ์ รายงานการสำรองข้อมูล รายงานการปรับปรุงแพตช์ รายการสิทธิ์ผู้ใช้งาน ผลการตรวจสอบช่องโหว่ และเอกสารการอนุมัติการเปลี่ยนแปลงระบบ

๔) การตรวจสอบต้องบันทึกขอบเขต วิธีการตรวจสอบ ข้อค้นพบ ระดับความรุนแรง ข้อเสนอแนะ และผู้รับผิดชอบในการแก้ไขอย่างชัดเจน

๕) กรณีพบข้อค้นพบที่มีความรุนแรงสูง ต้องรายงานผู้บริหารและผู้รับผิดชอบโดยเร็ว เพื่อดำเนินการควบคุมหรือแก้ไขความเสี่ยงทันที

๓.๖ การตรวจสอบช่องโหว่และการทดสอบความมั่นคงปลอดภัย

๑) ให้มีการตรวจสอบช่องโหว่ของระบบ เครือข่าย เว็บไซต์ และอุปกรณ์สำคัญตามแผนหรือระดับความเสี่ยง

๒) ระบบที่เปิดให้บริการผ่านอินเทอร์เน็ต ระบบสำคัญ หรือระบบที่มีข้อมูลสำคัญ ต้องได้รับการตรวจสอบช่องโหว่ก่อนเปิดใช้งาน และเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

๓) ให้มีการทดสอบความมั่นคงปลอดภัยของระบบตามความเหมาะสม เช่น การทดสอบการเจาะระบบ การทดสอบการตั้งค่าความมั่นคงปลอดภัย หรือการทดสอบการกู้คืนระบบ

๔) การตรวจสอบหรือทดสอบต้องได้รับอนุมัติ กำหนดขอบเขต ช่วงเวลา ผู้รับผิดชอบ และวิธีการป้องกันผลกระทบต่อระบบงานอย่างชัดเจน

๕) ข้อบกพร่องหรือช่องโหว่ที่พบต้องได้รับการจัดลำดับความรุนแรง กำหนดผู้รับผิดชอบ และแก้ไขหรือกำหนดมาตรการควบคุมทดแทนภายในระยะเวลาที่กำหนด

๓.๗ การประเมินผู้ให้บริการภายนอก

๑) ผู้ให้บริการภายนอกที่เข้าถึงข้อมูล ระบบสำคัญ หรือโครงสร้างพื้นฐานสารสนเทศขององค์การ ต้องได้รับการประเมินความเสี่ยงก่อนเริ่มใช้บริการ และทบทวนตามรอบระยะเวลาที่กำหนด

๒) ให้ประเมินการปฏิบัติตามข้อตกลง ระดับการให้บริการ มาตรการคุ้มครองข้อมูล การแจ้งเหตุการณ์ การควบคุมสิทธิ์ และการแก้ไขข้อบกพร่องของผู้ให้บริการ

๓) กรณีพบว่าผู้ให้บริการไม่ปฏิบัติตามข้อกำหนด ให้หน่วยงานเจ้าของสัญญาดำเนินการติดตามแผนแก้ไขปรับปรุง และรายงานผู้บริหารเมื่อมีผลกระทบหรือความเสี่ยงสูง

๔) ผลการประเมินผู้ให้บริการต้องนำไปใช้ประกอบการพิจารณาต่ออายุสัญญา ปรับปรุงเงื่อนไขการให้บริการ หรือกำหนดมาตรการควบคุมเพิ่มเติม

๓.๘ การรายงาน การติดตาม และการทบทวน

๑) ให้รายงานผลการประเมินความเสี่ยง ผลการตรวจสอบ ข้อค้นพบ เหตุการณ์สำคัญ และสถานะการแก้ไขต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องตามรอบระยะเวลาที่กำหนด

๒) รายงานต้องแสดงระดับความเสี่ยง ประเด็นสำคัญ แนวโน้ม สถานะการแก้ไข ปัญหาอุปสรรค และข้อเสนอแนะในการปรับปรุงอย่างชัดเจน

๓) ให้ติดตามข้อค้นพบและแผนจัดการความเสี่ยงจนกว่าจะดำเนินการแล้วเสร็จ หรือได้รับอนุมัติให้ยอมรับความเสี่ยงตามกระบวนการที่กำหนด

๔) ให้ทบทวนการประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี กระบวนการทำงาน ผู้ให้บริการ กฎหมาย หรือเมื่อเกิดเหตุการณ์ที่มีนัยสำคัญ

๕) ให้นำผลการประเมินและการตรวจสอบมาใช้ในการปรับปรุงนโยบาย มาตรการควบคุม แผนงบประมาณ แผนพัฒนาระบบ และแผนสร้างความรู้ความเข้าใจด้านความมั่นคงปลอดภัยสารสนเทศ

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้สำนักเทคโนโลยีดิจิทัลและส่วนงานบริหารความเสี่ยงจัดทำคู่มือ แบบฟอร์ม และรายการตรวจสอบที่เกี่ยวข้อง เช่น แบบประเมินความเสี่ยง ทะเบียนความเสี่ยง แบบติดตามแผนจัดการความเสี่ยง และแบบรายงานข้อค้นพบ

๔.๓ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารบทบาทหน้าที่ด้านการประเมินความเสี่ยงและการแก้ไขข้อค้นพบแก่บุคลากรในสังกัด

๔.๔ ให้จัดอบรมหรือชี้แจงแก่เจ้าของระบบ เจ้าของข้อมูล ผู้ดูแลระบบ และผู้ปฏิบัติงานที่เกี่ยวข้องเกี่ยวกับวิธีการระบุ ประเมิน และรายงานความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๔.๕ ให้สื่อสารผลการตรวจสอบ ข้อค้นพบที่สำคัญ และบทเรียนจากเหตุการณ์แก่ผู้เกี่ยวข้องตามระดับความจำเป็น โดยไม่เปิดเผยรายละเอียดทางเทคนิคที่อาจเพิ่มความเสี่ยงต่อองค์การ

๔.๖ ให้ผู้ให้บริการภายนอกที่เกี่ยวข้องรับทราบข้อกำหนดด้านการประเมินความเสี่ยง การตรวจสอบ และการส่งมอบหลักฐานตามเงื่อนไขในสัญญาหรือข้อตกลง

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การประเมินความเสี่ยง	ร้อยละของระบบและทรัพย์สินสารสนเทศสำคัญที่ได้รับการประเมินความเสี่ยงตามรอบระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
ทะเบียนความเสี่ยง	ร้อยละของความเสี่ยงที่มีการระบุเจ้าของความเสี่ยง มาตรการควบคุม และแผนจัดการความเสี่ยงครบถ้วน	ร้อยละ ๑๐๐
การจัดการความเสี่ยงสูง	ร้อยละของความเสี่ยงระดับสูงและสูงมากที่มีแผนจัดการหรือได้รับการยอมรับความเสี่ยงอย่างถูกต้อง	ร้อยละ ๑๐๐
การดำเนินงานตามแผน	ร้อยละของแผนจัดการความเสี่ยงที่ดำเนินการแล้วเสร็จภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐
การตรวจสอบตามแผน	ร้อยละของกิจกรรมตรวจสอบด้านสารสนเทศที่ดำเนินการได้ตามแผนตรวจสอบประจำปี	ไม่น้อยกว่าร้อยละ ๙๐
การตรวจสอบช่องโหว่	ร้อยละของระบบสำคัญและระบบที่เชื่อมต่ออินเทอร์เน็ตที่ได้รับการตรวจสอบช่องโหว่ตามแผน	ร้อยละ ๑๐๐
การแก้ไขช่องโหว่	ร้อยละของช่องโหว่ระดับวิกฤตและระดับสูงที่ได้รับการแก้ไขหรือมีมาตรการควบคุมทดแทนภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การติดตามข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบที่ได้รับการแก้ไขและปิดประเด็นภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐
การประเมินผู้ให้บริการ	ร้อยละของผู้ให้บริการภายนอกที่มีความเสี่ยงสูงและได้รับการประเมินตามรอบที่กำหนด	ร้อยละ ๑๐๐
การรายงานผู้บริหาร	ร้อยละของรายงานผลการประเมินความเสี่ยงและผลการตรวจสอบที่เสนอผู้บริหารตามกำหนดเวลา	ร้อยละ ๑๐๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลร่วมกับส่วนงานบริหารความเสี่ยงและหน่วยตรวจสอบภายใน รวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้ติดตามความเสี่ยงระดับสูง ความเสี่ยงที่เกี่ยวข้องกับระบบสำคัญ และข้อค้นพบระดับร้ายแรงเป็นรายเดือนหรือรายไตรมาส จนกว่าจะดำเนินการแก้ไขแล้วเสร็จ

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี ภารกิจ รูปแบบการให้บริการ หรือเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่มีนัยสำคัญ

ส่วนที่ ๕
นโยบายและแนวปฏิบัติการสร้างความรู้ความเข้าใจเกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ
(Information Security Awareness and Training)

๑. วัตถุประสงค์

๑.๑ เพื่อส่งเสริมให้คณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้รับจ้าง และผู้ให้บริการภายนอก มีความรู้ ความเข้าใจ และตระหนักถึงความสำคัญของการรักษาความมั่นคงปลอดภัยสารสนเทศ

๑.๒ เพื่อให้ผู้เกี่ยวข้องสามารถปฏิบัติตามนโยบาย มาตรฐาน และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศขององค์การคลังสินค้าได้อย่างถูกต้องและเหมาะสมตามบทบาทหน้าที่

๑.๓ เพื่อลดความเสี่ยงจากการกระทำของบุคลากรโดยรู้เท่าไม่ถึงการณ์ ความผิดพลาดจากการปฏิบัติงาน การหลอกลวงทางอิเล็กทรอนิกส์ การเปิดเผยข้อมูลโดยมิได้รับอนุญาต และภัยคุกคามทางไซเบอร์รูปแบบต่าง ๆ

๑.๔ เพื่อพัฒนาทักษะของบุคลากรที่มีหน้าที่เฉพาะด้าน เช่น ผู้ดูแลระบบ ผู้พัฒนาระบบ เจ้าของข้อมูล และผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ให้สามารถป้องกัน ตรวจจับ และตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้มีแผนการสร้างความรู้ความเข้าใจ การติดตามผล หลักฐานการดำเนินงาน ตัวชี้วัด และการปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้พัฒนาระบบ เจ้าของข้อมูล ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นที่เข้าถึงหรือใช้งานข้อมูล ระบบสารสนเทศ หรือทรัพย์สินสารสนเทศขององค์การคลังสินค้า

๒.๒ ครอบคลุมการสื่อสาร การฝึกอบรม การถ่ายทอดความรู้ การทดสอบความตระหนัก การแจ้งเตือนภัยคุกคาม การเผยแพร่คู่มือ และการประเมินผลด้านความมั่นคงปลอดภัยสารสนเทศ

๒.๓ ครอบคลุมเนื้อหาความรู้ที่เกี่ยวข้องกับการรักษาความมั่นคงปลอดภัยสารสนเทศ เช่น การใช้งานบัญชีผู้ใช้และรหัสผ่าน การคุ้มครองข้อมูล การใช้อีเมลและอินเทอร์เน็ต การป้องกันฟิชชิงและโปรแกรมไม่ประสงค์ดี การใช้อุปกรณ์พกพา การปฏิบัติงานจากระยะไกล และการแจ้งเหตุการณ์

๒.๔ ให้สำนักเทคโนโลยีดิจิทัลร่วมกับสำนักทรัพยากรมนุษย์ หน่วยงานเจ้าของข้อมูล และผู้บังคับบัญชาของแต่ละหน่วยงาน รับผิดชอบในการกำหนดแผน ดำเนินการ และติดตามผลตามนโยบายนี้

๓. แนวปฏิบัติ

๓.๑ การจัดทำแผนสร้างความรู้ความเข้าใจ

๑) ให้สำนักเทคโนโลยีดิจิทัลจัดทำแผนการสร้างความรู้ความเข้าใจและการฝึกอบรมด้านความมั่นคงปลอดภัยสารสนเทศประจำปี

๒) แผนการสร้างความรู้ความเข้าใจต้องกำหนดกลุ่มเป้าหมาย หัวข้อการสื่อสาร วิธีการดำเนินงาน ระยะเวลา ผู้รับผิดชอบ งบประมาณ และตัวชี้วัดผลสำเร็จอย่างชัดเจน

๓) ให้พิจารณาจัดทำเนื้อหาให้สอดคล้องกับบทบาทหน้าที่ ระดับสิทธิ์การเข้าถึงข้อมูล ระดับความเสี่ยง และลักษณะการปฏิบัติงานของบุคลากรแต่ละกลุ่ม

๔) ให้ทบทวนและปรับปรุงแผนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงนโยบาย ระบบเทคโนโลยี กฎหมาย หรือภัยคุกคามที่มีนัยสำคัญ

๓.๒ การอบรมและการรับทราบนโยบาย

๑) บุคลากรทุกคนต้องได้รับการสื่อสารหรืออบรมความรู้พื้นฐานด้านความมั่นคงปลอดภัยสารสนเทศ

อย่างน้อยปีละ ๑ ครั้ง

๒) บุคลากรเข้าใหม่ต้องได้รับการชี้แจงนโยบาย ระเบียบ และแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศก่อนหรือภายในระยะเวลาที่องค์การกำหนดหลังเริ่มปฏิบัติงาน

๓) บุคลากรที่มีหน้าที่เฉพาะด้าน เช่น ผู้ดูแลระบบ ผู้พัฒนาระบบ ผู้ดูแลฐานข้อมูล ผู้ดูแลเครือข่าย และเจ้าของข้อมูล ต้องได้รับการอบรมเชิงลึกตามบทบาทหน้าที่และระดับความเสี่ยง

๔) ผู้รับจ้าง ผู้ให้บริการภายนอก หรือบุคคลภายนอกที่ได้รับอนุญาตให้เข้าถึงข้อมูลหรือระบบขององค์การ ต้องได้รับทราบและยอมรับข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศก่อนเริ่มปฏิบัติงาน

๕) ให้มีการจัดเก็บหลักฐานการเข้าร่วมอบรม การรับทราบนโยบาย หรือการผ่านการทดสอบของผู้เกี่ยวข้อง เพื่อใช้ในการตรวจสอบย้อนหลัง

๓.๓ หัวข้อการสร้างความรู้ความเข้าใจ

๑) ให้มีเนื้อหาขั้นพื้นฐานสำหรับบุคลากรทุกคน อย่างน้อยดังต่อไปนี้

- การใช้บัญชีผู้ใช้งาน รหัสผ่าน และการพิสูจน์ตัวตนอย่างปลอดภัย
- การจำแนก การจัดเก็บ การใช้ และการส่งต่อข้อมูลตามชั้นความลับ
- การป้องกันข้อมูลส่วนบุคคลและข้อมูลสำคัญขององค์การ
- การใช้อีเมล เว็บไซต์ อินเทอร์เน็ต และสื่อสังคมออนไลน์อย่างเหมาะสม
- การสังเกตและป้องกันอีเมลหลอกลวง ฟิชชิง ลิงก์อันตราย และไฟล์แนบที่น่าสงสัย
- การป้องกันโปรแกรมไม่ประสงค์ดีและแรนซัมแวร์
- การใช้งานอุปกรณ์คอมพิวเตอร์ อุปกรณ์พกพา และสื่อบันทึกข้อมูลอย่างปลอดภัย
- การปฏิบัติงานจากระยะไกลและการเชื่อมต่อผ่านเครือข่ายสาธารณะ
- ขั้นตอนและช่องทางการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๒) ให้มีเนื้อหาเฉพาะสำหรับผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศตามความรับผิดชอบ เช่น การจัดการช่องโหว่ การบริหารสิทธิ์ผู้ดูแลระบบ การจัดการบันทึกเหตุการณ์ การสำรองและกู้คืนข้อมูล การพัฒนาระบบอย่างมั่นคงปลอดภัย และการตอบสนองต่อเหตุการณ์

๓) ให้ปรับปรุงเนื้อหาการสื่อสารและการอบรมให้ทันต่อรูปแบบภัยคุกคาม เหตุการณ์ หรือข้อค้นพบจากการตรวจสอบที่เกิดขึ้นกับองค์การหรือหน่วยงานที่มีลักษณะใกล้เคียงกัน

๓.๔ การสื่อสารและการสร้างความตระหนักอย่างต่อเนื่อง

๑) ให้จัดกิจกรรมสื่อสารสร้างความตระหนักอย่างต่อเนื่อง เช่น ข่าวสาร บทความ อินโฟกราฟิก อีเมลแจ้งเตือน คู่มือ วิดีโอสั้น แบบทดสอบ หรือกิจกรรมรณรงค์

๒) ให้สื่อสารข้อมูลเกี่ยวกับภัยคุกคาม ช่องโหว่ เหตุการณ์ที่สำคัญ หรือแนวทางป้องกันแก่บุคลากรและผู้เกี่ยวข้องโดยรวดเร็ว

๓) การสื่อสารต้องใช้ภาษาที่เข้าใจง่าย เหมาะสมกับกลุ่มเป้าหมาย และระบุแนวทางปฏิบัติที่ชัดเจน

๔) ให้ผู้บังคับบัญชาทุกระดับสนับสนุนและกำกับดูแลให้บุคลากรในสังกัดเข้าร่วมกิจกรรมการสร้างความรู้ความเข้าใจตามแผนที่กำหนด

๕) ให้จัดทำช่องทางสำหรับให้บุคลากรสอบถามข้อสงสัย ขอคำแนะนำ หรือรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศได้อย่างสะดวกและรวดเร็ว

๓.๕ การทดสอบความตระหนักและการประเมินผล

๑) ให้มีการประเมินความรู้ ความเข้าใจ และพฤติกรรมด้านความมั่นคงปลอดภัยสารสนเทศของบุคลากรตามความเหมาะสม เช่น แบบทดสอบก่อนและหลังอบรม แบบประเมินออนไลน์ หรือการสำรวจความเข้าใจ

๒) ให้มีการทดสอบสถานการณ์จำลอง เช่น การทดสอบอีเมลฟิชชิง การจำลองเหตุการณ์ข้อมูลรั่วไหล

หรือการฝึกซ้อมแจ้งเหตุ เพื่อประเมินความพร้อมของบุคลากร

๓) การทดสอบต้องดำเนินการโดยคำนึงถึงความเหมาะสม ไม่กระทบต่อการปฏิบัติงาน และใช้ผลการทดสอบเพื่อพัฒนาความรู้ความเข้าใจ มิใช่เพื่อมุ่งลงโทษบุคลากร

๔) กรณีพบว่าบุคลากรมีผลการประเมินต่ำ หรือมีการปฏิบัติที่ไม่สอดคล้องกับนโยบาย ให้จัดการอบรมเพิ่มเติม ให้คำแนะนำ หรือกำหนดมาตรการแก้ไขตามความเหมาะสม

๕) ให้รวบรวม วิเคราะห์ และสรุปผลการอบรม การทดสอบ และเหตุการณ์ที่เกิดจากปัจจัยด้านบุคลากร เพื่อนำไปปรับปรุงแผนและเนื้อหาการสื่อสารในรอบถัดไป

๓.๖ การจัดการเมื่อมีการไม่ปฏิบัติตามนโยบาย

๑) บุคลากรที่ไม่ปฏิบัติตามนโยบายหรือแนวปฏิบัติด้านความมั่นคงปลอดภัยสารสนเทศ ต้องได้รับคำแนะนำ ตักเตือน หรือดำเนินการตามระเบียบ ข้อบังคับ และอำนาจหน้าที่ขององค์การ

๒) กรณีการไม่ปฏิบัติตามเกิดจากการขาดความรู้หรือความเข้าใจ ให้หน่วยงานที่เกี่ยวข้องจัดให้มีการทบทวนความรู้หรืออบรมเพิ่มเติมโดยเร็ว

๓) กรณีพบการกระทำที่อาจก่อให้เกิดความเสียหายร้ายแรงต่อข้อมูล ระบบ หรือชื่อเสียงขององค์การ ให้รายงานผู้บังคับบัญชาและดำเนินการตามกระบวนการบริหารจัดการเหตุการณ์และระเบียบที่เกี่ยวข้อง

๔) ให้บันทึกข้อค้นพบ สาเหตุ และมาตรการป้องกัน เพื่อใช้พัฒนาการสื่อสารและลดโอกาสเกิดเหตุซ้ำ

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้บุคลากรรับทราบและถือปฏิบัติอย่างต่อเนื่อง

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำสื่อประชาสัมพันธ์ คู่มือ และสื่อการเรียนรู้ที่เหมาะสมกับกลุ่มเป้าหมาย เช่น คู่มือการใช้รหัสผ่านอย่างปลอดภัย แนวทางป้องกันฟิชชิง คู่มือการแจ้งเหตุ และข้อควรระวังในการใช้งานอุปกรณ์พกพา

๔.๔ ให้จัดอบรมหรือกิจกรรมสร้างความตระหนักแก่บุคลากรทุกระดับอย่างน้อยปีละ ๑ ครั้ง รวมถึงการสื่อสารเพิ่มเติมเมื่อเกิดภัยคุกคามหรือเหตุการณ์สำคัญ

๔.๕ ให้สื่อสารข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศแก่ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลภายนอกที่เกี่ยวข้องก่อนอนุญาตให้เข้าถึงข้อมูลหรือระบบขององค์การ

๔.๖ ให้เผยแพร่ช่องทางติดต่อและขั้นตอนการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างชัดเจน เพื่อให้บุคลากรสามารถแจ้งเหตุได้โดยเร็ว

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การดำเนินการตามแผน	ร้อยละของกิจกรรมการสร้างความรู้ความเข้าใจที่ดำเนินการได้ตามแผนประจำปี	ไม่น้อยกว่าร้อยละ ๙๐
การรับทราบนโยบาย	ร้อยละของบุคลากรและผู้เกี่ยวข้องที่ลงนามรับทราบหรือผ่านการรับทราบนโยบาย	ร้อยละ ๑๐๐
การเข้าร่วมอบรม	ร้อยละของบุคลากรกลุ่มเป้าหมายที่เข้าร่วมการอบรมหรือกิจกรรมตามแผน	ไม่น้อยกว่าร้อยละ ๙๐
ผลการประเมินความรู้	ร้อยละของผู้เข้าร่วมอบรมที่ผ่านเกณฑ์การประเมินหลังการอบรม	ไม่น้อยกว่าร้อยละ ๙๐

การอบรมบุคลากรเข้าใหม่	ร้อยละของบุคลากรเข้าใหม่ที่ได้รับการสื่อสารหรืออบรมภายในระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
การอบรมตามบทบาท	ร้อยละของผู้ดูแลระบบ ผู้พัฒนาระบบ และผู้ปฏิบัติงานเฉพาะด้านที่ได้รับการอบรมตามบทบาทหน้าที่	ไม่น้อยกว่าร้อยละ ๙๐
การทดสอบฟิชชิง	อัตราการคลิกลิงก์หรือเปิดไฟล์ต้องสงสัย และอัตราการรายงานอีเมลต้องสงสัยจากการทดสอบ	อัตราการคลิกลดลง และอัตราการรายงานเพิ่มขึ้นอย่างต่อเนื่อง
การแจ้งเหตุ	จำนวนและความรวดเร็วของการแจ้งเหตุการณ์หรือข้อสงสัยด้านความมั่นคงปลอดภัยโดยบุคลากร	เป็นไปตามขั้นตอนและระยะเวลาที่กำหนด
เหตุการณ์จากปัจจัยบุคลากร	จำนวนเหตุการณ์ด้านความมั่นคงปลอดภัยที่เกิดจากการไม่ปฏิบัติตามนโยบายหรือขาดความรู้	ลดลงอย่างต่อเนื่อง
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการประเมินหรือการทดสอบที่ได้รับการแก้ไขหรือจัดอบรมเพิ่มเติมภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลร่วมกับสำนักทรัพยากรมนุษย์รวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้มีการติดตามผลการเข้าร่วมอบรม การรับทราบนโยบาย และผลการทดสอบเป็นรายไตรมาสหรือรายรอบกิจกรรม เพื่อแก้ไขกรณีที่บุคลากรยังไม่ได้เข้าร่วมตามแผน

๕.๓ ให้นำผลการประเมิน เหตุการณ์ ข้อร้องเรียน และข้อค้นพบจากการตรวจสอบ มาใช้ทบทวนและปรับปรุงแผน เนื้อหา วิธีการสื่อสาร และมาตรการสร้างความรู้ความเข้าใจอย่างต่อเนื่อง

ส่วนที่ ๖
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศ
(Data and Information Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดนโยบายและแนวปฏิบัติในการคุ้มครองข้อมูลสารสนเทศขององค์การคลังสินค้า ให้มีความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และความพร้อมใช้งาน (Availability)

๑.๒ เพื่อป้องกันความเสี่ยง ความเสียหาย การสูญหาย การรั่วไหล การแก้ไขเปลี่ยนแปลง การทำลาย หรือการเข้าถึงข้อมูลสารสนเทศโดยมิได้รับอนุญาต

๑.๓ เพื่อกำหนดให้มีการจำแนกข้อมูล กำหนดเจ้าของข้อมูล ควบคุมการเข้าถึง ใช้งาน จัดเก็บ รับส่ง สำรอง และทำลายข้อมูลอย่างเหมาะสมตามระดับความสำคัญของข้อมูล

๑.๔ เพื่อสนับสนุนการบริหารจัดการข้อมูล การเชื่อมโยงและแลกเปลี่ยนข้อมูล การบริหารความเสี่ยงด้านเทคโนโลยีดิจิทัล และการตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศอย่างเป็นระบบ

๑.๕ เพื่อให้การดำเนินงานขององค์การคลังสินค้าเป็นไปตามกฎหมาย ระเบียบ ข้อบังคับ มาตรฐาน และหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัลที่เกี่ยวข้อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับข้อมูลสารสนเทศทุกประเภทขององค์การคลังสินค้า ไม่ว่าจะอยู่ในรูปแบบเอกสาร ข้อมูลอิเล็กทรอนิกส์ ฐานข้อมูล ภาพ เสียง วิดีโอ สื่อบันทึกข้อมูล ระบบคลาวด์ หรือรูปแบบอื่นใด

๒.๒ ครอบคลุมข้อมูลที่อยู่ระหว่างการจัดเก็บ การประมวลผล การใช้งาน การสำรอง การรับส่ง การเผยแพร่ การแลกเปลี่ยน และการทำลายข้อมูล

๒.๓ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการภายนอก และบุคคลอื่นใดที่ได้รับอนุญาตให้เข้าถึง ใช้งาน หรือบริหารจัดการข้อมูลสารสนเทศขององค์การคลังสินค้า

๒.๔ ให้หน่วยงานเจ้าของข้อมูล เจ้าของระบบ และสำนักเทคโนโลยีดิจิทัลร่วมกันรับผิดชอบในการปฏิบัติตามนโยบายนี้

๓. แนวปฏิบัติ

๓.๑ การกำหนดเจ้าของข้อมูลและการจัดทำทะเบียนข้อมูล

๑) ให้แต่ละหน่วยงานกำหนดผู้รับผิดชอบข้อมูลหรือเจ้าของข้อมูล (Data Owner) สำหรับข้อมูลที่อยู่ในความรับผิดชอบของหน่วยงานอย่างชัดเจน

๒) เจ้าของข้อมูลมีหน้าที่กำหนดระดับชั้นความลับ วัตถุประสงค์การใช้งาน ผู้มีสิทธิ์เข้าถึง ระยะเวลาการเก็บรักษา และแนวทางการทำลายข้อมูล

๓) ให้จัดทำและทบทวนทะเบียนข้อมูลสารสนเทศที่สำคัญขององค์การอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสาระสำคัญ

๔) ข้อมูลสารสนเทศที่มีความสำคัญต่อภารกิจ การเงิน การจัดเก็บสินค้า คู่ค้า หรือข้อมูลส่วนบุคคล ต้องได้รับการระบุและกำหนดมาตรการคุ้มครองเป็นพิเศษ

๓.๒ การจำแนกประเภทและชั้นความลับของข้อมูล

๑) ให้จำแนกข้อมูลสารสนเทศตามความสำคัญ ผลกระทบ และความอ่อนไหวของข้อมูล อย่างน้อยเป็น ๔ ระดับ ดังนี้

- **ข้อมูลสาธารณะ:** ข้อมูลที่เปิดเผยต่อสาธารณะได้ตามกฎหมายหรือได้รับอนุมัติแล้ว
- **ข้อมูลใช้ภายใน:** ข้อมูลสำหรับใช้ในการปฏิบัติงานภายในองค์การ
- **ข้อมูลลับ:** ข้อมูลที่หากเปิดเผยอาจส่งผลกระทบต่อการดำเนินงาน สิทธิประโยชน์ หรือชื่อเสียงขององค์การ
- **ข้อมูลลับมาก:** ข้อมูลที่หากเปิดเผย สูญหาย หรือถูกแก้ไข อาจก่อให้เกิดผลกระทบร้ายแรงต่อองค์การ บุคคล หรือภารกิจสำคัญ

๒) ให้มีการแสดงชั้นความลับบนเอกสาร แฟ้มข้อมูล ระบบ หรือสื่อบันทึกข้อมูลตามความเหมาะสม

๓) การเปลี่ยนแปลงชั้นความลับ การเปิดเผย หรือการส่งต่อข้อมูล ต้องได้รับอนุมัติจากเจ้าของข้อมูลหรือผู้มีอำนาจตามที่กำหนด

๓.๓ การควบคุมการเข้าถึงข้อมูล

๑) ให้กำหนดสิทธิ์เข้าถึงข้อมูลตามหน้าที่ ความรับผิดชอบ และความจำเป็นในการปฏิบัติงาน โดยยึดหลักสิทธิ์น้อยที่สุดเท่าที่จำเป็น (Least Privilege) และหลักการจำเป็นต้องรู้ (Need-to-Know)

๒) ผู้ใช้งานต้องใช้บัญชีผู้ใช้งานของตนเอง ห้ามใช้บัญชีร่วมกัน หรือเปิดเผยรหัสผ่านให้ผู้อื่นทราบ ๓) การขอใช้ การเปลี่ยนแปลง และการยกเลิกสิทธิ์เข้าถึงข้อมูลหรือระบบ ต้องดำเนินการตามขั้นตอนที่องค์การกำหนด และได้รับอนุมัติจากผู้บังคับบัญชาหรือเจ้าของข้อมูล

๔) ให้ทบทวนสิทธิ์เข้าถึงข้อมูลและระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง และดำเนินการยกเลิกสิทธิ์ทันทีเมื่อพนักงานพ้นสภาพ โยกย้ายหน้าที่ หรือไม่มีความจำเป็นต้องใช้งาน

๕) การเข้าถึงข้อมูลลับหรือข้อมูลลับมาก ต้องมีมาตรการยืนยันตัวตนที่เหมาะสม และมีการบันทึกประวัติการเข้าถึงเพื่อให้ตรวจสอบย้อนหลังได้

๓.๔ การจัดเก็บ ใช้งาน และรับส่งข้อมูล

๑) ให้จัดเก็บข้อมูลตามชั้นความลับในสถานที่ ระบบ หรือสื่อที่มีมาตรการป้องกันเหมาะสม

๒) ข้อมูลลับ ข้อมูลลับมาก ข้อมูลส่วนบุคคล และข้อมูลสำคัญขององค์การ ต้องได้รับการคุ้มครองระหว่างการจัดเก็บและการรับส่ง เช่น การกำหนดสิทธิ์เข้าถึง การเข้ารหัสข้อมูล หรือการใช้ช่องทางรับส่งที่ปลอดภัย

๓) ห้ามจัดเก็บข้อมูลขององค์การไว้ในอุปกรณ์ส่วนบุคคล บัญชีอีเมลส่วนบุคคล หรือบริการจัดเก็บข้อมูลภายนอกที่องค์การไม่ได้อนุมัติ

๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะหรืออินเทอร์เน็ต ต้องใช้ช่องทางการสื่อสารที่มีการเข้ารหัสและได้รับอนุมัติจากองค์การ

๕) ห้ามคัดลอก ส่งต่อ เผยแพร่ ถ่ายภาพหน้าจอ หรือเปิดเผยข้อมูลแก่บุคคลภายนอก เว้นแต่ได้รับอนุมัติจากเจ้าของข้อมูลและเป็นไปตามกฎหมายหรือระเบียบที่เกี่ยวข้อง

๖) การนำสื่อบันทึกข้อมูลแบบพกพามาใช้งาน ต้องได้รับอนุญาตและผ่านการตรวจสอบด้านความมั่นคงปลอดภัยตามที่สำนักเทคโนโลยีดิจิทัลกำหนด

๓.๕ การสำรอง กู้คืน และการเก็บรักษาข้อมูล

๑) ให้หน่วยงานที่รับผิดชอบระบบสารสนเทศจัดทำแผนสำรองข้อมูลสำหรับข้อมูลและระบบที่สำคัญตามระดับความเสี่ยงและความจำเป็นทางธุรกิจ

๒) ข้อมูลสำรองต้องได้รับการป้องกันจากการเข้าถึงโดยไม่ได้รับอนุญาต การสูญหาย การแก้ไข หรือการถูกทำลาย

๓) ให้ทดสอบการกู้คืนข้อมูลและระบบสำคัญตามแผนอย่างน้อยปีละ ๑ ครั้ง และบันทึกผลการทดสอบเพื่อใช้ปรับปรุง

๔) ให้กำหนดระยะเวลาการเก็บรักษาข้อมูลให้สอดคล้องกับกฎหมาย ระเบียบ ภารกิจ และความจำเป็น

ขององค์การ

๕) เมื่อครบกำหนดระยะเวลาการเก็บรักษา ให้ดำเนินการลบ ทำลาย หรือทำให้ข้อมูลไม่สามารถระบุตัวบุคคลได้อย่างปลอดภัยตามประเภทของข้อมูลและสื่อบันทึกข้อมูล

๓.๖ การแลกเปลี่ยน เชื่อมโยง และเปิดเผยข้อมูล

๑) การแลกเปลี่ยนหรือเชื่อมโยงข้อมูลกับหน่วยงานภายนอก ต้องมีวัตถุประสงค์ ขอบเขต ประเภทข้อมูล ผู้รับผิดชอบ และมาตรการรักษาความมั่นคงปลอดภัยที่ชัดเจน

๒) ก่อนส่งหรือเปิดเผยข้อมูล ให้ตรวจสอบความถูกต้อง ครบถ้วน ความเหมาะสมของผู้รับ และสิทธิในการเปิดเผยข้อมูล

๓) กรณีมีการส่งข้อมูลให้ผู้ให้บริการภายนอก ต้องกำหนดเงื่อนไขการรักษาความลับ การคุ้มครองข้อมูล การควบคุมสิทธิ์ การแจ้งเหตุละเมิด และการคืนหรือทำลายข้อมูลไว้ในสัญญาหรือข้อตกลง

๔) การเปิดเผยข้อมูลสู่สาธารณะต้องผ่านการตรวจสอบและอนุมัติจากผู้มีอำนาจก่อนทุกครั้ง

๓.๗ การบริหารจัดการเหตุการณ์ด้านข้อมูลสารสนเทศ

๑) ผู้ใช้งานที่พบหรือสงสัยว่าข้อมูลสูญหาย รั่วไหล ถูกเข้าถึง ถูกแก้ไข หรือถูกทำลายโดยมิได้รับอนุญาต ต้องแจ้งสำนักเทคโนโลยีดิจิทัลหรือผู้รับผิดชอบโดยทันที

๒) หน่วยงานที่เกี่ยวข้องต้องประเมินผลกระทบ ควบคุมเหตุการณ์ รวบรวมพยานหลักฐาน ดำเนินการกู้คืน และรายงานผู้บริหารตามระดับความรุนแรงของเหตุการณ์

๓) ให้มีการบันทึกเหตุการณ์ วิเคราะห์สาเหตุ และกำหนดมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ

๔) เหตุการณ์ที่เกี่ยวข้องกับข้อมูลส่วนบุคคลหรือข้อมูลสำคัญ ต้องดำเนินการตามกฎหมาย ระเบียบ และกระบวนการแจ้งเหตุที่องค์การกำหนด

๓.๘ การประเมินความเสี่ยงและการตรวจสอบ

๑) ให้มีการประเมินความเสี่ยงด้านข้อมูลสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ กระบวนการ ข้อมูล หรือภัยคุกคามที่สำคัญ

๒) ให้กำหนดมาตรการควบคุมความเสี่ยงตามระดับความเสี่ยง และติดตามผลการดำเนินงานจนกว่าความเสี่ยงจะอยู่ในระดับที่ยอมรับได้

๓) ให้มีการตรวจสอบการปฏิบัติตามนโยบาย การทบทวนการเข้าถึงข้อมูล คุณภาพข้อมูล และประสิทธิผลของมาตรการควบคุมอย่างสม่ำเสมอ

๔) ให้นำผลการตรวจสอบ เหตุการณ์ และผลการวัดประสิทธิผลมาใช้ปรับปรุงนโยบาย แนวปฏิบัติ และแผนบริหารจัดการข้อมูลอย่างต่อเนื่อง

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านช่องทางสื่อสารภายใน เช่น ระบบอินทราเน็ต ระบบสารบรรณอิเล็กทรอนิกส์ อีเมล หรือช่องทางอื่นที่เหมาะสม

๔.๒ ให้ผู้บริหารทุกระดับสื่อสารและกำกับดูแลให้บุคลากรในสังกัดรับทราบ เข้าใจ และถือปฏิบัติตามนโยบายนี้

๔.๓ ให้จัดอบรมหรือกิจกรรมสร้างความตระหนักด้านการรักษาความมั่นคงปลอดภัยของข้อมูลสารสนเทศแก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงนโยบายหรือเกิดภัยคุกคามสำคัญ

๔.๔ ให้บุคลากร ผู้รับจ้าง และผู้ให้บริการภายนอกที่เกี่ยวข้องลงนามรับทราบและยอมรับเงื่อนไขการรักษาความลับและการใช้ข้อมูลก่อนเข้าถึงข้อมูลขององค์การ

๔.๕ ให้เผยแพร่คู่มือหรือแนวปฏิบัติที่เกี่ยวข้อง เช่น การจำแนกข้อมูล การใช้งานอีเมล การรับส่งข้อมูล การจัดเก็บข้อมูล และการแจ้งเหตุด้านข้อมูล เพื่อให้บุคลากรนำไปใช้ได้อย่างถูกต้อง

๕. วิธีการวัดประสิทธิผล

ให้สำนักเทคโนโลยีดิจิทัลกำหนดและติดตามผลการดำเนินงานอย่างน้อยปีละ ๑ ครั้ง โดยใช้ตัวชี้วัด ดังนี้

ประเด็นวัดผล	ตัวชี้วัด/วิธีวัด
การกำกับดูแลข้อมูล	ร้อยละของข้อมูลสำคัญที่มีเจ้าของข้อมูล มีการจำแนกชั้นความลับ และมีทะเบียนข้อมูลครบถ้วน
การควบคุมการเข้าถึง	ร้อยละของระบบสำคัญที่ทบทวนสิทธิ์ผู้ใช้งานตามรอบระยะเวลาที่กำหนด
การสำรองและกู้คืนข้อมูล	ร้อยละความสำเร็จของการสำรองข้อมูล และผลการทดสอบกู้คืนข้อมูลหรือระบบสำคัญ
การคุ้มครองข้อมูล	จำนวนเหตุการณ์ข้อมูลสูญหาย รั่วไหล ถูกเข้าถึง หรือถูกแก้ไขโดยมิได้รับอนุญาต
การจัดการเหตุการณ์	ระยะเวลาเฉลี่ยในการตรวจพบ แจ้งเหตุ ควบคุม และแก้ไขเหตุการณ์ด้านข้อมูล
การสร้างความตระหนัก	ร้อยละของบุคลากรและผู้เกี่ยวข้องที่ผ่านการอบรมหรือรับทราบนโยบายตามแผน
การปฏิบัติตามนโยบาย	ผลการตรวจสอบภายใน จำนวนข้อไม่สอดคล้อง และร้อยละการดำเนินการแก้ไขแล้วเสร็จตามกำหนด
การปรับปรุงอย่างต่อเนื่อง	จำนวนและผลการนำข้อเสนอแนะจากการประเมินความเสี่ยง เหตุการณ์ และการตรวจสอบไปปรับปรุงกระบวนการ

ส่วนที่ ๗
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยทางกายภาพและสภาพแวดล้อม
(Physical and Environmental Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดมาตรการและแนวปฏิบัติในการป้องกันทรัพย์สินสารสนเทศขององค์การคลังสินค้า จากการเข้าถึง การรบกวน การทำลาย หรือการจารกรรมทางกายภาพ

๑.๒ เพื่อคุ้มครองศูนย์ข้อมูล (Data Center) พื้นที่ปฏิบัติงาน และอุปกรณ์เทคโนโลยีสารสนเทศสำคัญให้พ้นจากอันตรายที่เกิดจากภัยธรรมชาติ อุบัติเหตุ หรือเหตุการณ์ไม่พึงประสงค์อื่น ๆ

๑.๓ เพื่อให้มีระบบรักษาความปลอดภัยทางกายภาพที่เหมาะสม เช่น การควบคุมการเข้า-ออกพื้นที่ การเฝ้าระวัง การป้องกันภัยพิบัติ และการดูแลสภาพแวดล้อมที่จำเป็นต่อการปฏิบัติงาน

๑.๔ เพื่อให้บุคลากร ผู้รับจ้าง และผู้ให้บริการภายนอก มีความเข้าใจและปฏิบัติตามมาตรฐานความปลอดภัยทางกายภาพอย่างถูกต้อง

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยมีขั้นตอนการดำเนินงานที่ชัดเจน ตรวจสอบได้ และสามารถปรับปรุงให้เหมาะสมกับความเสี่ยงได้อย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับพื้นที่ที่มีความสำคัญด้านเทคโนโลยีสารสนเทศ ได้แก่ ศูนย์ข้อมูล (Data Center) ห้องควบคุมระบบเครือข่าย ตู้สื่อสาร พื้นที่จัดเก็บสื่อสำรองข้อมูล และพื้นที่ปฏิบัติงานที่มีอุปกรณ์สารสนเทศสำคัญ

๒.๒ ครอบคลุมการควบคุมทางกายภาพ ได้แก่ การออกแบบพื้นที่ การควบคุมการเข้า-ออก ระบบกล้องวงจรปิด ระบบแจ้งเตือนภัย ระบบป้องกันอัคคีภัย ระบบปรับอากาศ ระบบไฟฟ้าสำรอง รวมถึงอุปกรณ์ต่อพ่วงต่าง ๆ

๒.๓ ใช้บังคับกับบุคลากร ผู้ปฏิบัติงาน ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการภายนอก และบุคคลอื่นที่ได้รับอนุญาตให้เข้าถึงหรือปฏิบัติงานในพื้นที่ดังกล่าว

๓. แนวปฏิบัติ

๓.๑ การกำหนดและป้องกันพื้นที่ปลอดภัย

๑) ให้กำหนดพื้นที่สำหรับจัดวางอุปกรณ์สารสนเทศสำคัญเป็น “พื้นที่ควบคุม” และกำหนดมาตรการรักษาความปลอดภัยให้เข้มงวดกว่าพื้นที่ปฏิบัติงานทั่วไป

๒) ต้องออกแบบโครงสร้างพื้นที่ให้มีความมั่นคงปลอดภัย ป้องกันการเข้าถึงจากภายนอกหรือพื้นที่ที่ไม่ได้รับอนุญาต และจัดให้มีระดับการป้องกันที่เหมาะสมกับความสำคัญของทรัพย์สินภายใน

๓) พื้นที่ควบคุมต้องติดตั้งอุปกรณ์ป้องกันที่เหมาะสม เช่น ประตูที่แข็งแรง ระบบล็อกที่ปลอดภัย และระบบตรวจสอบการเข้า-ออก

๓.๒ การควบคุมการเข้า-ออกพื้นที่

๑) ให้มีการระบุตัวตนและตรวจสอบสิทธิ์ก่อนอนุญาตให้เข้าสู่พื้นที่ควบคุมทุกครั้ง

๒) ต้องจัดทำทะเบียนผู้มีสิทธิ์เข้า-ออกพื้นที่ และทบทวนรายชื่อดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงบุคลากร

๓) กรณีผู้มาติดต่อหรือผู้ให้บริการภายนอก ต้องลงทะเบียน เข้าใช้งานพร้อมแสดงบัตรประจำตัว และต้องอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่องค์การตลอดเวลาที่อยู่ในพื้นที่

๔) ให้ติดตั้งระบบกล้องวงจรปิด (CCTV) เฝ้าระวังพื้นที่ควบคุมและบริเวณทางเข้า-ออก โดยบันทึกภาพและเก็บรักษาข้อมูลไม่น้อยกว่าระยะเวลาที่องค์การกำหนด

๓.๓ การป้องกันภัยจากสภาพแวดล้อมและอุบัติภัย

๑) ต้องติดตั้งระบบป้องกันอัคคีภัยที่เหมาะสมกับอุปกรณ์ไฟฟ้าและสารสนเทศ เช่น ระบบตรวจจับควัน ระบบแจ้งเตือน และระบบดับเพลิงอัตโนมัติที่ไม่ทำลายอุปกรณ์

๒) ต้องมีระบบไฟฟ้าสำรอง (UPS) หรือระบบจ่ายไฟสำรองที่เพียงพอต่อการรองรับเหตุการณ์ไฟฟ้าขัดข้อง เพื่อป้องกันการหยุดชะงักของระบบสำคัญ

๓) ต้องควบคุมอุณหภูมิและความชื้นให้อยู่ในระดับมาตรฐานที่อุปกรณ์สารสนเทศต้องการ เพื่อยืดอายุการใช้งานและป้องกันความเสียหาย

๔) ต้องป้องกันความเสียหายจากน้ำท่วม หรือการรั่วไหลของของเหลวในพื้นที่ติดตั้งอุปกรณ์สารสนเทศ

๓.๔ การจัดการอุปกรณ์และการซ่อมบำรุง

๑) การเคลื่อนย้าย ติดตั้ง หรือเปลี่ยนตำแหน่งอุปกรณ์ในพื้นที่ควบคุม ต้องได้รับอนุมัติและมีการบันทึกหลักฐาน

๒) อุปกรณ์ที่อยู่นอกพื้นที่ควบคุมหรือติดตั้งในที่สาธารณะ ต้องมีมาตรการป้องกันการโจรกรรมหรือการเข้าถึงโดยไม่ได้รับอนุญาต เช่น การล็อกอุปกรณ์หรือการใช้สายล็อก

๓) การซ่อมบำรุงอุปกรณ์สารสนเทศในพื้นที่ควบคุม ต้องดำเนินการโดยผู้ได้รับอนุญาตและมีเจ้าหน้าที่กำกับดูแล

๓.๕ การจัดการการเข้าถึงและการเฝ้าระวังความปลอดภัย

๑) ให้มีการตรวจตราและตรวจสอบสถานะความปลอดภัยของพื้นที่ควบคุมเป็นประจำ เพื่อให้แน่ใจว่ามาตรการความปลอดภัยต่าง ๆ ทำงานได้ปกติ

๒) บันทึกการเข้า-ออกพื้นที่ควบคุม (Log) ต้องได้รับการเก็บรักษาและตรวจสอบอย่างสม่ำเสมอ เพื่อค้นหาเหตุการณ์ผิดปกติ

๓) เมื่อพบเหตุการณ์ผิดปกติ เช่น การพยายามบุกรุก อุปกรณ์เสียหาย หรือระบบรักษาความปลอดภัยขัดข้อง ให้ดำเนินการแจ้งเหตุและแก้ไขตามขั้นตอนการจัดการเหตุการณ์

๔. แนวทางการสื่อสารนโยบาย

๔.๑ เผยแพร่นโยบายและแนวปฏิบัตินี้ให้บุคลากรรับทราบผ่านระบบสื่อสารภายในขององค์การ

๔.๒ จัดทำป้ายเตือน ป้ายแจ้งระเบียบการเข้า-ออก และป้ายบอกทางในพื้นที่ควบคุมให้ชัดเจน

๔.๓ ให้บุคลากรและผู้เกี่ยวข้องลงนามรับทราบระเบียบการเข้า-ออกพื้นที่ และข้อกำหนดด้านความปลอดภัยทางกายภาพ

๔.๔ จัดอบรมด้านการปฏิบัติตนในพื้นที่ควบคุมและการแจ้งเหตุฉุกเฉินให้แก่ผู้ที่เกี่ยวข้องเป็นประจำ

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การควบคุมการเข้า-ออก	ร้อยละของบันทึกการเข้า-ออกพื้นที่ควบคุมที่ได้รับการตรวจสอบเป็นประจำ	ร้อยละ ๑๐๐
ระบบรักษาความปลอดภัย	ร้อยละของระบบ (CCTV, สัญญาณเตือน, ดับเพลิง) ที่ผ่านการทดสอบว่าใช้งานได้ดี	ร้อยละ ๑๐๐
ทะเบียนผู้มีสิทธิ์	ร้อยละของรายชื่อผู้มีสิทธิ์เข้าพื้นที่ที่ได้รับการทบทวนตามรอบ	ร้อยละ ๑๐๐
การจัดการเหตุการณ์	จำนวนเหตุการณ์บุกรุกหรืออุบัติภัยที่เกิดขึ้นและการแก้ไขตามแผน	ไม่เกิดขึ้น หรือแก้ไขได้ทันท่วงที

๕.๑ รายงานผลการตรวจสอบสถานะความปลอดภัยทางกายภาพต่อผู้บริหารอย่างน้อยปีละ ๑ ครั้ง เพื่อพิจารณาปรับปรุงมาตรการให้เหมาะสมกับสภาพความเสี่ยงที่เปลี่ยนแปลงไป

ส่วนที่ ๘
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยของระบบเครือข่ายสื่อสาร
(Communications Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดมาตรการและแนวปฏิบัติในการบริหารจัดการระบบเครือข่ายสื่อสารขององค์การคลังสินค้า ให้มีความมั่นคงปลอดภัย มีความพร้อมใช้งาน และสามารถรองรับภารกิจขององค์การได้อย่างต่อเนื่อง

๑.๒ เพื่อป้องกันมิให้บุคคลที่ไม่มีอำนาจหน้าที่เข้าถึง ล่วงรู้ ดักรับ แก้ไข เปลี่ยนแปลง ทำลาย หรือรบกวนการทำงานของระบบเครือข่ายสื่อสารและข้อมูลสารสนเทศขององค์การโดยมิได้รับอนุญาต

๑.๓ เพื่อกำหนดให้มีการแบ่งแยกเครือข่าย การควบคุมการเชื่อมต่อ การพิสูจน์ตัวตน การควบคุมอุปกรณ์เครือข่าย และการเฝ้าระวังเหตุการณ์ด้านเครือข่ายอย่างเป็นระบบ

๑.๔ เพื่อให้การเชื่อมต่อเครือข่ายภายใน เครือข่ายไร้สาย การเชื่อมต่อจากระยะไกล และการเชื่อมต่อกับหน่วยงานหรือผู้ให้บริการภายนอก เป็นไปตามหลักความจำเป็น ความเสี่ยง และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยกำหนดกระบวนการปฏิบัติงานที่เป็นมาตรฐาน สามารถปฏิบัติซ้ำได้ ตรวจสอบได้ วัดผลได้ และนำผลไปปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับระบบเครือข่ายสื่อสารทุกประเภทขององค์การคลังสินค้า ได้แก่ เครือข่ายภายใน (LAN) เครือข่ายระหว่างสาขาหรือหน่วยงาน เครือข่ายไร้สาย (Wireless LAN) ระบบเชื่อมต่ออินเทอร์เน็ต ระบบเชื่อมต่อจากระยะไกล (Remote Access) ระบบเครือข่ายส่วนตัวเสมือน (VPN) และระบบเชื่อมต่อกับหน่วยงานภายนอก

๒.๒ ครอบคลุมอุปกรณ์เครือข่ายและอุปกรณ์รักษาความมั่นคงปลอดภัย ได้แก่ Router, Switch, Firewall, Wireless Access Point, VPN Gateway, Network Access Control, ระบบตรวจจับและป้องกันการบุกรุก รวมถึงอุปกรณ์หรือบริการอื่นที่เกี่ยวข้องกับการติดต่อสื่อสารข้อมูล

๒.๓ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการภายนอก และบุคคลอื่นที่ได้รับอนุญาตให้เข้าถึงหรือใช้งานระบบเครือข่ายขององค์การคลังสินค้า

๒.๔ ครอบคลุมการออกแบบ ติดตั้ง ใช้งาน บำรุงรักษา เปลี่ยนแปลง ตรวจสอบ เฝ้าระวัง และยกเลิกการใช้งานระบบเครือข่ายสื่อสารตลอดวงจรชีวิต

๓. แนวปฏิบัติ

๓.๑ การกำหนดหน้าที่และความรับผิดชอบ

๑) ให้สำนักเทคโนโลยีดิจิทัลเป็นผู้รับผิดชอบหลักในการออกแบบ ควบคุม ดูแล บำรุงรักษา เฝ้าระวัง และปรับปรุงความมั่นคงปลอดภัยของระบบเครือข่าย

๒) ให้หน่วยงานเจ้าของระบบหรือเจ้าของข้อมูลร่วมกำหนดความต้องการในการเชื่อมต่อเครือข่าย ระดับความสำคัญของระบบ และสิทธิ์การเข้าถึงที่จำเป็นต่อการปฏิบัติงาน

๓) การขอเชื่อมต่อเครือข่าย การเปิดใช้บริการ การเปิดพอร์ต การเชื่อมต่อจากระยะไกล หรือการเชื่อมต่อกับบุคคลภายนอก ต้องได้รับอนุมัติตามกระบวนการที่องค์การกำหนดก่อนดำเนินการ

๓.๒ การจัดทำทะเบียนทรัพย์สินและผังเครือข่าย

๑) ให้จัดทำทะเบียนทรัพย์สินสารสนเทศสำหรับอุปกรณ์เครือข่ายทุกประเภท โดยระบุอย่างน้อย ชื่ออุปกรณ์ หมายเลขทรัพย์สิน รุ่น สถานที่ติดตั้ง ผู้รับผิดชอบ หมายเลข IP Address สถานะการใช้งาน และระดับ

ความสำคัญ

๒) ให้จัดทำและปรับปรุงแผนผังเครือข่าย (Network Diagram) ให้เป็นปัจจุบัน เพื่อแสดงการเชื่อมต่อระหว่างระบบภายใน ระบบภายนอก ระบบสำคัญ และอุปกรณ์รักษาความมั่นคงปลอดภัย

๓) ให้มีบัญชีรายชื่อการกำหนด IP Address ทั้งต้นทางและปลายทาง รวมถึงการเชื่อมต่อที่ได้รับอนุญาต เพื่อให้สามารถตรวจสอบและติดตามได้

๔) ให้ทบทวนทะเบียนทรัพย์สิน แผนผังเครือข่าย และสิทธิ์ผู้ดูแลระบบอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงสำคัญ

๓.๓ การแบ่งแยกและควบคุมเครือข่าย

๑) ให้มีการแบ่งแยกเครือข่ายตามลักษณะการใช้งาน ความสำคัญของระบบ และระดับความเสี่ยง เช่น เครือข่ายผู้ใช้งาน เครือข่ายแม่ข่าย เครือข่ายระบบงานสำคัญ เครือข่ายผู้มาติดต่อ และเครือข่ายผู้ให้บริการภายนอก

๒) ให้ใช้การแบ่งแยกเครือข่าย เช่น VLAN, Subnet, Firewall หรือมาตรการอื่นที่เหมาะสม เพื่อจำกัดการเข้าถึงและลดผลกระทบเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

๓) เครือข่ายสำหรับผู้มาติดต่อหรือบุคคลภายนอกต้องแยกออกจากเครือข่ายภายในขององค์การ และต้องไม่สามารถเข้าถึงระบบหรือข้อมูลภายในได้ เว้นแต่ได้รับอนุมัติเป็นกรณีเฉพาะ

๔) การเชื่อมต่อระหว่างเครือข่ายต้องกำหนดกฎการสื่อสารให้อนุญาตเฉพาะที่จำเป็นต่อการปฏิบัติงาน และต้องมีการทบทวนกฎดังกล่าวตามรอบระยะเวลาที่กำหนด

๓.๔ การควบคุมการเชื่อมต่อและการใช้งานบริการเครือข่าย

๑) ให้เปิดใช้เฉพาะบริการเครือข่าย โปรโตคอล และพอร์ตสื่อสารที่จำเป็นต่อการปฏิบัติงานเท่านั้น โดยปิดหรือระงับบริการและพอร์ตที่ไม่จำเป็นหรือมีความเสี่ยง

๒) การเปิดหรือเปลี่ยนแปลงพอร์ตสื่อสาร ต้องมีการประเมินความจำเป็น ผลกระทบ และความเสี่ยง ได้รับอนุมัติจากผู้มีอำนาจ และบันทึกรายละเอียดการเปลี่ยนแปลง

๓) ให้ตรวจสอบการเปิดใช้งานพอร์ตและบริการเครือข่ายอย่างน้อยสัปดาห์ละ ๑ ครั้ง หรือให้ใช้ระบบตรวจสอบอัตโนมัติตามความเหมาะสม

๔) ผู้ใช้งานต้องใช้บริการเครือข่ายเพื่อภารกิจขององค์การเท่านั้น ห้ามใช้เพื่อการกระทำที่ขัดต่อกฎหมาย ระเบียบ ศีลธรรมอันดี ละเมิดสิทธิของผู้อื่น หรือแสวงหาประโยชน์ส่วนตน

๕) ห้ามติดตั้ง ใช้งาน หรือเผยแพร่โปรแกรมที่ก่อให้เกิดความเสี่ยงต่อเครือข่าย เช่น โปรแกรมแบบ Peer-to-Peer โปรแกรมสแกนเครือข่าย โปรแกรมดักจับข้อมูล หรือโปรแกรมที่ไม่ได้รับอนุญาต เว้นแต่ได้รับอนุมัติจากสำนักเทคโนโลยีดิจิทัลเพื่อการปฏิบัติงาน

๓.๕ การควบคุมการเชื่อมต่อจากระยะไกล

๑) การเชื่อมต่อจากระยะไกลเข้าสู่ระบบหรือเครือข่ายขององค์การ ต้องใช้วิธีการเชื่อมต่อที่องค์การอนุมัติ เช่น VPN หรือเทคโนโลยีอื่นที่มีการเข้ารหัสข้อมูลอย่างเหมาะสม

๒) ผู้ใช้งานจากระยะไกลต้องได้รับอนุมัติให้ใช้งานเป็นรายบุคคล กำหนดระยะเวลาการใช้งาน และจำกัดสิทธิ์ตามความจำเป็น

๓) การเชื่อมต่อจากระยะไกลเพื่อเข้าถึงระบบสำคัญ บัญชีผู้ดูแลระบบ หรือข้อมูลสำคัญ ต้องใช้การพิสูจน์ตัวตนแบบหลายปัจจัย (Multi-Factor Authentication: MFA) ตามความเหมาะสม

๔) การเชื่อมต่อจากระยะไกลของผู้ให้บริการภายนอก ต้องอยู่ภายใต้การควบคุม กำหนดช่วงเวลา มีผู้รับผิดชอบขององค์การกำกับ และบันทึกประวัติการเข้าใช้งานไว้เพื่อการตรวจสอบ

๕) ให้ยกเลิกสิทธิ์การเชื่อมต่อจากระยะไกลทันทีเมื่อพ้นความจำเป็น สิ้นสุดสัญญา เปลี่ยนหน้าที่ หรือพบเหตุอันควรสงสัย

๓.๖ การรักษาความมั่นคงปลอดภัยของเครือข่ายไร้สาย

๑) การติดตั้งและใช้งานเครือข่ายไร้สายต้องได้รับอนุมัติจากสำนักเทคโนโลยีดิจิทัล และต้องมีการกำหนดจุดติดตั้งให้เหมาะสมกับพื้นที่ใช้งาน

๒) ต้องเปลี่ยนชื่อเครือข่ายเริ่มต้น (Default SSID) และรหัสผ่านเริ่มต้นของอุปกรณ์ รวมทั้งเปลี่ยนแปลงค่ากำหนดเริ่มต้นที่อาจก่อให้เกิดความเสี่ยง

๓) ให้ใช้มาตรฐานการเข้ารหัสเครือข่ายไร้สายที่มีความมั่นคงปลอดภัย เช่น WPA๓ หรือ WPA๒ ตามความสามารถของอุปกรณ์และความเหมาะสม

๔) ให้ควบคุมการเชื่อมต่ออุปกรณ์เข้าสู่เครือข่ายไร้สาย โดยกำหนดการลงทะเบียนอุปกรณ์ การพิสูจน์ตัวตน หรือมาตรการควบคุมการเข้าถึงอื่นที่เหมาะสม

๕) ให้แยกเครือข่ายไร้สายสำหรับบุคลากร เครือข่ายสำหรับผู้มาติดต่อ และเครือข่ายสำหรับอุปกรณ์เฉพาะงานออกจากกัน รวมทั้งควบคุมการสื่อสารระหว่างเครือข่าย

๖) ให้กำหนดกำลังส่งสัญญาณและตำแหน่งติดตั้งอุปกรณ์ให้เหมาะสม เพื่อลดความเสี่ยงจากการเข้าถึงสัญญาณนอกพื้นที่ควบคุม

๓.๗ การป้องกันและเฝ้าระวังระบบเครือข่าย

๑) ให้ติดตั้งและกำหนดค่าระบบป้องกันเครือข่าย เช่น Firewall ระบบตรวจจับและป้องกันการบุกรุก ระบบกรองเว็บไซต์ หรือระบบเฝ้าระวังอื่นตามระดับความเสี่ยงและความสำคัญของระบบ

๒) ต้องปรับปรุงซอฟต์แวร์ เฟิร์มแวร์ และแพตช์ความมั่นคงปลอดภัยของอุปกรณ์เครือข่ายตามระดับความรุนแรงของช่องโหว่และแนวทางบริหารจัดการการเปลี่ยนแปลงขององค์การ

๓) ให้มีการเฝ้าระวัง ตรวจสอบ และวิเคราะห์บันทึกเหตุการณ์ของอุปกรณ์เครือข่ายและระบบรักษาความมั่นคงปลอดภัย เพื่อค้นหาการใช้งานผิดปกติ การบุกรุก หรือภัยคุกคามทางไซเบอร์

๔) บันทึกเหตุการณ์ด้านเครือข่ายต้องได้รับการป้องกันการแก้ไขและเก็บรักษาไว้ตามระยะเวลาที่กฎหมายและองค์การกำหนด

๕) เมื่อพบเหตุการณ์หรือข้อบ่งชี้ว่าระบบเครือข่ายอาจถูกบุกรุก ถูกโจมตี หรือมีการใช้งานผิดปกติ ให้ผู้เกี่ยวข้องแจ้งสำนักเทคโนโลยีดิจิทัลโดยเร็ว และดำเนินการตามแผนตอบสนองต่อเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๓.๘ การควบคุมทางกายภาพของอุปกรณ์เครือข่าย

๑) ห้องศูนย์ข้อมูล ห้องควบคุมเครือข่าย ตู้สื่อสาร และพื้นที่ติดตั้งอุปกรณ์เครือข่าย ต้องมีมาตรการควบคุมการเข้า-ออกตามระดับความสำคัญ

๒) ให้กำหนดรายชื่อผู้มีสิทธิ์เข้า-ออกพื้นที่ควบคุม และบันทึกข้อมูลการเข้า-ออกของบุคลากร ผู้มาติดต่อ และผู้ให้บริการภายนอกทุกครั้ง

๓) บุคคลภายนอกที่เข้าพื้นที่ควบคุมต้องได้รับอนุญาต ลงทะเบียน และอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่ที่รับผิดชอบ

๔) ให้ตรวจสอบความถูกต้องของบันทึกการเข้า-ออกพื้นที่ควบคุมอย่างน้อยเดือนละ ๑ ครั้ง

๓.๙ การบริหารจัดการการเปลี่ยนแปลงและการสำรองค่ากำหนด

๑) การเปลี่ยนแปลงโครงสร้างเครือข่าย การกำหนดค่า Firewall การเปลี่ยนเส้นทางเครือข่าย การอัปเกรดอุปกรณ์ หรือการแก้ไขค่ากำหนดสำคัญ ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง

๒) ก่อนดำเนินการเปลี่ยนแปลง ต้องประเมินผลกระทบ ความเสี่ยง กำหนดแผนทดสอบ แผนย้อนกลับ และผู้รับผิดชอบอย่างชัดเจน

๓) ให้สำรองค่ากำหนดของอุปกรณ์เครือข่ายและอุปกรณ์รักษาความมั่นคงปลอดภัยอย่างสม่ำเสมอ และ

จัดเก็บในพื้นที่ที่มีการควบคุมสิทธิ์เข้าถึง

๔) การเปลี่ยนแปลงฉุกเฉินต้องได้รับอนุมัติจากผู้มีอำนาจตามที่กำหนด และบันทึกรายละเอียดเพื่อทบทวนภายหลัง

๓.๑๐ การประเมินความเสี่ยงและการทบทวน

๑) ให้ประเมินความเสี่ยงด้านระบบเครือข่ายสื่อสารอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงเทคโนโลยี โครงสร้างเครือข่าย ภัยคุกคาม หรือระบบสำคัญ

๒) ให้มีการตรวจสอบช่องโหว่และทดสอบความมั่นคงปลอดภัยของระบบเครือข่ายตามแผนและระดับความเสี่ยง

๓) ให้รายงานผลการตรวจสอบ เหตุการณ์ ข้อบกพร่อง และผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะทำงานที่เกี่ยวข้อง เพื่อนำไปสู่การแก้ไขและปรับปรุงอย่างต่อเนื่อง

๔. แนวทางการสื่อสารนโยบาย

๔.๑ เผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในขององค์การ

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้ปฏิบัติตามอย่างเคร่งครัด

๔.๓ จัดให้มีการอบรมหรือสื่อสารสร้างความตระหนักแก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง ในเรื่องการใช้งานเครือข่ายอย่างปลอดภัย การเชื่อมต่อ Wi-Fi การใช้งาน VPN การป้องกัน Phishing และการแจ้งเหตุผิดปกติ

๔.๔ จัดทำคู่มือหรือขั้นตอนปฏิบัติงานมาตรฐานสำหรับผู้ดูแลระบบเครือข่าย เช่น การขอเปิดพอร์ต การขอเชื่อมต่อจากระยะไกล การจัดการสิทธิ์ การเปลี่ยนแปลงค่ากำหนด และการตอบสนองต่อเหตุการณ์

๔.๕ แจ้งข้อกำหนดการใช้งานเครือข่ายแก่ผู้ให้บริการภายนอกและผู้มาติดต่อก่อนอนุญาตให้เข้าถึงระบบหรือพื้นที่ควบคุมขององค์การ

๔.๖ สื่อสารข้อมูลภัยคุกคาม ช่องโหว่ หรือเหตุการณ์ด้านเครือข่ายที่สำคัญแก่ผู้เกี่ยวข้องโดยรวดเร็ว เพื่อให้สามารถป้องกันและตอบสนองได้ทันเวลา

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การจัดทำทะเบียนเครือข่าย	ร้อยละของอุปกรณ์เครือข่ายที่มีข้อมูลทะเบียนทรัพย์สินและผู้รับผิดชอบครบถ้วน	ไม่น้อยกว่าร้อยละ ๙๕
การปรับปรุงผังเครือข่าย	ร้อยละของแผนผังเครือข่ายที่ได้รับการทบทวนหรือปรับปรุงตามการเปลี่ยนแปลง	ร้อยละ ๑๐๐ ต่อปี
การควบคุมพอร์ตและบริการ	ร้อยละของพอร์ตหรือบริการที่ไม่จำเป็นและได้รับการปิดหรือควบคุมตามกำหนด	ร้อยละ ๑๐๐ ของรายการที่ตรวจพบ
การแบ่งแยกเครือข่าย	ผลการตรวจสอบการแยกเครือข่ายสำคัญ เครือข่ายผู้มาติดต่อ และเครือข่ายภายนอก	ไม่พบการเชื่อมต่อที่ไม่ได้รับอนุญาต
การเชื่อมต่อระยะไกล	ร้อยละของผู้ใช้งาน Remote Access ที่ได้รับอนุมัติ มีการกำหนดสิทธิ์ และใช้การพิสูจน์ตัวตนตามข้อกำหนด	ร้อยละ ๑๐๐
การจัดการช่องโหว่	ร้อยละของช่องโหว่ระดับสูงหรือวิกฤตที่ได้รับการแก้ไขภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การเฝ้าระวังเหตุการณ์	ระยะเวลาเฉลี่ยตั้งแต่ตรวจพบเหตุการณ์จนถึงการรับทราบและเริ่มดำเนินการ	เป็นไปตามระดับความรุนแรงที่กำหนด
การควบคุมพื้นที่เครือข่าย	ผลการตรวจสอบบันทึกการเข้า-ออกห้องควบคุมระบบเครือข่ายรายเดือน	ตรวจสอบครบทุกเดือน
การสำรองค่ากำหนด	ร้อยละของอุปกรณ์เครือข่ายสำคัญที่มีการสำรองค่ากำหนดและสามารถกู้คืนได้	ร้อยละ ๑๐๐
การสร้างความตระหนัก	ร้อยละของบุคลากรกลุ่มเป้าหมายที่รับทราบนโยบายหรือผ่านการอบรม	ไม่น้อยกว่าร้อยละ ๙๐

การปรับปรุงต่อเนื่อง	ร้อยละของข้อค้นพบจากการตรวจสอบหรือประเมินความเสี่ยงที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และสรุปผลการวัดประสิทธิผลอย่างน้อยปีละ ๑ ครั้ง หรือบ่อยกว่านั้นสำหรับตัวชี้วัดที่มีความเสี่ยงสูง

๕.๒ ให้รายงานผลการวัด ประเด็นความเสี่ยง เหตุการณ์สำคัญ และแผนปรับปรุงต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง เพื่อใช้ในการทบทวนและพัฒนามาตรการให้มีประสิทธิผลอย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี ภารกิจ โครงสร้างเครือข่าย หรือภัยคุกคามที่มีนัยสำคัญ

ส่วนที่ ๙
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยในการปฏิบัติงานด้านเทคโนโลยีสารสนเทศ
(IT Operations Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดมาตรการและแนวปฏิบัติในการบริหารจัดการ การควบคุม และการปฏิบัติงานด้านเทคโนโลยีสารสนเทศขององค์การคลังสินค้า ให้มีความมั่นคงปลอดภัย มีความพร้อมใช้งาน และสนับสนุนการดำเนินงานขององค์การได้อย่างต่อเนื่อง

๑.๒ เพื่อป้องกันความเสียหาย การหยุดชะงัก การสูญหาย การแก้ไขเปลี่ยนแปลง หรือการเข้าถึงระบบและข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต อันอาจเกิดจากการปฏิบัติงาน การเปลี่ยนแปลงระบบ ความผิดพลาดของบุคลากร หรือภัยคุกคามด้านเทคโนโลยีสารสนเทศ

๑.๓ เพื่อให้มีขั้นตอนการปฏิบัติงานมาตรฐาน การแบ่งแยกหน้าที่ การบริหารจัดการการเปลี่ยนแปลง การสำรองและกู้คืนข้อมูล การบริหารจัดการเหตุการณ์ และการบันทึกเหตุการณ์ที่สามารถตรวจสอบย้อนหลังได้

๑.๔ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้การดำเนินงานด้านเทคโนโลยีสารสนเทศมีการกำหนดผู้รับผิดชอบ กระบวนการควบคุม หลักฐานการดำเนินงาน ตัวชี้วัด และการปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับระบบสารสนเทศ ระบบแม่ข่าย ฐานข้อมูล ระบบจัดเก็บข้อมูล ระบบสำรองข้อมูล ระบบเครือข่าย อุปกรณ์ความมั่นคงปลอดภัย ระบบคลาวด์ ระบบงานที่พัฒนาเองหรือจัดหาจากภายนอก และบริการด้านเทคโนโลยีสารสนเทศที่อยู่ภายใต้การดูแลขององค์การคลังสินค้า

๒.๒ ครอบคลุมการดำเนินงานตลอดวงจรชีวิตของระบบ ได้แก่ การติดตั้ง การกำหนดค่า การใช้งาน การบำรุงรักษา การเฝ้าระวัง การสำรองข้อมูล การกู้คืน การเปลี่ยนแปลง การจัดการเหตุการณ์ การยกเลิก และการทำลายข้อมูลหรืออุปกรณ์

๒.๓ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ผู้ดูแลระบบ ผู้พัฒนาระบบ ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นที่เข้าถึงหรือปฏิบัติงานกับระบบสารสนเทศขององค์การ

๓. แนวปฏิบัติ

๓.๑ การกำหนดหน้าที่และการแบ่งแยกหน้าที่

๑) ให้องค์การกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศเป็นลายลักษณ์อักษร เช่น ผู้ดูแลระบบ ผู้ดูแลฐานข้อมูล ผู้ดูแลเครือข่าย ผู้ดูแลความมั่นคงปลอดภัยสารสนเทศ ผู้ปฏิบัติงานสำรองข้อมูล และผู้รับผิดชอบการจัดการเหตุการณ์

๒) ให้มีการแบ่งแยกหน้าที่ระหว่างผู้ร้องขอ ผู้อนุมัติ ผู้พัฒนา ผู้ทดสอบ ผู้ติดตั้ง ผู้ดูแลระบบ และผู้ตรวจสอบ ตามความเหมาะสม เพื่อป้องกันความขัดแย้งของหน้าที่และลดความเสี่ยงจากการใช้อำนาจโดยมิชอบ

๓) การปฏิบัติงานที่เกี่ยวข้องกับระบบสำคัญ ข้อมูลสำคัญ หรือสิทธิ์ผู้ดูแลระบบ ต้องได้รับอนุมัติและมีการบันทึกหลักฐานการดำเนินงาน

๔) กรณีจำเป็นต้องปฏิบัติงานแทนกัน ให้กำหนดผู้ปฏิบัติงานสำรอง ระยะเวลาการปฏิบัติหน้าที่ และสิทธิ์ที่จำเป็นอย่างชัดเจน

๓.๒ การจัดทำขั้นตอนการปฏิบัติงานมาตรฐาน

๑) ให้สำนักเทคโนโลยีดิจิทัลจัดทำ ทบทวน และปรับปรุงคู่มือหรือขั้นตอนการปฏิบัติงานมาตรฐาน

(Standard Operating Procedure: SOP) สำหรับกระบวนการสำคัญ

๒) SOP อย่างน้อยต้องครอบคลุมการบริหารบัญชีผู้ใช้งาน การสำรองและกู้คืนข้อมูล การบริหารจัดการการเปลี่ยนแปลง การติดตั้งและปรับปรุงระบบ การเฝ้าระวังระบบ การจัดการเหตุการณ์ การจัดการสื่อบันทึกข้อมูล และการบริหารจัดการสิทธิ์ผู้ดูแลระบบ

๓) คู่มือและเอกสารการปฏิบัติงานต้องระบุผู้รับผิดชอบ ขั้นตอนการดำเนินงาน จุดควบคุม เอกสารหรือหลักฐานที่ต้องจัดเก็บ และขั้นตอนการส่งต่อหรือยกระดับเหตุการณ์

๔) ให้ทบทวน SOP อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบ เทคโนโลยี โครงสร้างการปฏิบัติงาน หรือพบข้อบกพร่องจากเหตุการณ์จริง

๓.๓ การบริหารจัดการการเปลี่ยนแปลงระบบ

๑) การเปลี่ยนแปลงระบบสารสนเทศ โครงสร้างพื้นฐาน การกำหนดค่าระบบ ซอฟต์แวร์ ฐานข้อมูล เครือข่าย หรืออุปกรณ์ความมั่นคงปลอดภัย ต้องดำเนินการตามกระบวนการบริหารจัดการการเปลี่ยนแปลง (Change Management)

๒) ก่อนดำเนินการเปลี่ยนแปลง ต้องมีการบันทึกรายละเอียดอย่างน้อย ได้แก่ วัตถุประสงค์ ขอบเขต ผู้ร้องขอ ผู้รับผิดชอบ ผลกระทบ การประเมินความเสี่ยง แผนทดสอบ แผนย้อนกลับ และช่วงเวลาที่จะดำเนินการ

๓) การเปลี่ยนแปลงต้องได้รับอนุมัติจากผู้มีอำนาจตามระดับความสำคัญของระบบก่อนดำเนินการ ยกเว้นการเปลี่ยนแปลงฉุกเฉิน

๔) การเปลี่ยนแปลงฉุกเฉินต้องดำเนินการเพื่อลดผลกระทบต่อระบบหรือภารกิจโดยเร็ว และต้องบันทึกเหตุผล ผู้อนุมัติ ผลกระทบ และผลการดำเนินงานเพื่อทบทวนภายหลัง

๕) การเปลี่ยนแปลงที่มีผลกระทบสูงต้องทดสอบในสภาพแวดล้อมทดสอบก่อนนำขึ้นใช้งานจริง และต้องมีการตรวจสอบผลหลังดำเนินการ

๓.๔ การบริหารจัดการการกำหนดค่าระบบ

๑) ให้จัดทำมาตรฐานการกำหนดค่าระบบอย่างมั่นคงปลอดภัย (Secure Configuration Baseline) สำหรับระบบแม่ข่าย ฐานข้อมูล อุปกรณ์เครือข่าย ระบบปฏิบัติการ และโปรแกรมประยุกต์ที่สำคัญ

๒) ต้องเปลี่ยนแปลงบัญชีผู้ใช้ รหัสผ่าน และค่าการกำหนดเริ่มต้นจากผู้ผลิตก่อนนำอุปกรณ์หรือระบบขึ้นใช้งาน

๓) ให้ปิดใช้งานบริการ บัญชีผู้ใช้ พอร์ต และโปรแกรมที่ไม่จำเป็นต่อการปฏิบัติงาน

๔) ให้มีการตรวจสอบค่าการกำหนดของระบบสำคัญตามรอบระยะเวลาที่กำหนด และปรับปรุงแก้ไขเมื่อพบค่าการกำหนดที่ไม่เป็นไปตามมาตรฐาน

๕) ให้สำรองค่าการกำหนดของระบบและอุปกรณ์สำคัญก่อนมีการเปลี่ยนแปลง และจัดเก็บในพื้นที่ที่มีการควบคุมสิทธิ์เข้าถึง

๓.๕ การบริหารจัดการช่องโหว่และการปรับปรุงระบบ

๑) ให้มีการติดตามข่าวสารภัยคุกคาม ช่องโหว่ และคำแนะนำด้านความมั่นคงปลอดภัยจากแหล่งข้อมูลที่น่าเชื่อถือ

๒) ให้ตรวจสอบช่องโหว่ของระบบและอุปกรณ์สารสนเทศตามแผน หรือตามระดับความเสี่ยงและความสำคัญของระบบ

๓) ช่องโหว่ระดับวิกฤตและระดับสูงต้องได้รับการประเมินผลกระทบและดำเนินการแก้ไข ลดความเสี่ยง หรือกำหนดมาตรการชดเชยภายในระยะเวลาที่องค์การกำหนด

๔) การติดตั้งแพตช์หรือปรับปรุงระบบต้องผ่านการทดสอบและอนุมัติตามกระบวนการบริหารจัดการการเปลี่ยนแปลง เว้นแต่กรณีฉุกเฉิน

๕) ให้จัดทำทะเบียนช่องโหว่ แผนการแก้ไข ผู้รับผิดชอบ กำหนดเวลา และรายงานสถานะการดำเนินงานต่อผู้บริหารที่เกี่ยวข้อง

๓.๖ การสำรองและการกู้คืนข้อมูล

๑) ให้กำหนดข้อมูล ระบบ และองค์ประกอบที่ต้องสำรองข้อมูล โดยพิจารณาจากความสำคัญของภารกิจ ระดับความเสี่ยง ระยะเวลาที่ยอมรับให้ระบบหยุดชะงักได้ และความสูญเสียของข้อมูลที่ยอมรับได้

๒) ต้องจัดทำแผนและตารางการสำรองข้อมูลที่ระบุประเภทข้อมูล ความถี่ วิธีการสำรอง สถานที่เก็บรักษา ระยะเวลาเก็บรักษา และผู้รับผิดชอบ

๓) ข้อมูลสำรองต้องได้รับการเข้ารหัสหรือมีมาตรการควบคุมสิทธิ์เข้าถึงตามระดับความสำคัญของข้อมูล และต้องจัดเก็บแยกจากระบบหลักตามความเหมาะสม

๔) ให้ตรวจสอบความสำเร็จของการสำรองข้อมูลทุกครั้ง และดำเนินการแก้ไขเมื่อพบการสำรองข้อมูลล้มเหลว

๕) ต้องทดสอบการกู้คืนข้อมูลและระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงระบบที่มีนัยสำคัญ พร้อมบันทึกผลการทดสอบและข้อเสนอแนะเพื่อปรับปรุง

๓.๗ การเฝ้าระวังและบันทึกเหตุการณ์

๑) ให้ระบบสารสนเทศ ระบบแม่ข่าย ฐานข้อมูล อุปกรณ์เครือข่าย และอุปกรณ์รักษาความมั่นคงปลอดภัยที่สำคัญ มีการบันทึกเหตุการณ์การใช้งานและเหตุการณ์ด้านความมั่นคงปลอดภัยอย่างเหมาะสม

๒) บันทึกเหตุการณ์อย่างน้อยควรครอบคลุมการเข้าสู่ระบบและออกจากระบบ การเข้าถึงข้อมูลสำคัญ การเปลี่ยนแปลงสิทธิ์ การเปลี่ยนแปลงค่าการกำหนดระบบ การใช้งานบัญชีผู้ดูแลระบบ และเหตุการณ์ผิดปกติ

๓) ให้มีการปรับเวลาอุปกรณ์และระบบให้เป็นมาตรฐานเดียวกัน เพื่อให้สามารถวิเคราะห์ลำดับเหตุการณ์ได้ถูกต้อง

๔) บันทึกเหตุการณ์ต้องได้รับการป้องกันจากการแก้ไข ลบ หรือเข้าถึงโดยมิได้รับอนุญาต และเก็บรักษาไว้ไม่น้อยกว่าระยะเวลาที่กฎหมายและองค์การกำหนด

๕) ให้มีการตรวจสอบและวิเคราะห์บันทึกเหตุการณ์ตามความสำคัญและความเสี่ยงของระบบ รวมถึงกำหนดกระบวนการแจ้งเตือนเมื่อพบเหตุการณ์ผิดปกติ

๓.๘ การบริหารจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๑) ให้กำหนดช่องทางและขั้นตอนการแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่ชัดเจน เพื่อให้บุคลากรสามารถแจ้งเหตุได้โดยรวดเร็ว

๒) เมื่อพบหรือสงสัยว่าเกิดเหตุการณ์ เช่น ระบบหยุดชะงัก ข้อมูลรั่วไหล การบุกรุก การติดมัลแวร์ หรือการเข้าถึงโดยมิได้รับอนุญาต ให้ผู้พบเหตุแจ้งสำนักเทคโนโลยีดิจิทัลหรือผู้รับผิดชอบทันที

๓) หน่วยงานที่รับผิดชอบต้องดำเนินการบันทึกเหตุการณ์ ประเมินระดับความรุนแรง ควบคุมและจำกัดผลกระทบ รวบรวมหลักฐาน กู้คืนระบบ และรายงานผู้บริหารตามขั้นตอนที่กำหนด

๔) ให้มีการวิเคราะห์หาสาเหตุของเหตุการณ์ และจัดทำบทเรียนหรือมาตรการป้องกันไม่ให้เกิดเหตุซ้ำ

๕) กรณีเหตุการณ์มีผลกระทบต่อข้อมูลส่วนบุคคล ระบบสำคัญ หรือผู้ใช้บริการ ให้ดำเนินการแจ้งหน่วยงานหรือบุคคลที่เกี่ยวข้องตามกฎหมาย ระเบียบ และขั้นตอนขององค์การ

๓.๙ การบริหารจัดการความจุและความพร้อมใช้งาน

๑) ให้มีการติดตามการใช้ทรัพยากรของระบบ เช่น หน่วยประมวลผล หน่วยความจำ พื้นที่จัดเก็บข้อมูล และปริมาณการใช้งานเครือข่าย เพื่อวางแผนรองรับความต้องการใช้งาน

๒) ให้กำหนดค่าระดับแจ้งเตือนเมื่อทรัพยากรมีแนวโน้มไม่เพียงพอ หรือมีการใช้งานผิดปกติ

๓) ระบบสำคัญต้องได้รับการออกแบบหรือกำหนดมาตรการรองรับความพร้อมใช้งานตามความ

เหมาะสม เช่น การสำรองระบบ อุปกรณ์ทดแทน ระบบไฟฟ้าสำรอง หรือการให้บริการจากสถานที่สำรอง

๔) ให้ทบทวนความสามารถในการรองรับการใช้งานของระบบสำคัญอย่างน้อยปีละ ๑ ครั้ง และจัดทำแผนเพิ่มขีดความสามารถเมื่อมีความจำเป็น

๓.๑๐ การควบคุมการใช้สิทธิ์ผู้ดูแลระบบ

๑) บัญชีผู้ดูแลระบบต้องกำหนดเป็นรายบุคคล และห้ามใช้บัญชีผู้ดูแลระบบร่วมกัน เว้นแต่กรณีจำเป็นซึ่งต้องมีมาตรการควบคุมและบันทึกการใช้งาน

๒) ให้จำกัดสิทธิ์ผู้ดูแลระบบเฉพาะบุคลากรที่ได้รับมอบหมายและมีความจำเป็นต่อหน้าที่

๓) การใช้งานสิทธิ์ผู้ดูแลระบบต้องได้รับการบันทึกและสามารถตรวจสอบย้อนหลังได้

๔) ต้องทบทวนสิทธิ์ผู้ดูแลระบบอย่างน้อยทุก ๖ เดือน และยกเลิกหรือปรับลดสิทธิ์เมื่อผู้ใช้งานเปลี่ยนหน้าที่ พ้นสภาพ หรือไม่มีความจำเป็น

๕) รหัสผ่านหรือข้อมูลยืนยันตัวตนของบัญชีผู้ดูแลระบบต้องได้รับการควบคุมอย่างรัดกุม และเปลี่ยนแปลงเมื่อมีเหตุอันควรสงสัยว่าถูกเปิดเผย

๓.๑๑ การจัดการสื่อบันทึกข้อมูลและการทำลายข้อมูล

๑) การใช้สื่อบันทึกข้อมูล เช่น External Drive, USB Drive หรือสื่อสำรองข้อมูล ต้องได้รับอนุญาตและควบคุมตามระดับความสำคัญของข้อมูล

๒) สื่อบันทึกข้อมูลที่จัดเก็บข้อมูลสำคัญต้องมีการเข้ารหัสหรือมาตรการป้องกันที่เหมาะสม

๓) ให้มีทะเบียนควบคุมการรับ-จ่าย การยืม-คืน และการเก็บรักษาสื่อบันทึกข้อมูลสำคัญ

๔) ก่อนนำอุปกรณ์หรือสื่อบันทึกข้อมูลไปซ่อม ส่งต่อ จำหน่าย หรือทำลาย ต้องลบหรือทำลายข้อมูลด้วยวิธีที่ไม่สามารถกู้คืนได้ตามมาตรฐานที่องค์การกำหนด

๓.๑๒ การบริหารจัดการผู้ให้บริการภายนอกในการปฏิบัติงาน

๑) การให้ผู้ให้บริการภายนอกเข้าดำเนินการกับระบบขององค์การ ต้องได้รับอนุมัติ กำหนดขอบเขตงาน ระยะเวลา สิทธิ์เข้าถึง และผู้รับผิดชอบกำกับดูแลอย่างชัดเจน

๒) ผู้ให้บริการภายนอกต้องปฏิบัติตามข้อตกลงรักษาความลับ ข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ และขั้นตอนการปฏิบัติงานขององค์การ

๓) การเข้าถึงระบบจากระยะไกลของผู้ให้บริการภายนอกต้องใช้ช่องทางที่ปลอดภัย จำกัดเวลาและสิทธิ์ รวมทั้งบันทึกประวัติการปฏิบัติงาน

๔) เมื่อสิ้นสุดงานหรือสิ้นสุดสัญญา ต้องยกเลิกสิทธิ์เข้าถึง ส่งมอบเอกสาร บัญชีผู้ใช้ ค่าการกำหนด และข้อมูลที่เกี่ยวข้องให้ครบถ้วน

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบอินทราเน็ต ระบบสารบรรณอิเล็กทรอนิกส์ อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้บุคลากรถือปฏิบัติตามอย่างเคร่งครัด

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำและเผยแพร่ SOP คู่มือ แบบฟอร์ม และรายการตรวจสอบที่เกี่ยวข้อง เช่น แบบคำขอเปลี่ยนแปลงระบบ คู่มือสำรองข้อมูล คู่มือแจ้งเหตุการณ์ และแนวปฏิบัติการใช้สิทธิ์ผู้ดูแลระบบ

๔.๔ จัดให้มีการอบรม ถ่ายทอดความรู้ หรือทบทวนแนวปฏิบัติสำหรับผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศอย่างน้อยปีละ ๑ ครั้ง รวมถึงเมื่อมีการเปลี่ยนแปลงระบบ กระบวนการ หรือเทคโนโลยีที่สำคัญ

๔.๕ ให้ผู้ให้บริการภายนอก ผู้รับจ้าง และบุคลากรที่เกี่ยวข้อง รับทราบและยอมรับข้อกำหนดด้านการ

ปฏิบัติงานและการรักษาความมั่นคงปลอดภัยสารสนเทศก่อนเริ่มปฏิบัติงาน

๔.๖ ให้มีการสื่อสารแจ้งเตือนช่องโหว่ ภัยคุกคาม เหตุการณ์ และบทเรียนที่สำคัญแก่ผู้ดูแลระบบและผู้เกี่ยวข้องโดยรวดเร็ว เพื่อให้สามารถดำเนินการป้องกันหรือแก้ไขได้ทันเวลา

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
คู่มือการปฏิบัติงาน	ร้อยละของกระบวนการปฏิบัติงานสำคัญที่มี SOP ครบถ้วนและได้รับการทบทวน	ร้อยละ ๑๐๐ ต่อปี
การเปลี่ยนแปลงระบบ	ร้อยละของรายการเปลี่ยนแปลงที่มีคำขอ การประเมินผลกระทบ การอนุมัติ และหลักฐานการทดสอบครบถ้วน	ไม่น้อยกว่าร้อยละ ๙๕
การเปลี่ยนแปลงฉุกเฉิน	ร้อยละของการเปลี่ยนแปลงฉุกเฉินที่ได้รับการทบทวนและจัดทำเอกสารย้อนหลัง	ร้อยละ ๑๐๐
การจัดการช่องโหว่	ร้อยละของช่องโหว่ระดับวิกฤตและระดับสูงที่ได้รับการแก้ไขหรือมีมาตรการชดเชยภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การสำรองข้อมูล	ร้อยละความสำเร็จของการสำรองข้อมูลตามแผน	ไม่น้อยกว่าร้อยละ ๙๘
การกู้คืนข้อมูล	ร้อยละของการทดสอบกู้คืนข้อมูลและระบบสำคัญที่ดำเนินการสำเร็จตามแผน	ร้อยละ ๑๐๐ ต่อปี
การเฝ้าระวังระบบ	ร้อยละของระบบสำคัญที่มีการบันทึกเหตุการณ์และมีการทบทวนบันทึกตามรอบ	ร้อยละ ๑๐๐
การจัดการเหตุการณ์	ระยะเวลาเฉลี่ยในการรับทราบ ควบคุม และเริ่มแก้ไขเหตุการณ์ตามระดับความรุนแรง	เป็นไปตามเกณฑ์ที่องค์การกำหนด
สิทธิ์ผู้ดูแลระบบ	ร้อยละของบัญชีผู้ดูแลระบบที่ได้รับการทบทวนสิทธิ์ตามรอบระยะเวลา	ร้อยละ ๑๐๐ ทุก ๖ เดือน
ความพร้อมใช้งานของระบบ	ร้อยละความพร้อมใช้งานของระบบสำคัญเทียบกับเป้าหมายการให้บริการ	ไม่น้อยกว่าร้อยละ ๙๙ หรือเป็นไปตาม SLA
การอบรมผู้ปฏิบัติงาน	ร้อยละของบุคลากรด้านเทคโนโลยีสารสนเทศที่ได้รับการอบรมหรือทบทวน SOP ตามแผน	ไม่น้อยกว่าร้อยละ ๙๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบ เหตุการณ์ หรือการประเมินความเสี่ยงที่ปิดการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และสรุปผลการวัดประสิทธิผลตามตัวชี้วัดที่กำหนดอย่างน้อยปีละ ๑ ครั้ง โดยตัวชี้วัดที่เกี่ยวข้องกับระบบสำคัญ เหตุการณ์ หรือช่องโหว่ระดับสูง อาจติดตามเป็นรายเดือนหรือรายไตรมาส

๕.๒ ให้รายงานผลการดำเนินงาน เหตุการณ์สำคัญ ความเสี่ยง ข้อค้นพบ และแผนปรับปรุงต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้อง เพื่อพิจารณากำกับติดตามและสนับสนุนทรัพยากรที่จำเป็น

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านระบบ เทคโนโลยี ภารกิจ กฎหมาย โครงสร้างองค์กร หรือภัยคุกคามที่มีนัยสำคัญ

ส่วนที่ ๑๐
นโยบายและแนวปฏิบัติการจัดหาและการพัฒนาระบบเทคโนโลยีสารสนเทศ
(System Acquisition and Development)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดนโยบายและแนวปฏิบัติสำหรับการจัดหา การพัฒนา การปรับปรุง การทดสอบ การตรวจรับ และการนำระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้าขึ้นใช้งานอย่างมีความมั่นคงปลอดภัย

๑.๒ เพื่อให้ความต้องการด้านความมั่นคงปลอดภัยสารสนเทศ การคุ้มครองข้อมูลส่วนบุคคล การบริหารความเสี่ยง และการดำเนินงานอย่างต่อเนื่อง ถูกกำหนดเป็นส่วนหนึ่งของโครงการตั้งแต่ระยะเริ่มต้น

๑.๓ เพื่อป้องกันความเสี่ยงจากช่องโหว่ ข้อผิดพลาดในการออกแบบ การพัฒนาที่ไม่เป็นไปตามมาตรฐาน การเข้าถึงข้อมูลโดยไม่ได้รับอนุญาต การเปลี่ยนแปลงระบบโดยมิชอบ และการรั่วไหลของข้อมูล

๑.๔ เพื่อให้ระบบเทคโนโลยีสารสนเทศที่จัดหา พัฒนา หรือเชื่อมต่อกับระบบขององค์การ มีคุณภาพ ปลอดภัย สามารถตรวจสอบได้ และรองรับภารกิจขององค์การคลังสินค้าได้อย่างต่อเนื่อง

๑.๕ เพื่อให้มีหลักฐานการดำเนินงาน ผู้รับผิดชอบ ตัวชี้วัด และการทบทวนปรับปรุงอย่างต่อเนื่อง อันสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับโครงการจัดหา พัฒนา ปรับปรุง ดัดแปลง เชื่อมโยง ย้ายระบบ หรือเลิกใช้งานระบบเทคโนโลยีสารสนเทศขององค์การคลังสินค้า

๒.๒ ครอบคลุมระบบงาน โปรแกรมประยุกต์ เว็บไซต์ แอปพลิเคชันบนอุปกรณ์เคลื่อนที่ ฐานข้อมูล ระบบคลาวด์ ระบบรายงาน ระบบเชื่อมโยงและแลกเปลี่ยนข้อมูล อุปกรณ์ ฮาร์ดแวร์ ซอฟต์แวร์ รวมถึงส่วนเชื่อมต่อระบบ (Application Programming Interface: API)

๒.๓ ครอบคลุมการจัดหาระบบจากผู้ให้บริการภายนอก การพัฒนาระบบโดยบุคลากรขององค์การ การจ้างพัฒนาระบบ การจัดซื้อซอฟต์แวร์สำเร็จรูป และการใช้บริการซอฟต์แวร์ผ่านระบบคลาวด์

๒.๔ ใช้บังคับกับคณะกรรมการ ผู้บริหาร เจ้าของโครงการ เจ้าของระบบ เจ้าของข้อมูล ผู้พัฒนาระบบ ผู้ทดสอบระบบ ผู้ดูแลระบบ ผู้ใช้งาน ผู้รับจ้าง ที่ปรึกษา ผู้ให้บริการภายนอก และบุคคลอื่นที่เกี่ยวข้องกับการจัดหาและพัฒนาระบบ

๓. แนวปฏิบัติ

๓.๑ การกำหนดบทบาท หน้าที่ และความรับผิดชอบ

๑) ให้กำหนดเจ้าของโครงการ เจ้าของระบบ (System Owner) เจ้าของข้อมูล (Data Owner) ผู้พัฒนาระบบ ผู้ทดสอบระบบ ผู้ดูแลระบบ และผู้อนุมัติการนำระบบขึ้นใช้งานอย่างชัดเจน

๒) เจ้าของโครงการมีหน้าที่กำกับให้การจัดหาและพัฒนาระบบเป็นไปตามวัตถุประสงค์ ขอบเขต งบประมาณ ระยะเวลา และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

๓) เจ้าของระบบและเจ้าของข้อมูลมีหน้าที่กำหนดความต้องการทางธุรกิจ ระดับความสำคัญของระบบ ชั้นความลับของข้อมูล สิทธิ์การเข้าถึง และเกณฑ์การตรวจรับระบบ

๔) ให้มีการแบ่งแยกหน้าที่ระหว่างผู้พัฒนา ผู้ทดสอบ ผู้อนุมัติ และผู้นำระบบขึ้นใช้งานจริงตามความเหมาะสม เพื่อป้องกันความขัดแย้งของหน้าที่และลดความเสี่ยงจากการแก้ไขระบบโดยมิชอบ

๓.๒ การวิเคราะห์ความต้องการและการประเมินความเสี่ยง

๑) ก่อนเริ่มโครงการจัดหาหรือพัฒนาระบบ ต้องมีการวิเคราะห์ความต้องการของผู้ใช้งาน กระบวนการทำงาน ข้อมูลที่เกี่ยวข้อง การเชื่อมโยงกับระบบอื่น และผลกระทบต่อการดำเนินงานขององค์การ

๒) ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศอย่างน้อยในเรื่องการพิสูจน์ตัวตน การควบคุมสิทธิ์ การบันทึกเหตุการณ์ การเข้ารหัสข้อมูล การสำรองข้อมูล การกู้คืนระบบ และการคุ้มครองข้อมูลส่วนบุคคล ตามความเหมาะสมกับระดับความเสี่ยง

๓) ต้องประเมินความเสี่ยงด้านเทคโนโลยีสารสนเทศและความเสี่ยงด้านข้อมูลก่อนการจัดหา พัฒนา หรือปรับปรุงระบบที่มีนัยสำคัญ

๔) กรณีระบบมีการจัดเก็บ ใช้ หรือเปิดเผยข้อมูลส่วนบุคคล ข้อมูลลับ ข้อมูลทางการเงิน หรือข้อมูลสำคัญขององค์การ ต้องกำหนดมาตรการคุ้มครองข้อมูลเพิ่มเติมตามกฎหมาย ระเบียบ และนโยบายขององค์การ

๕) ให้จัดทำเอกสารความต้องการด้านความมั่นคงปลอดภัยสารสนเทศเป็นส่วนหนึ่งของเอกสารข้อกำหนดโครงการ หรือเอกสารคุณลักษณะเฉพาะของระบบ

๓.๓ การจัดหาระบบและการคัดเลือกผู้ให้บริการ

๑) การจัดหาระบบ ซอฟต์แวร์ ฮาร์ดแวร์ หรือบริการคลาวด์ ต้องกำหนดคุณลักษณะด้านความมั่นคงปลอดภัยสารสนเทศไว้ในขอบเขตงาน (Terms of Reference: TOR) หรือเอกสารคุณลักษณะเฉพาะ

๒) การพิจารณาคัดเลือกผู้ให้บริการ ต้องประเมินความสามารถ ประสบการณ์ มาตรการรักษาความมั่นคงปลอดภัย การคุ้มครองข้อมูล การสนับสนุนหลังการขาย และความสามารถในการตอบสนองต่อเหตุการณ์

๓) สัญญาหรือข้อตกลงกับผู้ให้บริการต้องกำหนดข้อกำหนดอย่างน้อย ดังนี้

- หน้าที่ในการรักษาความลับและคุ้มครองข้อมูลขององค์การ
- ขอบเขตและสิทธิ์ในการเข้าถึงระบบหรือข้อมูล
- มาตรการด้านความมั่นคงปลอดภัยสารสนเทศที่ผู้ให้บริการต้องปฏิบัติ
- ระดับการให้บริการและระยะเวลาในการแก้ไขปัญหา
- การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยหรือข้อมูลรั่วไหล
- การสำรองข้อมูล การกู้คืนระบบ และการส่งมอบข้อมูล
- การตรวจสอบการปฏิบัติงานของผู้ให้บริการ
- การคืน ลบ หรือทำลายข้อมูลเมื่อสิ้นสุดสัญญา

๔) ซอฟต์แวร์ที่จัดหามาใช้ต้องมีลิขสิทธิ์ถูกต้อง ได้รับการสนับสนุนจากผู้ผลิตตามความเหมาะสม และไม่เป็นซอฟต์แวร์ที่หมดอายุการสนับสนุนหรือมีช่องโหว่ร้ายแรงโดยไม่มีมาตรการลดความเสี่ยง

๓.๔ การพัฒนาระบบอย่างมั่นคงปลอดภัย

๑) ให้ดำเนินการพัฒนาระบบตามกระบวนการพัฒนาระบบที่กำหนด โดยคำนึงถึงความมั่นคงปลอดภัยตั้งแต่ขั้นตอนวิเคราะห์ ออกแบบ พัฒนา ทดสอบ ติดตั้ง และบำรุงรักษา

๒) ให้มีการออกแบบสถาปัตยกรรมระบบและฐานข้อมูลโดยคำนึงถึงการแบ่งแยกส่วนงาน การควบคุมสิทธิ์ การลดการเข้าถึงข้อมูลโดยไม่จำเป็น และการป้องกันการเชื่อมต่อที่ไม่ปลอดภัย

๓) ผู้พัฒนาระบบต้องปฏิบัติตามแนวทางการเขียนโปรแกรมอย่างมั่นคงปลอดภัย เช่น การตรวจสอบข้อมูลนำเข้า การป้องกันการเข้าถึงข้อมูลโดยมิชอบ การจัดการข้อผิดพลาดอย่างเหมาะสม และการไม่เปิดเผยข้อมูลสำคัญผ่านข้อความข้อผิดพลาด

๔) ห้ามฝังรหัสผ่าน กุญแจเข้ารหัส โทเคน หรือข้อมูลลับไว้ในรหัสต้นฉบับ เอกสารสาธารณะ หรือแฟ้มกำหนดค่าที่ไม่มีการควบคุมการเข้าถึง

๕) ต้องใช้ระบบควบคุมเวอร์ชันสำหรับรหัสต้นฉบับ เอกสาร และค่าการกำหนดที่สำคัญ โดยจำกัดสิทธิ์เข้าถึงเฉพาะผู้ที่ได้รับอนุญาต

๖) การเปลี่ยนแปลงรหัสต้นฉบับต้องได้รับการทบทวนโดยผู้มีหน้าที่หรือผู้ที่ได้รับมอบหมายก่อนนำไปใช้งานจริง ตามระดับความสำคัญและความเสี่ยงของระบบ

๗) กรณีใช้ซอฟต์แวร์โอเพนซอร์ส หรือส่วนประกอบจากภายนอก ต้องตรวจสอบลิขสิทธิ์ ความน่าเชื่อถือ ช่องโหว่ และความเหมาะสมก่อนนำมาใช้งาน

๓.๕ การแยกสภาพแวดล้อมของระบบ

๑) ต้องแยกสภาพแวดล้อมสำหรับการพัฒนา (Development) การทดสอบ (Testing) การอบรม (Training) และการใช้งานจริง (Production) ออกจากกันตามความเหมาะสม

๒) ผู้พัฒนาระบบไม่ควรมีสิทธิ์เข้าถึงสภาพแวดล้อมการใช้งานจริง เว้นแต่ได้รับอนุมัติเป็นกรณีจำเป็น มีการกำหนดระยะเวลา และบันทึกการปฏิบัติงานเพื่อการตรวจสอบ

๓) ห้ามนำข้อมูลจริงในระบบงานไปใช้ในการพัฒนาหรือทดสอบ เว้นแต่ได้รับอนุมัติจากเจ้าของข้อมูล และมีมาตรการปกปิดข้อมูล จำกัดสิทธิ์ และควบคุมการใช้งานอย่างเหมาะสม

๔) ข้อมูลทดสอบที่มีข้อมูลส่วนบุคคลหรือข้อมูลสำคัญต้องผ่านการปกปิด ลดทอน หรือแปลงข้อมูล เพื่อไม่ให้สามารถระบุตัวบุคคลหรือเปิดเผยข้อมูลสำคัญได้โดยไม่จำเป็น

๓.๖ การทดสอบและตรวจสอบความมั่นคงปลอดภัย

๑) ก่อนนำระบบขึ้นใช้งานจริง ต้องมีการทดสอบการทำงานตามข้อกำหนดทางธุรกิจ การทดสอบการเชื่อมโยงระบบ การทดสอบประสิทธิภาพ และการทดสอบด้านความมั่นคงปลอดภัยตามความเหมาะสม

๒) ระบบที่มีความสำคัญสูงหรือเปิดให้บริการผ่านเครือข่ายอินเทอร์เน็ต ต้องได้รับการตรวจสอบช่องโหว่และทดสอบการเจาะระบบตามระดับความเสี่ยงก่อนเปิดใช้งานหรือหลังมีการเปลี่ยนแปลงสาระสำคัญ

๓) ข้อบกพร่องหรือช่องโหว่ที่ตรวจพบต้องได้รับการบันทึก ประเมินระดับความรุนแรง กำหนดผู้รับผิดชอบ และแก้ไขให้แล้วเสร็จก่อนนำระบบขึ้นใช้งานจริง หรือจัดให้มีมาตรการควบคุมความเสี่ยงที่ได้รับอนุมัติ

๔) ต้องจัดทำผลการทดสอบ รายงานข้อบกพร่อง และผลการแก้ไขเป็นหลักฐานประกอบการตรวจรับและอนุมัติใช้งานระบบ

๓.๗ การตรวจรับและการนำระบบขึ้นใช้งานจริง

๑) การตรวจรับระบบต้องพิจารณาความครบถ้วนตามขอบเขตงาน ความถูกต้องของการทำงาน ความมั่นคงปลอดภัย เอกสารประกอบ การถ่ายทอดความรู้ และการส่งมอบทรัพย์สินที่เกี่ยวข้อง

๒) ก่อนนำระบบขึ้นใช้งานจริง ต้องได้รับอนุมัติจากเจ้าของระบบ เจ้าของข้อมูล หน่วยงานเทคโนโลยีสารสนเทศ และผู้มีอำนาจตามที่องค์การกำหนด

๓) ต้องจัดทำแผนการนำระบบขึ้นใช้งานจริง ซึ่งอย่างน้อยต้องระบุวันและเวลา ผู้รับผิดชอบ ผลกระทบ แผนสื่อสาร แผนสำรอง แผนย้อนกลับ และขั้นตอนตรวจสอบหลังนำระบบขึ้นใช้งาน

๔) ต้องกำหนดบัญชีผู้ใช้งาน สิทธิ์การเข้าถึง การบันทึกเหตุการณ์ การสำรองข้อมูล และการเฝ้าระวังระบบให้พร้อมก่อนเปิดให้บริการจริง

๕) ภายหลังนำระบบขึ้นใช้งานจริง ให้ติดตามผลการดำเนินงาน ปัญหาที่เกิดขึ้น ความพึงพอใจของผู้ใช้งาน และประเด็นความมั่นคงปลอดภัย เพื่อปรับปรุงระบบตามความเหมาะสม

๓.๘ การจัดทำและส่งมอบเอกสารระบบ

๑) ผู้พัฒนาหรือผู้ให้บริการต้องจัดทำและส่งมอบเอกสารระบบให้ครบถ้วนตามที่กำหนดในโครงการ

๒) เอกสารอย่างน้อยควรประกอบด้วย เอกสารวิเคราะห์และออกแบบระบบ ผังสถาปัตยกรรมระบบ คู่มือผู้ใช้งาน คู่มือผู้ดูแลระบบ คู่มือการติดตั้งและกู้คืนระบบ รายการฐานข้อมูล รายการส่วนเชื่อมต่อระบบ และรายงานผลการทดสอบ

๓) ให้จัดเก็บเอกสาร รหัสต้นฉบับ ใบอนุญาตใช้ซอฟต์แวร์ ข้อมูลบัญชีผู้ดูแลระบบ และทรัพย์สินทางเทคนิคของระบบไว้ในพื้นที่ที่มีการควบคุมการเข้าถึง

๓.๙ การบริหารจัดการการเปลี่ยนแปลงและการบำรุงรักษาระบบ

๑) การแก้ไข ปรับปรุง เพิ่มฟังก์ชัน หรือเปลี่ยนแปลงค่าการกำหนดของระบบภายหลังนำขึ้นใช้งานจริง ต้องปฏิบัติตามกระบวนการบริหารจัดการการเปลี่ยนแปลงขององค์การ

๒) ก่อนเปลี่ยนแปลงระบบ ต้องประเมินผลกระทบต่อข้อมูล การเชื่อมโยงระบบ ความมั่นคงปลอดภัย ผู้ใช้งาน และการให้บริการ

๓) การเปลี่ยนแปลงที่มีผลกระทบสูงต้องทดสอบในสภาพแวดล้อมทดสอบ และมีแผนย้อนกลับกรณีการเปลี่ยนแปลงไม่เป็นไปตามที่กำหนด

๔) ให้ติดตามประกาศการสิ้นสุดการสนับสนุนของผู้ผลิต ระบบปฏิบัติการ ซอฟต์แวร์ และอุปกรณ์ที่ใช้งาน เพื่อจัดทำแผนปรับปรุงหรือทดแทนก่อนเกิดผลกระทบต่อความมั่นคงปลอดภัย

๓.๑๐ การยกเลิกระบบและการทำลายข้อมูล

๑) การยกเลิกระบบต้องได้รับอนุมัติจากเจ้าของระบบและผู้มีอำนาจ พร้อมประเมินผลกระทบต่อภารกิจ ข้อมูล ระบบเชื่อมโยง และผู้ใช้งาน

๒) ก่อนยกเลิกระบบ ต้องสำรอง ส่งมอบ เก็บรักษา หรือโอนย้ายข้อมูลตามระยะเวลาที่กฎหมาย ระเบียบ และองค์การกำหนด

๓) ต้องยกเลิกบัญชีผู้ใช้งาน สิทธิ์การเข้าถึง การเชื่อมต่อระบบ ใบรับรองดิจิทัล และบริการที่เกี่ยวข้อง เมื่อสิ้นสุดการใช้งาน

๔) ต้องลบหรือทำลายข้อมูล รหัสต้นฉบับ สื่อบันทึกข้อมูล และอุปกรณ์ที่เลิกใช้ด้วยวิธีที่เหมาะสม ปลอดภัย และสามารถตรวจสอบได้

๔. แนวทางการสื่อสารนโยบาย

๔.๑ เผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในขององค์การ

๔.๒ ให้ผู้บริหาร เจ้าของโครงการ และผู้บังคับบัญชาสื่อสารนโยบายแก่บุคลากร ผู้พัฒนาระบบ และผู้เกี่ยวข้องก่อนเริ่มโครงการจัดหา หรือพัฒนาระบบทุกโครงการ

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำคู่มือ แบบฟอร์ม และรายการตรวจสอบมาตรฐาน เช่น แบบวิเคราะห์ความต้องการ แบบประเมินความเสี่ยง แบบคำขอเปลี่ยนแปลงระบบ และรายการตรวจรับด้านความมั่นคงปลอดภัย

๔.๔ จัดให้มีการอบรมหรือถ่ายทอดความรู้แก่ผู้พัฒนาระบบ ผู้ทดสอบ ผู้ดูแลระบบ และเจ้าของโครงการอย่างน้อยปีละ ๑ ครั้ง ในเรื่องการพัฒนาระบบอย่างมั่นคงปลอดภัย การคุ้มครองข้อมูล และการทดสอบช่องโหว่

๔.๕ ให้ผู้รับจ้างและผู้ให้บริการภายนอกรับทราบข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ ลงนามในข้อตกลงรักษาความลับ และปฏิบัติตามเงื่อนไขในสัญญาก่อนเริ่มดำเนินงาน

๔.๖ ให้สื่อสารผลการตรวจสอบ ข้อบกพร่อง ช่องโหว่ เหตุการณ์ และบทเรียนที่เกี่ยวข้องแก่ผู้รับผิดชอบโครงการและผู้บริหาร เพื่อใช้ในการปรับปรุงการดำเนินงาน

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การกำหนดความต้องการด้านความมั่นคงปลอดภัย	ร้อยละของโครงการจัดหา/พัฒนาระบบที่กำหนดข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลตั้งแต่ระยะเริ่มต้น	ร้อยละ ๑๐๐

การประเมินความเสี่ยงโครงการ	ร้อยละของโครงการที่มีการประเมินความเสี่ยงก่อนเริ่มดำเนินการ	ร้อยละ ๑๐๐
การแยกสภาพแวดล้อม	ร้อยละของระบบสำคัญที่แยกสภาพแวดล้อมพัฒนา ทดสอบ และใช้งานจริง	ร้อยละ ๑๐๐
การทดสอบก่อนใช้งานจริง	ร้อยละของระบบที่ผ่านการทดสอบการทำงานและทดสอบด้านความมั่นคงปลอดภัยก่อนขึ้นใช้งานจริง	ร้อยละ ๑๐๐
การแก้ไขช่องโหว่	ร้อยละของช่องโหว่ระดับสูงหรือระดับวิกฤตที่แก้ไขหรือมีมาตรการลดความเสี่ยงก่อนเปิดใช้ระบบ	ร้อยละ ๑๐๐
การตรวจรับระบบ	ร้อยละของโครงการที่มีเอกสารตรวจรับ รายงานผลทดสอบ และเอกสารส่งมอบระบบครบถ้วน	ไม่น้อยกว่าร้อยละ ๙๕
การควบคุมการเปลี่ยนแปลง	ร้อยละของการเปลี่ยนแปลงระบบที่ผ่านการอนุมัติ ทดสอบ และมีแผนย้อนกลับตามกระบวนการ	ไม่น้อยกว่าร้อยละ ๙๕
การจัดการผู้ให้บริการ	ร้อยละของสัญญาหรือข้อตกลงที่มีข้อกำหนดด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลครบถ้วน	ร้อยละ ๑๐๐
คุณภาพระบบหลังใช้งาน	จำนวนข้อบกพร่องหรือเหตุการณ์ด้านความมั่นคงปลอดภัยระดับสูงที่พบภายหลังนำระบบขึ้นใช้งานจริง	ลดลงอย่างต่อเนื่อง
การอบรมผู้เกี่ยวข้อง	ร้อยละของผู้พัฒนา ผู้ดูแลระบบ และเจ้าของโครงการที่ผ่านการอบรมตามแผน	ไม่น้อยกว่าร้อยละ ๙๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบหรือประเมินความเสี่ยงที่ได้รับการแก้ไขภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลร่วมกับเจ้าของโครงการรวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้ทบทวนผลการวัด ข้อร้องเรียน ปัญหาจากการใช้งาน ผลการตรวจสอบ และเหตุการณ์ด้านความมั่นคงปลอดภัย เพื่อนำไปปรับปรุงมาตรฐานการจัดหาและการพัฒนาระบบอย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย เทคโนโลยี ภารกิจ รูปแบบการให้บริการ หรือภัยคุกคามที่มีนัยสำคัญ

ส่วนที่ ๑๑
นโยบายและแนวปฏิบัติการบริหารจัดการผู้ให้บริการภายนอก
(Third Party Management)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดนโยบายและแนวปฏิบัติในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่เกิดจากการใช้บริการ การว่าจ้าง หรือการเชื่อมต่อระบบกับผู้ให้บริการภายนอก

๑.๒ เพื่อให้ผู้ให้บริการภายนอก ผู้รับจ้าง ที่ปรึกษา ผู้พัฒนาระบบ ผู้ให้บริการคลาวด์ และคู่สัญญาที่เกี่ยวข้องกับข้อมูลหรือระบบสารสนเทศขององค์การคลังสินค้า ปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ การรักษาความลับ และการคุ้มครองข้อมูลขององค์การ

๑.๓ เพื่อกำหนดกระบวนการคัดเลือก ประเมินความเสี่ยง กำหนดเงื่อนไขในสัญญา ควบคุมการเข้าถึง ติดตามผลการให้บริการ และยุติการให้บริการของผู้ให้บริการภายนอกอย่างเป็นระบบ

๑.๔ เพื่อป้องกันการเข้าถึง การใช้ การเปิดเผย การสูญหาย การแก้ไขเปลี่ยนแปลง หรือการทำลายข้อมูลสารสนเทศขององค์การโดยไม่ได้รับอนุญาต อันเกิดจากการดำเนินงานของผู้ให้บริการภายนอก

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้มีหลักฐานการกำกับดูแลผู้ให้บริการภายนอก การประเมินผล การติดตามความเสี่ยง และการปรับปรุงการบริหารจัดการอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับผู้ให้บริการภายนอกทุกประเภทที่มีส่วนเกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศ ข้อมูลสารสนเทศ หรือทรัพย์สินสารสนเทศขององค์การคลังสินค้า

๒.๒ ครอบคลุมผู้ให้บริการ เช่น ผู้พัฒนาระบบ ผู้ดูแลและบำรุงรักษาระบบ ผู้ให้บริการเครือข่าย ผู้ให้บริการศูนย์ข้อมูล ผู้ให้บริการคลาวด์ ผู้ให้บริการจัดเก็บหรือสำรองข้อมูล ผู้รับจ้างปฏิบัติงานด้านเทคโนโลยีสารสนเทศ ที่ปรึกษา และผู้ให้บริการระบบรักษาความมั่นคงปลอดภัยสารสนเทศ

๒.๓ ครอบคลุมการเข้าถึงข้อมูล ระบบเครือข่าย ศูนย์ข้อมูล อุปกรณ์สารสนเทศ ห้องควบคุมระบบ สื่อบันทึกข้อมูล บัญชีผู้ใช้งาน ระบบงาน หรือบริการดิจิทัลขององค์การ ทั้งการเข้าถึงภายในสถานที่และการเข้าถึงจากระยะไกล

๒.๔ ใช้บังคับกับคณะกรรมการ ผู้บริหาร เจ้าของสัญญา เจ้าของโครงการ เจ้าของระบบ เจ้าของข้อมูล ส่วนงานพัสดุ สำสักกฎหมาย สำนักเทคโนโลยีดิจิทัล ผู้ดูแลระบบ และบุคลากรของผู้ให้บริการภายนอกที่เกี่ยวข้อง

๓. แนวปฏิบัติ

๓.๑ การจำแนกและประเมินความเสี่ยงของผู้ให้บริการภายนอก

๑) ให้หน่วยงานเจ้าของสัญญาหรือเจ้าของโครงการจัดทำทะเบียนผู้ให้บริการภายนอกที่เกี่ยวข้องกับระบบหรือข้อมูลสารสนเทศขององค์การ

๒) ทะเบียนผู้ให้บริการภายนอกอย่างน้อยต้องระบุชื่อผู้ให้บริการ ประเภทบริการ ระบบหรือข้อมูลที่เกี่ยวข้อง ระดับความสำคัญของบริการ ผู้รับผิดชอบสัญญา ระยะเวลาสัญญา ขอบเขตการเข้าถึง และผลการประเมินความเสี่ยง

๓) ก่อนคัดเลือกหรือเริ่มใช้บริการ ต้องประเมินความเสี่ยงของผู้ให้บริการภายนอกตามลักษณะบริการ ระดับความสำคัญของระบบ ประเภทข้อมูลที่เข้าถึง ผลกระทบหากบริการหยุดชะงัก และความสามารถด้านการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการ

๔) ผู้ให้บริการที่เข้าถึงข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ระบบสำคัญ หรือโครงสร้างพื้นฐานดิจิทัลขององค์การ ต้องได้รับการประเมินความเสี่ยงในระดับสูงและกำหนดมาตรการควบคุมเพิ่มเติมตามความเหมาะสม

๕) ให้ทบทวนผลการประเมินความเสี่ยงของผู้ให้บริการอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงขอบเขตบริการ เกิดเหตุการณ์ด้านความมั่นคงปลอดภัย หรือมีการต่ออายุสัญญา

๓.๒ การคัดเลือกและตรวจสอบผู้ให้บริการภายนอก

๑) การคัดเลือกผู้ให้บริการต้องพิจารณาความสามารถ ประสบการณ์ ความน่าเชื่อถือ สถานะทางกฎหมาย ความพร้อมในการให้บริการ และมาตรการด้านความมั่นคงปลอดภัยสารสนเทศควบคู่กับเงื่อนไขด้านราคาและคุณภาพบริการ

๒) ให้พิจารณาหลักฐานหรือข้อมูลที่แสดงถึงมาตรการรักษาความมั่นคงปลอดภัยสารสนเทศของผู้ให้บริการตามความเหมาะสม เช่น นโยบายความมั่นคงปลอดภัย มาตรฐานการให้บริการ รายงานการตรวจสอบ การรับรองมาตรฐาน แผนความต่อเนื่องทางธุรกิจ และกระบวนการบริหารจัดการเหตุการณ์

๓) กรณีผู้ให้บริการใช้ผู้รับจ้างช่วง (Subcontractor) ผู้ให้บริการต้องแจ้งให้องค์การทราบล่วงหน้า และต้องกำหนดให้ผู้รับจ้างช่วงปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศไม่น้อยกว่าที่องค์การกำหนด

๔) ผู้ให้บริการภายนอกต้องแต่งตั้งผู้ประสานงานที่รับผิดชอบด้านการให้บริการและด้านความมั่นคงปลอดภัยสารสนเทศ เพื่อใช้ติดต่อ ประสานงาน และแจ้งเหตุการณ์กับองค์การ

๓.๓ การกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยในสัญญา

๑) สัญญา ข้อตกลง หรือขอบเขตงานกับผู้ให้บริการภายนอก ต้องกำหนดข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศให้สอดคล้องกับระดับความเสี่ยงและความสำคัญของบริการ

๒) ข้อกำหนดในสัญญาอย่างน้อยควรครอบคลุมเรื่องดังต่อไปนี้

- การรักษาความลับของข้อมูลสารสนเทศและข้อมูลส่วนบุคคล
- วัตถุประสงค์ ขอบเขต และระยะเวลาการใช้ข้อมูลขององค์การ
- การควบคุมสิทธิ์เข้าถึงข้อมูล ระบบ และสถานที่ปฏิบัติงาน
- การใช้มาตรการป้องกันข้อมูล เช่น การเข้ารหัส การสำรองข้อมูล และการบันทึกเหตุการณ์
- การรักษาความมั่นคงปลอดภัยของระบบและอุปกรณ์ที่ใช้ให้บริการ
- ระดับการให้บริการ (Service Level Agreement: SLA) ระยะเวลาการตอบสนอง และระยะเวลาแก้ไขปัญหา
- การแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยหรือเหตุข้อมูลรั่วไหล
- การจัดการเหตุการณ์ การสืบค้นข้อเท็จจริง และการให้ความร่วมมือกับองค์การ
- สิทธิขององค์การในการตรวจสอบ ประเมิน หรือขอหลักฐานการปฏิบัติตามข้อกำหนด
- การห้ามนำข้อมูลขององค์การไปใช้เพื่อวัตถุประสงค์อื่น เปิดเผย ส่งต่อ หรือประมวลผลนอกขอบเขตที่ได้รับอนุญาต
- การจัดการข้อมูล การคืนข้อมูล การลบหรือทำลายข้อมูล และการยกเลิกสิทธิ์เมื่อสิ้นสุดสัญญา
- ความรับผิดชอบและการเยียวยาความเสียหายกรณีผู้ให้บริการไม่ปฏิบัติตามเงื่อนไข

๓) ผู้ให้บริการและบุคลากรที่เกี่ยวข้องต้องลงนามในข้อตกลงรักษาความลับก่อนเข้าถึงข้อมูล ระบบหรือทรัพย์สินสารสนเทศขององค์การ

๓.๔ การควบคุมการเข้าถึงของผู้ให้บริการภายนอก

๑) การให้สิทธิ์เข้าถึงข้อมูล ระบบเครือข่าย ระบบงาน ศูนย์ข้อมูล หรือพื้นที่ควบคุมแก่ผู้ให้บริการภายนอก ต้องได้รับอนุมัติจากเจ้าของระบบ เจ้าของข้อมูล หรือผู้มีอำนาจตามที่กำหนด

๒) ให้กำหนดสิทธิ์เข้าถึงตามหลักความจำเป็นในการปฏิบัติงาน และให้สิทธิ์เท่าที่จำเป็นตามระยะเวลาและขอบเขตของงาน

๓) บัญชีผู้ใช้งานของผู้ให้บริการภายนอกต้องเป็นบัญชีเฉพาะบุคคล ห้ามใช้บัญชีร่วมกัน เว้นแต่มีความ

จำเป็นและมีมาตรการควบคุมที่สามารถตรวจสอบผู้ใช้งานได้

๔) การเข้าถึงจากระยะไกลต้องใช้ช่องทางที่องค์การอนุมัติ มีการเข้ารหัสข้อมูล และใช้การพิสูจน์ตัวตนที่เหมาะสม โดยเฉพาะกรณีเข้าถึงระบบสำคัญหรือบัญชีผู้ดูแลระบบ

๕) การเข้าพื้นที่ศูนย์ข้อมูล ห้องควบคุมระบบ หรือตู้สื่อสาร ต้องลงทะเบียน ได้รับอนุญาตล่วงหน้า และอยู่ภายใต้การกำกับดูแลของเจ้าหน้าที่องค์การตามความเหมาะสม

๖) ให้มีการบันทึกและตรวจสอบประวัติการเข้าถึง การปฏิบัติงาน และการเปลี่ยนแปลงระบบของผู้ให้บริการภายนอก เพื่อให้สามารถตรวจสอบย้อนหลังได้

๗) ต้องทบทวนและยกเลิกสิทธิ์เข้าถึงทันทีเมื่อสิ้นสุดภารกิจ สิ้นสุดสัญญา เปลี่ยนบุคลากร หรือไม่มีความจำเป็นในการเข้าถึงอีกต่อไป

๓.๕ การคุ้มครองข้อมูลและการใช้บริการคลาวด์

๑) ผู้ให้บริการภายนอกต้องใช้ข้อมูลขององค์การเฉพาะตามวัตถุประสงค์และขอบเขตที่ระบุในสัญญาหรือข้อตกลงเท่านั้น

๒) การส่ง จัดเก็บ ประมวลผล หรือสำรองข้อมูลขององค์การในระบบของผู้ให้บริการ ต้องมีมาตรการคุ้มครองข้อมูลตามระดับชั้นความลับและระดับความเสี่ยงของข้อมูล

๓) กรณีใช้บริการคลาวด์ ต้องกำหนดขอบเขตความรับผิดชอบระหว่างองค์การและผู้ให้บริการให้ชัดเจน รวมถึงการควบคุมสิทธิ์ การตั้งค่าความมั่นคงปลอดภัย การสำรองข้อมูล การกู้คืน และการจัดการเหตุการณ์

๔) ผู้ให้บริการต้องแจ้งให้องค์การทราบ หากมีการเปลี่ยนแปลงสถานที่จัดเก็บหรือประมวลผลข้อมูล การใช้ผู้รับจ้างช่วง หรือการเปลี่ยนแปลงสถาปัตยกรรมที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของข้อมูล

๕) ห้ามผู้ให้บริการนำข้อมูลขององค์การไปใช้เพื่อการวิเคราะห์ การพัฒนาผลิตภัณฑ์ การตลาด หรือวัตถุประสงค์อื่น เว้นแต่ได้รับอนุมัติเป็นลายลักษณ์อักษรจากองค์การและเป็นไปตามกฎหมายที่เกี่ยวข้อง

๓.๖ การติดตามและประเมินผลการให้บริการ

๑) ให้หน่วยงานเจ้าของสัญญาติดตามผลการให้บริการของผู้ให้บริการภายนอกตามขอบเขตงาน SLA และข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ

๒) ให้มีการประเมินผู้ให้บริการตามรอบระยะเวลาที่กำหนด โดยพิจารณาอย่างน้อยเรื่องคุณภาพบริการ ความพร้อมใช้งานของระบบ การปฏิบัติตาม SLA เหตุการณ์ด้านความมั่นคงปลอดภัย การแก้ไขปัญหา และข้อร้องเรียน

๓) ผู้ให้บริการต้องรายงานสถานะการให้บริการ เหตุขัดข้อง การบำรุงรักษา การเปลี่ยนแปลงที่สำคัญ และผลการดำเนินงานด้านความมั่นคงปลอดภัยตามระยะเวลาที่กำหนดในสัญญา

๔) กรณีผู้ให้บริการไม่เป็นไปตามข้อตกลง ต้องจัดทำแผนแก้ไขปรับปรุง กำหนดผู้รับผิดชอบ และระยะเวลาแล้วเสร็จ โดยหน่วยงานเจ้าของสัญญาต้องติดตามผลจนกว่าจะแก้ไขครบถ้วน

๕) ให้รายงานผลการประเมินผู้ให้บริการภายนอกที่มีความเสี่ยงสูงหรือเกี่ยวข้องกับระบบสำคัญต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๓.๗ การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับผู้ให้บริการภายนอก

๑) ผู้ให้บริการภายนอกต้องแจ้งเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศที่อาจมีผลกระทบต่อข้อมูล ระบบ หรือการให้บริการขององค์การแก่ผู้ประสานงานที่กำหนดโดยเร็ว

๒) เหตุการณ์ที่ต้องแจ้งรวมถึงการเข้าถึงระบบโดยไม่ได้รับอนุญาต ข้อมูลรั่วไหล การติดมัลแวร์ ระบบหยุดชะงัก การสูญหายของข้อมูล หรือเหตุอื่นที่อาจส่งผลกระทบต่อองค์การ

๓) ผู้ให้บริการต้องให้ความร่วมมือในการควบคุมเหตุการณ์ รวบรวมพยานหลักฐาน วิเคราะห์สาเหตุ กู้คืนระบบหรือข้อมูล และจัดทำรายงานสรุปเหตุการณ์

๔) หน่วยงานเจ้าของสัญญาและสำนักเทคโนโลยีดิจิทัลต้องประเมินผลกระทบจากเหตุการณ์ กำหนดมาตรการแก้ไข และติดตามการดำเนินการของผู้ให้บริการจนแล้วเสร็จ

๕) เมื่อเกิดเหตุการณ์ที่มีนัยสำคัญ ให้ทบทวนความเสี่ยง เงื่อนไขการให้บริการ และมาตรการควบคุมของผู้ให้บริการ เพื่อป้องกันไม่ให้เกิดเหตุซ้ำ

๓.๘ การเปลี่ยนแปลงและการยุติการให้บริการ

๑) ผู้ให้บริการต้องแจ้งให้องค์การทราบและได้รับอนุมัติก่อนดำเนินการเปลี่ยนแปลงที่อาจส่งผลกระทบต่อระบบ ข้อมูล ความมั่นคงปลอดภัย หรือความต่อเนื่องในการให้บริการ

๒) การเปลี่ยนแปลงสำคัญ เช่น การเปลี่ยนโครงสร้างพื้นฐาน การย้ายศูนย์ข้อมูล การเปลี่ยนผู้รับจ้างช่วง หรือการเปลี่ยนวิธีประมวลผลข้อมูล ต้องได้รับการประเมินผลกระทบและความเสี่ยงก่อนดำเนินการ

๓) ก่อนสิ้นสุดสัญญาหรือยุติการให้บริการ ให้หน่วยงานเจ้าของสัญญาจัดทำแผนส่งมอบหรือโอนย้ายบริการ เพื่อป้องกันผลกระทบต่อภารกิจและความต่อเนื่องในการดำเนินงาน

๔) เมื่อสิ้นสุดสัญญา ผู้ให้บริการต้องส่งคืนข้อมูล เอกสาร ทรัพย์สิน รหัสต้นฉบับ ค่าการกำหนดระบบ และสิ่งอื่นที่เกี่ยวข้องให้ครบถ้วนตามข้อตกลง

๕) ผู้ให้บริการต้องลบหรือทำลายข้อมูลขององค์การในความครอบครองอย่างปลอดภัย และจัดส่งหลักฐานการลบหรือทำลายข้อมูลให้องค์การตามที่กำหนด

๖) ให้สำนักเทคโนโลยีดิจิทัลยกเลิกบัญชีผู้ใช้งาน สิทธิ์การเข้าถึง การเชื่อมต่อจากระยะไกล ใบรับรองดิจิทัล และสิทธิ์อื่นของผู้ให้บริการทันทีเมื่อสิ้นสุดสัญญาหรือพ้นความจำเป็น

๓.๙ การตรวจสอบและทบทวนการปฏิบัติตาม

๑) องค์การคลังสินค้ามีสิทธิ์ตรวจสอบหรือขอเอกสารหลักฐานจากผู้ให้บริการ เพื่อยืนยันการปฏิบัติตามข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศตามสัญญาหรือข้อตกลง

๒) การตรวจสอบอาจดำเนินการโดยการตรวจเอกสาร การประชุมติดตาม การประเมินตนเอง การตรวจสอบสถานที่ หรือวิธีการอื่นตามความเหมาะสมและเงื่อนไขในสัญญา

๓) หากพบข้อบกพร่องหรือการไม่ปฏิบัติตามข้อกำหนด ให้ผู้ให้บริการจัดทำแผนแก้ไขปรับปรุงภายในระยะเวลาที่องค์การกำหนด

๔) ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงกฎหมาย รูปแบบบริการ เทคโนโลยี ความเสี่ยง หรือเกิดเหตุการณ์สำคัญ

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้หน่วยงานเจ้าของสัญญา ส่วนงานพัสดุ สำนักกฎหมาย และสำนักเทคโนโลยีดิจิทัล รับทราบและนำแนวปฏิบัตินี้ไปใช้ในการจัดทำ TOR สัญญา ข้อตกลง และการกำกับติดตามผู้ให้บริการภายนอก

๔.๓ ให้ผู้ให้บริการภายนอกได้รับทราบข้อกำหนดด้านความมั่นคงปลอดภัยสารสนเทศ การรักษาความลับ การคุ้มครองข้อมูล และขั้นตอนการแจ้งเหตุ ก่อนเริ่มปฏิบัติงาน

๔.๔ ให้จัดทำคู่มือ แบบฟอร์ม และรายการตรวจสอบที่เกี่ยวข้อง เช่น แบบประเมินความเสี่ยงผู้ให้บริการ แบบทบทวน SLA แบบคำขอสิทธิ์เข้าถึงระบบ และแบบประเมินผลการให้บริการ

๔.๕ ให้จัดการประชุมทบทวนผลการให้บริการกับผู้ให้บริการที่มีความสำคัญหรือมีความเสี่ยงสูงตามระยะเวลาที่กำหนด เพื่อสื่อสารปัญหา ข้อค้นพบ ความเสี่ยง และแนวทางปรับปรุง

๔.๖ ให้สื่อสารเหตุการณ์ด้านความมั่นคงปลอดภัย ข้อบกพร่อง หรือการเปลี่ยนแปลงที่มีผลกระทบต่อบริการแก่ผู้บริหาร เจ้าของระบบ และผู้เกี่ยวข้องโดยรวดเร็ว

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การจัดทำทะเบียนผู้ให้บริการ	ร้อยละของผู้ให้บริการที่เกี่ยวข้องกับระบบหรือข้อมูลสารสนเทศที่มีข้อมูลในทะเบียนครบถ้วนและเป็นปัจจุบัน	ร้อยละ ๑๐๐
การประเมินความเสี่ยง	ร้อยละของผู้ให้บริการรายใหม่และผู้ให้บริการความเสี่ยงสูงที่ได้รับการประเมินก่อนเริ่มใช้บริการหรือก่อนต่ออายุสัญญา	ร้อยละ ๑๐๐
ข้อกำหนดในสัญญา	ร้อยละของสัญญาที่เกี่ยวข้องกับระบบหรือข้อมูลสารสนเทศ ซึ่งกำหนดเงื่อนไขด้านความมั่นคงปลอดภัยและการคุ้มครองข้อมูลครบถ้วน	ร้อยละ ๑๐๐
ข้อตกลงรักษาความลับ	ร้อยละของบุคลากรผู้ให้บริการที่เข้าถึงข้อมูลหรือระบบขององค์การและลงนามข้อตกลงรักษาความลับแล้ว	ร้อยละ ๑๐๐
การควบคุมสิทธิ์เข้าถึง	ร้อยละของบัญชีผู้ใช้หรือสิทธิ์ผู้ให้บริการที่ได้รับการทบทวนและยกเลิกเมื่อหมดความจำเป็น	ร้อยละ ๑๐๐
การปฏิบัติตาม SLA	ร้อยละของการให้บริการที่เป็นไปตามระดับการให้บริการที่กำหนดในสัญญา	ไม่น้อยกว่าร้อยละ ๙๕
การแจ้งเหตุการณ์	ร้อยละของเหตุการณ์จากผู้ให้บริการที่แจ้งต่อองค์การภายในระยะเวลาตามที่กำหนด	ร้อยละ ๑๐๐
การแก้ไขข้อบกพร่อง	ร้อยละของข้อบกพร่องหรือข้อค้นพบจากการประเมินผู้ให้บริการที่ได้รับการแก้ไขภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐
การประเมินผลผู้ให้บริการ	ร้อยละของผู้ให้บริการที่ได้รับการประเมินผลการให้บริการตามรอบระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
การยุติบริการ	ร้อยละของการสิ้นสุดสัญญาที่มีการคืนข้อมูล ยกเลิกสิทธิ์ และมีหลักฐานการลบหรือทำลายข้อมูลครบถ้วน	ร้อยละ ๑๐๐

๕.๑ ให้หน่วยงานเจ้าของสัญญาร่วมกับสำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง

๕.๒ ให้ติดตามผู้ให้บริการที่มีผลการประเมินต่ำ ไม่เป็นไปตาม SLA หรือมีเหตุการณ์ด้านความมั่นคงปลอดภัย โดยกำหนดแผนแก้ไขปรับปรุงและระยะเวลาแล้วเสร็จอย่างชัดเจน

๕.๓ ให้นำผลการประเมิน ข้อร้องเรียน เหตุการณ์ ข้อค้นพบ และความเสี่ยงจากผู้ให้บริการภายนอกไปใช้ในการทบทวนสัญญา ปรับปรุงข้อกำหนด และพัฒนากระบวนการบริหารจัดการผู้ให้บริการอย่างต่อเนื่อง

ส่วนที่ ๑๒
นโยบายและแนวปฏิบัติการป้องกันโปรแกรมไม่ประสงค์ดี
(Malicious Software Prevention)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดมาตรการป้องกัน ตรวจจับ ระงับเหตุการณ์ และกู้คืนความเสียหายที่เกิดจากโปรแกรมไม่ประสงค์ดี เช่น ไวรัสคอมพิวเตอร์ เวิร์ม โทรจัน สปายแวร์ ฟิชชิง แรนซัมแวร์ และโปรแกรมอันตรายรูปแบบอื่น

๑.๒ เพื่อคุ้มครองข้อมูลสารสนเทศ ระบบสารสนเทศ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ลูกข่าย อุปกรณ์พกพา และทรัพย์สินสารสนเทศขององค์การคลังสินค้า ให้มีความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งาน

๑.๓ เพื่อกำหนดให้มีการใช้ซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี การปรับปรุงระบบ การตรวจสอบไฟล์และสื่อบันทึกข้อมูล การเฝ้าระวัง และการแจ้งเหตุอย่างเป็นระบบ

๑.๔ เพื่อลดโอกาสและผลกระทบจากเหตุการณ์โจมตีทางไซเบอร์ โดยเฉพาะการโจมตีผ่านอีเมล เว็บไซต์ สื่อบันทึกข้อมูล การเชื่อมต่อจากระยะไกล และช่องโหว่ของระบบ

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยกำหนดให้มีผู้รับผิดชอบหลักฐานการดำเนินงาน ตัวชี้วัดผลลัพธ์ การติดตาม และการปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับระบบสารสนเทศและอุปกรณ์ทุกประเภทที่อยู่ภายใต้ความรับผิดชอบขององค์การคลังสินค้า ได้แก่ เครื่องคอมพิวเตอร์แม่ข่าย เครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา อุปกรณ์เคลื่อนที่ ระบบเครือข่าย อุปกรณ์จัดเก็บข้อมูล ระบบอีเมล ระบบเว็บไซต์ และระบบคลาวด์

๒.๒ ครอบคลุมซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี ระบบตรวจจับและตอบสนองภัยคุกคามที่ปลายทาง ระบบกรองอีเมล ระบบกรองเว็บไซต์ ระบบจัดการแพตช์ และระบบหรืออุปกรณ์ที่ใช้สนับสนุนการป้องกันภัยคุกคาม

๒.๓ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้พัฒนาระบบ ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานระบบหรืออุปกรณ์ขององค์การ

๒.๔ ครอบคลุมการป้องกันโปรแกรมไม่ประสงค์ดีตลอดวงจรชีวิตของอุปกรณ์และระบบ ตั้งแต่การติดตั้ง กำหนดค่าใช้งาน เฝ้าระวัง ปรับปรุง แก้ไขเหตุการณ์ จนถึงการยกเลิกใช้งาน

๓. แนวปฏิบัติ

๓.๑ การติดตั้งและใช้งานซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี

๑) เครื่องคอมพิวเตอร์ลูกข่าย เครื่องคอมพิวเตอร์พกพา และอุปกรณ์ที่องค์การกำหนด ต้องติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดีที่องค์การอนุมัติ และต้องเปิดใช้งานการป้องกันแบบต่อเนื่องตลอดระยะเวลาที่ใช้งาน

๒) เครื่องคอมพิวเตอร์แม่ข่ายที่ให้บริการบริหารจัดการหรือกระจายข้อมูลซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี ต้องได้รับการปรับปรุงฐานข้อมูลภัยคุกคามและโปรแกรมให้เป็นปัจจุบันอย่างสม่ำเสมอ

๓) สำนักเทคโนโลยีดิจทัลต้องกำหนดค่าการสแกน ตรวจจับ กักกัน และแจ้งเตือนภัยคุกคามให้เหมาะสมกับประเภทอุปกรณ์ ระดับความสำคัญของระบบ และความเสี่ยง

๔) ผู้ใช้งานห้ามปิด ปรับเปลี่ยน ถอนการติดตั้ง ขัดขวาง หรือรบกวนการทำงานของซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี เว้นแต่ได้รับอนุมัติจากสำนักเทคโนโลยีดิจทัล

๕) กรณีอุปกรณ์ไม่สามารถติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดีได้ เนื่องจากข้อจำกัดทางเทคนิค ให้สำนักเทคโนโลยีดิจทัลประเมินความเสี่ยงและกำหนดมาตรการควบคุมทดแทนเป็นลายลักษณ์อักษร

๓.๒ การปรับปรุงระบบและการจัดการช่องโหว่

๑) ระบบปฏิบัติการ เว็บเบราว์เซอร์ โปรแกรมประยุกต์ โปรแกรมสำนักงาน และซอฟต์แวร์ที่ติดตั้งในอุปกรณ์ขององค์การ ต้องได้รับการปรับปรุงแพตช์ความมั่นคงปลอดภัยตามรอบระยะเวลาที่กำหนด

๒) สำนักเทคโนโลยีดิจิทัลต้องติดตามข่าวสารช่องโหว่ ภัยคุกคาม และคำแนะนำด้านความมั่นคงปลอดภัยจากแหล่งข้อมูลที่น่าเชื่อถือ เพื่อประเมินผลกระทบต่อระบบขององค์การ

๓) ช่องโหว่ระดับวิกฤตหรือระดับสูงต้องได้รับการประเมินและดำเนินการแก้ไข ลดความเสี่ยง หรือกำหนดมาตรการควบคุมทดแทนภายในระยะเวลาที่องค์การกำหนด

๔) การติดตั้งแพตช์หรือปรับปรุงระบบที่อาจกระทบต่อการให้บริการ ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง ทดสอบ และบันทึกผลการดำเนินงานตามความเหมาะสม

๕) ห้ามใช้งานซอฟต์แวร์ที่หมดอายุการสนับสนุนหรือไม่มีผู้ผลิตดูแล เว้นแต่มีการประเมินความเสี่ยงและกำหนดมาตรการควบคุมทดแทนที่ได้รับอนุมัติ

๓.๓ การตรวจสอบอีเมล ไฟล์ และเว็บไซต์

๑) ผู้ใช้งานต้องระมัดระวังอีเมล ข้อความ ลิงก์ หรือไฟล์แนบที่ไม่คุ้นเคย มีลักษณะผิดปกติ หรือมาจากผู้ส่งที่ไม่สามารถยืนยันตัวตนได้

๒) ก่อนเปิดไฟล์แนบจากอีเมล หรือไฟล์ที่ดาวน์โหลดจากอินเทอร์เน็ต ผู้ใช้งานต้องตรวจสอบแหล่งที่มาและสแกนไฟล์ด้วยซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี

๓) ห้ามผู้ใช้งานเปิดใช้งานคำสั่งอัตโนมัติ เช่น Macro หรือดาวน์โหลดโปรแกรมจากแหล่งที่ไม่น่าเชื่อถือ เว้นแต่มีความจำเป็นต่อการปฏิบัติงานและได้รับอนุมัติ

๔) สำนักเทคโนโลยีดิจิทัลควรจัดให้มีระบบกรองอีเมลและเว็บไซต์ เพื่อป้องกันอีเมลขยะ Phishing ไฟล์แนบอันตราย เว็บไซต์หลอกลวง และเว็บไซต์ที่มีความเสี่ยง

๕) เมื่อพบอีเมล เว็บไซต์ หรือไฟล์ที่สงสัยว่าเป็นภัยคุกคาม ผู้ใช้งานต้องไม่ส่งต่อ ไม่คลิกลิงก์ ไม่เปิดไฟล์ และแจ้งสำนักเทคโนโลยีดิจิทัลโดยเร็ว

๓.๔ การควบคุมสื่อบันทึกข้อมูลและอุปกรณ์ภายนอก

๑) ผู้ใช้งานต้องตรวจสอบสื่อบันทึกข้อมูลแบบพกพา เช่น USB Drive, External Drive หรือสื่ออื่นก่อนนำมาเชื่อมต่อกับอุปกรณ์ขององค์การ

๒) สื่อบันทึกข้อมูลจากภายนอกต้องผ่านการสแกนหาโปรแกรมไม่ประสงค์ดีก่อนใช้งานทุกครั้ง

๓) องค์การอาจกำหนดให้จำกัด ปิดใช้งาน หรือควบคุมการใช้พอร์ตเชื่อมต่อและสื่อบันทึกข้อมูลแบบพกพา ตามระดับความเสี่ยงของหน่วยงานหรือระบบ

๔) ห้ามนำสื่อบันทึกข้อมูลส่วนบุคคลหรือไม่ทราบแหล่งที่มาเชื่อมต่อกับเครื่องคอมพิวเตอร์หรือระบบเครือข่ายขององค์การ เว้นแต่ได้รับอนุญาต

๕) สื่อบันทึกข้อมูลที่ใช้จัดเก็บข้อมูลสำคัญต้องได้รับการควบคุมสิทธิ์ เข้ารหัส หรือใช้มาตรการป้องกันอื่นตามระดับชั้นความลับของข้อมูล

๓.๕ การควบคุมการใช้โปรแกรมและการเชื่อมต่ออินเทอร์เน็ต

๑) ผู้ใช้งานต้องติดตั้งและใช้งานเฉพาะซอฟต์แวร์ที่ได้รับอนุญาต มีลิขสิทธิ์ถูกต้อง และมีความจำเป็นต่อการปฏิบัติงาน

๒) ห้ามดาวน์โหลด ติดตั้ง สร้าง เก็บ หรือเผยแพร่โปรแกรมไม่ประสงค์ดี โปรแกรมละเมิดลิขสิทธิ์ โปรแกรมที่ไม่ทราบแหล่งที่มา หรือโปรแกรมที่อาจก่อให้เกิดความเสี่ยงต่อระบบและเครือข่ายขององค์การ

๓) ห้ามใช้โปรแกรมที่มีลักษณะเสี่ยงต่อความมั่นคงปลอดภัย เช่น โปรแกรมแชร์ไฟล์แบบไม่ผ่านการควบคุม โปรแกรมขุดสินทรัพย์ดิจิทัล โปรแกรมดักจับข้อมูล หรือโปรแกรมสแกนเครือข่าย เว้นแต่ได้รับอนุมัติเพื่อ

ภารกิจด้านเทคนิคโดยเฉพาะ

๔) เครื่องคอมพิวเตอร์แม่ข่ายควรจำกัดหรือปิดการเชื่อมต่ออินเทอร์เน็ต เว้นแต่มีความจำเป็นต่อการให้บริการ โดยต้องกำหนดมาตรการป้องกันและควบคุมการเชื่อมต่อที่เหมาะสม

๕) การอนุญาตให้ระบบหรืออุปกรณ์เชื่อมต่ออินเทอร์เน็ตต้องพิจารณาตามความจำเป็น ระดับความเสี่ยง และหน้าที่การใช้งาน

๓.๖ การเฝ้าระวัง ตรวจจับ และตอบสนองต่อเหตุการณ์

๑) สำนักเทคโนโลยีดิจทัลต้องเฝ้าระวังสถานะการทำงานของซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี เหตุการณ์ตรวจพบภัยคุกคาม และอุปกรณ์ที่ไม่เป็นไปตามข้อกำหนด

๒) เมื่อระบบตรวจพบโปรแกรมไม่ประสงค์ดี ให้ดำเนินการกักกันไฟล์ แยกอุปกรณ์ออกจากเครือข่าย จำกัดผลกระทบ และดำเนินการตามขั้นตอนการจัดการเหตุการณ์ด้านความมั่นคงปลอดภัยสารสนเทศ

๓) ผู้ใช้งานที่พบหรือสงสัยว่าอุปกรณ์ติดโปรแกรมไม่ประสงค์ดี เช่น เครื่องทำงานผิดปกติ มีข้อความเรียกค่าไถ่ มีไฟล์ถูกเข้ารหัส หรือพบการเชื่อมต่อที่ผิดปกติ ต้องหยุดใช้งานอุปกรณ์และแจ้งสำนักเทคโนโลยีดิจทัลทันที

๔) สำนักเทคโนโลยีดิจทัลต้องบันทึกรายละเอียดเหตุการณ์ วิเคราะห์สาเหตุ รวบรวมหลักฐาน ประเมินผลกระทบ และดำเนินการกู้คืนระบบหรือข้อมูลตามความเหมาะสม

๕) ภายหลังเหตุการณ์ ต้องจัดทำรายงานสรุปบทเรียนและกำหนดมาตรการป้องกันการเกิดเหตุซ้ำ รวมถึงทบทวนการตั้งค่าระบบ ขั้นตอนปฏิบัติงาน และการสื่อสารสร้างความตระหนัก

๓.๗ การสำรองและกู้คืนข้อมูลกรณีถูกโจมตี

๑) ข้อมูลและระบบสำคัญต้องมีการสำรองข้อมูลตามแผนที่กำหนด เพื่อให้สามารถกู้คืนได้เมื่อเกิดเหตุการณ์จากโปรแกรมไม่ประสงค์ดีหรือแรนซัมแวร์

๒) ข้อมูลสำรองต้องได้รับการป้องกันจากการเข้าถึง แก้ไข หรือลบโดยไม่ได้รับอนุญาต และควรจัดเก็บแยกจากระบบงานหลักตามความเหมาะสม

๓) ต้องทดสอบการกู้คืนข้อมูลและระบบสำคัญตามแผนอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีเหตุการณ์ที่มีนัยสำคัญ

๔) ผลการทดสอบกู้คืนต้องได้รับการบันทึก วิเคราะห์ข้อจำกัด และนำไปปรับปรุงแผนสำรองข้อมูลหรือแผนความต่อเนื่องทางธุรกิจ

๓.๘ การสร้างความตระหนักและการปฏิบัติของผู้ใช้งาน

๑) ให้บุคลากรทุกคนตระหนักว่าการป้องกันโปรแกรมไม่ประสงค์ดีเป็นความรับผิดชอบร่วมกัน และต้องปฏิบัติตามนโยบายอย่างเคร่งครัด

๒) ให้จัดอบรมหรือทดสอบความตระหนักเรื่องภัยจากอีเมล Phishing ไฟล์แนบ ลิงก์อันตราย การใช้สื่อบันทึกข้อมูล และการแจ้งเหตุอย่างน้อยปีละ ๑ ครั้ง

๓) ผู้ใช้งานต้องปฏิบัติตามคำแนะนำหรือประกาศแจ้งเตือนจากสำนักเทคโนโลยีดิจทัลโดยทันที โดยเฉพาะกรณีพบภัยคุกคามหรือช่องโหว่ที่มีความเสี่ยงสูง

๔) ผู้ดูแลระบบ ผู้พัฒนาระบบ และผู้ปฏิบัติงานด้านเทคโนโลยีสารสนเทศต้องได้รับการอบรมเฉพาะด้านที่เกี่ยวข้องกับการตรวจจับ วิเคราะห์ และตอบสนองต่อภัยคุกคามตามบทบาทหน้าที่

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบอินทราเน็ต ระบบสารบรรณอิเล็กทรอนิกส์ อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้มีการ

ปฏิบัติตามอย่างต่อเนื่อง

๔.๓ ให้สำนักเทคโนโลยีดิจทัลจัดทำคู่มือหรือสื่อประชาสัมพันธ์ที่เข้าใจง่าย เช่น แนวทางตรวจสอบอีเมลและไฟล์แนบ วิธีแจ้งเหตุอุปกรณ์ติดมัลแวร์ ข้อควรระวังในการใช้ USB และแนวทางใช้งานอินเทอร์เน็ตอย่างปลอดภัย

๔.๔ ให้จัดอบรม สื่อสารเตือนภัย หรือทดสอบสถานการณ์จำลองเกี่ยวกับฟิชชิง แรนซัมแวร์ และภัยคุกคามรูปแบบใหม่แก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง

๔.๕ ให้แจ้งเตือนภัยคุกคาม ช่องโหว่ หรือเหตุการณ์สำคัญแก่ผู้ใช้งานและผู้เกี่ยวข้องโดยเร็ว พร้อมระบุแนวทางปฏิบัติที่ชัดเจน

๔.๖ ให้ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคลากรที่ได้รับอนุญาตให้เข้าถึงระบบขององค์การ รับทราบและปฏิบัติตามข้อกำหนดนี้ก่อนเริ่มปฏิบัติงาน

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การติดตั้งระบบป้องกันมัลแวร์	ร้อยละของอุปกรณ์ในทะเบียนที่ติดตั้งและเปิดใช้งานซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี	ร้อยละ ๑๐๐
ความเป็นปัจจุบันของฐานข้อมูลภัยคุกคาม	ร้อยละของอุปกรณ์ที่มีฐานข้อมูลภัยคุกคามและโปรแกรมป้องกันมัลแวร์เป็นปัจจุบัน	ไม่น้อยกว่าร้อยละ ๙๕
การบริหารจัดการแพตช์	ร้อยละของระบบหรืออุปกรณ์ที่ได้รับการปรับปรุงแพตช์ตามกรอบระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การจัดการช่องโหว่ร้ายแรง	ร้อยละของช่องโหว่ระดับวิกฤตและระดับสูงที่ได้รับการแก้ไขหรือมีมาตรการลดความเสี่ยงภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การตรวจพบและระงับเหตุ	ระยะเวลาเฉลี่ยตั้งแต่ตรวจพบภัยคุกคามจนถึงการกักกันหรือควบคุมเหตุการณ์	เป็นไปตามเกณฑ์ระดับความรุนแรงที่องค์การกำหนด
เหตุการณ์มัลแวร์	จำนวนเหตุการณ์มัลแวร์ที่ส่งผลกระทบต่อระบบสำคัญหรือทำให้บริการหยุดชะงัก	ลดลงอย่างต่อเนื่อง และไม่เกิดเหตุร้ายแรงซ้ำจากสาเหตุเดิม
การสำรองและกู้คืนข้อมูล	ร้อยละความสำเร็จของการสำรองข้อมูล และผลการทดสอบกู้คืนข้อมูลหรือระบบสำคัญ	สำรองสำเร็จไม่น้อยกว่าร้อยละ ๙๘ และทดสอบกู้คืนสำเร็จร้อยละ ๑๐๐ ตามแผน
การสร้างความตระหนัก	ร้อยละของบุคลากรกลุ่มเป้าหมายที่ผ่านการอบรมหรือรับทราบนโยบาย	ไม่น้อยกว่าร้อยละ ๙๐
การทดสอบฟิชชิง	อัตราการรายงานอีเมลต้องสงสัย และอัตราการคลิกลิงก์หรือเปิดไฟล์ที่เป็นอันตรายจากการทดสอบ	อัตราการรายงานเพิ่มขึ้นและอัตราการคลิกลดลงอย่างต่อเนื่อง
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบ เหตุการณ์ หรือการประเมินความเสี่ยงที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจทัลรวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง โดยตัวชี้วัดด้านสถานะการป้องกันภัยคุกคาม เหตุการณ์มัลแวร์ และการปรับปรุงแพตช์ ควรติดตามเป็นรายเดือนหรือรายไตรมาส

๕.๒ ให้มีการวิเคราะห์แนวโน้มของเหตุการณ์ ผลการทดสอบ และข้อค้นพบ เพื่อกำหนดมาตรการแก้ไขปรับปรุงการป้องกัน และพัฒนาความตระหนักของบุคลากรอย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีภัยคุกคาม เหตุการณ์ เทคโนโลยี หรือข้อกำหนดที่เกี่ยวข้องเปลี่ยนแปลงอย่างมีนัยสำคัญ

ส่วนที่ ๑๓
นโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยเว็บไซต์และการใช้งานอินเทอร์เน็ต
(Website and Internet Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดนโยบายและแนวปฏิบัติในการบริหารจัดการเว็บไซต์ ระบบงานที่ให้บริการผ่านเครือข่ายอินเทอร์เน็ต และการใช้อินเทอร์เน็ตขององค์การคลังสินค้า ให้มีความมั่นคงปลอดภัย เหมาะสม และตรวจสอบได้

๑.๒ เพื่อป้องกันเว็บไซต์ ระบบเว็บแอปพลิเคชัน ข้อมูล และผู้ใช้งาน จากการโจมตี การเข้าถึงโดยมิได้รับอนุญาต การปลอมแปลงเว็บไซต์ การแก้ไขข้อมูล การรั่วไหลของข้อมูล การแพร่กระจายโปรแกรมไม่ประสงค์ดี และการหยุดชะงักของบริการ

๑.๓ เพื่อกำหนดมาตรการควบคุมการเผยแพร่ข้อมูลผ่านเว็บไซต์ การกำหนดสิทธิ์ผู้ดูแลเว็บไซต์ การใช้ใบรับรองดิจิทัล การทดสอบช่องโหว่ การสำรองข้อมูล และการตอบสนองต่อเหตุการณ์ด้านเว็บไซต์

๑.๔ เพื่อกำหนดแนวทางการใช้อินเทอร์เน็ตของบุคลากรให้เป็นไปเพื่อประโยชน์ในการปฏิบัติงาน ไม่ก่อให้เกิดผลกระทบต่อระบบเครือข่าย ความมั่นคงปลอดภัย ชื่อเสียง หรือภาพลักษณ์ขององค์การคลังสินค้า

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยกำหนดให้มีผู้รับผิดชอบหลักฐานการควบคุม การติดตามผล ตัวชี้วัด และการปรับปรุงมาตรการอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับเว็บไซต์หลัก เว็บไซต์ย่อย ระบบเว็บแอปพลิเคชัน ระบบบริการอิเล็กทรอนิกส์ ระบบรับเรื่องร้องเรียน ระบบรับสมัครหรือรับคำขอออนไลน์ ระบบที่เชื่อมต่อกับประชาชนหรือหน่วยงานภายนอก รวมถึงระบบชื่อโดเมน (Domain Name) และระบบบริหารจัดการเนื้อหาเว็บไซต์

๒.๒ ครอบคลุมเครื่องแม่ข่ายเว็บไซต์ ฐานข้อมูล ระบบจัดเก็บไฟล์ ระบบชื่อโดเมน ใบรับรองดิจิทัล ระบบรักษาความมั่นคงปลอดภัยเว็บไซต์ ระบบบันทึกเหตุการณ์ และบริการคลาวด์ที่เกี่ยวข้องกับเว็บไซต์ขององค์การ

๒.๓ ครอบคลุมการเข้าถึงและการใช้งานอินเทอร์เน็ตของคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้พัฒนา ผู้รับจ้าง ผู้ให้บริการภายนอก และผู้ใช้งานที่ได้รับอนุญาต

๒.๔ ครอบคลุมการออกแบบ พัฒนา ทดสอบ เผยแพร่ บำรุงรักษา ปรับปรุง เฝ้าระวัง สำรอง กู้คืน และยกเลิกเว็บไซต์หรือระบบที่ให้บริการผ่านอินเทอร์เน็ต

๓. แนวปฏิบัติ

๓.๑ การกำหนดหน้าที่และความรับผิดชอบ

๑) ให้กำหนดเจ้าของเว็บไซต์ เจ้าของระบบ ผู้ดูแลเว็บไซต์ ผู้เผยแพร่เนื้อหา ผู้ดูแลระบบ ผู้ดูแลฐานข้อมูล และผู้อนุมัติการเผยแพร่ข้อมูลอย่างชัดเจน

๒) เจ้าของเว็บไซต์หรือเจ้าของระบบมีหน้าที่กำหนดวัตถุประสงค์ ขอบเขตบริการ กลุ่มผู้ใช้งาน ระดับความสำคัญของข้อมูล และข้อกำหนดด้านความมั่นคงปลอดภัยของเว็บไซต์

๓) ผู้ดูแลเว็บไซต์และผู้เผยแพร่เนื้อหาต้องตรวจสอบความถูกต้อง ความเหมาะสม ความเป็นปัจจุบัน และสิทธิในการเผยแพร่ข้อมูลก่อนนำข้อมูลขึ้นเว็บไซต์

๔) การกำหนดหรือเปลี่ยนแปลงสิทธิ์ผู้ดูแลเว็บไซต์ ผู้ดูแลระบบ หรือผู้เผยแพร่เนื้อหา ต้องได้รับอนุมัติจากผู้มีอำนาจ และบันทึกหลักฐานการดำเนินการ

๓.๒ การจดทะเบียนและบริหารจัดการชื่อโดเมน

๑) ชื่อโดเมนที่ใช้ในภารกิจขององค์การต้องจดทะเบียนในนามองค์การคลังสินค้า หรือผู้ที่องค์การ

มอบหมายอย่างเป็นทางการ

๒) ให้จัดทำทะเบียนชื่อโดเมนและโดเมนย่อย โดยระบุผู้รับผิดชอบ วัตถุประสงค์ วันที่หมดอายุ ผู้ให้บริการ และระบบที่เกี่ยวข้อง

๓) ให้ต่ออายุชื่อโดเมนก่อนวันหมดอายุ และกำหนดผู้รับผิดชอบตรวจสอบสถานะชื่อโดเมนอย่างน้อยเดือนละ ๑ ครั้ง

๔) บัญชีผู้ดูแลชื่อโดเมนและระบบ DNS ต้องจำกัดสิทธิ์เฉพาะผู้ได้รับมอบหมาย ใช้รหัสผ่านที่รัดกุม และใช้การพิสูจน์ตัวตนหลายปัจจัยตามความสามารถของระบบ

๕) การแก้ไขข้อมูล DNS การเพิ่มโดเมนย่อย หรือการเปลี่ยนผู้ให้บริการ ต้องผ่านกระบวนการบริหารจัดการการเปลี่ยนแปลง และมีการตรวจสอบความถูกต้องภายหลังดำเนินการ

๓.๓ การรักษาความมั่นคงปลอดภัยของเว็บไซต์และเว็บแอปพลิเคชัน

๑) เว็บไซต์และระบบเว็บแอปพลิเคชันที่เปิดให้บริการผ่านอินเทอร์เน็ต ต้องใช้การสื่อสารแบบเข้ารหัสผ่าน HTTPS โดยใช้ใบรับรองดิจิทัลที่ถูกต้อง เชื่อถือได้ และยังไม่หมดอายุ

๒) ให้ปิดหรือจำกัดการใช้งานโปรโตคอลและชุดการเข้ารหัสที่ล้าสมัยหรือมีความเสี่ยง และกำหนดค่าการเชื่อมต่อให้เหมาะสมตามมาตรฐานที่องค์การกำหนด

๓) ต้องกำหนดสิทธิ์การเข้าถึงเว็บไซต์และระบบหลังบ้านตามบทบาทหน้าที่ของผู้ใช้งาน และใช้หลักสิทธิ์ขั้นต่ำที่จำเป็น

๔) บัญชีผู้ดูแลระบบเว็บไซต์และบัญชีสิทธิ์สูงต้องเป็นบัญชีเฉพาะบุคคล ห้ามใช้บัญชีร่วมกัน และควรใช้การพิสูจน์ตัวตนหลายปัจจัย

๕) ห้ามใช้บัญชี ชื่อผู้ใช้ รหัสผ่าน หรือค่ากำหนดเริ่มต้นจากผู้ผลิตในระบบที่เปิดให้บริการจริง

๖) เว็บไซต์หรือระบบเว็บที่มีการรับส่งข้อมูลสำคัญ ต้องมีมาตรการควบคุมการหมดอายุของการใช้งาน การจัดการ Session และการป้องกันการเข้าถึงบัญชีผู้ใช้งานโดยมิชอบตามความเหมาะสม

๗) ต้องกำหนดหน้าข้อผิดพลาดของระบบให้ไม่เปิดเผยรายละเอียดด้านเทคนิค โครงสร้างระบบ ข้อมูลบัญชี หรือข้อมูลสำคัญที่อาจถูกนำไปใช้โจมตีระบบได้

๓.๔ การพัฒนาและทดสอบเว็บไซต์อย่างมั่นคงปลอดภัย

๑) การพัฒนา ปรับปรุง หรือแก้ไขเว็บไซต์และระบบเว็บแอปพลิเคชันต้องปฏิบัติตามแนวปฏิบัติการพัฒนาระบบอย่างมั่นคงปลอดภัยขององค์การ

๒) ต้องแยกสภาพแวดล้อมสำหรับการพัฒนา การทดสอบ และการใช้งานจริงออกจากกันตามความเหมาะสม

๓) ห้ามนำข้อมูลจริง ข้อมูลส่วนบุคคล หรือข้อมูลลับไปใช้ในการพัฒนาและทดสอบ เว้นแต่ได้รับอนุมัติและมีมาตรการปกปิดหรือแปลงข้อมูลเพื่อลดความเสี่ยง

๔) เว็บไซต์ที่เปิดให้บริการแก่บุคคลภายนอก หรือเว็บไซต์ที่มีข้อมูลสำคัญ ต้องได้รับการตรวจสอบช่องโหว่ก่อนเปิดใช้งานจริง และภายหลังการเปลี่ยนแปลงที่มีนัยสำคัญ

๕) ข้อบกพร่องหรือช่องโหว่ที่ตรวจพบต้องได้รับการบันทึก ประเมินระดับความรุนแรง แก้ไข และทดสอบซ้ำก่อนนำขึ้นใช้งานจริง หรือจัดให้มีมาตรการควบคุมความเสี่ยงที่ได้รับอนุมัติ

๖) ให้ควบคุมรหัสต้นฉบับ ไฟล์กำหนดค่า และข้อมูลลับของระบบด้วยระบบควบคุมเวอร์ชันหรือพื้นที่จัดเก็บที่มีการจำกัดสิทธิ์เข้าถึง

๓.๕ การบริหารจัดการเนื้อหาเว็บไซต์

๑) ข้อมูล ข่าว ประกาศ เอกสาร ภาพ หรือสื่ออื่นที่จะเผยแพร่ผ่านเว็บไซต์ ต้องได้รับการตรวจสอบความถูกต้อง ความครบถ้วน ความเหมาะสม และการอนุมัติก่อนเผยแพร่

๒) ห้ามเผยแพร่ข้อมูลลับ ข้อมูลส่วนบุคคล ข้อมูลภายในที่ยังไม่ได้รับอนุมัติ หรือข้อมูลที่อาจก่อให้เกิดผลกระทบต่อองค์การหรือบุคคลอื่น เว้นแต่มีอำนาจตามกฎหมายหรือได้รับอนุมัติจากผู้มีอำนาจ

๓) ข้อมูลที่เผยแพร่ต้องมีแหล่งที่มา วันที่เผยแพร่ หรือข้อมูลอ้างอิงตามความเหมาะสม เพื่อให้ตรวจสอบและปรับปรุงได้

๔) ให้ผู้รับผิดชอบทบทวนเนื้อหาเว็บไซต์อย่างสม่ำเสมอ และปรับปรุง แก้ไข หรือยกเลิกข้อมูลที่ล้าสมัย ไม่ถูกต้อง หรือไม่จำเป็น

๕) เอกสารที่เผยแพร่ผ่านเว็บไซต์ต้องตรวจสอบข้อมูลแฝงในไฟล์ เช่น ชื่อผู้จัดทำ ความเห็นในเอกสาร ข้อมูลส่วนบุคคล หรือข้อมูลภายใน ก่อนเผยแพร่

๓.๖ การป้องกันและเฝ้าระวังเว็บไซต์

๑) เว็บไซต์หรือระบบเว็บที่มีความสำคัญต้องมีมาตรการป้องกันการโจมตีที่เหมาะสม เช่น Firewall สำหรับเว็บแอปพลิเคชัน ระบบป้องกันการโจมตีแบบปฏิเสธการให้บริการ ระบบตรวจจับการบุกรุก หรือมาตรการควบคุมอื่นตามผลการประเมินความเสี่ยง

๒) ต้องปรับปรุงระบบปฏิบัติการ เว็บเซิร์ฟเวอร์ ระบบจัดการเนื้อหา ส่วนเสริม โปรแกรมประยุกต์ และฐานข้อมูล ให้เป็นปัจจุบันและแก้ไขช่องโหว่ตามระยะเวลาที่กำหนด

๓) ห้ามติดตั้งส่วนเสริม ธีม โปรแกรม หรือองค์ประกอบจากแหล่งที่ไม่น่าเชื่อถือ หรือที่ไม่จำเป็นต่อการใช้งาน

๔) ให้มีการบันทึกเหตุการณ์ที่สำคัญ เช่น การเข้าสู่ระบบของผู้ดูแล การแก้ไขเนื้อหา การเปลี่ยนแปลงค่าระบบ การพยายามเข้าถึงที่ล้มเหลว และเหตุการณ์ผิดปกติ

๕) ต้องเฝ้าระวังและตรวจสอบบันทึกเหตุการณ์ตามความสำคัญของเว็บไซต์ เพื่อค้นหาการโจมตี การแก้ไขหน้าเว็บไซต์โดยมิชอบ การเข้าถึงผิดปกติ หรือการใช้งานที่อาจกระทบต่อการให้บริการ

๖) เมื่อพบเว็บไซต์ปลอม เว็บไซต์ที่แอบอ้างชื่อองค์การ หรือการเผยแพร่เนื้อหาที่กระทบต่อองค์การ ให้แจ้งสำนักเทคโนโลยีดิจิทัลและหน่วยงานที่เกี่ยวข้องโดยเร็ว เพื่อดำเนินการตรวจสอบ ระงับเหตุ และประสานงานตามความเหมาะสม

๓.๗ การสำรองและกู้คืนเว็บไซต์

๑) เว็บไซต์ ระบบฐานข้อมูล ไฟล์เนื้อหา และค่าการกำหนดที่สำคัญต้องได้รับการสำรองข้อมูลตามแผนที่กำหนด

๒) ข้อมูลสำรองต้องจัดเก็บในพื้นที่ที่มีการควบคุมสิทธิ์ ป้องกันการแก้ไขหรือลบโดยมิได้รับอนุญาต และแยกจากระบบที่ให้บริการจริงตามความเหมาะสม

๓) ให้ทดสอบการกู้คืนเว็บไซต์ ข้อมูล และค่าการกำหนดของระบบที่สำคัญอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่มีนัยสำคัญ

๔) ต้องจัดทำแผนกู้คืนและแผนสื่อสารกรณีเว็บไซต์ไม่สามารถให้บริการได้ ถูกโจมตี หรือถูกแก้ไขโดยมิชอบ

๓.๘ การใช้งานอินเทอร์เน็ตของบุคลากร

๑) บุคลากรต้องใช้งานอินเทอร์เน็ตเพื่อสนับสนุนภารกิจและการปฏิบัติงานขององค์การอย่างเหมาะสม

๒) ห้ามใช้อินเทอร์เน็ตเพื่อเข้าถึง ดาวน์โหลด จัดเก็บ เผยแพร่ หรือส่งต่อข้อมูล ไฟล์ โปรแกรม หรือเนื้อหาที่ขัดต่อกฎหมาย ระเบียบ นโยบายขององค์การ หรือละเมิดสิทธิของผู้อื่น

๓) ห้ามดาวน์โหลดหรือติดตั้งโปรแกรม ไฟล์ หรือส่วนขยายของเว็บเบราว์เซอร์จากแหล่งที่ไม่น่าเชื่อถือ หรือที่ไม่ได้รับอนุญาตจากสำนักเทคโนโลยีดิจิทัล

๔) ห้ามกรอกรหัสผ่าน ข้อมูลส่วนบุคคล ข้อมูลขององค์การ หรือข้อมูลสำคัญลงในเว็บไซต์หรือ

แบบฟอร์มออนไลน์ที่ไม่สามารถยืนยันความน่าเชื่อถือได้

๕) ผู้ใช้งานต้องตรวจสอบชื่อเว็บไซต์ ความถูกต้องของชื่อโดเมน และการเชื่อมต่อแบบ HTTPS ก่อนเข้าสู่ระบบหรือทำรายการที่เกี่ยวข้องกับข้อมูลสำคัญ

๖) ห้ามใช้เครื่องมือหรือวิธีการหลีกเลี่ยงมาตรการควบคุมการใช้งานอินเทอร์เน็ตขององค์การ เว้นแต่ได้รับอนุญาตเพื่อการปฏิบัติงานโดยเฉพาะ

๗) การใช้งานสื่อสังคมออนไลน์ในนามองค์การ ต้องได้รับมอบหมายหรืออนุมัติจากผู้มีอำนาจ และต้องปฏิบัติตามแนวทางการสื่อสารขององค์การ

๓.๙ การจัดการเหตุการณ์ด้านเว็บไซต์และอินเทอร์เน็ต

๑) ผู้ใช้งานหรือผู้ดูแลระบบที่พบหรือสงสัยว่าเว็บไซต์ถูกโจมตี ถูกแก้ไข ถูกปลอมแปลง มีข้อมูลรั่วไหล หรือไม่สามารถให้บริการได้ ต้องแจ้งสำนักเทคโนโลยีดิจิทัลโดยเร็ว

๒) สำนักเทคโนโลยีดิจิทัลต้องดำเนินการประเมินระดับความรุนแรง ควบคุมเหตุการณ์ รวบรวมหลักฐาน แก้ไขช่องโหว่ กู้คืนบริการ และรายงานผู้บริหารหรือผู้เกี่ยวข้องตามขั้นตอนที่กำหนด

๓) กรณีเว็บไซต์ถูกแก้ไขโดยมิชอบ ให้ดำเนินการระงับการเข้าถึงหรือแยกระบบตามความเหมาะสม รักษาหลักฐาน ตรวจสอบสาเหตุ และกู้คืนจากข้อมูลสำรองที่เชื่อถือได้

๔) ภายหลังเหตุการณ์ ต้องวิเคราะห์สาเหตุ จัดทำรายงานสรุปบทเรียน และกำหนดมาตรการป้องกันเพื่อไม่ให้เกิดเหตุซ้ำ

๔. แนวทางการสื่อสารนโยบาย

๔.๑ เผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในขององค์การ

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารแนวปฏิบัติการใช้งานอินเทอร์เน็ตที่เหมาะสมแก่บุคลากรในสังกัด และกำกับดูแลให้ถือปฏิบัติ

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำคู่มือหรือรายการตรวจสอบสำหรับผู้ดูแลเว็บไซต์ ผู้เผยแพร่เนื้อหา และผู้ใช้งานอินเทอร์เน็ต เช่น ขั้นตอนการเผยแพร่ข่าว การตรวจสอบไฟล์ก่อนอัปโหลด วิธีแจ้งเหตุเว็บไซต์ผิดปกติ และข้อควรระวังจากเว็บไซต์หลอกลวง

๔.๔ จัดให้มีการอบรมหรือกิจกรรมสร้างความตระหนักอย่างน้อยปีละ ๑ ครั้ง ในเรื่องการใช้งานอินเทอร์เน็ตอย่างปลอดภัย การตรวจสอบเว็บไซต์ปลอม การป้องกันฟิชชิง และการคุ้มครองข้อมูลก่อนเผยแพร่

๔.๕ แจ้งเตือนข้อมูลเกี่ยวกับช่องโหว่ ภัยคุกคาม เว็บไซต์ปลอม เหตุการณ์โจมตี หรือการเปลี่ยนแปลงข้อกำหนดที่สำคัญแก่ผู้ดูแลเว็บไซต์และผู้เกี่ยวข้องโดยเร็ว

๔.๖ ให้ผู้รับจ้าง ผู้พัฒนาระบบ และผู้ให้บริการภายนอกที่เกี่ยวข้องกับเว็บไซต์หรือระบบเว็บ รับทราบและปฏิบัติตามข้อกำหนดนี้ก่อนเริ่มปฏิบัติงาน

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การบริหารชื่อโดเมน	ร้อยละของชื่อโดเมนและโดเมนย่อยที่มีทะเบียนข้อมูลผู้รับผิดชอบ และสถานะวันหมดอายุครบถ้วน	ร้อยละ ๑๐๐
การใช้การเชื่อมต่อที่ปลอดภัย	ร้อยละของเว็บไซต์และระบบเว็บที่เปิดให้บริการภายนอกผ่าน HTTPS และมีใบรับรองดิจิทัลที่ถูกต้อง	ร้อยละ ๑๐๐
การควบคุมบัญชีสิทธิ์สูง	ร้อยละของบัญชีผู้ดูแลเว็บไซต์ที่เป็นรายบุคคล ได้รับการทบทวนสิทธิ์ และใช้การยืนยันตัวตนตามข้อกำหนด	ร้อยละ ๑๐๐

การปรับปรุงช่องโหว่	ร้อยละของช่องโหว่ระดับวิกฤตและระดับสูงของเว็บไซต์ที่ได้รับการแก้ไขหรือมีมาตรการลดความเสี่ยงภายในระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การทดสอบความมั่นคงปลอดภัย	ร้อยละของเว็บไซต์หรือระบบเว็บสำคัญที่ได้รับการตรวจสอบช่องโหว่ตามแผน	ร้อยละ ๑๐๐ ต่อปี
การสำรองและกู้คืน	ร้อยละของเว็บไซต์สำคัญที่มีการสำรองข้อมูลตามแผน และผลการทดสอบกู้คืนสำเร็จ	สำรองสำเร็จไม่น้อยกว่าร้อยละ ๙๘ และทดสอบกู้คืนสำเร็จร้อยละ ๑๐๐ ตามแผน
การทบทวนเนื้อหา	ร้อยละของเนื้อหาเว็บไซต์ที่ผ่านการทบทวนตามรอบระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๐
เหตุการณ์เว็บไซต์	จำนวนเหตุการณ์เว็บไซต์ถูกโจมตี ถูกแก้ไขโดยมิชอบ เว็บไซต์ปลอม หรือระบบหยุดชะงัก และระยะเวลาในการตอบสนอง	ลดลงอย่างต่อเนื่อง และดำเนินการตามเกณฑ์เวลาที่กำหนด
การสร้างความตระหนัก	ร้อยละของผู้ดูแลเว็บไซต์ ผู้เผยแพร่เนื้อหา และบุคลากรกลุ่มเป้าหมายที่ผ่านการอบรมหรือรับทราบนโยบาย	ไม่น้อยกว่าร้อยละ ๙๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบ เหตุการณ์ หรือการประเมินความเสี่ยงที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลร่วมกับเจ้าของเว็บไซต์รวบรวม วิเคราะห์ และสรุปผลการวัดประสิทธิผลอย่างน้อยปีละ ๑ ครั้ง โดยตัวชี้วัดด้านใบรับรองดิจิทัล ช่องโหว่ และความพร้อมใช้งานของเว็บไซต์ ควรติดตามเป็นรายเดือนหรือรายไตรมาส

๕.๒ ให้รายงานเหตุการณ์สำคัญ ผลการตรวจสอบ ข้อบกพร่อง และแผนปรับปรุงต่อผู้บริหารหรือคณะทำงานที่เกี่ยวข้อง เพื่อกำกับติดตามและพัฒนามาตรการอย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านเทคโนโลยี รูปแบบการให้บริการ เว็บไซต์ ระบบงาน กฎหมาย หรือภัยคุกคามที่มีนัยสำคัญ

ส่วนที่ ๑๔
นโยบายและแนวปฏิบัติการรักษาความปลอดภัยในอุปกรณ์ที่ใช้ปฏิบัติงาน
(Endpoint Security)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยของอุปกรณ์ที่ใช้ปฏิบัติงานขององค์การคลังสินค้า ให้มีความปลอดภัย พร้อมใช้งาน และไม่เป็นช่องทางให้เกิดการเข้าถึงระบบหรือข้อมูลโดยมิได้รับอนุญาต

๑.๒ เพื่อป้องกันความเสี่ยงจากการสูญหาย ถูกโจรกรรม การใช้งานผิดวัตถุประสงค์ การติดโปรแกรมไม่ประสงค์ดี การรั่วไหลของข้อมูล และการโจมตีผ่านอุปกรณ์ปลายทาง

๑.๓ เพื่อกำหนดมาตรการควบคุมอุปกรณ์คอมพิวเตอร์ อุปกรณ์พกพา อุปกรณ์เคลื่อนที่ สื่อบันทึกข้อมูล และอุปกรณ์อื่นที่เชื่อมต่อกับระบบเครือข่ายหรือระบบสารสนเทศขององค์การ

๑.๔ เพื่อให้มีการบริหารจัดการทรัพย์สินสารสนเทศ การควบคุมสิทธิ์ การกำหนดค่าความมั่นคงปลอดภัย การปรับปรุงระบบ การเข้ารหัสข้อมูล และการจัดการอุปกรณ์เมื่อสิ้นสุดการใช้งานอย่างเป็นระบบ

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยกำหนดให้มีผู้รับผิดชอบหลักฐานการควบคุม ตัวชี้วัด การติดตามผล และการปรับปรุงมาตรการรักษาความมั่นคงปลอดภัยอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับอุปกรณ์ที่องค์การคลังสินค้าเป็นเจ้าของ เช่า ยืม หรืออนุญาตให้ใช้เพื่อการปฏิบัติงาน ได้แก่ เครื่องคอมพิวเตอร์ตั้งโต๊ะ เครื่องคอมพิวเตอร์พกพา เครื่องคอมพิวเตอร์แม่ข่าย อุปกรณ์เคลื่อนที่ โทรศัพท์เคลื่อนที่ แท็บเล็ต เครื่องพิมพ์ เครื่องสแกน สื่อบันทึกข้อมูล และอุปกรณ์เชื่อมต่อเครือข่าย

๒.๒ ครอบคลุมอุปกรณ์ส่วนบุคคลที่ได้รับอนุญาตให้นำมาใช้เพื่อปฏิบัติงานหรือเชื่อมต่อกับระบบขององค์การ รวมถึงการปฏิบัติงานจากระยะไกล

๒.๓ ครอบคลุมการจัดหา การลงทะเบียน การส่งมอบ การติดตั้ง การกำหนดค่า การใช้งาน การบำรุงรักษา การซ่อมแซม การโยกย้าย การยืม-คืน การสูญหาย การจำหน่าย และการทำลายอุปกรณ์หรือสื่อบันทึกข้อมูล

๒.๔ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้รับจ้าง ผู้ให้บริการภายนอก และบุคคลอื่นที่ได้รับอนุญาตให้ใช้งานอุปกรณ์หรือเข้าถึงระบบสารสนเทศขององค์การ

๓. แนวปฏิบัติ

๓.๑ การบริหารจัดการทะเบียนอุปกรณ์และทรัพย์สินสารสนเทศ

๑) ให้หน่วยงานที่รับผิดชอบจัดทำทะเบียนอุปกรณ์สารสนเทศให้ครบถ้วน เป็นปัจจุบัน และสามารถตรวจสอบได้

๒) ทะเบียนอุปกรณ์อย่างน้อยต้องระบุประเภทอุปกรณ์ ยี่ห้อ รุ่น หมายเลขประจำเครื่อง หมายเลขทรัพย์สิน ผู้รับผิดชอบ หน่วยงาน สถานที่ติดตั้ง สถานะการใช้งาน และวันที่ส่งมอบหรือรับคืน

๓) อุปกรณ์ที่ใช้จัดเก็บหรือประมวลผลข้อมูลสำคัญต้องระบุระดับความสำคัญของอุปกรณ์ และกำหนดมาตรการคุ้มครองตามระดับความเสี่ยง

๔) ให้ตรวจนับและทบทวนทะเบียนอุปกรณ์อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการโยกย้าย ส่งมอบ เปลี่ยนแปลง หรือเลิกใช้งานอุปกรณ์

๓.๒ การส่งมอบและการรับผิดชอบอุปกรณ์

๑) การส่งมอบอุปกรณ์ให้บุคลากรใช้งาน ต้องมีการบันทึกการรับมอบ ระบุผู้รับผิดชอบ และให้ผู้รับมอบ

รับทราบเงื่อนไขการใช้งานอย่างปลอดภัย

๒) ผู้รับมอบอุปกรณ์มีหน้าที่ดูแลรักษา ป้องกันการสูญหายหรือถูกโจรกรรม และใช้อุปกรณ์เพื่อประโยชน์ในการปฏิบัติงานขององค์การ

๓) ห้ามผู้ใช้งานให้บุคคลอื่นยืม ใช้งาน หรือเข้าถึงอุปกรณ์ของตนโดยไม่ได้รับอนุญาต เว้นแต่มีความจำเป็นในการปฏิบัติงานและได้รับความเห็นชอบจากผู้มีอำนาจ

๔) เมื่อมีการเปลี่ยนหน้าที่ ย้ายหน่วยงาน พ้นสภาพ หรือสิ้นสุดสัญญา ผู้ใช้งานต้องส่งคืนอุปกรณ์และทรัพย์สินสารสนเทศที่ได้รับมอบหมาย พร้อมให้มีการตรวจสอบและยกเลิกสิทธิ์ที่เกี่ยวข้อง

๓.๓ การกำหนดค่าความมั่นคงปลอดภัยของอุปกรณ์

๑) อุปกรณ์ที่ใช้งานในองค์การต้องได้รับการติดตั้งและกำหนดค่าความมั่นคงปลอดภัยตามมาตรฐานที่สำนักเทคโนโลยีดิจิทัลกำหนด

๒) ต้องเปลี่ยนชื่อผู้ใช้งาน รหัสผ่าน และค่าการกำหนดเริ่มต้นจากผู้ผลิตก่อนนำอุปกรณ์ขึ้นใช้งาน

๓) ต้องปิดหรือถอนการติดตั้งโปรแกรม บริการ บัญชีผู้ใช้ และการเชื่อมต่อที่ไม่จำเป็นต่อการปฏิบัติงาน

๔) ต้องกำหนดให้หน้าจอล็อกโดยอัตโนมัติเมื่อไม่มีการใช้งานภายในระยะเวลาที่องค์การกำหนด และผู้ใช้งานต้องล็อกหน้าจอทุกครั้งเมื่อออกจากอุปกรณ์หรือพื้นที่ปฏิบัติงาน

๕) ต้องกำหนดให้มีการพิสูจน์ตัวตนก่อนเข้าใช้งานอุปกรณ์ด้วยรหัสผ่าน รหัสผ่านส่วนบุคคล หรือวิธีการยืนยันตัวตนอื่นที่เหมาะสม

๖) ห้ามใช้งานบัญชีผู้ดูแลระบบสำหรับการปฏิบัติงานทั่วไป เว้นแต่มีความจำเป็นและได้รับอนุมัติตามกระบวนการที่กำหนด

๓.๔ การควบคุมการเข้าถึงและรหัสผ่าน

๑) ผู้ใช้งานต้องใช้บัญชีผู้ใช้งานของตนเอง ห้ามใช้บัญชีผู้ใช้งานร่วมกัน หรือเปิดเผยรหัสผ่านแก่ผู้อื่น

๒) รหัสผ่านต้องมีความรัดกุมตามมาตรฐานที่องค์การกำหนด และต้องไม่ใช้รหัสผ่านที่คาดเดาได้ง่ายหรือซ้ำกับบัญชีส่วนบุคคลที่มีความเสี่ยง

๓) อุปกรณ์ที่เข้าถึงข้อมูลสำคัญ ระบบงานสำคัญ หรือเชื่อมต่อจากระยะไกล ควรใช้การพิสูจน์ตัวตนหลายปัจจัยตามระดับความเสี่ยง

๔) ให้ทบทวนสิทธิ์การเข้าถึงของผู้ใช้งานตามรอบระยะเวลาที่กำหนด และยกเลิกสิทธิ์ทันทีเมื่อพ้นความจำเป็น

๓.๕ การป้องกันโปรแกรมไม่ประสงค์ดีและการปรับปรุงระบบ

๑) อุปกรณ์ปลายทางต้องติดตั้งซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดีที่องค์การอนุมัติ และต้องเปิดใช้งานการป้องกันอย่างต่อเนื่อง

๒) ผู้ใช้งานห้ามปิด ปรับเปลี่ยน ถอนการติดตั้ง หรือขัดขวางการทำงานของซอฟต์แวร์ป้องกันโปรแกรมไม่ประสงค์ดี เว้นแต่ได้รับอนุมัติจากสำนักเทคโนโลยีดิจิทัล

๓) ระบบปฏิบัติการ โปรแกรมประยุกต์ และซอฟต์แวร์ที่เกี่ยวข้อง ต้องได้รับการปรับปรุงแพตช์ด้านความมั่นคงปลอดภัยตามระยะเวลาที่กำหนด

๔) ห้ามติดตั้งซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ ไม่ได้รับอนุญาต หมดอายุการสนับสนุน หรือมาจากแหล่งที่ไม่น่าเชื่อถือ

๕) สำนักเทคโนโลยีดิจิทัลต้องติดตามและตรวจสอบสถานะการปรับปรุงแพตช์ การติดตั้งโปรแกรมป้องกันมัลแวร์ และการปฏิบัติตามมาตรฐานของอุปกรณ์อย่างสม่ำเสมอ

๓.๖ การเข้ารหัสข้อมูลและการป้องกันอุปกรณ์พกพา

๑) อุปกรณ์พกพา เช่น เครื่องคอมพิวเตอร์พกพา โทรศัพท์เคลื่อนที่ และแท็บเล็ต ที่จัดเก็บหรือเข้าถึง

ข้อมูลสำคัญ ต้องได้รับการเข้ารหัสข้อมูลตามมาตรฐานที่องค์การกำหนด

๒) อุปกรณ์เคลื่อนที่ต้องเปิดใช้การล็อกหน้าจอ การลบข้อมูลจากระยะไกล หรือมาตรการควบคุมอื่นตามความเหมาะสมและความสามารถของอุปกรณ์

๓) ห้ามจัดเก็บข้อมูลลับ ข้อมูลลับมาก ข้อมูลส่วนบุคคล หรือข้อมูลสำคัญไว้ในอุปกรณ์พกพา เว้นแต่มีความจำเป็น ได้รับอนุมัติ และมีมาตรการป้องกันที่เหมาะสม

๔) ผู้ใช้งานต้องไม่ทิ้งอุปกรณ์พกพาไว้ในสถานที่สาธารณะ ยานพาหนะ หรือพื้นที่ที่ไม่มีการควบคุมดูแล

๕) กรณีอุปกรณ์สูญหาย ถูกโจรกรรม หรือสงสัยว่าถูกเข้าถึงโดยมิได้รับอนุญาต ต้องแจ้งผู้บังคับบัญชาและสำนักเทคโนโลยีดิจิทัลโดยทันที

๓.๗ การควบคุมสื่อบันทึกข้อมูลและอุปกรณ์ภายนอก

๑) การใช้สื่อบันทึกข้อมูลแบบพกพา เช่น USB Drive, External Drive หรืออุปกรณ์จัดเก็บข้อมูลอื่นต้องเป็นไปตามความจำเป็นในการปฏิบัติงานและได้รับอนุญาตตามที่องค์การกำหนด

๒) สื่อบันทึกข้อมูลจากภายนอกต้องผ่านการตรวจสอบหาโปรแกรมไม่ประสงค์ดีก่อนเชื่อมต่อกับอุปกรณ์ขององค์การ

๓) ข้อมูลสำคัญที่บันทึกในสื่อพกพาต้องได้รับการเข้ารหัส หรือมีมาตรการป้องกันอื่นตามระดับชั้นความลับของข้อมูล

๔) ห้ามใช้อุปกรณ์จัดเก็บข้อมูลส่วนบุคคลที่ไม่ผ่านการอนุมัติ หรือสื่อบันทึกข้อมูลที่ไม่ทราบแหล่งที่มาเชื่อมต่อกับระบบหรืออุปกรณ์ขององค์การ

๕) สำนักเทคโนโลยีดิจิทัลอาจจำกัดหรือปิดการใช้งานพอร์ตเชื่อมต่อและสื่อบันทึกข้อมูลในอุปกรณ์ที่มีความเสี่ยงสูงตามความเหมาะสม

๓.๘ การปฏิบัติงานจากระยะไกลและการใช้อุปกรณ์ส่วนบุคคล

๑) การปฏิบัติงานจากระยะไกลต้องใช้อุปกรณ์และช่องทางเชื่อมต่อที่องค์การอนุมัติ เช่น ระบบ VPN หรือระบบการเข้าถึงจากระยะไกลที่มีการเข้ารหัส

๒) ผู้ใช้งานต้องหลีกเลี่ยงการใช้งานเครือข่ายสาธารณะที่ไม่ปลอดภัย หากมีความจำเป็นต้องใช้งาน ต้องเชื่อมต่อผ่านช่องทางที่องค์การกำหนดและใช้มาตรการป้องกันที่เหมาะสม

๓) การใช้อุปกรณ์ส่วนบุคคลเพื่อปฏิบัติงานหรือเข้าถึงข้อมูลขององค์การ ต้องได้รับอนุญาตจากผู้มีอำนาจ และต้องปฏิบัติตามมาตรฐานความมั่นคงปลอดภัยที่องค์การกำหนด

๔) อุปกรณ์ส่วนบุคคลที่ได้รับอนุญาตต้องติดตั้งโปรแกรมป้องกันมัลแวร์ มีการกำหนดรหัสผ่าน ล็อกหน้าจอ ปรับปรุงระบบให้เป็นปัจจุบัน และต้องไม่ถูกดัดแปลงระบบในลักษณะที่ลดทอนความมั่นคงปลอดภัย

๓.๙ การแจ้งเหตุ สูญหาย และการจัดการอุปกรณ์ผิดปกติ

๑) ผู้ใช้งานที่พบว่าอุปกรณ์สูญหาย ถูกโจรกรรม ถูกทำลาย มีการทำงานผิดปกติ หรือต้องสงสัยว่าติดโปรแกรมไม่ประสงค์ดี ต้องแจ้งสำนักเทคโนโลยีดิจิทัลและผู้บังคับบัญชาโดยเร็ว

๒) เมื่อพบเหตุการณ์ที่อาจกระทบต่อข้อมูลหรือระบบขององค์การ สำนักเทคโนโลยีดิจิทัลต้องประเมินผลกระทบ จำกัดความเสียหาย รวบรวมหลักฐาน และดำเนินการกู้คืนตามกระบวนการจัดการเหตุการณ์

๓) กรณีอุปกรณ์สูญหายหรือถูกโจรกรรม ให้ดำเนินการยกเลิกสิทธิ์ เปลี่ยนรหัสผ่าน ระงับบัญชีผู้ใช้งาน หรือลบข้อมูลจากระยะไกลตามความเหมาะสม

๔) ให้บันทึกรายละเอียดเหตุการณ์ สาเหตุ มาตรการแก้ไข และบทเรียนที่ได้รับ เพื่อป้องกันการเกิดเหตุซ้ำ

๓.๑๐ การซ่อมบำรุง โอนย้าย และการทำลายอุปกรณ์

๑) การซ่อมบำรุงอุปกรณ์ที่มีข้อมูลสำคัญ ต้องดำเนินการโดยผู้ได้รับอนุญาต และอยู่ภายใต้การควบคุม

ของหน่วยงานที่รับผิดชอบ

๒) ก่อนส่งอุปกรณ์ไปซ่อม ส่งมอบให้บุคคลภายนอก โอนย้าย หรือจำหน่าย ต้องสำรอง ลบ หรือทำลายข้อมูลในอุปกรณ์อย่างเหมาะสมตามประเภทและชั้นความลับของข้อมูล

๓) การจำหน่ายหรือทำลายอุปกรณ์และสื่อบันทึกข้อมูล ต้องดำเนินการด้วยวิธีที่ทำให้ข้อมูลไม่สามารถกู้คืนได้ และต้องจัดเก็บหลักฐานการดำเนินการไว้เพื่อการตรวจสอบ

๔) ให้ยกเลิกบัญชีผู้ใช้งาน ใบรับรองดิจิทัล การเชื่อมต่อเครือข่าย และสิทธิ์ที่เกี่ยวข้องก่อนนำอุปกรณ์ออกจากการใช้งาน

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้ผู้ใช้งานอุปกรณ์ปฏิบัติตามอย่างเคร่งครัด

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำคู่มือหรือสื่อประชาสัมพันธ์ที่เข้าใจง่าย เช่น แนวทางการล็อกหน้าจอ การใช้เครื่องคอมพิวเตอร์พกพาอย่างปลอดภัย การใช้ USB การทำงานจากระยะไกล และวิธีแจ้งเหตุอุปกรณ์สูญหาย

๔.๔ ให้จัดอบรมหรือกิจกรรมสร้างความตระหนักด้านการรักษาความปลอดภัยของอุปกรณ์แก่บุคลากรอย่างน้อยปีละ ๑ ครั้ง และเมื่อมีการเปลี่ยนแปลงเทคโนโลยีหรือแนวทางปฏิบัติที่สำคัญ

๔.๕ ให้ผู้รับมอบอุปกรณ์ ผู้รับจ้าง และผู้ให้บริการภายนอกที่ได้รับอนุญาตให้ใช้อุปกรณ์หรือเข้าถึงระบบขององค์การ ลงนามรับทราบและยอมรับเงื่อนไขการใช้งานอุปกรณ์อย่างปลอดภัย

๔.๖ ให้แจ้งเตือนช่องโหว่ ภัยคุกคาม เหตุการณ์อุปกรณ์สูญหาย หรือแนวทางป้องกันใหม่แก่ผู้ใช้งานและผู้เกี่ยวข้องโดยเร็ว

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
ทะเบียนอุปกรณ์	ร้อยละของอุปกรณ์ที่มีข้อมูลทะเบียน ผู้รับผิดชอบ และสถานะการใช้งานครบถ้วน	ร้อยละ ๑๐๐
การกำหนดค่ามาตรฐาน	ร้อยละของอุปกรณ์ที่ผ่านการตรวจสอบการกำหนดค่าความมั่นคงปลอดภัยตามมาตรฐาน	ไม่น้อยกว่าร้อยละ ๙๕
โปรแกรมป้องกันมัลแวร์	ร้อยละของอุปกรณ์ที่ติดตั้ง เปิดใช้งาน และปรับปรุงโปรแกรมป้องกันมัลแวร์ให้เป็นปัจจุบัน	ไม่น้อยกว่าร้อยละ ๙๕
การปรับปรุงแพตช์	ร้อยละของอุปกรณ์ที่ได้รับการปรับปรุงแพตช์ตามระยะเวลาที่กำหนด	ไม่น้อยกว่าร้อยละ ๙๕
การเข้ารหัสอุปกรณ์พกพา	ร้อยละของเครื่องคอมพิวเตอร์พกพาและอุปกรณ์เคลื่อนที่ที่จัดเก็บข้อมูลสำคัญและได้รับการเข้ารหัส	ร้อยละ ๑๐๐
การควบคุมสิทธิ์	ร้อยละของบัญชีผู้ใช้งานและสิทธิ์ผู้ดูแลระบบที่ได้รับการทบทวนตามรอบระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
การแจ้งเหตุอุปกรณ์สูญหาย	ระยะเวลาเฉลี่ยตั้งแต่ได้รับแจ้งเหตุจนถึงการระงับสิทธิ์หรือดำเนินมาตรการควบคุม	เป็นไปตามเกณฑ์เวลาที่องค์การกำหนด
การรับคืนอุปกรณ์	ร้อยละของบุคลากรที่พ้นสภาพหรือเปลี่ยนหน้าที่และส่งคืนอุปกรณ์ พร้อมยกเลิกสิทธิ์ครบถ้วน	ร้อยละ ๑๐๐

การทำลายข้อมูล	ร้อยละของอุปกรณ์หรือสื่อบันทึกข้อมูลที่จำหน่ายหรือเลิกใช้และมีหลักฐานการลบหรือทำลายข้อมูลครบถ้วน	ร้อยละ ๑๐๐
การสร้างความตระหนัก	ร้อยละของบุคลากรกลุ่มเป้าหมายที่ผ่านการอบรมหรือรับทราบแนวปฏิบัติด้าน Endpoint Security	ไม่น้อยกว่าร้อยละ ๙๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบหรือประเมินความเสี่ยงที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง โดยตัวชี้วัดด้านสถานะอุปกรณ์ การปรับปรุงแพตช์ และโปรแกรมป้องกันมัลแวร์ ควรติดตามเป็นรายเดือนหรือรายไตรมาส

๕.๒ ให้นำผลการตรวจสอบ เหตุการณ์อุปกรณ์สูญหาย เหตุการณ์มัลแวร์ และข้อร้องเรียนของผู้ใช้งานมาวิเคราะห์เพื่อกำหนดมาตรการแก้ไขและพัฒนาการควบคุมอุปกรณ์อย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านเทคโนโลยี รูปแบบการปฏิบัติงาน ภัยคุกคาม หรือข้อกำหนดที่เกี่ยวข้องอย่างมีนัยสำคัญ

ส่วนที่ ๑๕
นโยบายและแนวปฏิบัติการบริหารจัดการการเข้ารหัสข้อมูลสารสนเทศและการบริหารจัดการกุญแจ
(Cryptography and Key Management)

๑. วัตถุประสงค์

๑.๑ เพื่อกำหนดหลักเกณฑ์และแนวปฏิบัติในการใช้การเข้ารหัสข้อมูลสารสนเทศ เพื่อคุ้มครองความลับ ความถูกต้องครบถ้วน และความพร้อมใช้งานของข้อมูลสารสนเทศขององค์การคลังสินค้า

๑.๒ เพื่อป้องกันการเข้าถึง การเปิดเผย การดักรับ การแก้ไขเปลี่ยนแปลง การทำสำเนา หรือการใช้ข้อมูลสำคัญโดยมิได้รับอนุญาต ทั้งในระหว่างการจัดเก็บ การประมวลผล การสำรอง และการรับส่งข้อมูล

๑.๓ เพื่อกำหนดการบริหารจัดการกุญแจเข้ารหัสและใบรับรองดิจิทัลให้มีความมั่นคงปลอดภัย ครอบคลุมการสร้าง การอนุมัติ การจัดเก็บ การแจกจ่าย การใช้งาน การสำรอง การเปลี่ยน การเพิกถอน และการทำลายกุญแจ

๑.๔ เพื่อกำหนดบทบาท หน้าที่ และความรับผิดชอบของผู้ที่เกี่ยวข้องกับการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจอย่างชัดเจน

๑.๕ เพื่อสนับสนุนหลักเกณฑ์การประเมินการพัฒนาเทคโนโลยีดิจิทัล โดยให้มีกระบวนการ มาตรการควบคุม หลักฐานการดำเนินงาน การวัดประสิทธิผล และการปรับปรุงอย่างต่อเนื่อง

๒. ขอบเขต

๒.๑ นโยบายและแนวปฏิบัตินี้ใช้บังคับกับข้อมูลสารสนเทศ ระบบสารสนเทศ ฐานข้อมูล ระบบเครือข่าย เว็บไซต์ ระบบคลาวด์ ระบบสำรองข้อมูล สื่อบันทึกข้อมูล และอุปกรณ์ที่อยู่ภายใต้ความรับผิดชอบขององค์การคลังสินค้า

๒.๒ ครอบคลุมข้อมูลทุกประเภทที่มีความสำคัญหรือมีความอ่อนไหว เช่น ข้อมูลลับ ข้อมูลลับมาก ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลการจัดเก็บสินค้า ข้อมูลคู่ค้า ข้อมูลบุคลากร และข้อมูลที่มีผลกระทบต่อภารกิจขององค์การ

๒.๓ ครอบคลุมการเข้ารหัสข้อมูลขณะจัดเก็บข้อมูล (Data at Rest) ขณะรับส่งข้อมูล (Data in Transit) และตามความเหมาะสมในระหว่างการประมวลผลข้อมูล

๒.๔ ครอบคลุมกุญแจเข้ารหัส รหัสผ่านที่ใช้ป้องกันไฟล์ ใบรับรองดิจิทัล กุญแจสำหรับระบบ VPN กุญแจสำหรับฐานข้อมูล กุญแจสำหรับการสำรองข้อมูล และข้อมูลลับอื่นที่ใช้ยืนยันความถูกต้องหรือป้องกันการเข้าถึงข้อมูล

๒.๕ ใช้บังคับกับคณะกรรมการ ผู้บริหาร พนักงาน ลูกจ้าง ผู้ปฏิบัติงาน ผู้ดูแลระบบ ผู้พัฒนาระบบ เจ้าของข้อมูล ผู้ให้บริการภายนอก ผู้รับจ้าง และบุคคลอื่นที่ได้รับอนุญาตให้เข้าถึงหรือบริหารจัดการข้อมูลและระบบสารสนเทศขององค์การ

๓. แนวปฏิบัติ

๓.๑ การกำหนดบทบาท หน้าที่ และความรับผิดชอบ

๑) ให้องค์การกำหนดผู้รับผิดชอบด้านการเข้ารหัสข้อมูลและการบริหารจัดการกุญแจอย่างชัดเจน โดยอย่างน้อยประกอบด้วย

- **เจ้าของข้อมูล (Data Owner):** กำหนดชั้นความลับ ระดับความสำคัญ และความจำเป็นในการเข้ารหัสข้อมูล
- เจ้าของระบบ (System Owner): กำหนดความต้องการด้านการเข้ารหัสและการจัดการกุญแจของระบบ
- ผู้ดูแลกุญแจ (Key Custodian): รับผิดชอบการเก็บรักษา ควบคุมการเข้าถึง และดูแลความ

ปลอดภัยของกุญแจ

- ผู้บริหารจัดการกุญแจ (Key Administrator): รับผิดชอบการสร้าง แจกจ่าย เปลี่ยน เพิกถอน สำรอง และทำลายกุญแจตามขั้นตอนที่กำหนด
- ผู้ใช้งานกุญแจ (Authorized User): ใช้งานกุญแจภายในขอบเขตหน้าที่และสิทธิ์ที่ได้รับอนุญาต
- ผู้รับผิดชอบ**การกู้คืนกุญแจ:** ดำเนินการกู้คืนหรือเปลี่ยนกุญแจกรณีสูญหาย เสียหาย รั่วไหล หรือไม่สามารถใช้งานได้

๒) ให้มีการแบ่งแยกหน้าที่ระหว่างผู้สร้างกุญแจ ผู้อนุมัติ ผู้ดูแลกุญแจ และผู้ใช้งานกุญแจตามความเหมาะสม เพื่อป้องกันความขัดแย้งของหน้าที่และลดความเสี่ยงจากการใช้งานโดยมิชอบ

๓) การเข้าถึงกุญแจเข้ารหัส กุญแจหลัก หรือข้อมูลลับที่เกี่ยวข้องกับการเข้ารหัส ต้องได้รับอนุมัติจากผู้มีอำนาจ และต้องมีการบันทึกการเข้าถึงเพื่อให้ตรวจสอบย้อนหลังได้

๓.๒ การจำแนกข้อมูลและการพิจารณาใช้การเข้ารหัส

๑) เจ้าของข้อมูลต้องจำแนกชั้นความลับและประเมินความเสี่ยงของข้อมูลก่อนกำหนดมาตรการเข้ารหัส โดยพิจารณาจากผลกระทบหากข้อมูลถูกเปิดเผย สูญหาย ถูกแก้ไข หรือไม่สามารถใช้งานได้

๒) ข้อมูลลับ ข้อมูลลับมาก ข้อมูลส่วนบุคคล ข้อมูลทางการเงิน ข้อมูลเกี่ยวกับการดำเนินงานที่สำคัญ และข้อมูลที่กฎหมายหรือระเบียบกำหนดให้คุ้มครอง ต้องใช้การเข้ารหัสตามความเหมาะสม

๓) การเลือกวิธีการเข้ารหัสต้องพิจารณาจากระดับความเสี่ยง ประเภทข้อมูล ปริมาณข้อมูล ลักษณะการใช้งาน ข้อกำหนดของระบบ และความสามารถในการกู้คืนข้อมูล

๔) ให้จัดทำบัญชีรายการระบบ ชุดข้อมูล หรือสื่อบันทึกข้อมูลสำคัญที่ต้องใช้การเข้ารหัส พร้อมระบุผู้รับผิดชอบ วิธีการเข้ารหัส และรอบการทบทวนมาตรการ

๓.๓ มาตรฐานและวิธีการเข้ารหัสข้อมูล

๑) การเข้ารหัสข้อมูลต้องใช้มาตรฐาน อัลกอริทึม และขนาดกุญแจที่เป็นที่ยอมรับ มีความมั่นคงปลอดภัย และได้รับอนุมัติจากสำนักเทคโนโลยีดิจิทัล

๒) ห้ามใช้อัลกอริทึม วิธีการเข้ารหัส หรือโปรโตคอลที่ล้าสมัย มีช่องโหว่ หรือไม่เหมาะสมกับการคุ้มครองข้อมูลสำคัญ เว้นแต่ได้รับการประเมินความเสี่ยงและกำหนดมาตรการควบคุมทดแทนเป็นลายลักษณ์อักษร

๓) การจัดเก็บรหัสผ่านในฐานข้อมูล ต้องไม่จัดเก็บในรูปแบบที่อ่านได้โดยตรง และต้องใช้วิธีการแฮชรหัสผ่านที่มีความมั่นคงปลอดภัย พร้อมค่า Salt และมาตรการป้องกันที่เหมาะสม

๔) สำหรับระบบที่พัฒนาหรือปรับปรุงใหม่ ห้ามใช้ MD๕ หรือวิธีการแฮชที่ไม่ปลอดภัยสำหรับการจัดเก็บรหัสผ่านหรือการคุ้มครองข้อมูลสำคัญ

๕) รหัสผ่าน กุญแจเข้ารหัส โทเคน ใบรับรองดิจิทัล หรือข้อมูลลับอื่น ห้ามบันทึกไว้ในรหัสต้นฉบับ ไฟล์ข้อความทั่วไป อีเมล เอกสารที่เปิดเผย หรือพื้นที่จัดเก็บที่ไม่มีการควบคุมสิทธิ์

๓.๔ การเข้ารหัสข้อมูลขณะรับส่งข้อมูล

๑) การรับส่งข้อมูลสำคัญผ่านเครือข่ายภายใน เครือข่ายระหว่างหน่วยงาน หรือเครือข่ายอินเทอร์เน็ต ต้องใช้ช่องทางที่มีการเข้ารหัสอย่างเหมาะสม

๒) เว็บไซต์และระบบเว็บแอปพลิเคชันขององค์การที่มีการเข้าสู่ระบบ รับส่งข้อมูล หรือทำธุรกรรม ต้องใช้ HTTPS และใบรับรองดิจิทัลที่ถูกต้อง เชื่อถือได้ และไม่หมดอายุ

๓) การเชื่อมต่อจากระยะไกลเข้าสู่ระบบหรือเครือข่ายขององค์การ ต้องใช้ระบบ VPN หรือช่องทางที่มีการเข้ารหัสและการพิสูจน์ตัวตนตามมาตรฐานที่องค์การกำหนด

๔) การแลกเปลี่ยนข้อมูลสำคัญกับหน่วยงานภายนอกหรือผู้ให้บริการภายนอก ต้องกำหนดวิธีการเข้ารหัส ช่องทางรับส่ง ผู้รับผิดชอบ และมาตรการยืนยันตัวตนของคู่สัญญาอย่างชัดเจน

๕) ห้ามรับส่งข้อมูลลับหรือข้อมูลลับมากผ่านอีเมลส่วนบุคคล โปรแกรมสนทนาส่วนบุคคล หรือช่องทางที่ไม่ได้รับอนุมัติจากองค์การ

๓.๕ การเข้ารหัสข้อมูลขณะจัดเก็บข้อมูล

๑) ข้อมูลสำคัญที่จัดเก็บในฐานข้อมูล ระบบจัดเก็บไฟล์ ระบบคลาวด์ เครื่องคอมพิวเตอร์พกพา อุปกรณ์เคลื่อนที่ สื่อบันทึกข้อมูลแบบพกพา และระบบสำรองข้อมูล ต้องได้รับการเข้ารหัสตามระดับความเสี่ยง

๒) เครื่องคอมพิวเตอร์พกพา อุปกรณ์เคลื่อนที่ หรือสื่อบันทึกข้อมูลที่มีข้อมูลลับ ข้อมูลส่วนบุคคล หรือข้อมูลสำคัญขององค์การ ต้องใช้การเข้ารหัสข้อมูลทั้งอุปกรณ์หรือเข้ารหัสแฟ้มข้อมูลตามความเหมาะสม

๓) การจัดเก็บข้อมูลบนระบบคลาวด์ ต้องกำหนดมาตรการเข้ารหัส การควบคุมสิทธิ์ และความรับผิดชอบระหว่างองค์การกับผู้ให้บริการให้ชัดเจน

๔) ไฟล์เอกสารที่มีชั้นความลับต้องแสดงชั้นความลับตามแนวปฏิบัติขององค์การ และต้องมีการป้องกันด้วยรหัสผ่านหรือการเข้ารหัสตามระดับความสำคัญของข้อมูล

๕) ห้ามจัดเก็บกุญแจเข้ารหัสไว้ในตำแหน่งเดียวกับข้อมูลที่เข้ารหัส เว้นแต่ระบบมีมาตรการป้องกันและการบริหารจัดการกุญแจที่ได้รับอนุมัติ

๓.๖ การสร้างและการแจกจ่ายกุญแจเข้ารหัส

๑) การสร้างกุญแจเข้ารหัสต้องดำเนินการด้วยวิธีการหรือระบบที่เชื่อถือได้ และให้มีความยาวหรือคุณลักษณะตามมาตรฐานที่องค์การกำหนด

๒) กุญแจเข้ารหัสต้องมีการระบุรหัสกุญแจ วัตถุประสงค์ ระบบหรือข้อมูลที่เกี่ยวข้อง เจ้าของกุญแจ วันที่สร้าง วันเริ่มใช้งาน วันหมดอายุ และผู้รับผิดชอบอย่างชัดเจน

๓) การแจกจ่ายหรือส่งมอบกุญแจเข้ารหัสต้องดำเนินการผ่านช่องทางที่ปลอดภัย และจำกัดเฉพาะผู้ที่ได้รับอนุญาต

๔) ห้ามส่งกุญแจเข้ารหัส รหัสผ่าน หรือข้อมูลยืนยันตัวตนผ่านช่องทางเดียวกับข้อมูลที่เข้ารหัส เว้นแต่มีมาตรการป้องกันที่เหมาะสม

๕) กรณีต้องส่งมอบรหัสผ่านเพื่อเข้าถึงไฟล์หรือข้อมูลสำคัญ ให้ส่งมอบผ่านช่องทางที่แยกจากการส่งไฟล์ หรือใช้วิธีการที่สามารถยืนยันตัวตนของผู้รับได้

๓.๗ การจัดเก็บและการควบคุมกุญแจเข้ารหัส

๑) กุญแจเข้ารหัสต้องจัดเก็บในระบบหรือพื้นที่ที่มีมาตรการควบคุมการเข้าถึงตามระดับความสำคัญของกุญแจ

๒) กุญแจหลัก กุญแจสำหรับระบบสำคัญ หรือกุญแจที่ใช้ป้องกันข้อมูลลับมาก ต้องได้รับการป้องกันเป็นพิเศษ เช่น การจัดเก็บในระบบบริหารจัดการกุญแจ หรืออุปกรณ์ที่มีความมั่นคงปลอดภัยตามความเหมาะสม

๓) ให้กำหนดสิทธิ์เข้าถึงกุญแจตามหลักความจำเป็นในการปฏิบัติงาน และทบทวนสิทธิ์ดังกล่าวอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงหน้าที่ของผู้เกี่ยวข้อง

๔) ห้ามทำสำเนากุญแจเข้ารหัสโดยไม่ได้รับอนุญาต ห้ามเปิดเผยกุญแจแก่ผู้ไม่มีสิทธิ์ และห้ามใช้กุญแจเพื่อวัตถุประสงค์นอกเหนือจากที่กำหนด

๕) ต้องมีการบันทึกเหตุการณ์เกี่ยวกับการเข้าถึง การใช้งาน การเปลี่ยนแปลง การส่งมอบ และการทำลายกุญแจ เพื่อให้สามารถตรวจสอบย้อนหลังได้

๓.๘ การสำรอง การกู้คืน และการเปลี่ยนกุญแจ

๑) ต้องมีการสำรองกุญแจเข้ารหัสที่มีความสำคัญ เพื่อรองรับกรณีระบบขัดข้อง กุญแจสูญหาย ผู้รับผิดชอบไม่สามารถปฏิบัติหน้าที่ หรือเกิดเหตุฉุกเฉิน

๒) กุญแจสำรองต้องได้รับการเข้ารหัสหรือป้องกันด้วยมาตรการที่เหมาะสม จัดเก็บแยกจากกุญแจที่ใช้

งาน และจำกัดสิทธิ์เข้าถึงเฉพาะผู้ได้รับมอบหมาย

๓) ต้องกำหนดขั้นตอนการกู้คืนกุญแจและข้อมูลที่เข้ารหัส โดยระบุผู้มีอำนาจอนุมัติ ผู้ดำเนินการ และหลักฐานการดำเนินงาน

๔) ให้เปลี่ยนกุญแจเข้ารหัสตามอายุการใช้งาน ระดับความเสี่ยง ประเภทกุญแจ หรือเมื่อมีเหตุอันควรสงสัยว่ากุญแจถูกเปิดเผย สูญหาย ถูกโจรกรรม หรือถูกใช้งานโดยมิชอบ

๕) ใบรับรองดิจิทัลต้องได้รับการติดตามวันหมดอายุและต่ออายุล่วงหน้าตามระยะเวลาที่เหมาะสม เพื่อป้องกันผลกระทบต่อการให้บริการของระบบ

๓.๙ การเพิกถอนและการทำลายกุญแจ

๑) ให้เพิกถอน ระงับ หรือยกเลิกการใช้งานกุญแจเข้ารหัสโดยทันที เมื่อกุญแจหมดอายุ สูญหาย ถูกเปิดเผย ถูกโจรกรรม หรือไม่มีความจำเป็นต้องใช้งาน

๒) เมื่อสิ้นสุดอายุการใช้งานของกุญแจ ต้องดำเนินการทำลายกุญแจด้วยวิธีที่ไม่สามารถนำกลับมาใช้ได้ เว้นแต่มีความจำเป็นต้องเก็บรักษาตามกฎหมายหรือเพื่อการกู้คืนข้อมูลที่ได้รับอนุมัติ

๓) การทำลายกุญแจต้องมีการบันทึกรายละเอียดอย่างน้อย ได้แก่ รหัสกุญแจ วัตถุประสงค์ ผู้อนุมัติ ผู้ดำเนินการ วันที่ทำลาย และวิธีการทำลาย

๔) กรณีผู้ให้บริการภายนอกสิ้นสุดสัญญา หรือบุคลากรพ้นสภาพหรือเปลี่ยนหน้าที่ ต้องทบทวนและยกเลิกสิทธิ์เข้าถึงกุญแจ บัญชีผู้ใช้งาน ใบรับรองดิจิทัล และข้อมูลลับที่เกี่ยวข้องทันที

๓.๑๐ การจัดการเหตุการณ์เกี่ยวกับกุญแจและการเข้ารหัส

๑) ผู้พบเหตุหรือสงสัยว่ากุญแจ รหัสผ่าน ใบรับรองดิจิทัล หรือข้อมูลลับที่เกี่ยวข้องกับการเข้ารหัสสูญหาย รั่วไหล ถูกเปิดเผย หรือถูกใช้งานโดยมิชอบ ต้องแจ้งสำนักเทคโนโลยีดิจิทัลและผู้รับผิดชอบโดยทันที

๒) หน่วยงานที่รับผิดชอบต้องดำเนินการประเมินผลกระทบ ระงับหรือเพิกถอนกุญแจ เปลี่ยนกุญแจ จำกัดความเสียหาย ตรวจสอบการเข้าถึง และกู้คืนข้อมูลหรือระบบตามความเหมาะสม

๓) เหตุการณ์ที่เกี่ยวข้องกับข้อมูลลับ ข้อมูลส่วนบุคคล หรือระบบสำคัญ ต้องได้รับการรายงานและดำเนินการตามขั้นตอนการจัดการเหตุการณ์ขององค์การและข้อกำหนดทางกฎหมายที่เกี่ยวข้อง

๔) ภายหลังเหตุการณ์ ต้องวิเคราะห์หาสาเหตุ จัดทำรายงานบทเรียน และทบทวนมาตรการบริหารจัดการกุญแจเพื่อป้องกันไม่ให้เกิดเหตุซ้ำ

๓.๑๑ การทบทวนและการตรวจสอบ

๑) ให้สำนักเทคโนโลยีดิจิทัลร่วมกับเจ้าของระบบและเจ้าของข้อมูลทบทวนมาตรการเข้ารหัสและการบริหารจัดการกุญแจอย่างน้อยปีละ ๑ ครั้ง

๒) ให้มีการตรวจสอบรายการกุญแจ วันหมดอายุ สิทธิ์การเข้าถึง สถานะการสำรองกุญแจ และบันทึกเหตุการณ์การใช้งานกุญแจตามรอบระยะเวลาที่กำหนด

๓) ให้ประเมินความเสี่ยงเพิ่มเติมเมื่อมีการเปลี่ยนแปลงระบบ การเชื่อมโยงข้อมูล การใช้บริการคลาวด์ การเปลี่ยนผู้ให้บริการ หรือเมื่อพบภัยคุกคามและช่องโหว่ใหม่

๔) ให้นำผลการตรวจสอบ เหตุการณ์ ข้อค้นพบ และผลการวัดประสิทธิผลมาใช้ปรับปรุงแนวปฏิบัติ มาตรฐาน และแผนบริหารจัดการกุญแจอย่างต่อเนื่อง

๔. แนวทางการสื่อสารนโยบาย

๔.๑ ให้องค์การคลังสินค้าเผยแพร่นโยบายและแนวปฏิบัตินี้ผ่านระบบสารบรรณอิเล็กทรอนิกส์ ระบบอินทราเน็ต อีเมล หรือช่องทางสื่อสารภายในที่เหมาะสม

๔.๒ ให้ผู้บริหารและผู้บังคับบัญชาทุกระดับสื่อสารนโยบายแก่บุคลากรในสังกัด และกำกับดูแลให้มีการปฏิบัติตามอย่างเคร่งครัด

๔.๓ ให้สำนักเทคโนโลยีดิจิทัลจัดทำคู่มือหรือแนวทางปฏิบัติสำหรับผู้ใช้งาน ผู้ดูแลระบบ และผู้พัฒนาระบบ เช่น แนวทางการส่งไฟล์ลับอย่างปลอดภัย การใช้ VPN การตั้งรหัสผ่านไฟล์ การเข้ารหัสอุปกรณ์พกพา และการแจ้งเหตุกุญแจสูญหาย

๔.๔ ให้จัดอบรมหรือถ่ายทอดความรู้แก่ผู้ดูแลระบบ ผู้พัฒนาระบบ เจ้าของข้อมูล และบุคลากรที่เกี่ยวข้อง อย่างน้อยปีละ ๑ ครั้ง ในเรื่องการเข้ารหัส การจัดการกุญแจ การจัดเก็บรหัสผ่าน และการคุ้มครองข้อมูลสำคัญ

๔.๕ ให้ผู้ให้บริการภายนอก ผู้รับจ้าง และผู้พัฒนาระบบที่เกี่ยวข้องกับข้อมูลหรือกุญแจเข้ารหัสรับทราบและปฏิบัติตามข้อกำหนดด้านการเข้ารหัสและการรักษาความลับก่อนเริ่มปฏิบัติงาน

๔.๖ ให้สื่อสารแจ้งเตือนเกี่ยวกับช่องโหว่ด้านการเข้ารหัส การหมดอายุของใบรับรองดิจิทัล เหตุการณ์กุญแจรั่วไหล หรือการเปลี่ยนแปลงมาตรฐานที่สำคัญแก่ผู้เกี่ยวข้องโดยเร็ว

๕. วิธีการวัดประสิทธิผล

ประเด็นวัดผล	ตัวชี้วัด/วิธีการวัด	ค่าเป้าหมาย
การระบุข้อมูลที่ต้องเข้ารหัส	ร้อยละของระบบหรือชุดข้อมูลสำคัญที่ได้รับการจำแนกและกำหนดมาตรการเข้ารหัสตามผลการประเมินความเสี่ยง	ร้อยละ ๑๐๐
การเข้ารหัสข้อมูลขณะรับส่ง	ร้อยละของระบบเว็บและระบบรับส่งข้อมูลสำคัญที่ใช้ช่องทางเข้ารหัสตามมาตรฐานที่กำหนด	ร้อยละ ๑๐๐
การเข้ารหัสข้อมูลขณะจัดเก็บ	ร้อยละของอุปกรณ์พกพา สื่อบันทึกข้อมูล และระบบสำรองข้อมูลที่จัดเก็บข้อมูลสำคัญและได้รับการเข้ารหัส	ร้อยละ ๑๐๐
การบริหารกุญแจ	ร้อยละของกุญแจเข้ารหัสที่มีข้อมูลทะเบียน ระบุเจ้าของ วัตถุประสงค์ วันหมดอายุ และผู้รับผิดชอบครบถ้วน	ร้อยละ ๑๐๐
การทบทวนสิทธิ์กุญแจ	ร้อยละของสิทธิ์เข้าถึงกุญแจเข้ารหัสที่ได้รับการทบทวนตามรอบระยะเวลาที่กำหนด	ร้อยละ ๑๐๐
การเปลี่ยนและต่ออายุกุญแจ	ร้อยละของกุญแจและใบรับรองดิจิทัลที่ได้รับการเปลี่ยนหรือต่ออายุก่อนหมดอายุ	ร้อยละ ๑๐๐
การสำรองและกู้คืนกุญแจ	ร้อยละของกุญแจสำคัญที่มีการสำรอง และผลการทดสอบกู้คืนกุญแจหรือข้อมูลสำเร็จตามแผน	ร้อยละ ๑๐๐ ตามแผน
การจัดการเหตุการณ์	จำนวนเหตุการณ์กุญแจสูญหาย รั่วไหล หรือถูกใช้งานโดยมิชอบ และระยะเวลาในการเพิกถอนหรือควบคุมเหตุ	ลดลงอย่างต่อเนื่อง และดำเนินการตามเกณฑ์เวลาที่กำหนด
การปฏิบัติตามมาตรฐาน	ร้อยละของระบบใหม่หรือระบบที่ปรับปรุง ซึ่งผ่านการตรวจสอบว่าไม่ใช้วิธีเข้ารหัสหรือวิธีแฮชที่ล้าสมัยสำหรับข้อมูลสำคัญ	ร้อยละ ๑๐๐
การสร้างความตระหนัก	ร้อยละของบุคลากรกลุ่มเป้าหมายที่ผ่านการอบรมหรือรับทราบแนวปฏิบัติด้านการเข้ารหัสและการจัดการกุญแจ	ไม่น้อยกว่าร้อยละ ๙๐
การแก้ไขข้อค้นพบ	ร้อยละของข้อค้นพบจากการตรวจสอบ การประเมินความเสี่ยง หรือเหตุการณ์ ที่ได้รับการแก้ไขภายในกำหนด	ไม่น้อยกว่าร้อยละ ๙๐

๕.๑ ให้สำนักเทคโนโลยีดิจิทัลรวบรวม วิเคราะห์ และรายงานผลการวัดประสิทธิผลต่อผู้บริหารหรือคณะกรรมการที่เกี่ยวข้องอย่างน้อยปีละ ๑ ครั้ง โดยตัวชี้วัดเกี่ยวกับใบรับรองดิจิทัล กุญแจที่ใกล้หมดอายุ และเหตุการณ์ด้านกุญแจ ควรติดตามเป็นรายเดือนหรือรายไตรมาส

๕.๒ ให้มีการวิเคราะห์แนวโน้มของผลการตรวจสอบ เหตุการณ์ ข้อบกพร่อง และผลการวัด เพื่อกำหนดแผนปรับปรุงมาตรการเข้ารหัส การควบคุมกุญแจ และการสร้างความตระหนักแก่ผู้เกี่ยวข้องอย่างต่อเนื่อง

๕.๓ ให้ทบทวนนโยบายและแนวปฏิบัตินี้อย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงด้านกฎหมาย มาตรฐาน เทคโนโลยี รูปแบบการให้บริการ ระบบสารสนเทศ หรือภัยคุกคามที่มีนัยสำคัญ