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

ประกาศองค์การคลังสินค้า
ที่ ๕๖ / ๒๕๖๙
เรื่อง นโยบายการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์การคลังสินค้า

.....

องค์การคลังสินค้า ตระหนักถึงความสำคัญของการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ข้อมูลและระบบสารสนเทศเป็นสินทรัพย์ที่มีค่าและมีความสำคัญอย่างยิ่งต่อการให้บริการ การตัดสินใจ และการดำเนินธุรกิจอย่างต่อเนื่อง การบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศที่มีประสิทธิภาพจึงเป็นสิ่งจำเป็น เพื่อปกป้องข้อมูลและระบบสารสนเทศจากภัยคุกคามต่าง ๆ ลดผลกระทบที่อาจเกิดขึ้น และสร้างความเชื่อมั่นให้กับผู้มีส่วนได้ส่วนเสียทุกกลุ่ม และเพื่อใช้เป็นกรอบแนวทางการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กร ให้สอดคล้องกับกฎหมาย ระเบียบ ข้อบังคับ มาตรฐานสากล และบริบทขององค์กร โดยครอบคลุมถึงกระบวนการ ระเบียบ วิธีปฏิบัติ โครงสร้างองค์กร บทบาทหน้าที่ และการสื่อสาร จึงกำหนดนโยบาย ดังนี้

๑. กำหนดกระบวนการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๒. กำหนดปัจจัยภายในและภายนอกที่สอดคล้องกับวัตถุประสงค์และบริบทขององค์กร

๓. กำหนดโครงสร้างองค์กรและบทบาทหน้าที่ของผู้เกี่ยวข้องในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๔. กำหนดหลักเกณฑ์ ระเบียบ วิธีปฏิบัติในการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๕. สื่อสารนโยบายหรือแผนความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศขององค์กรให้ผู้เกี่ยวข้องทราบและเข้าใจ

๖. กำหนดแนวทางหรือวิธีการวัดประสิทธิผลของการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ

๗. กำหนดแนวทางการบริหารความต่อเนื่องทางธุรกิจในมิติของความมั่นคงปลอดภัยไซเบอร์ (Cyber Business Continuity Management: Cyber BCM) ที่อาจส่งผลให้ระบบสารสนเทศหรือบริการสำคัญหยุดชะงัก เพื่อให้สามารถดำเนินภารกิจหลักและการให้บริการได้อย่างต่อเนื่องภายในระยะเวลาที่ยอมรับได้ ครอบคลุมประเด็นสำคัญ ดังนี้

๗.๑ ให้มีการวิเคราะห์ผลกระทบทางธุรกิจจากเหตุการณ์ไซเบอร์ (Cyber Business Impact Analysis: Cyber BIA) ให้มีการวิเคราะห์และระบุระบบสารสนเทศ กระบวนการทางธุรกิจ และบริการที่มีความสำคัญ รวมถึงผลกระทบที่อาจเกิดขึ้นจากเหตุการณ์ระบบล่ม การโจมตีทางไซเบอร์ หรือการสูญเสียข้อมูล เพื่อกำหนดลำดับความสำคัญในการกู้คืนระบบ

๗.๒ ให้กำหนดแนวทางสำรองระบบ การทำสำเนาข้อมูล การมีศูนย์สำรอง หรือการใช้โครงสร้างพื้นฐานทดแทน เพื่อให้สามารถให้บริการได้อย่างต่อเนื่องเมื่อเกิดเหตุขัดข้องด้านไซเบอร์

๗.๓ ให้มีการจัดทำแผนความต่อเนื่องทางธุรกิจและแผนกู้คืนระบบสารสนเทศ (BCP/DRP) ที่ครอบคลุมสถานการณ์ภัยคุกคามไซเบอร์ พร้อมกำหนดขั้นตอนการตอบสนอง การสื่อสาร และการฟื้นฟูระบบอย่างชัดเจน และให้มีการทบทวนปรับปรุงแผนอย่างสม่ำเสมอ

/๗.๔ ให้มี...

๗.๔ ให้มีการทดสอบและฝึกซ้อมแผนรับมือเหตุการณ์ไซเบอร์เป็นระยะ เพื่อให้มั่นใจว่าบุคลากรที่เกี่ยวข้องมีความเข้าใจบทบาทหน้าที่ และสามารถปฏิบัติได้จริงเมื่อเกิดเหตุ

๗.๕ ให้กำหนดค่าเป้าหมายระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) และระดับข้อมูลที่ยอมรับได้ (Recovery Point Objective: RPO) สำหรับระบบสำคัญ เพื่อใช้เป็นกรอบในการออกแบบมาตรการความต่อเนื่อง

๗.๖ ให้การบริหารความต่อเนื่องทางธุรกิจด้านไซเบอร์เชื่อมโยงกับกระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และกระบวนการตอบสนองต่อเหตุการณ์ (Incident Response) เพื่อให้การดำเนินงานเป็นไปอย่างสอดคล้องและมีประสิทธิภาพ

๗.๗ ให้กำหนดแนวทางการสื่อสารภายในองค์กร และกับหน่วยงานภายนอกที่เกี่ยวข้องในกรณีเกิดเหตุการณ์ไซเบอร์ เพื่อให้การจัดการสถานการณ์เป็นไปอย่างรวดเร็ว ถูกต้อง และลดผลกระทบต่อผู้รับบริการ

ทั้งนี้ ผู้บริหาร พนักงาน ผู้มีส่วนได้ส่วนเสีย ต้องให้ความร่วมมือในส่วนที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์การคลังสินค้า

ประกาศ ณ วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๙

เรือโท

(วีระชัย โกสาแสง)

รองผู้อำนวยการองค์การคลังสินค้า

รักษาการแทนผู้อำนวยการองค์การคลังสินค้า

๗.๔ ให้มีการทดสอบและฝึกซ้อมแผนรับมือเหตุการณ์ไซเบอร์เป็นระยะ เพื่อให้มั่นใจว่าบุคลากรที่เกี่ยวข้องมีความเข้าใจบทบาทหน้าที่ และสามารถปฏิบัติได้จริงเมื่อเกิดเหตุ

๗.๕ ให้กำหนดค่าเป้าหมายระยะเวลาการกู้คืนระบบ (Recovery Time Objective: RTO) และระดับข้อมูลที่ยอมรับได้ (Recovery Point Objective: RPO) สำหรับระบบสำคัญ เพื่อใช้เป็นกรอบในการออกแบบมาตรการความต่อเนื่อง

๗.๖ ให้การบริหารความต่อเนื่องทางธุรกิจด้านไซเบอร์เชื่อมโยงกับกระบวนการบริหารความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ และกระบวนการตอบสนองต่อเหตุการณ์ (Incident Response) เพื่อให้การดำเนินงานเป็นไปอย่างสอดคล้องและมีประสิทธิภาพ

๗.๗ ให้กำหนดแนวทางการสื่อสารภายในองค์กร และกับหน่วยงานภายนอกที่เกี่ยวข้องในกรณีเกิดเหตุการณ์ไซเบอร์ เพื่อให้การจัดการสถานการณ์เป็นไปอย่างรวดเร็ว ถูกต้อง และลดผลกระทบต่อผู้รับบริการ

ทั้งนี้ ผู้บริหาร พนักงาน ผู้มีส่วนได้ส่วนเสีย ต้องให้ความร่วมมือในส่วนที่เกี่ยวข้องในการบริหารจัดการความเสี่ยงด้านความมั่นคงปลอดภัยสารสนเทศ (Information Security Risk Management) ขององค์การคลังสินค้า

ประกาศ ณ วันที่ ๒๕ พฤษภาคม พ.ศ. ๒๕๖๙

เรือโท

(วีระชัย โกสาแสง)

รองผู้อำนวยการองค์การคลังสินค้า

รักษาการแทนผู้อำนวยการองค์การคลังสินค้า