ประกาศสำนักงานคณะกรรมการส่งเสริมการลงทุน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๖๐

---

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสาร ของสำนักงานคณะกรรมการส่งเสริมการลงทุน เป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัย และสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงาน อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง สำนักงานจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานจึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการส่งเสริมการลงทุน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๖๐”

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกอบด้วยสาระสำคัญ ดังต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศ ซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ให้เป็นไปตามนโยบาย คู่มือปฏิบัติงาน และวิธีปฏิบัติงาน ที่สำนักงานได้กำหนดไว้ตามเอกสารแนบท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน

ทั้งนี้ สำนักงานได้กำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้มีความสอดคล้องกับระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 ซึ่งเป็นมาตรการสำหรับใช้ในการควบคุมระบบสารสนเทศให้มีเสถียรภาพและมั่นคงปลอดภัย โดยครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity) และการรักษาสภาพ

ความพร้อมใช้งาน (Availability) ของระบบสารสนเทศ รวมถึงเป็นไปตามพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ.๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ.๒๕๕๓ และฉบับที่ ๒ พ.ศ.๒๕๕๖ ที่ได้กำหนดไว้

ข้อ ๔ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศ จะกระทำโดยผู้ตรวจสอบหน่วยงานภายในของรัฐ (Internal Auditor) และผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก (External Auditor) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้หน่วยงานของรัฐได้ทราบถึงระดับความเสี่ยงและระดับความมั่นคงปลอดภัยสารสนเทศของหน่วยงาน

ข้อ ๕ ให้เลขาธิการคณะกรรมการส่งเสริมการลงทุน ซึ่งเป็นผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายใดๆ ที่เกิดขึ้นแก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๖ ให้สำนักสารสนเทศการลงทุน เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อสำนักงาน

ข้อ ๗ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๖ พฤศจิกายน พ.ศ. ๒๕๖๐

(นางสาวดวงใจ อัศวจินตจิตร์)
เลขาธิการคณะกรรมการส่งเสริมการลงทุน

**<u>บัญชีเอกสารแนบท้าย</u>**

**ประกาศสำนักงานคณะกรรมการส่งเสริมการลงทุน**

**เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ**

**ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๖๐**

๑. คู่มือระบบบริหารความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual)

๒. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy)

๓. คำประกาศการนำไปใช้งาน (Statement of Applicability : SOA)

๔. แนวทางการประเมินความเสี่ยงสารสนเทศ (Risk Assessment Approach)

๕. รายงานการประเมินความเสี่ยง (Risk Assessment Report)

๖. แผนการจัดการความเสี่ยง (Risk Treatment Plan)

๗. แผนสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity Plan: BCP)

๘. คู่มือปฏิบัติงาน และวิธีปฏิบัติงาน ระบบบริหารความมั่นคงปลอดภัยสารสนเทศ ตามมาตรฐาน ISO/IEC 27001 ของสำนักงานคณะกรรมการส่งเสริมการลงทุน

---