ประกาศสำนักงานคณะกรรมการส่งเสริมการลงทุน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๕๘

เพื่อให้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานคณะกรรมการส่งเสริมการลงทุนเป็นไปอย่างมีประสิทธิภาพ มีความมั่นคงปลอดภัยและสามารถดำเนินงานได้อย่างต่อเนื่อง รวมทั้งป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้งานระบบสารสนเทศและการสื่อสารที่ไม่ถูกต้อง ตลอดจนการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักงาน อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ และกฎหมายอื่นที่เกี่ยวข้อง สำนักงานจึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๕ มาตรา ๗ และมาตรา ๘ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และด้วยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ สำนักงานจึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศคณะกรรมการส่งเสริมการลงทุน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๕๘”

ข้อ ๒ นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน ให้เป็นไปตามนโยบาย คู่มือปฏิบัติงาน และวิธีปฏิบัติงาน ที่สำนักงานได้กำหนดไว้ตามเอกสารแนบท้ายนี้ และต้องพิจารณาให้สอดคล้องกับระดับความเสี่ยงที่ได้จากการประเมิน ทั้งนี้สำนักงานได้กำหนดนโยบาย คู่มือปฏิบัติงาน และวิธีปฏิบัติงาน ดังกล่าว ให้มีความสอดคล้องกับมาตรฐานการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๐๕ ซึ่งเป็นมาตรการสำหรับใช้ในการควบคุมให้ระบบสารสนเทศมีความมั่นคงปลอดภัย โดยครอบคลุมการรักษาความลับ (Confidentiality) การรักษาความครบถ้วน (Integrity)

และการรักษาสภาพพร้อมใช้งาน (Availability) ของระบบสารสนเทศ รวมถึงเป็นไปตามพระราชกฤษฎีกาฯ ที่คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้กำหนดไว้

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและประเมินความเสี่ยงสินทรัพย์ด้านสารสนเทศอย่างน้อยปีละ ๑ ครั้ง หรือภายใน ๑ เดือน เมื่อมีการเปลี่ยนแปลงที่สำคัญเกิดขึ้น

ข้อ ๕ ให้เลขาธิการ ซึ่งเป็นผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยงเสียหาย หรืออันตรายที่เกิดขึ้น กรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใดๆ แก่องค์กรหรือผู้หนึ่งผู้ใดอันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๖ ให้สำนักสารสนเทศการลงทุน เป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง หรือเมื่อมีการเปลี่ยนแปลงที่สำคัญต่อสำนักงาน

ข้อ ๗ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ดังนั้น เพื่อให้นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยในด้านสารสนเทศของสำนักงานตามเอกสารแนบท้ายบรรลุวัตถุประสงค์ตามที่กำหนดไว้ จึงให้หน่วยงานในสังกัดนำนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ไปใช้ในการปฏิบัติงานของสำนักงาน และถือปฏิบัติอย่างเคร่งครัดต่อไป

จึงประกาศให้ทราบโดยทั่วกัน

ประกาศ ณ วันที่ ๑๒ มกราคม พ.ศ. ๒๕๕๘

(นางหิรัญญา สุจินัย)
ที่ปรึกษาด้านการลงทุน รักษาราชการแทน
เลขาธิการคณะกรรมการส่งเสริมการลงทุน

บัญชีเอกสารแนบท้ายประกาศสำนักงานคณะกรรมการส่งเสริมการลงทุน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานคณะกรรมการส่งเสริมการลงทุน พ.ศ. ๒๕๕๘

๑. คู่มือบริหารระบบความมั่นคงปลอดภัยสารสนเทศ (ISMS Manual)
๒. นโยบายความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศและการสื่อสาร (ICT Security Policy)
๓. คำประกาศการนำไปใช้งาน (Statement of Applicability : SOA)
๔. รายงานการประเมินความเสี่ยง (Risk Assessment Report)
๕. แผนการจัดการความเสี่ยง (Risk Treatment Plan)
๖. แผนสร้างความต่อเนื่องให้กับธุรกิจ (Business Continuity Plan: BCP)
๗. คู่มือปฏิบัติงาน และวิธีปฏิบัติงาน ระบบบริหารความมั่นคงปลอดภัยของระบบสารสนเทศ ตามมาตรฐาน ISO/IEC ๒๗๐๐๑:๒๐๐๕ ของสำนักงานคณะกรรมการส่งเสริมการลงทุน
