



ประกาศสำนักงานคณะกรรมการพัฒนาระบบราชการ

เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ของสำนักงานคณะกรรมการพัฒนาระบบราชการ

ด้วยสำนักงานคณะกรรมการพัฒนาระบบราชการตระหนักถึงปัญหาด้านการรักษาความมั่นคงปลอดภัยให้กับระบบสารสนเทศ ซึ่งอาจส่งผลกระทบต่อภาครัฐที่มีการดำเนินงานในรูปแบบของข้อมูลอิเล็กทรอนิกส์ผ่านระบบสารสนเทศของสำนักงานคณะกรรมการพัฒนาระบบราชการ ประกอบกับสำนักงานคณะกรรมการพัฒนาระบบราชการได้นำระบบสารสนเทศมาประยุกต์ใช้ในภารกิจของสำนักงานคณะกรรมการพัฒนาระบบราชการ จึงเห็นความสำคัญที่จะนำกฎหมายและข้อบังคับต่าง ๆ มาบังคับใช้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ เพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์ของสำนักงานคณะกรรมการพัฒนาระบบราชการมีความมั่นคงปลอดภัย จึงเห็นสมควรกำหนดนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานเพื่อบังคับใช้ต่อไป

โดยที่มาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ สำนักงานคณะกรรมการพัฒนาระบบราชการจึงได้จัดทำประกาศฉบับนี้เพื่อเป็นนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ดังต่อไปนี้

ข้อ ๑ คำนิยาม

“สำนักงาน” หมายถึง สำนักงานคณะกรรมการพัฒนาระบบราชการ

“แนวนโยบาย” หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งสำนักงานคณะกรรมการพัฒนาระบบราชการได้กำหนดไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานคณะกรรมการพัฒนาระบบราชการที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน และเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ และประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓

“**แนวปฏิบัติ**” หมายถึง หมายถึง ขั้นตอนวิธีการที่สำนักงานคณะกรรมการพัฒนาระบบราชการได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของข้าราชการและเจ้าหน้าที่ โดยมีจุดมุ่งหมาย เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

“**สินทรัพย์**” หมายถึง สิ่งใดก็ตามที่เกี่ยวข้องกับระบบเทคโนโลยีสารสนเทศที่มีคุณค่าสำหรับสำนักงานคณะกรรมการพัฒนาระบบราชการ

“**ระบบเทคโนโลยีสารสนเทศ**” หมายถึง ระบบงานของสำนักงานคณะกรรมการพัฒนาระบบราชการที่นำเอาเทคโนโลยีสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายมาช่วยในการสร้างสารสนเทศที่หน่วยงานสามารถนำมาใช้ประโยชน์ในการวางแผน การบริหาร การสนับสนุนการให้บริการ การพัฒนาและควบคุมการติดต่อสื่อสาร ซึ่งมีองค์ประกอบ ได้แก่ ระบบคอมพิวเตอร์ ระบบเครือข่าย โปรแกรม ข้อมูลและสารสนเทศ และอื่นๆ

“**การรักษาความมั่นคงปลอดภัย**” หมายถึง การรักษาความมั่นคงปลอดภัยสำหรับระบบเทคโนโลยีสารสนเทศของสำนักงานคณะกรรมการพัฒนาระบบราชการ

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยสารสนเทศของสำนักงานคณะกรรมการพัฒนาระบบราชการ ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่าง ๆ ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) การจัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ต้องจัดให้มีการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบเทคโนโลยีสารสนเทศ ตรวจสอบประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและประเมินทบทวนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๔ สร้างความรู้ความเข้าใจให้กับข้าราชการและเจ้าหน้าที่ของสำนักงานคณะกรรมการพัฒนาระบบราชการ เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้ระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการดังต่อไปนี้

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักงานคณะกรรมการพัฒนาระบบราชการ ระบบสารสนเทศสำนักงานคณะกรรมการพัฒนาระบบราชการ และสื่อต่าง ๆ ให้แก่ข้าราชการและเจ้าหน้าที่ของสำนักงานคณะกรรมการพัฒนาระบบราชการและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ข้าราชการและเจ้าหน้าที่ในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) และจัดทำคู่มือการใช้งานระบบสารสนเทศเป็นประจำ

ข้อ ๕ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๖ กรณีระบบคอมพิวเตอร์ ระบบสารสนเทศ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงานคณะกรรมการพัฒนาระบบราชการ หน่วยงาน หรือบุคคลใดอันเนื่องมาจาก ความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัย สารสนเทศ ให้ผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของหน่วยงาน (Chief Information Officer: CIO) เป็นผู้รับผิดชอบความเสี่ยง ความเสียหาย และอันตรายที่เกิดขึ้น

ข้อ ๗ ให้กลุ่มเทคโนโลยีสารสนเทศ สำนักงานเลขาธิการ เป็นผู้รับผิดชอบดำเนินการให้ เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันและสอดคล้อง ครบถ้วน ตามที่กฎหมายกำหนดไว้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๘ ธันวาคม พ.ศ. ๒๕๖๖



(นางอารีย์พันธ์ เจริญสุข)

รองเลขาธิการ ก.พ.ร. ปฏิบัติราชการแทน

เลขาธิการ ก.พ.ร.

ผู้บริหารเทคโนโลยีสารสนเทศระดับสูง