ประกาศสำนักงานป้องกันและปราบปรามการฟอกเงิน
เรื่อง แนวนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๖๕

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน จึงออกประกาศไว้ ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

"**สำนักงาน**" หมายถึง สำนักงานป้องกันและปราบปรามการฟอกเงิน

"**นโยบาย**" หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมทางอิเล็กทรอนิกส์ที่สำนักงานจัดไว้ให้บริการประชาชน ซึ่งสำนักงานประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

"**แนวปฏิบัติ**" หมายถึง ขั้นตอนวิธีการที่สำนักงานได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

"**ผู้ใช้งาน**" หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของสำนักงาน ผู้บริหารสำนักงาน ผู้ใช้บริการ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของสำนักงาน

"**บัญชีผู้ใช้งาน**" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

"**สิทธิของผู้ใช้งาน**" หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

/"การเข้าถึง...

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์ และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"สินทรัพย์" หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"สินทรัพย์คอมพิวเตอร์" หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"สารสนเทศ" หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจหรือใช้ประโยชน์ต่างๆ ตามภารกิจของสำนักงาน

"เครือข่าย" หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ ๒ เครื่องขึ้นไปเข้าด้วยกัน เพื่อสะดวกต่อการร่วมใช้ข้อมูล โปรแกรม หรือเครื่องพิมพ์ และอำนวยความสะดวกในการติดต่อแลกเปลี่ยนข้อมูลระหว่างเครื่องได้ตลอดเวลา

"ความมั่นคงปลอดภัยด้านสารสนเทศ" หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

"เหตุการณ์ด้านความมั่นคงปลอดภัย" หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted or unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ผู้บริหารระดับสูงสุด"หมายความว่า เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน หรือผู้รักษาราชการ

/ ข้อ ๒ นโยบาย ...

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ แนวนโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศตามเป้าหมายครอบคลุม ๔ เรื่อง ดังนี้

- การเข้าถึงสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชันและสารสนเทศ

(๒) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

(๔) การกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจต้องมีแนวปฏิบัติในการบริหารจัดการสิทธิในแต่ละกลุ่ม รวมถึงการระงับสิทธิ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานให้เป็นไปตามที่กำหนดไว้ในแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานป้องกันและปราบปรามการฟอกเงิน พ.ศ. ๒๕๖๕

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบ และควบคุมคุณภาพระบบงานเทคโนโลยีสารสนเทศ และตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศของสำนักงานอย่างน้อยปีละ ๑ ครั้ง ด้วยผู้ตรวจสอบภายในหน่วยงานของสำนักงาน หรือ ผู้ตรวจสอบอิสระด้านความมั่นคงปลอดภัยจากภายนอก

ข้อ ๕ สร้างความรู้ความเข้าใจให้แก่ผู้ใช้งานของสำนักงาน เพื่อให้เกิดความตระหนักความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ โดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ ดังนี้

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักงาน ระบบเครือข่ายภายใน (Intranet) และหนังสือเวียนภายในให้ผู้ใช้งาน

/ และบุคคล ...

และบุคคลภายนอกทราบ เพื่อให้เข้าถึงเข้าใจและปฏิบัติตามได้อย่างถูกต้อง โดยให้มีการทบทวนปรับปรุงนโยบายและแนวปฏิบัติฯ ให้เป็นปัจจุบันอยู่เสมอ

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (Information Security Awareness Training) เพื่อป้องกันการเข้าถึงโดยผู้ซึ่งไม่ได้รับการอนุญาต

(๓) แจ้งให้ผู้รับบริการทางอิเล็กทรอนิกส์แก่สำนักงาน ทราบ

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่นๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๗ ให้ผู้บริหารระดับสูงสุดเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นกรณีระบบคอมพิวเตอร์ หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่องค์กรหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ ฉบับนี้

ประกาศ ณ วันที่ ๑๗ ตุลาคม พ.ศ. ๒๕๖๕

(นายเทพสุ บวรโชติดารา)
รองเลขาธิการฯ รักษาราชการแทน
เลขาธิการคณะกรรมการป้องกันและปราบปรามการฟอกเงิน