ประกาศสำนักงานบริหารหนี้สาธารณะ
เรื่อง นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ปีงบประมาณ พ.ศ. 2559

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549 มาตรา 5 และมาตรา 7 กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ผู้อำนวยการสำนักงานบริหารหนี้สาธารณะ โดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกประกาศไว้ ดังต่อไปนี้

ข้อ 1 ในประกาศนี้

"สำนักงาน" หมายถึง สำนักงานบริหารหนี้สาธารณะ

"นโยบาย" หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ที่สำนักงานบริหารหนี้สาธารณะจัดไว้ให้บริการประชาชน ซึ่งสำนักประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. 2549

"แนวปฏิบัติ" หมายถึง ขั้นตอนวิธีการที่สำนักงานได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

"ผู้ใช้งาน" หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบของสำนักงานผู้บริหารองค์กร ผู้รับบริการ และผู้ใช้งานที่ใช้บริการระบบเทคโนโลยีสารสนเทศของสำนักงาน

"บัญชีผู้ใช้งาน" หมายความว่า บัญชีรายชื่อผู้เข้าถึงและรหัสผ่านในการใช้งานระบบเทคโนโลยีสารสนเทศของสำนักงาน

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

"สินทรัพย์" หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"สินทรัพย์คอมพิวเตอร์" หมายความว่า โปรแกรมคอมพิวเตอร์ เครื่องคอมพิวเตอร์ อุปกรณ์เครือข่าย และให้หมายความรวมถึงอุปกรณ์คอมพิวเตอร์ที่เกี่ยวข้องด้วย

"ข้อมูลคอมพิวเตอร์" หมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

"สารสนเทศ" หมายถึง ข้อมูลในรูปแบบต่างๆ ที่สามารถนำมาใช้ประกอบการตัดสินใจ หรือใช้ประโยชน์ต่าง ๆ ตามภารกิจของสำนักงาน

"เครือข่าย" หมายความว่า ระบบการสื่อสารที่เป็นการเชื่อมต่อคอมพิวเตอร์ ตั้งแต่ 2 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 กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

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

ข้อ 2 นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน แบ่งเป็น 2 ส่วน ได้แก่

ส่วนที่ 1 แนวนโยบาย

ส่วนที่ 2 แนวปฏิบัติ

รายละเอียดภายในของทั้งสองส่วน ประกอบด้วยเนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(1) การกำหนดการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ตามเป้าหมายครอบคลุม 4 เรื่อง ดังนี้

- การเข้าถึงสารสนเทศ
- การเข้าถึงระบบเครือข่าย
- การเข้าถึงระบบปฏิบัติการ
- การเข้าถึงโปรแกรมประยุกต์หรือแอพพลิเคชั่นและสารสนเทศ

(2) การจัดระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(3) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ