ประกาศสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน พ.ศ. ๒๕๖๒

อาศัยอำนาจตามความในมาตรา ๕ และมาตรา ๗ แห่งพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๙ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล โดยความเห็นชอบของคณะกรรมการธุรกรรมอิเล็กทรอนิกส์จึงออกประกาศดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า "ประกาศสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน พ.ศ. ๒๕๖๒"

ข้อ ๒ ในประกาศนี้

๒.๑ ผู้บริหารระดับสูง หมายความว่า ผู้จัดการสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานซึ่งเป็นผู้รับผิดชอบการสั่งการตามแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๒.๒ ผู้บริหาร หมายความว่า ผู้จัดการ รองผู้จัดการสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน หรือผู้ที่ผู้จัดการฯ มอบหมายให้ดูแลรับผิดชอบงานด้านเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๒.๓ "ผู้ดูแลระบบ" หมายความว่า ผู้ที่ได้รับมอบหมายจากผู้จัดการฯให้มีหน้าที่ดูแลรับผิดชอบรักษาดูแลรักษาข้อมูลสารสนเทศ ระบบสารสนเทศ และระบบเครือข่าย สำหรับผู้ใช้งานภายใน ผู้ใช้งานที่เกี่ยวข้อง และผู้ใช้งานภายนอก

๒.๔ "นโยบาย" หมายความว่า หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการทำธุรกรรมอิเล็กทรอนิกส์ซึ่งสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานจัดไว้ให้บริการประชาชน ซึ่งสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกันและเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เรื่อง แนวนโยบายและแนวปฏิบัติใน

การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ และที่แก้ไขเพิ่มเติม

๒.๕ "แนวปฏิบัติ" หมายความว่าขั้นตอนวิธีการที่สำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานได้กำหนดไว้โดยภาพรวม สำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานที่เกี่ยวข้องกับการทำธุรกรรมทางอิเล็กทรอนิกส์ โดยมีจุดมุ่งหมายเพื่อให้การทำธุรกรรมทางอิเล็กทรอนิกส์นั้น มีวิธีที่มั่นคงปลอดภัย

๒.๖ ผู้ใช้งาน หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานราชการ ลูกจ้างประจำ/ชั่วคราว ลูกจ้างตามสัญญาจ้าง ผู้ดูแลระบบ ผู้บริหารของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน รวมถึงบุคคลภายนอกที่เป็นหน่วยงานราชการ รัฐวิสาหกิจ ผู้ประกอบการที่เกี่ยวข้องกับสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน หรือผู้ที่ได้รับอนุญาตให้ใช้เครื่องคอมพิวเตอร์และระบบเครือข่ายของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๒.๗ สิทธิของผู้ใช้งาน หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๒.๘ สินทรัพย์ หมายความว่า ทรัพย์สินหรือสิ่งใดก็ตามทั้งที่มีตัวตนและไม่มีตัวตนอันมีมูลค่าหรือคุณค่าสำหรับสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๒.๙ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายและระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และกายภาพรวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก

๒.๑๐ ความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของระบบเทคโนโลยีสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิดชอบ (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

๒.๑๑ เหตุการณ์ด้านความมั่นคงปลอดภัย (Information Security Event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

๒.๑๒ สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or Unexpected) ซึ่งอาจทำให้ระบบของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๓ การจัดให้มีข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน ประกอบด้วยกระบวนการ ดังนี้

๓.๑ จัดทำข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๓.๒ ประกาศนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้ที่เกี่ยวข้องทั้งหมดทราบ เพื่อให้สามารถเข้าถึง เข้าใจ และปฏิบัติตามนโยบายและข้อปฏิบัติได้

๓.๓ กำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

๓.๔ ทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบัน

ข้อ ๔ การรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานตามประกาศนี้มี ๒ ส่วน ดังนี้

๔.๑ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๖

๔.๒ แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ต้องมีเนื้อหาอย่างน้อยครอบคลุมตามข้อ ๗-๑๕

ข้อ ๕ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ตามประกาศนี้ มี ๒ ส่วน ดังนี้

๕.๑ ส่วนที่ว่าด้วยการจัดทำนโยบาย

(๑) ผู้บริหาร เจ้าหน้าที่ปฏิบัติการด้านคอมพิวเตอร์และผู้ใช้งานได้มีส่วนร่วมในการทำนโยบาย

(๒) นโยบายได้ทำเป็นลายลักษณ์อักษร โดยประกาศให้ผู้ใช้งานทราบและสามารถเข้าถึงได้อย่างสะดวกผ่านทางเว็บไซต์อินทราเน็ตของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

(๓) กำหนดผู้รับผิดชอบตามนโยบายและแนวปฏิบัติดังกล่าวให้ชัดเจน

(๔) มีการทบทวนและปรับปรุงนโยบายให้เป็นปัจจุบัน

๕.๒ ส่วนที่ว่าด้วยรายละเอียดของนโยบาย

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ มีการบริการระบบเทคโนโลยีสารสนเทศแก่ผู้ใช้และประชาชนอย่างทั่วถึง โดยให้ผู้ใช้งานประชาชนสามารถเข้าถึงและใช้งานระบบสารสนเทศได้อย่างสะดวกรวดเร็ว รวมทั้งมีการให้ความคุ้มครองข้อมูลที่ไม่พึงเปิดเผย

(๒) ระบบสารสนเทศและระบบสำรองข้อมูลสารสนเทศ มีการบริหารจัดการระบบสารสนเทศที่ได้มาตรฐาน โดยมีการแยกประเภทและจัดเก็บเทคโนโลยีสารสนเทศเป็นหมวดหมู่ มีระบบสำรองข้อมูลระบบสารสนเทศที่สมบูรณ์พร้อมใช้งาน รวมทั้งมีแผนฉุกเฉินในการใช้งานเพื่อให้สามารถทำงานได้อย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศ มีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศอย่างสม่ำเสมอ รวมถึงกำหนดมาตรการในการควบคุมความเสี่ยงด้านสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

(๔) การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ สร้างความรู้ความเข้าใจ โดยการจัดทำคู่มือ จัดฝึกอบรม และเผยแพร่การใช้งานระบบสารสนเทศให้แก่ผู้ใช้งาน

ข้อ ๖ กำหนดการเข้าถึงหรือควบคุมการใช้งานระบบสารสนเทศ (Access Control) อย่างน้อย ดังนี้

๖.๑ มีการควบคุมการเข้าถึงข้อมูลและอุปกรณ์ในการประมวลผลข้อมูล โดยคำนึงถึงการใช้งานและความมั่นคงปลอดภัย

๖.๒ ในการกำหนดกฎเกณฑ์เกี่ยวกับการอนุญาตให้เข้าถึง ต้องกำหนดตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน

๖.๓ ต้องกำหนดเกี่ยวกับประเภทของข้อมูล ลำดับความสำคัญ หรือลำดับชั้นความลับของข้อมูลรวมทั้งระดับชั้นการเข้าถึง และช่องทางการเข้าถึง

ข้อ ๗ กำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงระบบสารสนเทศ (Business Requirements for Access Control) โดยแบ่งการจัดทำข้อมูลปฏิบัติเป็น ๒ ส่วน คือ การควบคุมการเข้าถึงระบบสารสนเทศ และการปรับปรุงให้สอดคล้องกับข้อกำหนดใช้งานตามภารกิจและข้อกำหนดด้านความมั่นคงปลอดภัย

ข้อ ๘ กำหนดการบริหารจัดการการเข้าถึงข้อมูลผู้ใช้งาน (User Access Management) เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตแล้ว เพื่อป้องกันการเข้าถึงจากผู้ซึ่งไม่ได้รับอนุญาต อย่างน้อย ดังนี้

๘.๑ สร้างความรู้ความเข้าใจให้กับผู้ใช้งาน (User Awareness) เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ รวมทั้งกำหนดให้มีมาตรการเชิงป้องกันตามความเหมาะสม

๘.๒ การลงทะเบียนผู้ใช้งาน (User Registration) ต้องกำหนดให้มีขั้นตอนทางปฏิบัติสำหรับการลงทะเบียนผู้ใช้งานเมื่อมีการอนุญาตให้เข้าถึงระบบสารสนเทศ และการตัดออกจากทะเบียนของผู้ใช้งานเมื่อมีการยกเลิกเพิกถอนการอนุญาตดังกล่าว

๘.๓ การบริหารจัดการสิทธิของผู้ใช้งาน (User Management) ต้องจัดให้มีการควบคุมและจำกัดสิทธิเพื่อเข้าถึงและใช้งานระบบสารสนเทศแต่ละชนิดตามความเหมาะสม ทั้งนี้รวมถึงสิทธิจำเพาะ สิทธิพิเศษและสิทธิอื่น ๆ ที่เกี่ยวข้องกับการเข้าถึง

๘.๔ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน (User Password Management) ต้องจัดให้มีกระบวนการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานอย่างรัดกุม

๘.๕ การทบทวนสิทธิการเข้าถึงของผู้ใช้งาน (Review of User Access Right) ต้องจัดให้มีกระบวนการทบทวนสิทธิการเข้าถึงข้อมูลของผู้ใช้งานระบบสารสนเทศตามระยะเวลาที่กำหนดไว้

ข้อ ๙ กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต การเปิดเผย การล่วงรู้ หรือการลักลอบทำสำเนาข้อมูลระบบสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลสารสนเทศ มีเนื้อหาอย่างน้อย ดังนี้

๙.๑ การใช้งานรหัสผ่าน (Password Use) กำหนดแนวปฏิบัติที่ดีสำหรับผู้ใช้งานในการกำหนดรหัสผ่าน การใช้งานรหัสผ่าน และการเปลี่ยนรหัสผ่านที่มีคุณภาพ

๙.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งานอุปกรณ์ กำหนดแนวปฏิบัติที่เหมาะสมเพื่อป้องกันไม่ให้ผู้ไม่มีสิทธิสามารถเข้าถึงอุปกรณ์ของกระทรวงในขณะที่ไม่มีผู้ดูแล

๙.๓ การควบคุมสินทรัพย์สารสนเทศและการใช้งานระบบคอมพิวเตอร์ (Clear Desk and Clear Screen Policy) ต้องควบคุมไม่ให้สินทรัพย์สารสนเทศ เช่น เอกสาร สื่อบันทึกข้อมูล คอมพิวเตอร์หรือสารสนเทศอยู่ในภาวะเสี่ยงต่อการเข้าถึงโดยผู้ซึ่งไม่มีสิทธิ และต้องกำหนดให้ผู้ใช้งานออกจากระบบสารสนเทศเมื่อว่างเว้นจากการใช้งาน

๙.๔ ให้มีการทำลายข้อมูลบนสื่อบันทึกข้อมูลของระบบหรืออุปกรณ์คอมพิวเตอร์ที่จะมีการแทงจำหน่ายหรือก่อนที่จะอนุญาตให้ผู้อื่นนำระบบหรืออุปกรณ์นั้นไปใช้งานต่อเพื่อป้องกันการเข้าถึงข้อมูลสำคัญบนสื่อบันทึกข้อมูล

๙.๕ ผู้ใช้งานอาจนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ โดยให้ปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔

ข้อ ๑๐ กำหนดการควบคุมการเข้าถึงเครือข่าย (Network Access Control) เพื่อป้องกันการเข้าถึงบริการทางเครือข่ายโดยไม่ได้รับอนุญาต อย่างน้อยดังนี้

๑๐.๑ การใช้บริการเครือข่าย ต้องกำหนดให้ผู้ใช้งานสามารถเข้าถึงระบบสารสนเทศได้แต่เพียงบริการที่ได้รับอนุญาตให้เข้าถึงเท่านั้น

๑๐.๒ การยืนยันตัวบุคคลสำหรับผู้ใช้งานที่อยู่ภายนอกสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน (User Authentication for External Connections) ต้องกำหนดให้มีการยืนยันตัวบุคคลก่อนที่จะอนุญาตให้ผู้ใช้งานที่อยู่ภายนอกสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงานได้

๑๐.๓ การระบุอุปกรณ์บนเครือข่าย (Equipment Identification in Networks) ต้องมีวิธีการที่สามารถระบุอุปกรณ์บนเครือข่ายได้ และควรใช้การระบุอุปกรณ์บนเครือข่ายเป็นการยืนยัน

๑๐.๔ การป้องกันพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบ (Remote Diagnostic and Configuration Port Protection) ต้องควบคุมการเข้าถึงพอร์ตที่ใช้สำหรับตรวจสอบและปรับแต่งระบบทั้งการเข้าถึงทางกายภาพและทางเครือข่าย

๑๐.๕ การควบคุมการเชื่อมต่อทางเครือข่าย (Network Connection Control) ต้องควบคุมการเข้าถึงหรือใช้งานเครือข่ายที่มีการใช้งานร่วมกันหรือเชื่อมต่อระหว่างกันให้สอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึง

๑๐.๖ การควบคุมการจัดเส้นทางบนเครือข่าย (Network Routing Control) ต้องควบคุมการจัดเส้นทางบนเครือข่ายเพื่อให้การเชื่อมต่อของคอมพิวเตอร์และ

การส่งผ่านหรือไหลเวียนของข้อมูลหรือสารสนเทศสอดคล้องกับแนวปฏิบัติการควบคุมการเข้าถึงหรือการประยุกต์ใช้งานตามภารกิจ

ข้อ ๑๑ กำหนดการควบคุมการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการเข้าถึงระบบปฏิบัติการโดยไม่ได้รับอนุญาต อย่างน้อย ดังนี้

๑๑.๑ กำหนดขั้นตอนปฏิบัติเพื่อการเข้าใช้งานที่มั่นคงปลอดภัย การเข้าถึงระบบปฏิบัติการต้องควบคุมโดยวิธีการยืนยันตัวตนที่มั่นคงปลอดภัย

๑๑.๒ การระบุและยืนยันตัวตนของผู้ใช้งาน (user identification and authentication) ต้องกำหนดให้ผู้ใช้งานมีข้อมูลเฉพาะเจาะจงซึ่งสามารถระบุตัวตนของผู้ใช้งาน และเลือกใช้ขั้นตอนทางเทคนิคในการยืนยันตัวตนที่เหมาะสมเพื่อรองรับการกล่าวอ้างว่าเป็นผู้ใช้งานที่ระบุถึง

๑๑.๓ การบริหารจัดการรหัสมี (password management system) ต้องจัดทำหรือจัดให้มีระบบบริหารจัดการรหัสมีที่สามารถทำงานเชิงโต้ตอบ (interactive) หรือมีการทำงานในลักษณะอัตโนมัติ ซึ่งเอื้อต่อการกำหนดรหัสมีที่มีคุณภาพ

๑๑.๔ การใช้งานโปรแกรมอรรถประโยชน์ (User of System Utilities) ต้องจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

๑๑.๕ เมื่อมีการว่างเว้นจากการใช้งานในระยะเวลาหนึ่งให้ยุติการใช้งานระบบสารสนเทศนั้น (session time-out)

๑๑.๖ การใช้งานโปรแกรมอรรถประโยชน์ (use of system utilities) ควรจำกัดและควบคุมการใช้งานโปรแกรมประเภทอรรถประโยชน์ เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงมาตรการความมั่นคงปลอดภัยที่ได้กำหนดไว้หรือที่มีอยู่แล้ว

ข้อ ๑๒ กำหนดการควบคุมการเข้าถึงโปรแกรมประยุกต์หรือแอปพลิเคชั่นและสารสนเทศ (Application and Information Access Control)

๑๒.๑ การจำกัดการเข้าถึงระบบสารสนเทศ ต้องจำกัดหรือควบคุมการเข้าถึงหรือเข้าใช้งานของผู้ใช้งานและบุคลากรฝ่ายสนับสนุนการเข้าใช้งานในการเข้าถึงระบบสารสนเทศและฟังก์ชั่นต่าง ๆ ของโปรแกรมประยุกต์หรือแอปพลิเคชั่น ทั้งนี้ โดยให้สอดคล้องตามนโยบายควบคุมการเข้าถึงระบบสารสนเทศที่ได้กำหนดไว้

๑๒.๒ ระบบซึ่งไวต่อการรบกวน มีผลกระทบและมีความสำคัญสูงต่อองค์กร ต้องได้รับการแยกออกจากระบบอื่น ๆ และมีการควบคุมสภาพแวดล้อมของตนเองโดยเฉพาะ ให้มีการควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่และการปฏิบัติงานจากภายนอกองค์กร (mobile computing and teleworking)

๑๒.๓ การควบคุมอุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่ ต้องกำหนดข้อปฏิบัติและมาตรการที่เหมาะสมเพื่อปกป้องสารสนเทศจากความเสี่ยงของการใช้อุปกรณ์คอมพิวเตอร์และสื่อสารเคลื่อนที่

๑๒.๔ การปฏิบัติงานจากภายนอกสำนักงาน (teleworking) ต้องกำหนดข้อปฏิบัติ แผนงาน และขั้นตอนปฏิบัติเพื่อปรับใช้สำหรับการปฏิบัติงานขององค์กรจากภายนอกสำนักงาน

ข้อ ๑๓ จัดทำระบบสำรองสำหรับระบบสารสนเทศ ตามแนวทางต่อไปนี้

๑๓.๑ ต้องพิจารณาคัดเลือกและจัดทำระบบสำรองที่เหมาะสมให้อยู่ในสภาพพร้อมใช้งานที่เหมาะสม

๑๓.๒ ต้องจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานระบบสารสนเทศได้ตามปกติอย่างต่อเนื่อง โดยต้องปรับปรุงแผนเตรียมความพร้อมกรณีฉุกเฉินดังกล่าวให้สามารถปรับใช้ได้อย่างเหมาะสมและสอดคล้องกับการใช้งานตามภารกิจ

๑๓.๓ ต้องมีการกำหนดหน้าที่และความรับผิดชอบของบุคลากรซึ่งดูแลรับผิดชอบระบบสารสนเทศ ระบบสำรอง และจัดทำแผนเตรียมพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

๑๓.๔ ต้องมีการทดสอบสภาพพร้อมใช้งานระบบสารสนเทศ ระบบสำรอง และระบบแผนเตรียมพร้อมกรณีฉุกเฉินอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง

๑๓.๕ มีการปฏิบัติและทบทวนแนวทางการจัดทำระบบสำรอง อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๔ กำหนดให้มีการตรวจสอบและประเมินความเสี่ยงด้านระบบสารสนเทศที่อาจเกิดขึ้นกับระบบสารสนเทศ อย่างน้อยปีละ ๑ ครั้ง

ข้อ ๑๕ กรณีระบบคอมพิวเตอร์หรือข้อมูลระบบสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน หรือผู้ใดผู้หนึ่ง อันเนื่องมาจากความบกพร่องละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๑๖ องค์ประกอบของนโยบาย จัดทำเป็นมาตรฐานด้านการบริหารรักษาความมั่นคงปลอดภัยของระบบสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน โดยอ้างอิงรายละเอียดแนวปฏิบัติจากเอกสารแนบท้ายประกาศ เรื่อง “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน พ.ศ. ๒๕๖๒” เพื่อใช้เป็นแนวทางในการดำเนินงานด้วยวิธีการทางอิเล็กทรอนิกส์ให้มีความมั่นคงปลอดภัยเชื่อถือได้ และเป็นไปตามกฎหมายและระเบียบที่เกี่ยวข้อง ซึ่งเจ้าหน้าที่ของสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน และหน่วยงานภายนอกต้องถือปฏิบัติตามอย่างเคร่งครัด

ข้อ ๑๗ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ประกาศ ณ วันที่ ๑๔ สิงหาคม พ.ศ. ๒๕๖๒

(นายธนธัช จังพานิช)
ผู้จัดการสำนักงานบริหารกองทุนเพื่อส่งเสริมการอนุรักษ์พลังงาน