ประกาศสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ
เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
พ.ศ. ๒๕๕๕

ด้วยคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ได้มีประกาศเรื่องแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงานของรัฐ พ.ศ. ๒๕๕๓ ลงในราชกิจจานุเบกษา เมื่อวันที่ ๒๓ มิถุนายน พ.ศ. ๒๕๕๓ ข้อ ๒ กำหนดให้ หน่วยงานของรัฐต้องจัดให้มีนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศเป็นลายลักษณ์อักษร พร้อมทั้งต้องจัดทำข้อปฏิบัติที่สอดคล้องกับนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของหน่วยงาน เพื่อให้การดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐหรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล

สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจซึ่งเป็นหน่วยงานของรัฐจึงได้มีการจัดทำแนวนโยบายและแนวปฏิบัติการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศ เพื่อให้เป็นไปตามข้อกำหนดของประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าว ดังต่อไปนี้

ข้อ ๑ ประกาศนี้เรียกว่า “ประกาศสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ เรื่อง นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๕๕”

ข้อ ๒ ประกาศนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศ เป็นต้นไป

ข้อ ๓ ในประกาศนี้

“นโยบาย” หมายความว่า นโยบายการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ พ.ศ. ๒๕๕๕

/“สำนักงาน...

“สำนักงาน” หมายความว่า สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ

“ผู้อำนวยการ” หมายความว่า ผู้อำนวยการสำนักงาน

“ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ” หมายความว่า รองผู้อำนวยการสำนักงานหรือผู้ที่ได้รับแต่งตั้งให้เป็นผู้ดำรงตำแหน่งเป็นผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศ (CIO) ของสำนักงาน

“ผู้บริหาร” หมายความว่า ผู้อำนวยการ ที่ปรึกษา รองผู้อำนวยการ ผู้อำนวยการสำนัก ผู้อำนวยการศูนย์ เลขานุการกรม

“คณะกรรมการ” หมายความว่า คณะกรรมการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของสำนักงาน

“เจ้าหน้าที่” หมายความว่า ข้าราชการ ลูกจ้างประจำ ลูกจ้างชั่วคราว พนักงานราชการ และเจ้าหน้าที่ประจำโครงการของสำนักงาน

“ผู้ใช้งาน” หมายความว่า เจ้าหน้าที่และหน่วยงานภายนอกที่มีสิทธิเข้าถึงสินทรัพย์ประเภทข้อมูลสารสนเทศ

“สินทรัพย์” หมายความว่า สิ่งที่มีคุณค่าหรือมูลค่าต่อสำนักงานและเป็นสิ่งที่เกี่ยวข้องกับการประมวลผลสารสนเทศที่สำนักงานเป็นเจ้าของหรือผู้ถือลิขสิทธิ์หรือสิทธิการใช้งานอย่างถูกต้องตามกฎหมาย ซึ่งรวมถึงทรัพย์สินทางปัญญา ไม่ว่าจะได้มาจากการเช่า การว่าจ้าง การพัฒนาหรือการจัดซื้อ ได้แก่ข้อมูลสารสนเทศ (Information Asset) ด้านกายภาพ (Physical Asset) ด้านซอฟท์แวร์ (Software Asset) การบริการและกระบวนการ (Services and Processes Asset) และบุคลากร (People Asset)

“ข้อมูลสารสนเทศ” หมายความว่า ข้อมูล (Data) หรือสารสนเทศ (Information) ที่อยู่ในรูปของอิเล็กทรอนิกส์หรือเอกสาร ไม่ว่าจะเป็นแฟ้มข้อมูล (File) หรือฐานข้อมูล (Database) หรือเอกสารที่มีการแปลงให้อยู่ในรูปแบบอิเล็กทรอนิกส์ (e-Document)

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิในการเข้าถึงระบบปฏิบัติการ สิทธิการใช้โปรแกรมระบบงานคอมพิวเตอร์ สิทธิการใช้งานเครือข่าย รวมถึงสิทธิที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

“หน่วยงานภายนอก” หมายความว่า บุคคลจากหน่วยงานราชการหรือบุคคลจากหน่วยงานราชการอื่น หรือบุคคลจากบริษัทที่สำนักงาน อนุญาตให้มีสิทธิในการเข้าถึงและใช้งานข้อมูลหรือสินทรัพย์ต่างๆ ของหน่วยงาน โดยจะได้สิทธิในการใช้ระบบตามอำนาจหน้าที่และต้องรับผิดชอบในการรักษาความลับของข้อมูล

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิ

/หรือการ...

หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับหน่วยงานภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“ความมั่นคงปลอดภัยด้านสารสนเทศ” (information security) หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)” หมายความว่า เหตุการณ์ที่เกิดขึ้นแล้วหรือเหตุการณ์ที่เป็นจุดอ่อนหรือสงสัยว่าเป็นจุดอ่อน ที่เกิดกับสินทรัพย์ ซึ่งจะสร้างความเสียหายให้กับสำนักงานในลักษณะใดลักษณะหนึ่ง

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident)” หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Unwanted or unexpected) ซึ่งอาจทำให้ระบบของสำนักงานถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

ข้อ ๔ ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามประกาศนี้ ให้คณะกรรมการเป็นผู้วินิจฉัยชี้ขาดและนำเสนอผู้อำนวยการเพื่ออนุมัติ

หมวด ๑
คณะกรรมการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ
(IT Security Committee)

ข้อ ๕ ให้มีคณะกรรมการคณะหนึ่ง เรียกว่า “คณะกรรมการด้านความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศ” ประกอบด้วย ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศของสำนักงาน เป็นประธานกรรมการ ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศของสำนักงานเป็นกรรมการและเลขานุการ และผู้บริหารของสำนักงานซึ่งผู้อำนวยการเป็นผู้แต่งตั้งอีกไม่เกิน ๕ คน เป็นกรรมการ

หมวด ๒
การจัดการนโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศ
(Information Technology Security Policy)

ข้อ ๖ นโยบายป้องกันและรักษาความปลอดภัยเทคโนโลยีสารสนเทศของสำนักงาน

โดยคณะกรรมการ มีหน้าที่ทบทวน กลั่นกรอง และนำเสนอผู้อำนวยการอนุมัติประกาศใช้

สำนักงานจะกำหนดทิศทางความปลอดภัยด้านเทคโนโลยีสารสนเทศของสำนักงาน โดยอ้างอิงมาตรฐานสากล ได้แก่ ISO ๒๗๐๐๑ และเป็นไปตามพระราชบัญญัติว่าด้วยการประกอบธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๔๔ พระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ พระราชกฤษฎีกาว่าด้วยวิธีการแบบปลอดภัยในการทำธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. ๒๕๕๓ พร้อมกับกำหนดข้อปฏิบัติที่เป็นไปตามนโยบายนี้

เพื่อให้บรรลุนโยบายนี้ ให้คณะกรรมการกำหนดแผนงานปฏิบัติประจำปี และมีการจัดการเผยแพร่ อบรม สื่อสารให้ผู้บริหารและเจ้าหน้าที่รับทราบ ยอมรับ และปฏิบัติ เพื่อให้ระบบเทคโนโลยีสารสนเทศของสำนักงานมีความมั่นคง ปลอดภัย โดยมีกระบวนการตรวจสอบ สอบทาน ประเมินผลการปฏิบัติที่โปร่งใส เป็นที่ยอมรับและเชื่อถือได้ พร้อมทั้งมีการปรับปรุงเนื้อหาของนโยบายตามระยะเวลาที่เหมาะสม เพื่อให้สอดคล้องกับการเปลี่ยนแปลงและแนวโน้มของความเสี่ยงที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงาน การมีรายชื่อและข้อมูลสำหรับการติดต่อกับหน่วยงานอื่นและกลุ่มที่มีความรู้ ความสนใจเรื่องความมั่นคงปลอดภัยด้านสารสนเทศ

หมวด ๓
โครงสร้างทางด้านความมั่นคงปลอดภัยสำหรับสำนักงาน
(Organization of Information Security)

ข้อ ๗ ให้คณะกรรมการจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศเพื่อลดความเสี่ยงด้านสารสนเทศภายในสำนักงาน โดยกำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ การกำหนดหน้าที่ความรับผิดชอบด้านความมั่นคงปลอดภัย การประสานงานความมั่นคงปลอดภัยด้านสารสนเทศภายในสำนักงาน กระบวนการอนุมัติการใช้งานอุปกรณ์ประมวลผลสารสนเทศ การลงนามมิให้เปิดเผยข้อมูลสารสนเทศที่เป็นความลับของสำนักงาน และกำหนดให้คณะกรรมการและ/หรือผู้ตรวจสอบอิสระ ทำหน้าที่ทบทวนความมั่นคงปลอดภัยเทคโนโลยีสารสนเทศของสำนักงาน

ข้อ ๘ ให้คณะกรรมการจัดการด้านความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศที่เกี่ยวข้องกับรัฐวิสาหกิจหรือหน่วยงานภายนอก เพื่อลดความเสี่ยงด้านสารสนเทศจากภัยคุกคามภายนอก โดยกำหนดให้มีการบริหารจัดการความมั่นคงปลอดภัยด้านสารสนเทศ และอุปกรณ์ประมวลผลสารสนเทศของสำนักงานที่มีการเข้าถึง

/หรือใช้...

หรือใช้ในการประมวลผลหรือใช้ในการติดต่อสื่อสารกับรัฐวิสาหกิจหรือหน่วยงานภายนอก ซึ่งครอบคลุมเรื่องการประเมินความเสี่ยงของการเข้าถึงสารสนเทศโดยหน่วยงานภายนอก ทั้งทางกายภาพ (Physical Access) และจากระยะไกล (Remote Access) การระบุและจัดทำข้อกำหนดสำหรับหน่วยงานภายนอกที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศของสำนักงานและการระบุข้อกำหนดสำหรับผู้ใช้บริการที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ

หมวด ๔

การบริหารจัดการสินทรัพย์ของสำนักงาน (Asset Management)

ข้อ ๙ ให้กำหนดมาตรการที่เหมาะสมเพื่อป้องกันสินทรัพย์ของสำนักงาน โดยให้สอดคล้องกับผลการประเมินความเสี่ยงด้านสารสนเทศและเป็นไปตามกฎหมายลิขสิทธิ์

ข้อ ๑๐ ให้คณะกรรมการกำหนดผู้ดูแลรับผิดชอบสินทรัพย์ของสำนักงานเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น โดยครอบคลุมเรื่องการจัดทำทะเบียนบัญชีสินทรัพย์ การระบุผู้เป็นเจ้าของสินทรัพย์และการควบคุมการใช้งานสินทรัพย์ให้เหมาะสมสอดคล้องกับนโยบาย มาตรฐาน และขั้นตอนการปฏิบัติงานที่เกี่ยวกับความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๑๑ ให้มีการจัดหมวดหมู่สารสนเทศและกำหนดระดับการป้องกันสารสนเทศให้เหมาะสม รวมถึงการกำหนดแนวทางการจัดทำรายละเอียดข้อมูลเพื่อบ่งชี้ถึงสารสนเทศ การป้องกันการเข้าถึงและวิธีการสื่อสารที่ปลอดภัย

หมวด ๕

ความมั่นคงปลอดภัยที่เกี่ยวข้องกับบุคลากร (Human Resources Security)

ข้อ ๑๒ ให้กำหนดมาตรการกลั่นกรองก่อนรับเจ้าหน้าที่เข้ามาปฏิบัติงานในสำนักงาน (Prior to Employment) รวมถึงการว่าจ้างบุคลากรจากภายนอกหรือผู้รับจ้างเพื่อลดความเสี่ยงจากการโจรกรรมสินทรัพย์ การฉ้อโกงและการใช้งานอุปกรณ์ผิดวัตถุประสงค์

ข้อ ๑๓ ให้มีการสร้างความรู้ ความเข้าใจให้เจ้าหน้าที่ บุคลากรหรือผู้รับจ้างจากภายนอกตลอดจนหน่วยงานภายนอกที่สำนักงานใช้บริการเพื่อให้ตระหนักถึงภัยคุกคามด้านความมั่นคงปลอดภัย

ของสารสนเทศและให้ความสำคัญในการป้องกันภัยคุกคาม รวมถึงหน้าที่ ความรับผิดชอบและภาระผูกพันตามกฎหมาย เพื่อลดความเสี่ยงจากความผิดพลาดในระหว่างการปฏิบัติงาน (During Employment)

ข้อ ๑๔ ให้กำหนดมาตรการรวมถึงขั้นตอนที่ชัดเจน เมื่อมีการเปลี่ยนแปลงหน้าที่งานหรือสิ้นสภาพการจ้างงานหรือหมดสัญญาจ้างของเจ้าหน้าที่ บุคลากรหรือผู้รับจ้างจากภายนอก รวมถึงการยกเลิกสัญญา เพื่อให้ทราบถึงหน้าที่ความรับผิดชอบเมื่อสิ้นสุดการจ้างงานหรือเมื่อมีการเปลี่ยนแปลงหน้าที่งาน (Termination or Change of Employment)

หมวด ๖
การสร้างความมั่นคงปลอดภัยทางกายภาพและสิ่งแวดล้อม
(Physical and Environmental Security)

ข้อ ๑๕ ให้กำหนดมาตรการการรักษาความปลอดภัยด้านกายภาพและสภาพแวดล้อมของสถานที่ที่ใช้ในการปฏิบัติงาน การประมวลผล และการจัดเก็บข้อมูลสารสนเทศของสำนักงานให้เหมาะสม และสอดคล้องกับผลการประเมินความเสี่ยงด้านสารสนเทศ เพื่อป้องกันการเข้าถึงทางกายภาพโดยไม่ได้รับอนุญาต และเป็นการป้องกันความเสียหายและการรบกวนสินทรัพย์ของสำนักงาน ทั้งนี้ให้รวมถึงมาตรการป้องกันภัยคุกคามจากภัยธรรมชาติด้วย

ข้อ ๑๖ ให้กำหนดมาตรการการป้องกันสินทรัพย์ของสำนักงานจากการสูญหาย ความเสียหาย การถูกโจรกรรมหรือถูกเปิดเผยโดยไม่ได้รับอนุญาต รวมถึงการทำให้การดำเนินงานของสำนักงานเกิดอุปสรรคติดขัดหรือหยุดดำเนินการ ทั้งนี้ให้ครอบคลุมถึงการติดตั้งอุปกรณ์และระบบคอมพิวเตอร์ การจัดการระบบและอุปกรณ์สนับสนุนที่เหมาะสม รวมทั้งการตรวจสอบและการบำรุงรักษาอุปกรณ์อย่างต่อเนื่อง ตลอดจนมาตรการทำลายข้อมูลสารสนเทศที่อยู่ในสื่อบันทึกที่ยกเลิกการใช้งานแล้ว เพื่อป้องกันไม่ให้ผู้อื่นเข้าถึงข้อมูลได้และมาตรการการควบคุมดูแลที่ชัดเจนในกรณีที่มีการนำสินทรัพย์ของสำนักงานออกนอกสถานที่

หมวด ๗
การบริหารจัดการด้านการสื่อสารและการดำเนินงานสารสนเทศของสำนักงาน
(Communications and Operations Management)

ข้อ ๑๗ ให้กำหนดหน้าที่ความรับผิดชอบและขั้นตอนการปฏิบัติงานที่เกี่ยวข้องกับการประมวลผลสารสนเทศให้เป็นไปอย่างถูกต้องเหมาะสม ปลอดภัยและเป็นปัจจุบัน เพื่อลดความเสี่ยงจากการปฏิบัติงาน และสามารถใช้เป็นเอกสารอ้างอิงสำหรับการประเมินการตรวจสอบภายใน (Internal Audit) ได้ด้วย

/ข้อ ๑๘...

ข้อ ๑๘ ให้มีการกำหนดมาตรการการควบคุมและการตรวจสอบการให้บริการของหน่วยงานภายนอก ทั้งนี้ให้เป็นตามข้อตกลงระหว่างสำนักงานกับหน่วยงานภายนอก

ข้อ ๑๙ ให้มีการวางแผนการนำระบบเทคโนโลยีสารสนเทศมาใช้ในสำนักงานและกำหนดเกณฑ์การตรวจรับระบบที่จัดทำขึ้นใหม่ ระบบที่มีการปรับปรุงประสิทธิภาพและกำหนดเกณฑ์สำหรับการตรวจสอบระบบที่อยู่ระหว่างการพัฒนา เพื่อลดความเสี่ยงที่เกิดจากความล้มเหลวในการนำระบบไปใช้งานจริง (Production System)

ข้อ ๒๐ ให้กำหนดข้อห้ามการติดตั้งโปรแกรมหรือระบบสารสนเทศที่ไม่ได้รับอนุญาต การกำหนดมาตรการ หลักเกณฑ์ การควบคุมและการตรวจสอบการรับข้อมูลหรือไฟล์ที่ส่งจากภายนอกเข้ามายังผู้ใช้งานภายในสำนักงาน การติดตั้งอุปกรณ์หรือโปรแกรมหรือระบบสารสนเทศเพื่อป้องกันโปรแกรมที่ไม่ประสงค์ดีประเภทต่างๆ เพื่อปกป้องและรักษาสินทรัพย์ของสำนักงานให้มีความปลอดภัย รวมถึงข้อปฏิบัติและกำหนดผู้รับผิดชอบเมื่อเกิดความเสียหายจากโปรแกรมไม่ประสงค์ดี

ข้อ ๒๑ ให้กำหนดมาตรการการสำรอง (Backup) ข้อมูลสารสนเทศ โดยกำหนดวิธีการ (การสำรองข้อมูลแบบเต็ม (full backup) หรือการสำรองข้อมูลแบบส่วนต่าง (incremental backup)) ขั้นตอนการปฏิบัติ สถานที่จัดเก็บและผู้รับผิดชอบการสำรอง (Backup) ข้อมูลสารสนเทศแต่ละประเภทให้เหมาะสม รวมถึงการทดสอบการกู้คืนข้อมูลที่ได้สำรองไว้ เพื่อให้มั่นใจได้ว่าข้อมูลสารสนเทศที่ได้สำรองไว้สามารถนำกลับมาใช้งานได้เมื่อต้องการ

ข้อ ๒๒ ให้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยของข้อมูลในระบบเครือข่าย และอุปกรณ์ที่สนับสนุนการทำงาน เพื่อป้องกันการเข้าถึงข้อมูลที่ส่งผ่านระบบเครือข่ายโดยไม่ได้รับอนุญาต รวมถึง การจัดเก็บข้อมูลจราจรทางคอมพิวเตอร์ (Traffic Log) เพื่อการตรวจสอบ

ข้อ ๒๓ ให้กำหนดมาตรการการดูแลและจัดการสื่อ (Media) ที่ใช้บันทึกข้อมูลต่างๆ เพื่อป้องกันการเปิดเผย การแก้ไข การเปลี่ยนแปลง การลบหรือการทำลายโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อการสูญหายหรือข้อมูลความลับรั่วไหลและป้องกันไม่ให้การปฏิบัติงานของสำนักงานหยุดชะงัก

ข้อ ๒๔ ให้กำหนดมาตรการการแลกเปลี่ยนข้อมูลสารสนเทศและโปรแกรมที่ใช้ภายในสำนักงานหรือระหว่างสำนักงานกับหน่วยงานภายนอกที่ชัดเจน เพื่อลดความเสี่ยงข้อมูลสารสนเทศรั่วไหลและป้องกันการดักรับข้อมูลสารสนเทศระหว่างทาง

ข้อ ๒๕ ในกรณีมีการทำธุรกรรมผ่านระบบเครือข่าย (On-line Transaction) หรือการให้บริการพาณิชย์อิเล็กทรอนิกส์ (e-commerce Services) ให้กำหนดมาตรการการรักษาความมั่นคงปลอดภัยในการใช้งานและการเก็บข้อมูลสารสนเทศเพื่อการตรวจสอบหรืออ้างอิงได้

/ข้อ ๒๖...

ข้อ ๒๖ ให้กำหนดมาตรการการตรวจสอบและการเฝ้าระวัง (Monitoring) การใช้งานสารสนเทศของสำนักงาน เพื่อป้องกันการประมวลผลหรือการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาตและให้เป็นไปตามขอบเขตของกฎหมาย

หมวด ๘

การควบคุมการเข้าถึง (Access Control)

ข้อ ๒๗ ให้กำหนดมาตรการเพื่อการควบคุมการเข้าถึงข้อมูลสารสนเทศแต่ละประเภทให้เหมาะสม เพื่อป้องกันการเข้าถึง การล่วงรู้ การแก้ไขหรือการลักลอบนำไปใช้โดยไม่ได้รับอนุญาต โดยให้ครอบคลุมการเข้าถึงสถานที่เก็บหรือสถานที่ประมวลผลสารสนเทศด้วย

ข้อ ๒๘ ให้กำหนดวิธีการบริหารจัดการการเข้าถึงข้อมูลสารสนเทศและระบบสารสนเทศของผู้ใช้งาน (User Access Management) แต่ละประเภทและแต่ละระบบให้เหมาะสมและตรวจสอบได้ เพื่อป้องกันการเข้าถึงโดยผู้ไม่ได้รับอนุญาต โดยครอบคลุมถึงการลงทะเบียน การจัดการสิทธิผู้ใช้งาน รหัสผ่าน และให้มีการทบทวนสิทธิเป็นระยะ เพื่อให้มั่นใจว่าสอดคล้องกับภาระหน้าที่ความรับผิดชอบและความจำเป็นในการใช้งาน

ข้อ ๒๙ ให้กำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities) และสร้างความตระหนักถึงการไม่เปิดโอกาสในการเข้าถึงข้อมูลสารสนเทศของผู้อื่นโดยไม่ได้รับอนุญาต เพื่อลดความเสี่ยงต่อการลักลอบการเข้าถึงข้อมูลสารสนเทศ โดยผ่านการใช้สิทธิของผู้ใช้งานอื่น

ข้อ ๓๐ ให้กำหนดมาตรการการเข้าถึงเครือข่าย (Network Access Control) และการใช้บริการผ่านเครือข่ายและการเชื่อมต่อเครือข่ายทั้งจากภายในสำนักงานหรือจากภายนอกสำนักงาน เพื่อป้องกันการเข้าถึงข้อมูลสารสนเทศหรือระบบสารสนเทศของสำนักงานโดยไม่ได้รับอนุญาต

ข้อ ๓๑ ให้กำหนดมาตรการการเข้าถึงระบบปฏิบัติการ (Operating System Access Control) เพื่อป้องกันการใช้งานอุปกรณ์เพื่อการเข้าถึงข้อมูลสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๓๒ ให้กำหนดมาตรการการเข้าถึงโปรแกรมและระบบสารสนเทศของสำนักงาน (Application and Information Access Control) เพื่อป้องกันการเข้าถึงโดยไม่ได้รับอนุญาต

ข้อ ๓๓ ให้กำหนดมาตรการการใช้งานสื่อบันทึกข้อมูลหรืออุปกรณ์ประมวลผลสารสนเทศชนิดพกพาได้ (External Storage or Mobile Computing) และการปฏิบัติงานจากภายนอกสำนักงาน (Teleworking) เพื่อลดความเสี่ยงต่อการสูญหายหรือการรั่วไหลของข้อมูลสารสนเทศและป้องกันโปรแกรมไม่ประสงค์ดีที่ติดมาจากภายนอกสำนักงาน

/หมวด ๙...

หมวด ๙

การจัดหา การพัฒนา และการบำรุงรักษาระบบสารสนเทศ

(Information Systems Acquisition, Development and Maintenance)

ข้อ ๓๔ ให้มีการระบุข้อกำหนดด้านความมั่นคงปลอดภัยด้านสารสนเทศไว้เป็นส่วนหนึ่งในการจัดหา การพัฒนาและการบำรุงรักษาระบบสารสนเทศ เพื่อให้มั่นใจว่าระบบสารสนเทศที่ต้องการมีความมั่นคงปลอดภัยเพียงพอ

ข้อ ๓๕ ให้มีการระบุวิธีการและขั้นตอนการประมวลผลสารสนเทศ พร้อมการควบคุมที่เหมาะสม เพื่อป้องกันการประมวลผลผิดพลาด การสูญหายของข้อมูลสารสนเทศ การเปลี่ยนแปลงระบบสารสนเทศโดยไม่ได้รับอนุญาตหรือการใช้งานระบบสารสนเทศผิดวัตถุประสงค์

ข้อ ๓๖ ให้กำหนดมาตรการการเข้ารหัสข้อมูล (Cryptographic Control) ในข้อมูลสารสนเทศที่สำคัญ และสามารถยืนยันตัวตนของผู้ส่งได้ เพื่อรักษาความลับและความถูกต้องของข้อมูลสารสนเทศ

ข้อ ๓๗ ให้กำหนดมาตรการการสร้างความมั่นคงปลอดภัยของแฟ้มข้อมูลระบบสารสนเทศ (System Files or Application Source Codes) ทั้งในระยะการพัฒนา ระยะทดสอบ ระยะนำไปใช้งาน ระยะการปรับปรุง เพื่อให้มั่นใจได้ว่าระบบสารสนเทศที่นำมาใช้งานนั้นถูกต้องเป็นไปตามความต้องการ และมีการควบคุมและป้องกันการเข้าถึงแฟ้มข้อมูลระบบสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๓๘ ให้กำหนดวิธีการและขั้นตอนการปฏิบัติงานและการอนุมัติสำหรับการเปลี่ยนแปลงในกระบวนการพัฒนาระบบสารสนเทศ (Change Control Procedure) พร้อมกระบวนการทดสอบก่อนนำไปใช้งาน เพื่อลดผลกระทบและปัญหาที่อาจเกิดขึ้น

ข้อ ๓๙ ให้มีการบริหารจัดการเพื่อหาจุดอ่อนหรือช่องโหว่ทางด้านเทคนิค (Technical Vulnerability) ทั้งในระดับอุปกรณ์คอมพิวเตอร์ (Hardware Equipment) และโปรแกรมระบบ (Software) เพื่อลดความเสี่ยงจากการโจมตีจากผู้ไม่ประสงค์ดี

หมวด ๑๐

การบริหารจัดการเหตุการณ์ที่เกี่ยวข้องกับความมั่นคงปลอดภัยของสำนักงาน

(Information Security Incident Management)

ข้อ ๔๐ ให้กำหนดมาตรการการสื่อสาร การรายงานและการดำเนินการที่เหมาะสม ภายในเวลาที่กำหนดเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยหรือช่องโหว่ที่กระทบต่อความมั่นคงปลอดภัยด้านสารสนเทศ

/เพื่อให้มั่นใจ...

เพื่อให้มั่นใจได้ว่าเหตุการณ์ดังกล่าวได้รับการตรวจพบและดำเนินการแก้ไขอย่างถูกต้อง รวดเร็ว

ข้อ ๔๑ ให้มีการบริหารจัดการและการปรับปรุงแก้ไขเหตุการณ์ด้านความมั่นคงปลอดภัยทุกประเภท ได้แก่ ความล้มเหลวของการประมวลผลสารสนเทศ (Failure of Processing) ผลกระทบจากโปรแกรมไม่ประสงค์ดี (Malicious Code) การปฏิเสธการให้บริการ (Denial of Service) การละเมิดความลับและความถูกต้องสมบูรณ์ (Breaches of Confidentiality and Integrity) การใช้ระบบสารสนเทศผิดวัตถุประสงค์ (misuse of Information System) รวมไปถึงสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (Information security incident) เพื่อให้มั่นใจได้ว่าสำนักงาน จะสามารถดำเนินการตอบสนองต่อเหตุการณ์ได้อย่างเหมาะสม มีการควบคุมที่เป็นไปตามขั้นตอนและเป็นไปตามขอบเขตของกฎหมาย

หมวด ๑๑
การบริหารความต่อเนื่องในการดำเนินงานของสำนักงาน
(Business Continuity Management)

ข้อ ๔๒ ให้สำนักงานมีการบริหารความต่อเนื่องในการดำเนินงานของสำนักงาน (Business Continuity Management) เพื่อลดความเสี่ยงในกรณีเกิดเหตุการณ์ที่ไม่พึงประสงค์หรือภัยพิบัติที่ส่งผลกระทบต่อการดำเนินงานโดยปกติของสำนักงาน ทั้งนี้ ให้คณะกรรมการกำหนดมาตรการรองรับความเสี่ยงและแนวทางการดำเนินการจำกัดความเสียหายและการกู้คืนระบบสารสนเทศที่สำคัญหรือจำเป็นโดยให้ครอบคลุมการประเมินความเสี่ยง (Risk Assessment) การวิเคราะห์ผลกระทบต่อการดำเนินงาน (Business Impact Analysis) แผนงานและกระบวนการในการสร้างความต่อเนื่องกับการดำเนินงานของสำนักงาน (Business Continuity Planning) แผนงานและกระบวนการกู้คืนระบบสารสนเทศ (Disaster Recovery Planning) ทั้งนี้ กำหนดให้มีการทดสอบและปรับปรุงแผนต่างๆ อย่างน้อยปีละ ๑ ครั้ง หรือตามความเหมาะสมและสอดคล้องกับระดับความเสี่ยง

หมวด ๑๒
การปฏิบัติตามข้อกำหนด (Compliance)

ข้อ ๔๓ ให้มีการรวบรวมพระราชบัญญัติ พระราชกำหนด พระราชกฤษฎีกา กฎหมาย ระเบียบปฏิบัติหรือประกาศ รวมถึงสัญญาต่างๆ ที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้านสารสนเทศ และควบคุมเพื่อให้มีการปฏิบัติตามข้อกฎหมาย (Compliance with Legal Requirements) เพื่อหลีกเลี่ยงการละเมิดที่ทำให้เข้าข่ายการกระทำผิด

ข้อ ๔๔ ให้ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศของสำนักงานควบคุมดูแลให้เจ้าหน้าที่ปฏิบัติตามนโยบาย มาตรฐาน ระเบียบปฏิบัติและข้อกำหนดด้านเทคนิคที่เกี่ยวข้องกับความมั่นคงปลอดภัยด้าน

สารสนเทศ (Compliance with Security Policies, Standards, Procedures and Technical Compliance) เพื่อให้มั่นใจได้ว่าการใช้ระบบสารสนเทศของสำนักงานมีความมั่นคงปลอดภัย สอดคล้องกับนโยบายและมีความเป็นมาตรฐานสากล

ข้อ ๔๕ พิจารณากำหนดให้มีการตรวจประเมินระบบสารสนเทศ (Information System Audit Considerations) อย่างน้อย ๑ ครั้งต่อปี โดยผู้ตรวจสอบภายในหรือผู้ตรวจสอบที่เป็นอิสระภายนอก เพื่อให้มั่นใจได้ว่าการตรวจประเมินมีประสิทธิภาพและผลการตรวจสอบเป็นที่น่าเชื่อถือได้ ทั้งนี้ ต้องก่อให้เกิดการรบกวนการปฏิบัติงานหรือเป็นอุปสรรคต่อการดำเนินงานของสำนักงานน้อยที่สุด

ข้อ ๔๖ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหาย หรืออันตรายใด ๆ แก่สำนักงานหรือผู้หนึ่งผู้ใด อันเนื่องมาจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายและข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ ให้ผู้บริหารระดับสูงด้านเทคโนโลยีสารสนเทศเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

หมวด ๑๓
การขอยกเว้นการไม่ปฏิบัติตามนโยบาย

ข้อ ๔๗ หากมีความจำเป็นที่สำนักงานไม่สามารถปฏิบัติตามนโยบายหรือมาตรฐานการปฏิบัติงาน หรือหากเทคโนโลยีที่มีอยู่ไม่อำนวยต่อการปฏิบัติ ให้คณะกรรมการพิจารณาและนำเสนอขออนุมัติการไม่ปฏิบัติตามในส่วนดังกล่าวต่อผู้อำนวยการ ทั้งนี้ หน่วยงานผู้ร้องขอการยกเว้น จะต้องดำเนินการเพื่อนำเสนอต่อคณะกรรมการ ดังต่อไปนี้

(๑) วิเคราะห์ประโยชน์ที่จะได้รับในแต่ละทางเลือก และความเสี่ยงหรือผลกระทบที่อาจเกิดขึ้นต่อการไม่ปฏิบัติตาม รวมทั้งจัดทำเอกสารที่ระบุหลักการและเหตุผลหรือเอกสารหลักฐานที่สนับสนุนการตัดสินใจไม่ปฏิบัติตาม

(๒) พิจารณานำเสนอการควบคุมทดแทน (Compensated Control) เพื่อลดความเสี่ยงที่อาจเกิดขึ้นจากการไม่ปฏิบัติตาม โดยอาจจัดให้มีระเบียบหรือประกาศเฉพาะกาลเพื่อใช้ยกเว้นเป็นรายกรณี

ประกาศ ณ วันที่ ๒๑ ธันวาคม ๒๕๕๕

(นายประสงค์ พูนธเนศ)
ผู้อำนวยการสำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ