ระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ
ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๖๓

โดยที่เป็นการสมควรปรับปรุงระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านระบบสารสนเทศ

อาศัยอำนาจตามความในมาตรา ๑๕ (๔) แห่งพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ ผู้อำนวยการสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ จึงออกระเบียบไว้ดังต่อไปนี้

ข้อ ๑ ระเบียบนี้เรียกว่า "ระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๓"

ข้อ ๒ ระเบียบนี้ให้ใช้บังคับตั้งแต่วันถัดจากวันประกาศเป็นต้นไป

ข้อ ๓ ให้ยกเลิกระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ พ.ศ. ๒๕๖๐ ระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับที่ ๒) พ.ศ. ๒๕๖๑ และระเบียบสำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ว่าด้วยแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ (ฉบับที่ ๓) พ.ศ. ๒๕๖๒

บรรดาระเบียบ คำสั่ง หรือประกาศอื่นใดในส่วนที่กำหนดไว้แล้วในระเบียบนี้ หรือที่ขัดหรือแย้งกับระเบียบนี้ ให้ใช้ระเบียบนี้แทน

ข้อ ๔ ให้ผู้อำนวยการเป็นผู้รักษาการตามระเบียบนี้ และให้มีอำนาจออกคำสั่งหรือประกาศกำหนดหลักเกณฑ์หรือวิธีการปฏิบัติเพื่อให้เป็นไปตามระเบียบนี้

ในกรณีที่มีปัญหาเกี่ยวกับการปฏิบัติตามระเบียบนี้ ให้ผู้อำนวยการเป็นผู้มีอำนาจวินิจฉัยชี้ขาด และคำวินิจฉัยชี้ขาดให้ถือเป็นที่สุด

หมวด ๑
บททั่วไป

ข้อ ๕ ในระเบียบนี้

“สำนักงาน” หมายความว่า สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

“หน่วยงานเฉพาะทาง” หมายความว่า ศูนย์พันธุวิศวกรรมและเทคโนโลยีชีวภาพแห่งชาติ ศูนย์เทคโนโลยีโลหะและวัสดุแห่งชาติ ศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ หรือหน่วยงานเฉพาะทางอื่นที่จัดตั้งขึ้นตามมาตรา ๕ (๕) แห่งพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ และให้หมายความรวมถึงศูนย์บริหารจัดการเทคโนโลยีและสถาบันการจัดการเทคโนโลยีนวัตกรรมเกษตร

“คณะกรรมการบริหารเทคโนโลยีสารสนเทศ” หมายความว่า คณะกรรมการบริหารเทคโนโลยีสารสนเทศและการสื่อสารของสำนักงาน

“คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉิน” หมายความว่า คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินด้านสารสนเทศและระบบสารสนเทศของสำนักงาน

“ผู้อำนวยการ” หมายความว่า ผู้อำนวยการสำนักงาน

“พนักงาน” หมายความว่า บุคคลที่สำนักงานบรรจุและแต่งตั้งเป็นพนักงานของสำนักงาน

“พนักงานโครงการ” หมายความว่า ลูกจ้างตามพระราชบัญญัติพัฒนาวิทยาศาสตร์และเทคโนโลยี พ.ศ. ๒๕๓๔ ที่สำนักงานบรรจุและแต่งตั้งเป็นพนักงานโครงการของสำนักงานให้ปฏิบัติงานเป็นการชั่วคราวหรือปฏิบัติงานที่มีกำหนดระยะเวลาเริ่มต้นและสิ้นสุดแน่นอน

“หน่วยบริการเทคโนโลยีสารสนเทศ” หมายความว่า ส่วนงานระดับงานหรือระดับฝ่ายของสำนักงานที่มีหน้าที่ในการให้บริการระบบสารสนเทศ และให้หมายความรวมถึงส่วนงานระดับงานหรือระดับฝ่ายของหน่วยงานเฉพาะทางที่มีหน้าที่ดังกล่าวด้วย

“ผู้ดูแลระบบ” หมายความว่า พนักงานหรือพนักงานโครงการภายใต้หน่วยบริการเทคโนโลยีสารสนเทศ หรือบุคคลภายนอกที่สำนักงานว่าจ้างให้ทำหน้าที่ดูแลและพัฒนาระบบสารสนเทศ

“ผู้ใช้งาน” หมายความว่า พนักงาน พนักงานโครงการ บุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน ผู้รับบริการหรือผู้ซึ่งใช้งานระบบสารสนเทศของสำนักงาน

“สิทธิของผู้ใช้งาน” หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักงาน

“การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ” หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งานเข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติ

เกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

“สินทรัพย์” (Asset) หมายความว่า สินทรัพย์ด้านสารสนเทศและระบบสารสนเทศที่มีคุณค่าสำหรับสำนักงาน

“สารสนเทศ” หมายความว่า ข้อมูล เรื่องราว หรือข้อเท็จจริง ไม่ว่าจะปรากฏในรูปแบบของตัวอักษร ตัวเลข เสียง ภาพ หรือรูปแบบอื่นใดที่สื่อความหมายได้โดยสภาพของสิ่งนั้นเองหรือโดยผ่านวิธีการใด ๆ และให้หมายความรวมถึงคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในรูปแบบอิเล็กทรอนิกส์หรือระบบคอมพิวเตอร์ในสภาพที่เครื่องคอมพิวเตอร์ เครื่องบริการ และระบบคอมพิวเตอร์ อาจประมวลผลได้ ทั้งนี้ ให้หมายความรวมถึงข้อมูลทางอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

“ระบบสารสนเทศ” หมายความว่า ฮาร์ดแวร์ (เช่น เครื่องคอมพิวเตอร์ เครื่องบริการ เครื่องพิมพ์ อุปกรณ์สื่อสารพกพา เป็นต้น) ซอฟต์แวร์ (เช่น ระบบปฏิบัติการ หรือชุดโปรแกรมสำหรับสำนักงาน เป็นต้น) สื่อบันทึกข้อมูล (เช่น แผ่นดีวีดี สื่อบันทึกข้อมูลพกพาประเภท Flash drive เป็นต้น) สารสนเทศและบริการสารสนเทศต่าง ๆ (เช่น บริการอินเทอร์เน็ต บริการระบบบริหารทรัพยากรบุคคล เป็นต้น) รวมถึงระบบสารสนเทศที่สำนักงานพัฒนาขึ้นเองหรือว่าจ้างให้บุคคลอื่นพัฒนาเพื่อใช้ในการดำเนินการที่เกี่ยวกับคอมพิวเตอร์และเครือข่ายของสำนักงาน

“ความมั่นคงปลอดภัยด้านสารสนเทศ” (Information Security) หมายความว่า การธำรงไว้ซึ่งความลับ (Confidentiality) ความถูกต้องครบถ้วน (Integrity) และสภาพพร้อมใช้งาน (Availability) ของสารสนเทศรวมทั้งคุณสมบัติอื่น ได้แก่ ความถูกต้องแท้จริง (Authenticity) ความรับผิด (Accountability) การห้ามปฏิเสธความรับผิด (Non-Repudiation) และความน่าเชื่อถือ (Reliability)

“เหตุการณ์ด้านความมั่นคงปลอดภัย” (Information Security Event) หมายความว่า การเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว และรวมถึงเหตุการณ์อันอาจเกี่ยวข้องกับความมั่นคงปลอดภัยด้วย

“สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด” (Information Security Incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิดซึ่งอาจทำให้ระบบสารสนเทศถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยด้านสารสนเทศถูกคุกคาม

“ข้อมูลลับ” หมายความว่า สารสนเทศและระบบสารสนเทศที่มีความสำคัญและจำเป็นต้องได้รับการรักษาไว้ซึ่งความลับ (Confidentiality) ซึ่งหากข้อมูลดังกล่าวทั้งหมดหรือเพียงบางส่วนรั่วไหลไปถึงบุคคลผู้ที่ไม่มีหน้าที่เกี่ยวข้องได้รับทราบจะทำให้เกิดความเสียหายต่อสำนักงานหรือบุคคลอื่น โดยสำนักงานได้กำหนดลำดับชั้นความลับตามความสำคัญของเนื้อหา แหล่งที่มาของข้อมูล วิธีการนำไปใช้ประโยชน์ จำนวนบุคคลที่ต้องรับทราบและผลกระทบหรือระดับความร้ายแรงในกรณีที่มีการเปิดเผยหรือมีการรั่วไหลของข้อมูลลับนั้น

“ลับที่สุด” หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิด

ความเสียหายต่อสำนักงาน หรือเจ้าของข้อมูลอย่างร้ายแรงที่สุด

“ลับมาก” หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อสำนักงาน หรือเจ้าของข้อมูลอย่างร้ายแรง

“ลับ” หมายความว่า ข้อมูลลับซึ่งหากเปิดเผยทั้งหมดหรือเพียงบางส่วนจะก่อให้เกิดความเสียหายต่อสำนักงาน หรือเจ้าของข้อมูล

“ใช้ภายใน” หมายความว่า ข้อมูลลับซึ่งใช้ประโยชน์ภายในสำนักงานเท่านั้น ซึ่งจำเป็นต้องได้รับการป้องกันการเข้าถึงจากบุคคลภายนอก

หมวด ๒
แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศและระบบสารสนเทศ

ส่วนที่ ๑
การรักษาความมั่นคงปลอดภัยทั่วไป

ข้อ ๖ สารสนเทศและระบบสารสนเทศของสำนักงานต้องได้รับการป้องกันการเข้าถึงและควบคุมการใช้งานสารสนเทศและระบบสารสนเทศอย่างเหมาะสมตามมาตรฐานการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

ข้อ ๗ การควบคุมการเข้าถึงสารสนเทศและระบบสารสนเทศต่าง ๆ ของสำนักงานต้องครอบคลุมในทุกขั้นตอน ตั้งแต่การลงทะเบียนผู้ใช้งานใหม่ (User Registration) การเปลี่ยนแปลงสถานภาพต่าง ๆ ไปจนถึงการเพิกถอนสิทธิของผู้ใช้งาน โดยขั้นตอนและวิธีการปฏิบัติงานต่าง ๆ ต้องครอบคลุมและบังคับใช้กับสารสนเทศและระบบสารสนเทศทุกระบบที่อยู่ภายใต้ขอบเขตของสำนักงาน

ข้อ ๘ การลงทะเบียนผู้ใช้งานใหม่ ผู้ใช้งานที่เป็น

(๑) พนักงาน และพนักงานโครงการ ต้องผ่านกระบวนการสรรหาและคัดเลือกบุคคล

(๒) บุคคลภายนอกที่ปฏิบัติงานให้กับสำนักงาน ให้หน่วยงานผู้ว่าจ้างดำเนินการตรวจสอบประวัติวุฒิการศึกษา และความเชี่ยวชาญตามความเหมาะสม

ให้ดำเนินการลงทะเบียนผู้ใช้งานใหม่ตามกระบวนการตามที่หน่วยบริการเทคโนโลยีสารสนเทศกำหนดขึ้น

ข้อ ๙ การลงทะเบียนขอเข้าถึงสารสนเทศและระบบสารสนเทศของสำนักงานโดยผู้ใช้งานต้องได้รับการทบทวน และการพิจารณาอนุมัติตามขั้นตอนที่ระบุไว้อย่างเคร่งครัด และต้องมีการจำกัดสิทธิการเข้าถึงระบบของผู้ใช้งานให้อยู่ในระดับที่เหมาะสมต่อความจำเป็นในการทำงานตามหลักการ "Least Privilege" อยู่เสมอ นอกจากนี้ ต้องมีการแบ่งแยกอำนาจหน้าที่ (Segregation of Duties) ของผู้ใช้งานอย่างเหมาะสม เพื่อป้องกันมิให้ผู้ใช้งานผู้หนึ่งผู้ใดได้รับสิทธิในการเข้าถึงระบบเกินกว่าหน้าที่ความรับผิดชอบของตำแหน่งงาน

ข้อ ๑๐ ผู้ใช้งานต้องได้รับการตรวจพิสูจน์ตัวตนทุกครั้งเมื่อทำการ Log on เข้าสู่ระบบ สำหรับวิธีการตรวจพิสูจน์นั้น ให้คัดเลือกโดยยึดตามผลการประเมินความเสี่ยงและงบประมาณเป็นสำคัญ ซึ่งโดยทั่วไปแล้ววิธีการตรวจพิสูจน์ตัวตนของผู้ใช้งานนั้นสามารถแบ่งได้ออกเป็น ๓ ประเภท ดังนี้

(๑) การตรวจพิสูจน์จากสิ่งที่ผู้ใช้งานทราบ ได้แก่ รหัสผ่าน

(๒) การตรวจพิสูจน์จากสิ่งที่ผู้ใช้งานครอบครองอยู่ ได้แก่ กุญแจรหัส (Authentication Key) บัตรที่มีแถบแม่เหล็ก หรือบัตรสมาร์ทการ์ด

(๓) การตรวจพิสูจน์จากส่วนของร่างกายผู้ใช้งาน ได้แก่ ลายนิ้วมือ หรือรูม่านตา

ข้อ ๑๑ ในการใช้งานของผู้ใช้งานสำหรับโปรแกรมประยุกต์ แอพพลิเคชั่น สารสนเทศและระบบสารสนเทศที่สำคัญ ให้สำนักงานใช้วิธีการตรวจพิสูจน์ตัวตนของผู้ใช้งานตามข้อ ๑๐ ตั้งแต่ ๒ ประเภทขึ้นไป

ข้อ ๑๒ การส่งมอบรหัสผ่านให้แก่ผู้ใช้งาน ต้องกระทำผ่านช่องทางที่มั่นคงปลอดภัย ไม่ส่งผ่านจดหมายอิเล็กทรอนิกส์ที่เป็น Clear Text และรหัสผ่านตั้งต้นต้องเป็นรหัสผ่านที่ไม่สามารถเดาได้โดยง่าย สำหรับระบบที่ไม่ต้องถือครองรหัสผ่านร่วมกัน (Shared Password) ผู้ใช้งานต้องเปลี่ยนรหัสผ่านตั้งต้นให้เป็นรหัสผ่านของตนเองทันทีเมื่อได้รับการส่งมอบรหัสผ่าน

ข้อ ๑๓ กรณีที่ผู้ใช้งานเป็นพนักงานหรือพนักงานโครงการและมีการโอนย้ายตำแหน่งงาน ลาออกหรือพ้นจากสภาพการเป็นพนักงานหรือพนักงานโครงการ หรือผู้ใช้งานซึ่งเป็นบุคคลภายนอกที่หมดระยะเวลาการปฏิบัติงานกับสำนักงาน ให้ผู้อำนวยการฝ่ายที่รับผิดชอบด้านบริหารงานบุคคลหรือผู้ที่ได้รับมอบหมายจากผู้อำนวยการฝ่ายที่รับผิดชอบด้านบริหารงานบุคคล หรือผู้บังคับบัญชาของบุคคลดังกล่าว แจ้งให้หน่วยบริการเทคโนโลยีสารสนเทศเพิกถอนสิทธิการใช้งานระบบต่าง ๆ ของตำแหน่งงานเดิมทันที

ข้อ ๑๔ สารสนเทศและระบบสารสนเทศของสำนักงานต้องมีความถูกต้อง ครบถ้วน สมบูรณ์ เป็นปัจจุบัน และได้รับการรักษาความลับโดยทุกฝ่ายที่เกี่ยวข้องอย่างเหมาะสมในทุกขั้นตอน นับตั้งแต่การสร้าง การจัดเก็บ การใช้งานและการทำลายตามมาตรฐานการรักษาความมั่นคงปลอดภัยสารสนเทศ

ข้อ ๑๕ ให้หน่วยบริการเทคโนโลยีสารสนเทศจัดทำระบบสารสนเทศสำรองเฉพาะระบบสำคัญ รวมทั้งติดตามผลการวิเคราะห์ผลกระทบทางธุรกิจ ให้อยู่ในสภาพพร้อมใช้งานในกรณีที่เกิดเหตุฉุกเฉิน และภายในช่วงเวลาที่กำหนดหลังจากเกิดเหตุฉุกเฉิน โดยสอดคล้องกับแผนจัดเตรียมความพร้อมกรณีฉุกเฉินตามข้อ ๗๑

ข้อ ๑๖ ให้หน่วยบริการเทคโนโลยีสารสนเทศทำการตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศและระบบสารสนเทศอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

ส่วนที่ ๒
การบริการระบบสารสนเทศ

ข้อ ๑๗ เพื่อเป็นการลดความเสี่ยงทางอิเล็กทรอนิกส์ของสำนักงาน ผู้ใช้งานมีหน้าที่ปฏิบัติตามแนวปฏิบัติในการใช้งานระบบสารสนเทศของสำนักงาน รวมถึงการปกป้องบัญชีผู้ใช้งานและรหัสผ่านของตนเองไม่ให้บุคคลอื่นเข้าถึงได้ และการดูแลปกป้องระบบสารสนเทศเพื่อไม่ให้เกิดการเสียหายหรือสูญหาย

ข้อ ๑๘ สำนักงานจะส่งเสริมให้หน่วยบริการเทคโนโลยีสารสนเทศของสำนักงานที่มีระบบสารสนเทศที่ดีใช้งานอยู่ ขยายการให้บริการนั้นไปยังหน่วยงานเฉพาะทางอื่นภายใต้สำนักงาน เพื่อเพิ่มความคุ้มค่าของการใช้ทรัพยากรด้านเทคโนโลยีสารสนเทศของสำนักงาน

ข้อ ๑๙ เพื่อให้การจัดหา การพัฒนา หรือการปรับปรุงแก้ไขระบบสารสนเทศของสำนักงานมีคุณสมบัติสอดคล้องกับความต้องการและมาตรฐานของระบบสารสนเทศที่สำนักงานกำหนดไว้ ผู้ใช้งานและหน่วยบริการเทคโนโลยีสารสนเทศต้องร่วมกันพิจารณาคุณสมบัติของระบบสารสนเทศตามข้อกำหนดความต้องการของระบบสารสนเทศในด้านที่เกี่ยวกับหน้าที่งาน (Functional Requirements) ด้านประสิทธิภาพของระบบ (Performance) ด้านการรองรับงาน (Capacity) ด้านความยากง่ายในการ

ใช้งาน (Ease of Use) ด้านความเข้ากันได้กับระบบสารสนเทศเดิมที่มีอยู่ของสำนักงาน (Compatibility) และด้านความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security)

ส่วนที่ ๓
การบริการระบบเครือข่าย

ข้อ ๒๐ สำนักงานจะจัดให้มีการให้บริการระบบเครือข่ายทั้งแบบมีสายและไร้สายอย่างพอเพียง และมีความมั่นคงปลอดภัยในการใช้งาน โดยผู้ใช้งานต้องถูกควบคุมให้สามารถเข้าถึงบริการระบบเครือข่ายได้เฉพาะในส่วนที่ตนเองได้รับอนุญาตเท่านั้น

ข้อ ๒๑ เพื่อรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ สำนักงานจะบริหารจัดการควบคุมการเข้าถึงและจะจัดเก็บแฟ้มบันทึกการใช้งานระบบสารสนเทศของสำนักงานให้สอดคล้องตามกฎหมาย

ข้อ ๒๒ เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศและระบบสารสนเทศ สำนักงานจะบริหารจัดการความมั่นคงของระบบเครือข่ายด้วยวิธีการ ดังนี้

(๑) จัดให้มีอุปกรณ์รักษาความมั่นคงปลอดภัยทางเครือข่าย

(๒) จัดเก็บ Log ของระบบเครือข่าย รวมถึง Security Log ที่จำเป็นตามที่กำหนดโดยกฎหมายและมาตรฐานด้านการบริหารความมั่นคงปลอดภัยของสำนักงาน

(๓) ติดตามตรวจสอบ สถานะของระบบเครือข่าย การใช้งานบริการระบบเครือข่าย และ Security Log ที่เกี่ยวข้อง รวมถึงการเฝ้าระวังความผิดปกติต่าง ๆ ได้แก่ การพยายามบุกรุกเข้าสู่ระบบ การปฏิเสธการให้บริการ หรือการทำให้ประสิทธิภาพในการทำงานของระบบสารสนเทศลดลง

(๔) ควบคุมการเข้าถึงระบบบริหารจัดการระบบเครือข่ายให้ผ่านช่องทางที่ใช้งานโปรโตคอลที่มีความมั่นคงปลอดภัย

(๕) ใช้กระบวนการพิสูจน์ตัวตน (Authentication) กระบวนการพิจารณาอนุมัติ (Authorization) และการกำหนดขอบเขตความรับผิดชอบในการบริหารจัดการอุปกรณ์ระบบเครือข่าย

(๖) สำรองข้อมูลค่าการปรับแต่ง (Configuration) ของอุปกรณ์ระบบเครือข่ายอย่างสม่ำเสมอหรือทุกครั้งที่มีการเปลี่ยนแปลง

ข้อ ๒๓ เพื่อรักษาความมั่นคงปลอดภัยด้านสารสนเทศและระบบสารสนเทศของสำนักงาน การติดตั้งระบบเครือข่ายต้องได้รับการออกแบบและตั้งค่าอย่างเหมาะสมตามข้อ ๕๓

ข้อ ๒๔ กรณีที่ผู้ให้บริการเครือข่ายภายนอก ต้องการให้บริการในพื้นที่ของสำนักงาน ให้ผู้นั้นติดต่อหน่วยบริการเทคโนโลยีสารสนเทศเพื่อขออนุมัติจากผู้บริหารเทคโนโลยีสารสนเทศ

ส่วนที่ ๔
การบริการจดหมายอิเล็กทรอนิกส์

ข้อ ๒๕ สำนักงานจะจัดให้มีบริการจดหมายอิเล็กทรอนิกส์แก่พนักงานและพนักงานโครงการทุกคน เพื่อใช้ในการสื่อสารภายในสำนักงานและการปฏิบัติงานตามที่ได้รับมอบหมายจากสำนักงาน

ข้อ ๒๖ เพื่อให้การสื่อสารแก่บุคคลภายนอกเป็นไปอย่างมีเอกภาพ สำนักงานจะให้บริการบัญชีจดหมายอิเล็กทรอนิกส์ภายใต้ชื่อโดเมนของสำนักงาน (@nstda.or.th) ให้แก่พนักงานและพนักงานโครงการทุกคนและจะยกเลิกบัญชีนี้เมื่อพนักงานและพนักงานโครงการพ้นสภาพการเป็นพนักงานหรือพนักงานโครงการ

ข้อ ๒๗ เพื่อเพิ่มประสิทธิภาพการทำงานในลักษณะกลุ่มทั้งในระยะสั้นและระยะยาว และสนับสนุนการทำงานร่วมกันของพนักงานและพนักงานโครงการและบุคคลภายนอก สำนักงานจะสนับสนุนการให้บริการบัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม (Groupmail) เพื่อใช้ในการส่งจดหมายอิเล็กทรอนิกส์ไปยังคณะทำงานหรือคณะกรรมการ ซึ่งอาจมีสมาชิกได้ทั้งจากพนักงานและพนักงานโครงการและบุคคลภายนอกสำนักงานโดยต้องชี้แจงเหตุผลและความจำเป็นในการใช้งาน และเมื่อสิ้นสุดการใช้งาน ให้แจ้งหน่วยบริการเทคโนโลยีสารสนเทศทราบทันที

ส่วนที่ ๕
การตรวจสอบสารสนเทศและระบบสารสนเทศ

ข้อ ๒๘ สารสนเทศที่ถูกสร้าง เก็บรักษา หรือส่งผ่านระบบสารสนเทศ ถือเป็นทรัพย์สินของสำนักงาน โดยสำนักงานสามารถเปิดเผยหรือใช้เป็นหลักฐานในการสืบสวนความผิดต่าง ๆ โดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

สารสนเทศตามวรรคหนึ่งไม่รวมถึงสารสนเทศที่เป็นทรัพย์สินของลูกค้าหรือบุคคลภายนอก ซอฟต์แวร์หรือวัสดุอื่น ๆ ที่ได้รับการคุ้มครองโดยสิทธิบัตร ลิขสิทธิ์ หรือทรัพย์สินทางปัญญาอื่นใดของบุคคลภายนอก

ข้อ ๒๙ เพื่อวัตถุประสงค์ในการบริหารจัดการและรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ สำนักงานขอสงวนสิทธิ์ในการตรวจสอบการใช้งานเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ และระบบเครือข่ายของผู้ใช้งาน

ข้อ ๓๐ สำนักงานขอสงวนสิทธิ์ในการเข้าถึงและตรวจสอบจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานโดยไม่จำเป็นต้องแจ้งให้ผู้ใช้งานทราบล่วงหน้า

การเข้าถึงและการตรวจสอบตามวรรคหนึ่ง ให้ดำเนินการได้เมื่อมีความจำเป็นและห้ามผู้ตรวจสอบ เปิดเผยสารสนเทศใดของผู้ใช้งานที่ถูกตรวจสอบนั้น เว้นแต่เป็นการเปิดเผยตามคำสั่งศาลหรือตามบทบัญญัติแห่งกฎหมายให้กระทำได้ หรือได้รับความยินยอมจากผู้ใช้งาน แล้วแต่กรณี

หมวด ๓
การบริหารจัดการระบบสารสนเทศของสำนักงาน (สำหรับผู้ดูแลระบบ)

ส่วนที่ ๑
การบริหารระบบทั่วไป

ข้อ ๓๑ ผู้ดูแลระบบต้องตั้งค่าของเครื่องคอมพิวเตอร์ที่ใช้ในกิจการของสำนักงาน รวมถึงเครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา เครื่องบริการ หรือเครื่องคอมพิวเตอร์ประเภทอื่นใด ดังนี้

(๑) ให้ใช้รหัสผ่านบนระบบปฏิบัติการในการเข้าถึงทุกครั้ง

(๒) ตั้งค่าเริ่มต้นให้เครื่องคอมพิวเตอร์ส่วนบุคคล เครื่องคอมพิวเตอร์พกพา และอุปกรณ์สื่อสารพกพาใช้ Screen Saver เป็นเวลา ๑๕ นาที และต้องทำการล็อคหน้าจอทันทีที่จะลุกออกจากหน้าจอ หรือไม่ได้ใช้งาน โดยจะต้องปลดล็อคด้วยรหัสผ่าน

(๓) ตั้งค่าการยุติการใช้งานสำหรับระบบสารสนเทศ (Idle Timeout) เพื่อป้องกันการเข้าถึงสารสนเทศเมื่อผู้ใช้งานว่างเว้นจากการใช้งานเป็นระยะเวลา ๓๐ นาที

(๔) จำกัดระยะเวลาการเชื่อมต่อระบบสารสนเทศ (Connection Time Limit) ไว้ที่ ๓ ชั่วโมง สำหรับระบบสารสนเทศที่มีความเสี่ยงหรือความสำคัญสูง

ข้อ ๓๒ ผู้ดูแลระบบต้องจัดเตรียมวิธีการเข้าถึงระบบสารสนเทศให้ผู้ใช้งานสามารถเข้าถึงได้โดยผ่านช่องทางระบบเครือข่ายที่มีการเข้ารหัสลับเสมอ ได้แก่ สายสัญญาณระบบเครือข่ายที่มีการ

จัดเตรียมไว้ หรือ VPN หรือช่องทางสื่อสารอื่น ๆ ของสำนักงานที่มีการเข้ารหัสลับข้อมูลในการสื่อสารเพื่อความมั่นคงปลอดภัยแล้ว ยกเว้นการให้บริการข้อมูลเว็บสาธารณะส่วนที่มีการอ่านอย่างเดียว

ข้อ ๓๓ ผู้ดูแลระบบต้องจัดเตรียมให้ระบบสารสนเทศใช้การแสดงตนด้วยบัญชีผู้ใช้งานและรหัสผ่านที่เป็นมาตรฐานของสำนักงานก่อนที่ผู้ใช้งานจะเข้าถึงระบบสารสนเทศของสำนักงานทุกครั้ง

ข้อ ๓๔ หน่วยบริการเทคโนโลยีสารสนเทศ ได้จัดเตรียมเครื่องคอมพิวเตอร์ส่วนบุคคลและทีมให้ความช่วยเหลือ ดังนี้

(๑) จัดหาเครื่องคอมพิวเตอร์ส่วนบุคคลให้กับผู้ใช้งานตามที่สำนักงานกำหนด

(๒) จัดหาซอฟต์แวร์ที่เหมาะสมกับการทำงาน โดยสำนักงานจะต้องจัดเตรียมซอฟต์แวร์ Anti-Virus, Web Browser และ Office Suite รวมทั้งการเชื่อมต่อกับเครือข่าย

(๓) มีทีมให้ความช่วยเหลือในการแก้ไขปัญหาการใช้งาน (Help Desk) เครื่องคอมพิวเตอร์และระบบ โดยจะดูแลเฉพาะเครื่องคอมพิวเตอร์ของสำนักงานเท่านั้น และไม่รับผิดชอบในความเสียหายที่อาจจะเกิดขึ้นกับข้อมูล

ทั้งนี้ เมื่อสิ้นสุดการเป็นพนักงานหรือพนักงานโครงการ หรือสิ้นสุดการใช้เครื่องคอมพิวเตอร์ส่วนบุคคลแล้ว พนักงานหรือพนักงานโครงการมีหน้าที่จะต้องสำรองข้อมูล หรือจะต้องรับผิดชอบข้อมูลด้วยตนเอง พร้อมทั้งดำเนินการส่งเครื่องคอมพิวเตอร์คืนให้แก่หน่วยบริการเทคโนโลยีสารสนเทศเพื่อดำเนินการทำลายข้อมูลต่อไป

ข้อ ๓๕ ผู้ดูแลระบบหรือหน่วยบริการเทคโนโลยีสารสนเทศมีหน้าที่ตรวจสอบช่องโหว่ของเครื่องที่ให้บริการ รวมถึงช่องโหว่ของเว็บไซต์ (Website) ที่ให้บริการอย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง และรายงานผลต่องานบริหารความมั่นคงปลอดภัยดิจิทัล ฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล

ข้อ ๓๖ ผู้ดูแลระบบกำหนด ตั้งค่า และตรวจสอบการตั้งค่า Security Baseline ของเครื่องบริการอย่างสม่ำเสมอ หรือเมื่อมีการเปลี่ยนด้านซอฟต์แวร์ของเครื่องบริการ

ข้อ ๓๗ ผู้ดูแลระบบต้องกำหนดเวลาของเครื่องคอมพิวเตอร์ให้เป็นไปตามเวลามาตรฐานสากลโดยเทียบเวลาอัตโนมัติกับเครื่องบริการเวลาอ้างอิงผ่านเครือข่าย (Network Time Server) ได้แก่ clock.nstda.or.th หรือ clock.nectec.or.th หรือเครื่องบริการอื่นที่เชื่อถือได้ และมีกระบวนการตรวจสอบหรือปรับเวลาให้ตรงกันอย่างสม่ำเสมอไม่น้อยกว่าวันละ ๑ ครั้ง และจัดแสดงเวลาอ้างอิง

ดังกล่าวให้ผู้ใช้งานสามารถตรวจสอบเครื่องคอมพิวเตอร์ที่ใช้งานให้มีเวลาที่แม่นยำอยู่เสมอ

ข้อ ๓๘ การใช้งานโปรแกรมอรรถประโยชน์ (System Utilities) ต้องถูกจำกัดไว้เฉพาะผู้ดูแลระบบที่มีความจำเป็นต้องใช้งานเป็นประจำเท่านั้น เพื่อป้องกันการละเมิดหรือหลีกเลี่ยงกลไกการควบคุมด้านความมั่นคงปลอดภัยต่าง ๆ โดยประเภทของโปรแกรมที่ต้องจำกัดการติดตั้งและใช้งาน ได้แก่

(๑) โปรแกรมดักจับข้อมูลบนเครือข่าย (Network Packet Sniffer/Packet Dump)

(๒) โปรแกรมสร้างข้อมูลบนเครือข่าย (Network Packet Generator)

(๓) โปรแกรมเปลี่ยนแปลงหมายเลขประจำอุปกรณ์คอมพิวเตอร์ (Mac Address Changer)

(๔) โปรแกรมที่ใช้ในการสืบสวนหลักฐานดิจิทัล (Forensic Tools)

(๕) โปรแกรมแปลงหมายเลขไอพี (NAT/PAT/Packet Forward)

(๖) โปรแกรมเจาะรหัสผ่าน (Password Cracking)

ส่วนที่ ๒
การดูแลระบบจดหมายอิเล็กทรอนิกส์ (E-mail)

ข้อ ๓๙ ผู้ดูแลระบบต้องจัดเตรียมบัญชีจดหมายอิเล็กทรอนิกส์และกล่องรับจดหมายอิเล็กทรอนิกส์เพื่อให้ผู้ใช้งานสามารถเข้าถึงจดหมายอิเล็กทรอนิกส์ได้

ข้อ ๔๐ ผู้ดูแลระบบต้องจัดเตรียมบริการบัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม (Groupmail) เพื่อให้บริการแก่ผู้ใช้งานในการส่งจดหมายอิเล็กทรอนิกส์ไปยังคณะทำงานหรือคณะกรรมการซึ่งอาจมีสมาชิกได้ทั้งจากพนักงานและพนักงานโครงการและบุคคลภายนอกสำนักงาน

ข้อ ๔๑ ผู้ดูแลระบบต้องกำหนดให้ผู้ใช้งานใช้รหัสผ่านในการเข้าถึงบัญชีจดหมายอิเล็กทรอนิกส์และกำหนดให้การติดต่อระหว่างผู้ใช้งานกับเครื่องบริการจดหมายอิเล็กทรอนิกส์ผ่านช่องทางการสื่อสารที่มั่นคงปลอดภัยด้วยเทคโนโลยีการเข้ารหัสประเภท Secure Sockets Layer (SSL) หรือ Transport Layer Security (TLS) เป็นอย่างน้อย เพื่อป้องกันการถูกล่วงละเมิด การดักและการลักลอบนำรหัสผ่านไปใช้ในทางที่ผิด

ข้อ ๔๒ หน่วยบริการเทคโนโลยีสารสนเทศต้องกำหนดและแจ้งให้ผู้ใช้งานของตนได้ทราบถึงขนาดของกล่องรับจดหมายอิเล็กทรอนิกส์ (Mailbox Size) และขนาดจำกัดของจดหมายอิเล็กทรอนิกส์แต่ละฉบับซึ่งเป็นค่าที่เหมาะสมที่ระบบจะรองรับการทำงานได้

ข้อ ๔๓ หน่วยบริการเทคโนโลยีสารสนเทศต้องเตรียมวิธีการตั้งค่าในซอฟต์แวร์มาตรฐาน เพื่อให้ผู้ใช้งานสามารถตั้งค่าข้อมูลผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ประกอบด้วย ชื่อ-นามสกุลของผู้ส่งเป็นภาษาอังกฤษ และชื่อบัญชีจดหมายอิเล็กทรอนิกส์ของผู้ส่งเป็นอย่างน้อย และในกรณีที่ต้องการให้ผู้รับตอบกลับมาที่บัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม ต้องตั้งค่าบัญชีจดหมายอิเล็กทรอนิกส์กลุ่มนั้นที่ “Reply To” แทนการเปลี่ยนแปลงที่ข้อมูลผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender)

ข้อ ๔๔ เพื่อให้ผู้ใช้งานได้มีข้อความปฏิเสธความรับผิดชอบของสำนักงานต่อท้ายข้อความที่ผู้ใช้งานส่งทางจดหมายอิเล็กทรอนิกส์ (E-mail Disclaimer) ให้ผู้ดูแลระบบดำเนินการใส่ข้อความดังกล่าวลงในจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ส่งออกจากระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน

ข้อ ๔๕ เพื่อให้เกิดความต่อเนื่องในการดำเนินงานของสำนักงาน ในกรณีที่ผู้ใช้งานได้พ้นสภาพการเป็นพนักงานหรือพนักงานโครงการ หรือโอนย้ายหน่วยงานภายในสำนักงาน ให้ผู้ดูแลระบบจัดการฐานข้อมูลจดหมายอิเล็กทรอนิกส์ของพนักงานหรือพนักงานโครงการผู้นั้น ดังนี้

(๑) กรณีผู้ใช้งานพ้นสภาพการเป็นพนักงานหรือพนักงานโครงการ ให้ผู้ดูแลระบบส่งต่อข้อมูลจดหมายอิเล็กทรอนิกส์ของผู้ใช้งานนั้นไปยังกล่องรับจดหมายอิเล็กทรอนิกส์ของผู้บังคับบัญชาชั้นต้นของพนักงาน หรือพนักงานโครงการที่พ้นสภาพการเป็นพนักงานหรือพนักงานโครงการ เพื่อเก็บไว้เป็นระยะเวลา ๑ เดือน นับแต่วันที่พ้นสภาพการเป็นพนักงานหรือพนักงานโครงการ

(๒) กรณีโอนย้ายหน่วยงานภายในสำนักงาน ให้ผู้บังคับบัญชาชั้นต้นของพนักงานหรือพนักงานโครงการที่โอนย้ายนั้นมีสิทธิเลือกให้ส่งต่อข้อมูลจดหมายอิเล็กทรอนิกส์ของพนักงานผู้นั้นไปยังกล่องรับจดหมายอิเล็กทรอนิกส์ของตนเพื่อเก็บไว้เป็นระยะเวลา ๑ เดือน หรือส่งไปยังกล่องรับจดหมายอิเล็กทรอนิกส์ของพนักงานหรือพนักงานโครงการที่โอนย้ายไปแล้วนั้นได้

ส่วนที่ ๓
การบริหารจัดการสิทธิและรหัสผ่านอย่างมั่นคงปลอดภัย

ข้อ ๔๖ ให้หน่วยบริการเทคโนโลยีสารสนเทศร่วมกับผู้ปฏิบัติงานที่เกี่ยวข้องจัดทำข้อกำหนดการใช้งานตามภารกิจเพื่อควบคุมการเข้าถึงสารสนเทศ (Business Requirements for Access Control) ตามนโยบายที่เกี่ยวข้องกับการอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจของสำนักงาน โดยประกอบด้วยการควบคุมการเข้าถึงสารสนเทศและการปรับปรุงการเข้าถึงสารสนเทศ ต้องได้รับการตรวจพิสูจน์ตัวตนของผู้ใช้งานก่อนเสมอ และอนุญาตให้ใช้งานระบบสารสนเทศเท่าที่จำเป็น

ตามหลักการ "Need-to-know" เท่านั้น

ข้อ ๔๗ ให้ผู้ดูแลระบบมีขั้นตอนปฏิบัติในการลงทะเบียนผู้ใช้งานที่ได้รับอนุญาตจะมอบบัญชีส่วนตัวให้ผู้ใช้งานแต่ละคน และมอบสิทธิของผู้ใช้งานแต่ละระบบเฉพาะแก่ผู้ที่จำเป็นต้องใช้งานระบบสารสนเทศเท่านั้น และให้มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานอย่างน้อยปีละ ๑ ครั้ง รวมทั้งปรับปรุงทะเบียนผู้ใช้งานให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๔๘ ผู้ดูแลระบบต้องจัดให้มีการบันทึกรายละเอียดการเข้าถึงระบบสารสนเทศ การแก้ไขเปลี่ยนแปลงสิทธิต่าง ๆ ของระบบสารสนเทศของทั้งผู้ที่ได้รับอนุญาตและไม่ได้รับอนุญาต เพื่อเป็นหลักฐานในการตรวจสอบหากมีปัญหาเกิดขึ้น

ข้อ ๔๙ ผู้ดูแลระบบต้องจัดเตรียมระบบเพื่อรองรับการเปลี่ยนรหัสผ่านของผู้ใช้งานเมื่อเข้าใช้งานครั้งแรก และรองรับการเปลี่ยนรหัสผ่านของผู้ใช้งานสำหรับเครื่องคอมพิวเตอร์และระบบคอมพิวเตอร์อย่างสม่ำเสมอทุก ๑ ปี

ข้อ ๕๐ ผู้ดูแลระบบต้องเปลี่ยนรหัสผ่านและ/หรือคู่กุญแจรหัสลับ ภายใต้เงื่อนไข ดังต่อไปนี้

(๑) ผู้ดูแลระบบต้องตั้งและเปลี่ยนรหัสผ่านตามรูปแบบและความยาวเหมือนรหัสผ่านผู้ใช้งานทั่วไป

(๒) เปลี่ยนคู่กุญแจรหัสลับ ทั้งกุญแจผู้ใช้ส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ทุก ๓ ปี และไม่ควรใช้รหัสผ่านของกุญแจส่วนตัวเดิม

(๓) ในกรณีที่พบว่ามีการรั่วไหล ให้เปลี่ยนรหัสผ่านและหรือคู่กุญแจรหัสลับในทันที หรือ

(๔) วิธีการอื่นใดตามที่ประชุมคณะกรรมการบริหารเทคโนโลยีสารสนเทศกำหนด ยกเว้นไม่ต้องเปลี่ยนรหัสผ่านในกรณีระบบใช้การพิสูจน์ตัวตนแบบ OTP (One Time Password) หรือแบบ Multi-factor Authentication หรือการเข้าสู่ระบบผ่านหน้า console เครื่อง หรือข้อจำกัดของอุปกรณ์บางประเภท

ข้อ ๕๑ ผู้ดูแลระบบต้องจัดเตรียมระบบเชิงโต้ตอบที่สนับสนุนให้ผู้ใช้งานปฏิบัติตามหลักการตั้งรหัสผ่านที่มีความมั่นคงปลอดภัย ตามแนวทางดังนี้

(๑) รหัสผ่านต้องมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร เว้นแต่รหัสผ่านระดับ BIOS (Basic Input/Output System) ให้มีความยาวไม่น้อยกว่า ๔ ตัวอักษร

(๒) ห้ามผู้ใช้งานกำหนดรหัสผ่านจากบริบทของผู้ใช้งาน ดังต่อไปนี้

(ก) ชื่อจริงภาษาอังกฤษทั้งอักษรพิมพ์เล็ก และอักษรพิมพ์ใหญ่

(ข) นามสกุลจริงภาษาอังกฤษทั้งอักษรพิมพ์เล็ก และอักษรพิมพ์ใหญ่

(ค) รหัสพนักงาน

(ง) ชื่อย่อฝ่ายที่สังกัด

(จ) ชื่อย่องานที่สังกัด

(ฉ) หมายเลขโทรศัพท์

(ช) หมายเลขบัตรประจำตัวประชาชน

(ซ) ส่วนใดส่วนหนึ่งของวันเกิด

(ฌ) ปี พ.ศ. หรือ ค.ศ. ปัจจุบัน

(ญ) ชื่อผู้ใช้งานที่ใช้เข้าสู่ระบบ

(ฎ) ชื่อเฉพาะที่เกี่ยวข้องกับสำนักงาน

(ฏ) กลุ่มคำที่สำนักงานกำหนดให้เป็นคำต้องห้ามใช้

ส่วนที่ ๔
การบริหารจัดการสถานที่จัดเก็บหรือติดตั้งระบบสารสนเทศ

ข้อ ๕๒ ผู้ดูแลระบบต้องตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานที่มีระบบสารสนเทศจัดเก็บอยู่ เช่น พื้นที่ห้องเครื่องบริการ พื้นที่จัดเก็บสื่อบันทึกข้อมูล เป็นต้น เป็นประจำทุกวันเพื่อให้มั่นใจว่าระบบสารสนเทศได้รับการปกป้องทางกายภาพอย่างปลอดภัย รวมถึงต้องไม่เปิดเผยสถานที่ตั้งของระบบสารสนเทศต่อบุคคลภายนอกโดยเด็ดขาด เว้นแต่บุคคลภายนอกนั้นมีความจำเป็นต้องรับทราบเพื่อปฏิบัติงานให้เป็นไปตามที่กำหนดไว้ในสัญญาหรือกฎหมาย และไม่อนุญาตให้ผู้ที่ไม่เกี่ยวข้องเข้าถึงสถานที่ตั้งของเครื่องบริการได้โดยไม่จำเป็น ทั้งนี้ ผู้ดูแลระบบต้องเก็บบันทึกประวัติการเข้าออก (Log Book) ของพื้นที่ห้องเครื่องบริการที่มีรายละเอียด วัน เวลา และผู้เข้าออก และพิจารณาเลือกใช้มาตรการดูแลและป้องกัน ดังต่อไปนี้ ควบคู่ไปด้วย

(๑) ผู้ดูแลระบบต้องทำการติดตามการปฏิบัติงานของบุคคลภายนอกที่เข้ามาในสถานที่ตั้งของระบบสารสนเทศของสำนักงาน จนการปฏิบัติงานเสร็จสิ้น

(๒) มอบหมายให้มีผู้ตรวจสอบพื้นที่ที่มีระบบสารสนเทศจัดเก็บอยู่ เพื่อให้แน่ใจว่าไม่มีความผิดปกติทางกายภาพที่อาจส่งผลกระทบต่อระบบสารสนเทศได้

(๓) อาจมีการจัดแบ่งเวรยามให้มีบุคคลที่สามารถติดต่อได้ตลอด ๒๔ ชั่วโมง หากเกิดสถานการณ์เร่งด่วนคับขัน

ส่วนที่ ๕
การบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย

ข้อ ๕๓ ผู้ดูแลระบบต้องออกแบบ ติดตั้ง และตั้งค่าระบบเครือข่ายให้มีความเหมาะสม ดังนี้

(๑) ฮาร์ดแวร์ (Hardware) ที่เชื่อมต่อกับระบบเครือข่ายทั้งหมดต้องได้รับการตั้งค่าให้สนับสนุนการบริหารจัดการ และการตรวจสอบกิจกรรมต่าง ๆ ที่เกี่ยวข้องกับระบบเครือข่าย

(๒) สายสัญญาณระบบเครือข่ายต้องได้รับการรับรองตามมาตรฐานสากลหรือมาตรฐานผลิตภัณฑ์อุตสาหกรรม (มอก.) รวมไปถึงได้รับการติดตั้งและป้องกันอย่างเหมาะสม

(๓) ระบบป้องกันผู้บุกรุกจากภายนอก ควรได้รับการตั้งค่าตามคำแนะนำของผู้ผลิตหรือหน่วยงานด้านความมั่นคงปลอดภัยต่าง ๆ ได้แก่ SANS Institute หรือ NSA

(๔) Network Address ของระบบเครือข่ายต่าง ๆ ต้องได้รับการลงทะเบียน แจกจ่าย และบริหารจัดการ โดยผู้ดูแลระบบเครือข่ายที่ได้รับมอบหมายให้รับผิดชอบ และ Private IP Address ต้องไม่ถูกเปิดเผยต่อระบบเครือข่ายภายนอก

(๕) พอร์ต (Port) ที่ใช้สำหรับตรวจสอบและปรับแต่งระบบเครือข่าย (Diagnostic และ Configuration Port) ของอุปกรณ์ระบบเครือข่ายภายในของสำนักงาน ต้องถูกจำกัดให้สามารถใช้งานเฉพาะบุคคลที่เกี่ยวข้องเท่านั้น โดยกระทำผ่านช่องทางที่มีความมั่นคงปลอดภัย เช่น Secure Shell (SSH) หรือวิธีการอื่นใดที่มีการเข้ารหัสลับ ช่องทางการเชื่อมต่อและพอร์ตหรือบริการของอุปกรณ์เครือข่ายที่ไม่จำเป็นต่อการปฏิบัติงานต้องได้รับการปิดกั้นการเข้าถึงหรือยกเลิกการใช้งานอย่างเหมาะสม

(๖) อุปกรณ์ของระบบเครือข่ายที่สำคัญของสำนักงานต้องใช้ระบบไฟฟ้าสำรองเสมอ

(๗) ห้ามติดตั้งอุปกรณ์ใดเข้ากับระบบเครือข่ายของสำนักงานโดยไม่ได้รับอนุญาต

(๘) ระบบเครือข่ายต้องได้รับการตั้งค่าให้สามารถป้องกันการเชื่อมต่อจากเครือข่ายภายนอกเข้าสู่เครือข่ายภายในของสำนักงานได้ รวมทั้งต้องไม่อนุญาตให้มีการเชื่อมต่อเครือข่ายจากภายในสำนักงานสู่เครือข่ายภายนอกที่ไม่ได้รับอนุญาต

ข้อ ๕๔ ผู้ดูแลระบบต้องจัดการให้การเข้าถึงระบบเครือข่ายของสำนักงานจากระยะไกลมีกลไกในการพิสูจน์ตัวตนผู้ใช้งานอย่างเหมาะสม

ข้อ ๕๕ การเชื่อมต่ออุปกรณ์ของบุคคลภายนอกหรืออุปกรณ์ส่วนตัวของพนักงานเข้ากับระบบเครือข่ายของสำนักงานต้องได้รับการดูแลอย่างเหมาะสม อย่างน้อยดังต่อไปนี้

(๑) แยกกั้นระบบเครือข่าย (Network segregation) เครื่องของบุคคลภายนอกออกจากเครื่องของพนักงานหรือพนักงานโครงการ หรือเครื่องแม่ข่ายของสำนักงาน

(๒) อนุญาตให้ใช้งานระบบเครือข่ายหรือระบบอื่น ๆ เท่าที่จำเป็น

(๓) กรณีตรวจพบเหตุผิดปกติ ผู้ดูแลระบบเครือข่ายอาจดำเนินการด้านระบบเครือข่ายหรือระบบอื่นใดตามความเหมาะสมเพื่อควบคุมเหตุผิดปกติที่เกิดขึ้น

ข้อ ๕๖ ในการปฏิบัติงานค้นหาหรือตรวจสอบจุดบกพร่องของระบบสารสนเทศ เช่น การเข้าถึงสารสนเทศหรือเครื่องบริการ (Server) ที่ไม่ได้รับอนุญาต, การโจมตีระบบแบบ Denial of Service (DoS/DDoS), การปลอมแปลงข้อมูลในระบบเครือข่าย, การสร้างเส้นทางลวงระบบเครือข่าย (Forged Routing Information) และการทดสอบเจาะระบบ (Penetration Testing) จะต้องได้รับอนุมัติจากผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงานกลาง ก่อน

การตรวจประเมินช่องโหว่ผ่านเครื่องมือประเภท Vulnerability Assessment งานบริหารความมั่นคงปลอดภัยดิจิทัล ฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัลสามารถทำโดยไม่ต้องขออนุมัติ

ข้อ ๕๗ ผู้ดูแลระบบต้องทำการแบ่งแยกระบบเครือข่ายของสำนักงานออกเป็นกลุ่มตามความเหมาะสม และดำเนินการอย่างมั่นคงปลอดภัยอย่างน้อยต้องแบ่งแยกเครือข่าย ดังนี้

(๑) กลุ่มเครื่องแม่ข่ายบริการภายใน (Intranet)

(๒) กลุ่มเครื่องแม่ข่ายบริการภายในที่ต้องการความมั่นคงปลอดภัยสูง

(๓) กลุ่มเครื่องแม่ข่ายที่ให้บริการสำหรับบุคคลภายนอก (Public Internet)

(๔) กลุ่มเครื่องแม่ข่ายที่ให้บริการโดยบุคคลภายนอกโดยเบ็ดเสร็จ ที่ติดตั้งในระบบเครือข่ายภายในสำนักงาน (Outsource Service)

(๕) กลุ่มเครื่องของผู้ใช้งานที่เป็นพนักงาน

(๖) กลุ่มเครื่องของสำนักงานที่ทำงานอัตโนมัติ (IoT devices)

(๗) กลุ่มเครื่องของผู้ใช้งานที่เป็นบุคคลภายนอกที่ไม่ได้มาปฏิบัติงานประจำ

ข้อ ๕๘ การเข้าถึงระบบเครือข่ายหรือระบบสารสนเทศภายในของสำนักงานผ่านระบบเครือข่ายภายนอก เช่น เครือข่ายผู้ให้บริการโทรศัพท์เคลื่อนที่ต้องถูกจำกัด ให้ดำเนินการได้เฉพาะเท่าที่จำเป็นเท่านั้น และต้องได้รับการควบคุมดังนี้

(๑) อนุญาตให้ทำการเข้าถึงระบบจากระยะไกลได้เฉพาะกับบริการที่มีความจำเป็นเท่านั้น

(๒) ผู้ใช้งานที่ได้รับอนุญาตเท่านั้นที่มีสิทธิดำเนินการเข้าถึงระบบจากระยะไกล

(๓) การเข้าถึงระบบสำคัญหรือระบบที่เกี่ยวข้องกับสารสนเทศสำคัญจากระยะไกล ต้องได้รับการพิสูจน์ตัวตนผู้ใช้งานด้วยวิธีที่มีความมั่นคงปลอดภัย

(๔) การเข้าถึงระบบเครือข่ายหรือระบบสารสนเทศภายในของสำนักงาน ต้องใช้งานบนระบบเครือข่ายที่มีความมั่นคงปลอดภัยหรือเครือข่ายที่ผ่านการเข้ารหัสลับเท่านั้น ใช้งานได้ไม่เกิน ๑๒ ชั่วโมงต่อครั้ง (Session time) และตัดการเชื่อมต่ออัตโนมัติ เมื่อไม่มีการใช้งานใด ๆ เป็นระยะเวลาติดต่อกันเกิน ๓๐ นาที (Idle timeout)

ข้อ ๕๙ การเข้าถึงระบบเครือข่ายของสำนักงาน ต้องแบ่งแยกเส้นทางที่ใช้ในการติดตามตรวจสอบและบริหารจัดการระบบเครือข่าย ออกจากเส้นทางของระบบเครือข่ายใช้งานทั่วไป หรือใช้ช่องทางการเชื่อมต่อแบบเข้ารหัสลับ

ข้อ ๖๐ ผู้ดูแลระบบต้องรักษาความมั่นคงปลอดภัยทางเครือข่าย โดยใช้อุปกรณ์ประเภท Firewall หรือ IPS เป็นต้น เพื่อป้องกันการบุกรุก หรือควบคุมการเข้าถึงเครือข่าย หรือวิธีการอื่นใดเพื่อจัดการเส้นทางของระบบเครือข่ายของสำนักงาน เพื่อเพิ่มความมั่นคงปลอดภัยของสารสนเทศตามความเหมาะสม

ส่วนที่ ๖
การบริหารจัดการระบบเครือข่ายไร้สายของสำนักงาน

ข้อ ๖๑ ให้ฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงานกลาง หรือหน่วยงานอื่น ตามที่คณะกรรมการบริหารเทคโนโลยีสารสนเทศมอบหมาย ทำหน้าที่เป็นหน่วยประสานงานเครือข่ายไร้สายที่รับผิดชอบบริหารจัดการและให้บริการระบบเครือข่ายไร้สาย และให้มีหน้าที่ ดังนี้

(๑) กำหนดพื้นที่ให้บริการ คลื่นความถี่และมาตรฐานการใช้งาน ชื่อคลื่นที่ให้บริการและรูปแบบการเชื่อมต่อ รวมไปถึงวิธีการยืนยันตัวผู้ใช้ สำหรับบริการเครือข่ายไร้สายของสำนักงานทั้งหมด กลุ่มผู้ใช้งาน ระยะเวลาในการใช้งาน อายุการใช้งาน รวมไปถึงรายละเอียดการให้บริการอื่น ๆ โดยการเปลี่ยนแปลงใด ๆ ให้เสนอต่อผู้บริหารสารสนเทศระดับสูงเพื่อพิจารณาอนุมัติ โดยให้คงสภาพการบริการเครือข่ายไร้สายใน ณ วันที่ประกาศจนกว่าจะมีการเปลี่ยนแปลง

(๒) อนุมัติ หรือยกเลิกการให้บริการพนักงาน และ/หรือ อุปกรณ์ใด ๆ ของพนักงาน รวมไปถึงอุปกรณ์ใด ๆ ของสำนักงาน หรืออุปกรณ์ซึ่งใช้ในการปฏิบัติงานของสำนักงานในการใช้งานเครือข่ายไร้สายของสำนักงาน

(๓) อนุมัติให้บุคคลซึ่งมิใช่พนักงานของสำนักงาน และ/หรืออุปกรณ์อื่นใดของบุคคลซึ่งมิใช่พนักงานของสำนักงานเข้าใช้งานระบบเครือข่ายไร้สายของสำนักงาน

(๔) ผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงานกลางอาจมอบหมาย ตาม (๒) และ (๓) ให้หัวหน้างานหรือเจ้าหน้าที่ งานระบบสื่อสารและเครือข่าย

คอมพิวเตอร์ กระทำการแทนก็ได้

(๕) ติดตั้ง รื้อถอน ย้าย เปลี่ยนแปลง อุปกรณ์ระบบเครือข่าย อุปกรณ์ระบบเครือข่ายไร้สาย ตั้งค่าระบบเครือข่ายต่าง ๆ ตามความเหมาะสม

(๖) ตรวจสอบ ติดตาม หรือเฝ้าระวังการใช้งานระบบเครือข่ายและระบบเครือข่ายไร้สาย

(๗) ดำเนินการอื่นใดในส่วนที่เกี่ยวข้องกับระบบเครือข่ายและระบบเครือข่ายไร้สาย

ส่วนที่ ๗
การบริหารจัดการ การพัฒนาและจัดหาระบบสารสนเทศ

ข้อ ๖๒ หน่วยบริการเทคโนโลยีสารสนเทศต้องจัดทำข้อกำหนดความต้องการของระบบสารสนเทศที่จะจัดหา พัฒนา หรือปรับปรุงแก้ไข ในด้านความมั่นคงปลอดภัยสารสนเทศลงในเอกสารข้อกำหนด (Terms of Reference) ดังต่อไปนี้

(๑) มีการตรวจสอบความถูกต้องของสารสนเทศนำเข้า (Input Validation)

(๒) มีการตรวจสอบความถูกต้องของการประมวลผลข้อมูล (Processing Validation)

(๓) มีการจัดการกับข้อผิดพลาดในการประมวลผล (Error Handling)

(๔) มีการรายงานสถานะและการบันทึกการทำงานของระบบ (Monitoring and Logging)

(๕) มีการเข้ารหัสข้อมูล (Encryption) สำหรับข้อมูลลับ

(๖) มีการบริหารผู้ใช้งานและสิทธิ (User and Privilege Management)

(๗) มีการระบุและพิสูจน์ตัวตนผู้ใช้งาน (User Identification and Authentication)

ข้อ ๖๓ ในการจัดหาระบบสารสนเทศ หน่วยบริการเทคโนโลยีสารสนเทศจะต้องระบุความต้องการในด้านการสนับสนุนจากผู้ผลิต ผู้จัดจำหน่าย หรือผู้พัฒนาระบบสารสนเทศ ดังต่อไปนี้ลงในสัญญา เอกสารข้อกำหนด (Terms of Reference) หรือเอกสารอื่นใดที่มีผลบังคับใช้ได้ตามกฎหมาย

(๑) การฝึกอบรมเพื่อให้สามารถใช้งานได้

(๒) การจัดเตรียมคู่มือการใช้งาน

(๓) การจัดเตรียมวิธีการกู้คืนระบบสารสนเทศ

(๔) บริการระบบให้ความช่วยเหลือ (Help Desk) ในการแก้ไขปัญหาที่เกิดขึ้นในขั้นตอนการติดตั้งใช้งาน และปัญหาที่เกี่ยวข้อง

(๕) การบำรุงรักษาและการรับประกัน

ข้อ ๖๔ หน่วยบริการเทคโนโลยีสารสนเทศจะต้องกำหนดความต้องการด้านการพัฒนาระบบ รวมถึงดูแลขั้นตอนในการพัฒนาระบบ ในกรณีที่ทำการพัฒนาเองเพื่อใช้ภายในสำนักงาน ดังต่อไปนี้

(๑) มีการควบคุมเวอร์ชันของโค้ดต้นฉบับและสารสนเทศที่เกี่ยวข้อง และตรวจสอบได้ว่าการเปลี่ยนแปลงเกิดขึ้นเมื่อใดและโดยบุคคลใด รวมถึงเก็บรักษาเวอร์ชันเก่าไว้อย่างน้อย ๑ เวอร์ชัน

(๒) ต้องมีการทดสอบระบบงานก่อนการติดตั้งบนระบบให้บริการจริง และมีการทดสอบตามความต้องการทั้งหมดที่ระบุไว้ในเอกสารข้อกำหนด (Terms of Reference) มีการทดสอบข้อกำหนดความต้องการด้านความมั่นคงปลอดภัย (Security Test) การทดสอบทีละส่วน (Unit Test) การทดสอบโดยรวมทั้งระบบ (Integration Test) และการทดสอบเพื่อตรวจรับระบบ (User Acceptance Test) เป็นอย่างน้อย

(๓) ข้อมูลทดสอบที่ใช้เพื่อทดสอบระบบสารสนเทศที่พัฒนาแล้ว ต้องเป็นข้อมูลทดสอบที่ไม่มีข้อมูลลับหรือข้อมูลส่วนบุคคลอยู่ด้วย หากเป็นสารสนเทศที่นำมาจากข้อมูลจริงต้องได้รับการอนุญาตจากเจ้าของข้อมูล และมีการควบคุมการเข้าถึงข้อมูลทดสอบเฉพาะผู้ที่มีหน้าที่เกี่ยวข้องในการพัฒนาระบบเท่านั้น

ข้อ ๖๕ ผู้ดูแลระบบต้องจัดเก็บซอฟต์แวร์ต้นฉบับ (รวมถึงโค้ดต้นฉบับ (Source Code)) และเอกสารแสดงสิทธิการใช้งานของระบบสารสนเทศที่จัดหามาเพื่อใช้ในสำนักงานในสถานที่ปลอดภัย เพื่อป้องกันการสูญหาย และมีการควบคุมการเข้าถึง

ข้อ ๖๖ ห้ามผู้ดูแลระบบเปลี่ยนแปลงแก้ไขซอฟต์แวร์ต้นฉบับของระบบสารสนเทศที่จัดหามา เว้นแต่มีความจำเป็นและต้องการรักษาประโยชน์ของสำนักงาน โดยคณะกรรมการบริหารเทคโนโลยีสารสนเทศมอบหมายให้ผู้ดูแลระบบเทคโนโลยีสารสนเทศดำเนินการ และไม่ขัดกับข้อตกลงการใช้งานกับผู้ผลิต ผู้จัดจำหน่าย หรือผู้พัฒนาระบบสารสนเทศนั้น

ข้อ ๖๗ ผู้ดูแลระบบต้องตรวจสอบระบบสารสนเทศที่ส่งมอบ ไม่ให้มีข้อมูลทดสอบและช่องทางการเข้าถึงของผู้พัฒนาตกค้างอยู่ในระบบ

ส่วนที่ ๘
การป้องกันสารสนเทศรั่วไหล

ข้อ ๖๘ หน่วยบริการเทคโนโลยีสารสนเทศต้องจัดเตรียมวิธีการหรือเครื่องมือสำหรับเข้ารหัสลับและติดตั้งระบบเข้ารหัสลับสำหรับเครื่องคอมพิวเตอร์ที่ใช้ในกิจการของสำนักงาน ได้แก่

เครื่องคอมพิวเตอร์แบบพกพา และสื่อบันทึกข้อมูลพกพาประเภท Flash Driveหรือ External Harddisk รวมถึงเครื่องคอมพิวเตอร์ที่สำนักงานเช่าเพื่อใช้งาน เพื่อให้สารสนเทศที่มีชั้นความลับ ตั้งแต่ระดับลับขึ้นไปมีการเข้ารหัสลับเสมอ เพื่อป้องกันการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต

สำหรับเครื่องคอมพิวเตอร์ที่ไม่ได้เป็นของสำนักงาน แต่ใช้ในกิจการของสำนักงาน ให้หน่วยบริการเทคโนโลยีสารสนเทศจัดเตรียมวิธีการเข้ารหัสลับของสารสนเทศ หรือเตรียมเครื่องมือให้ผู้ใช้งานสามารถนำไปใช้งาน และร่วมเป็นส่วนหนึ่งในการให้ความรู้กับผู้ใช้งานถึงความจำเป็นของการรักษาความลับและวิธีการเข้ารหัสลับของข้อมูลลับ

ส่วนที่ ๙
การบริหารจัดการเมื่อเกิดเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๖๙ ให้หน่วยบริการเทคโนโลยีสารสนเทศจัดเตรียมช่องทางเพื่อให้ผู้ใช้งานรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย และจัดเตรียมกลไกในการติดตามดูแลก่อนเกิดเหตุการณ์ด้านความมั่นคงปลอดภัยแต่ละประเภท โดยผู้ดูแลระบบต้องตรวจสอบแฟ้มที่บันทึกการใช้งาน (Log File) และจัดเตรียมแผนหรือกระบวนการในการรับมือเหตุการณ์ด้านความมั่นคงปลอดภัยภายหลังจากได้รับรายงานเหตุการณ์ด้านความมั่นคงปลอดภัยแต่ละประเภท และแจ้งกลับไปยังผู้รายงานเหตุการณ์ด้านความมั่นคงปลอดภัยถึงการดำเนินการที่เกิดขึ้น

ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย มีดังต่อไปนี้

(๑) บัญชีผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานถูกละเมิด

(๒) เครื่องคอมพิวเตอร์ติดไวรัสหรือชุดคำสั่งไม่พึงประสงค์

(๓) ฮาร์ดแวร์หรืออุปกรณ์ภายในระบบสารสนเทศเกิดความเสียหาย หรือทำงานผิดปกติ

(๔) ซอฟต์แวร์ทำงานผิดปกติอันอาจจะก่อให้เกิดความเสียหายต่อสารสนเทศได้

(๕) การเข้าพื้นที่ทำงานหรือพื้นที่จัดเก็บระบบสารสนเทศโดยไม่ได้รับอนุญาต เช่น พื้นที่ห้องเครื่องบริการ พื้นที่จัดเก็บสื่อบันทึกข้อมูล เป็นต้น

(๖) การเข้าถึงระบบเครือข่ายและระบบเครือข่ายไร้สายของสำนักงานโดยไม่ได้รับอนุญาต

(๗) การเข้าถึงระบบสารสนเทศโดยไม่ได้รับอนุญาต

(๘) การรบกวนการทำงานของระบบเครือข่ายของสำนักงาน ได้แก่ การทำ Sniffing การทำ Pinged Floods การทำ Packet Spoofing การโจมตีแบบ Denial of Service หรือการทำ Forged Routing Information เป็นต้น

(๙) การทำ Port Scanning และ Security Scanning โดยไม่ได้รับอนุญาต

(๑๐) การติดตั้งฮาร์ดแวร์หรือซอฟต์แวร์ที่เกี่ยวข้องกับการให้บริการระบบเครือข่ายของสำนักงานโดยไม่ได้รับอนุญาต

(๑๑) การพยายามเข้าถึงสารสนเทศที่ไม่ได้รับอนุญาตให้รับรู้

(๑๒) การพยายามหลบเลี่ยงมาตรการด้านความมั่นคงปลอดภัยของระบบสารสนเทศ

ส่วนที่ ๑๐
การสำรองสารสนเทศและระบบสารสนเทศ

ข้อ ๗๐ ให้คณะกรรมการบริหารเทคโนโลยีสารสนเทศเตรียมความพร้อมในการบริหารความต่อเนื่องในการปฏิบัติงาน เพื่อรับมือต่อเหตุฉุกเฉินหรือภัยพิบัติที่อาจเกิดขึ้น

ให้คณะกรรมการบริหารเทคโนโลยีสารสนเทศจัดตั้งคณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉิน ประกอบด้วยตัวแทนจากเจ้าของระบบงาน หน่วยงานที่ดูแลข้อมูล และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงที่เกี่ยวข้อง

ข้อ ๗๑ ให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินดำเนินการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินเป็นลายลักษณ์อักษร เพื่อให้สามารถใช้งานสารสนเทศและระบบสารสนเทศของสำนักงานได้อย่างต่อเนื่อง และประชาสัมพันธ์แก่พนักงานและพนักงานโครงการเพื่อเสริมสร้างความรู้และความเข้าใจเกี่ยวกับแผนเตรียมความพร้อมกรณีฉุกเฉินรวมทั้งปรับปรุงให้ทันสมัยอยู่เสมอ

ข้อ ๗๒ ในการจัดทำแผนตามข้อ ๗๑ ให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินจัดทำรายการระบบสารสนเทศและสินทรัพย์ที่สำคัญ และมาตรการการสำรองสารสนเทศและระบบสารสนเทศที่มีอยู่ และให้จัดเรียงลำดับความสำคัญ โดยวิเคราะห์ผลกระทบที่จะเกิดขึ้นในกรณีเกิดเหตุที่ทำให้ระบบไม่สามารถใช้งานได้ เพื่อจัดทำระบบสารสนเทศสำรองให้พร้อมใช้งานในกรณีที่เกิดเหตุฉุกเฉิน และให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินทำการทบทวนรายการการจัดเรียงลำดับความสำคัญ เสนอต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศ ปีละ ๑ ครั้ง

ข้อ ๗๓ ให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินจัดทำระบบสารสนเทศสำรองซึ่งอยู่ในสภาพพร้อมใช้งานในกรณีที่เกิดเหตุฉุกเฉิน เพื่อให้สามารถใช้งานระบบสารสนเทศสำรองได้ในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ โดยนำเสนอต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศเพื่อพิจารณาความเหมาะสมของระบบสารสนเทศสำรองดังกล่าว รวมถึงค่าใช้จ่ายที่จะเกิดขึ้น ทั้งนี้ คณะกรรมการบริหารเทคโนโลยีสารสนเทศอาจใช้หลักการพิจารณาโดยการกำหนดระดับการให้บริการ (Service Level) ของทั้งระบบสารสนเทศ และกำหนดช่วงเวลาที่ยอมรับได้ในกรณีที่ระบบสารสนเทศไม่สามารถให้บริการได้

ข้อ ๗๔ ให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินจัดทำขั้นตอนการปฏิบัติตามแผนเตรียมความพร้อมกรณีฉุกเฉิน ตั้งแต่ขั้นตอนการแจ้งผู้ใช้งาน ขั้นตอนการเตรียมการสำรองสารสนเทศและการปิดระบบสารสนเทศ ขั้นตอนการเคลื่อนย้ายสารสนเทศและระบบสารสนเทศ และขั้นตอนการใช้งานระบบสารสนเทศสำรอง รวมถึงการกำหนดตัวผู้รับผิดชอบ และประมาณเวลาในการดำเนินการตามขั้นตอนต่าง ๆ เพื่อให้สามารถใช้งานระบบสารสนเทศสำรองได้ตามเป้าหมายที่กำหนดไว้ในแผนนั้น

ข้อ ๗๕ ให้คณะทำงานบริหารแผนเตรียมความพร้อมกรณีฉุกเฉินทำการทดสอบสภาพพร้อมใช้งาน ของระบบสารสนเทศสำรอง และระบบแผนเตรียมความพร้อมกรณีฉุกเฉินที่เตรียมไว้ อย่างน้อยปีละ ๑ ครั้ง และให้รายงานผลการทดสอบ ระยะเวลาการดำเนินการ และบทเรียนที่ได้รับจากการทดสอบต่อคณะกรรมการบริหารเทคโนโลยีสารสนเทศ

ส่วนที่ ๑๑
การบริหารจัดการผู้ให้บริการภายนอก

ข้อ ๗๖ ผู้ดูแลระบบศึกษาลักษณะงานจ้างผู้ให้บริการภายนอก กำหนดและตกลงความต้องการด้านความมั่นคงปลอดภัยสารสนเทศกับผู้ให้บริการภายนอกในเรื่องที่เกี่ยวข้องกับการเข้าถึง การประมวลผล การจัดเก็บ การสื่อสาร และการให้บริการระบบสารสนเทศและเครือข่ายของสำนักงาน

ข้อ ๗๗ ผู้ดูแลระบบนำแนวปฏิบัติที่เกี่ยวข้องในเอกสารฉบับนี้มากำหนดไว้ในสัญญาจ้างและให้ผู้ให้บริการภายนอกต้องปฏิบัติตามอย่างเคร่งครัด (ตามตารางด้านล่าง)

ลักษณะงานจ้าง	แนวปฏิบัติขั้นต่ำที่ควรนำไปกำหนดไว้ในสัญญาจ้าง
การพัฒนาระบบสารสนเทศให้มีความมั่นคงปลอดภัย	• แนวปฏิบัติด้านการบริหารจัดการการพัฒนาและจัดหาระบบสารสนเทศ (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • แนวปฏิบัติด้านการบริหารจัดการสิทธิและรหัสผ่านอย่างมั่นคงปลอดภัย (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • แนวปฏิบัติของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)

การบริหารจัดการระบบสารสนเทศ	• แนวปฏิบัติด้านการดูแลระบบทั่วไป (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • แนวปฏิบัติด้านการบริหารจัดการสิทธิและรหัสผ่านอย่างมั่นคงปลอดภัย (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • แนวปฏิบัติของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)
การบริหารจัดการระบบเครือข่าย	• แนวปฏิบัติด้านการบริหารจัดการความมั่นคงปลอดภัยของระบบเครือข่าย (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • การบริหารจัดการระบบเครือข่ายไร้สายของสำนักงาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง) • แนวปฏิบัติของผู้ใช้งาน (บางส่วนหรือทั้งหมดขึ้นอยู่กับความจำเป็นและความเกี่ยวข้อง)

ข้อ ๗๘ ผู้ดูแลระบบแจ้งให้ผู้ให้บริการภายนอกได้รับทราบถึงในการจ้างช่วงไปยังผู้รับจ้างอื่น ๆ ต้องมีการแจ้งให้สำนักงานได้รับทราบอย่างเป็นลายลักษณ์อักษรและระบุในสัญญาเกี่ยวกับความรับผิดชอบต่อความเสี่ยงที่เกิดขึ้นจากการจ้างช่วงนั้น ทั้งนี้ เพื่อป้องกันความเสี่ยงต่าง ๆ อันจะส่งผลกระทบต่อลักษณะงานจ้างที่สำนักงานกำหนด และผู้รับจ้างช่วงจะต้องผูกผันตามข้อกำหนดแนวปฏิบัติตามที่ผู้รับจ้างผูกพันตามสัญญานั้นด้วย

ข้อ ๗๙ ผู้ดูแลระบบ ติดตาม ทบทวน และประเมินการให้บริการของผู้ให้บริการภายนอกอย่างสม่ำเสมอให้สอดคล้องกับข้อกำหนดที่ระบุไว้ในสัญญาจ้าง

ข้อ ๘๐ กรณีมีการเปลี่ยนแปลงขอบเขตงานของผู้ให้บริการภายนอก ผู้ดูแลระบบบริหารจัดการการเปลี่ยนแปลงนั้น โดยดำเนินการตามข้อ ๗๖ ถึง ๗๘ ใหม่อีกครั้ง และกำหนดไว้ในสัญญาจ้าง

หมวด ๔
การตรวจสอบและประเมินความมั่นคงปลอดภัยด้านสารสนเทศ (สำหรับผู้ตรวจสอบ)

ข้อ ๘๑ ระบบสารสนเทศต้องได้รับการตรวจสอบและประเมินความมั่นคงปลอดภัยด้านสารสนเทศ (Information Security Audit and Assessment) อย่างสม่ำเสมอ อย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเกิดสถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด

ข้อ ๘๒ การตรวจสอบและประเมินความมั่นคงปลอดภัยด้านสารสนเทศ อาจทำโดยผู้ตรวจสอบภายในหรือภายนอกหน่วยบริการเทคโนโลยีสารสนเทศก็ได้ แต่ผู้ตรวจสอบต้องมีความเป็นอิสระและไม่ตรวจสอบระบบสารสนเทศที่ตนเองเป็นผู้ดูแลหรือบริหารจัดการอยู่ โดยผู้ตรวจสอบต้องรักษาความลับของสำนักงานโดยการลงนามในข้อตกลงการรักษาข้อมูลที่เป็นความลับ

หมวด ๕
การใช้งานสารสนเทศ ระบบสารสนเทศและเครือข่ายของสำนักงาน (สำหรับผู้ใช้งาน)

ส่วนที่ ๑
การใช้งานทั่วไป

ข้อ ๘๓ ระบบสารสนเทศเป็นระบบที่สำนักงานพัฒนาขึ้นหรือจัดหามาเพื่อใช้ในการดำเนินงานของสำนักงานเท่านั้น การใช้งานระบบสารสนเทศและอุปกรณ์ต่าง ๆ ของผู้ใช้งานเพื่อกิจธุระส่วนตัวอนุญาตให้สามารถใช้ได้ในขอบเขตที่จำกัดตามความเหมาะสม และต้องไม่เป็นการรบกวนต่อผู้อื่นหรือเป็นอุปสรรคต่อการทำงานตามตำแหน่งหน้าที่และความรับผิดชอบ

ข้อ ๘๔ ผู้ใช้งานต้องปฏิบัติตามกฎหมาย ข้อบังคับ ระเบียบ ประกาศ และคำสั่งของสำนักงานที่เกี่ยวข้องกับระบบสารสนเทศ ตลอดจนข้อกำหนดด้านการรักษาความมั่นคงปลอดภัยสารสนเทศและระบบสารสนเทศ

ข้อ ๘๕ ผู้ใช้งานต้องใช้งานระบบเครือข่ายทั้งแบบมีสายและไร้สายของสำนักงานภายใต้วัตถุประสงค์เพื่อการปฏิบัติงานและสนับสนุนการดำเนินงานของสำนักงานเท่านั้น

ข้อ ๘๖ ผู้ใช้งานต้องใช้งานระบบสารสนเทศอย่างระมัดระวัง และดูแลปกป้องเสมือนเป็นทรัพย์สินของตน

ข้อ ๘๗ ผู้ใช้งานต้องทำการออกจากระบบสารสนเทศ (Log off) ทุกครั้งหลังจากเลิกใช้งาน และใช้ฟังก์ชันการปกป้องด้วยรหัสผ่านของ Screen Saver โดยอัตโนมัติ หากไม่ได้ใช้งานอุปกรณ์เป็นระยะเวลาหนึ่ง

ข้อ ๘๘ ผู้ใช้งานที่ใช้เครื่องคอมพิวเตอร์ส่วนบุคคลที่มิใช่ของสำนักงานเชื่อมต่อเข้าระบบสารสนเทศต้องเข้าถึงผ่านช่องทาง VPN/SSL-VPN หรือช่องทางสื่อสารอื่น ๆ ที่สำนักงานได้จัดเตรียมไว้ ซึ่งมีการเข้ารหัสลับข้อมูลในการสื่อสารเพื่อความมั่นคงปลอดภัยแล้ว

ผู้ใช้งานต้องใช้ความระมัดระวังมากเป็นพิเศษ เพื่อปกป้องอุปกรณ์คอมพิวเตอร์พกพา รวมถึงสารสนเทศที่อยู่ในอุปกรณ์เหล่านั้นมิให้ถูกล่วงละเมิดโดยบุคคลที่ไม่ได้รับอนุญาตซึ่งรวมถึงสมาชิกในครอบครัวของพนักงานและพนักงานโครงการด้วย

ข้อ ๘๙ ผู้ใช้งานพึงปฏิบัติ ดังนี้

(๑) ใช้งานซอฟต์แวร์ตามที่สำนักงานติดตั้งให้ตามมาตรฐานการติดตั้งของสำนักงานเท่านั้น

(๒) ตรวจสอบการทำงานของระบบปฏิบัติการ รวมไปถึงการปรับปรุง patch อย่างสม่ำเสมอ

(๓) ตรวจสอบการทำงานของซอฟต์แวร์ป้องกันชุดคำสั่งไม่พึงประสงค์ ว่ายังสามารถทำงานเป็นปกติ และมีการปรับปรุงข้อมูลในการตรวจสอบอย่างสม่ำเสมอ อย่างน้อย ๑ ครั้งต่อสัปดาห์

(๔) ไม่ถอดถอน หรือระงับการทำงานของซอฟต์แวร์ หรือขัดขวางไม่ให้ซอฟต์แวร์ทำงานได้ตามปกติ สำหรับซอฟต์แวร์มาตรฐาน

(๕) หากมีความประสงค์จะติดตั้งใช้งานซอฟต์แวร์อื่นใดลงบนเครื่อง ผู้ใช้งานมีหน้าที่ต้องใช้ซอฟต์แวร์ที่มีลิขสิทธิ์การใช้งานอย่างถูกต้องเท่านั้น

(๖) หากพบความผิดปกติ เกิดขึ้นทั้งในส่วนของระบบปฏิบัติการ ซอฟต์แวร์ป้องกันชุดคำสั่งไม่พึงประสงค์ต่าง ๆ เช่น ซอฟต์แวร์ Anti-Virus Anti-Spyware Anti-Malware และ Firewall เป็นต้น รวมถึง Application อื่น ๆ ให้แจ้งต่อหน่วยบริการสารสนเทศโดยเร็ว

ข้อ ๙๐ ผู้ใช้งานต้องไม่ดัดแปลงหรือติดตั้งอุปกรณ์ใด ๆ เพิ่มเติมที่อาจส่งผลกระทบต่อความมั่นคงปลอดภัยของระบบสารสนเทศ และต้องไม่อนุญาตให้ผู้หนึ่งผู้ใดกระทำการดังกล่าว หากต้องการดัดแปลงหรือติดตั้งอุปกรณ์เพิ่มเติมเพื่อการวิจัยและพัฒนา ผู้ใช้งานต้องขออนุมัติต่อผู้บังคับบัญชาตามลำดับชั้นจนถึงผู้อำนวยการ หรือผู้อำนวยการหน่วยงานเฉพาะทางที่ตนสังกัด

แล้วแต่กรณี และอนุญาตให้กระทำในระบบปิดที่ไม่ส่งผลกระทบกับระบบสารสนเทศของสำนักงานเท่านั้น

ข้อ ๙๑ ผู้ใช้งานต้องไม่ติดตั้งระบบคอมพิวเตอร์บริการ ประเภทเครื่องบริการถ่ายโอนแฟ้มข้อมูล (FTP Server) หรือเครื่องบริการเว็บ (Web Server) เป็นต้น ยกเว้นมีวัตถุประสงค์เพื่อการวิจัยและพัฒนาโดยผู้ใช้งานต้องขออนุมัติต่อผู้บังคับบัญชาตามลำดับชั้นจนถึงผู้อำนวยการ หรือผู้อำนวยการหน่วยงานเฉพาะทางที่ตนสังกัด แล้วแต่กรณี และแจ้งต่อหน่วยบริการเทคโนโลยีสารสนเทศเพื่อให้ดำเนินการรักษาความมั่นคงปลอดภัยในส่วนที่เกี่ยวข้องต่อไป

ข้อ ๙๒ ผู้ใช้งานต้องตรวจสอบว่าเครื่องคอมพิวเตอร์ที่ใช้งานมีเวลาที่แม่นยำอยู่เสมอและตรวจสอบทุกครั้งที่ใช้งานเครื่องคอมพิวเตอร์ เพื่อให้การใช้งานซอฟต์แวร์และโปรแกรมต่าง ๆ มีความถูกต้อง หากสังเกตเห็นว่าเวลาที่ปรากฏบนเครื่องคอมพิวเตอร์แตกต่างจากเวลาปกติ ให้ดำเนินการแก้ไขวันที่หรือเวลาให้ถูกต้องหรือแจ้งผู้ดูแลระบบเพื่อดำเนินการตรวจสอบและแก้ไข

ข้อ ๙๓ ผู้ใช้งานต้องตั้งชื่อไฟล์สารสนเทศที่สามารถเข้าใจได้ง่ายโดยเริ่มต้นด้วยปี เดือน และวันที่สร้างสารสนเทศ ตามด้วยชื่อเรื่อง เพื่อให้ง่ายต่อการเรียกดูไฟล์เวอร์ชันเก่าในภายหลัง และให้เป็นภาษาอังกฤษและตัวเลขอารบิกเพื่อให้ลดปัญหาเรื่องการจัดเก็บชื่อไฟล์ภาษาไทยในระบบสารสนเทศ ตัวอย่างของชื่อไฟล์สารสนเทศที่เข้าใจง่ายคือ 20160101-draft.odt โดยให้เป็นไปตามมาตรฐานการกำหนดชื่อแฟ้มเอกสารและโฟลเดอร์ของสำนักงาน

ข้อ ๙๔ ในการปฏิบัติงานของสำนักงาน ผู้ใช้งานต้องไม่ใช้โปรแกรมบริการสาธารณะ ได้แก่ จดหมายอิเล็กทรอนิกส์ส่วนบุคคล (Personal E-mail/ Free E-mail) โปรแกรมประเภท Instant Messaging และบริการฝากไฟล์ (File Sharing) เป็นต้น ซึ่งผู้ให้บริการสามารถเก็บและเข้าถึงสารสนเทศของสำนักงานที่ส่งผ่านบริการเหล่านั้นได้ และใช้ความระมัดระวังในการสื่อสารข้อมูลผ่านทางอุปกรณ์สื่อสารเคลื่อนที่ซึ่งอาจมีความเสี่ยงที่ผู้ให้บริการจะเก็บและเข้าถึงสารสนเทศของสำนักงาน

ข้อ ๙๕ ผู้ใช้งานทุกคนต้องเข้ารับการฝึกอบรมเกี่ยวกับความมั่นคงปลอดภัยของระบบสารสนเทศและคอมพิวเตอร์ (Security Awareness) ทุกสามปี เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์

ข้อ ๙๖ ผู้ใช้งานต้องไม่ใช้ระบบสารสนเทศในการข่มขู่หรือคุกคามทุกรูปแบบต่อบุคคลภายในหรือภายนอกสำนักงาน หรือใช้ในการใด ๆ ที่ขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน

ข้อ ๙๗ ผู้ใช้งานต้องพึงระวังการส่งจดหมายอิเล็กทรอนิกส์ของสำนักงานถึงกลุ่มผู้รับขนาดใหญ่ โดยต้องไม่ใช้ระบบสารสนเทศในการแสดงความคิดเห็นหรือส่งข้อความใด ๆ ที่ไม่เกี่ยวข้องกับการปฏิบัติงานของสำนักงานไปหาบุคคลจำนวนมาก

ข้อ ๙๘ ห้ามมิให้ผู้ใช้งานใช้ระบบสารสนเทศของสำนักงานในลักษณะที่อาจก่อให้เกิดความเสียหายต่อสำนักงานหรือบุคคลอื่น หรือการละเมิดทรัพย์สินทางปัญญา หรือลิขสิทธิ์ หรือสัญญาอนุญาตการใช้งานซอฟต์แวร์ หรือละเมิดกฎหมายใด ๆ หรือการเผยแพร่ซอฟต์แวร์หรือเอกสารที่มีลิขสิทธิ์ไม่ถูกต้อง หรือเผยแพร่ข้อมูลลับของสำนักงาน หรือเผยแพร่ข้อมูลส่วนบุคคลซึ่งไม่อยู่ในเกณฑ์ที่ต้องเปิดเผย

ส่วนที่ ๒
การใช้งานซอฟต์แวร์ และโปรแกรมต่าง ๆ

ข้อ ๙๙ ห้ามมิให้ผู้ใช้งานติดตั้ง หรือเผยแพร่ซอฟต์แวร์ หรือละเมิดลิขสิทธิ์ในซอฟต์แวร์ หรือทำสำเนาของซอฟต์แวร์ หรือสารสนเทศที่มีลิขสิทธิ์ของสำนักงาน ไปใช้งานบนเครื่องคอมพิวเตอร์หรือระบบเครือข่ายอื่น ๆ ที่ไม่ได้รับอนุญาต การขออนุญาตให้ทำผ่านหัวหน้างานของหน่วยงานผ่านไปยังหน่วยบริการเทคโนโลยีสารสนเทศ

ข้อ ๑๐๐ หากผู้ใช้งานละเมิดตามข้อ ๘๙ ข้อ ๙๘ และ ข้อ ๙๙ ก่อให้เกิดความเสียหายหรือการฟ้องร้อง ผู้ใช้งานจะต้องรับผิดชอบค่าเสียหายที่เกิดขึ้นแต่เพียงผู้เดียว

ส่วนที่ ๓
การใช้งานจดหมายอิเล็กทรอนิกส์

ข้อ ๑๐๑ ผู้ใช้งานต้องใช้บัญชีจดหมายอิเล็กทรอนิกส์ที่สำนักงานจัดให้ด้วยความระมัดระวัง โดยคำนึงอยู่เสมอว่าตนเองเป็นผู้ส่งจดหมายอิเล็กทรอนิกส์นั้นในนามของสำนักงาน

ข้อ ๑๐๒ บัญชีจดหมายอิเล็กทรอนิกส์ทั้งหมด และจดหมายอิเล็กทรอนิกส์ทุกฉบับที่ถูกสร้างและเก็บรักษาอยู่บนระบบสารสนเทศถือเป็นทรัพย์สินของสำนักงาน

ข้อ ๑๐๓ ผู้ใช้งานต้องไม่ยินยอมให้บุคคลอื่นใช้บัญชีจดหมายอิเล็กทรอนิกส์ของตน และไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ของบุคคลอื่นด้วย

ข้อ ๑๐๔ ผู้ใช้งานมีหน้าที่ต้องบริหารจัดการกล่องรับจดหมายอิเล็กทรอนิกส์ (Mailbox) ของตนเองที่สำนักงานจัดสรรให้ เพื่อให้สามารถรับ-ส่งจดหมายอิเล็กทรอนิกส์ได้ตามปกติอยู่เสมอ และพึงตระหนักว่าสำนักงานมีพื้นที่ให้บริการกล่องรับจดหมายอิเล็กทรอนิกส์ที่มีขนาดจำกัด และเครื่องบริการ (Server) จะไม่สามารถรับ–ส่งจดหมายอิเล็กทรอนิกส์ได้หากจดหมายอิเล็กทรอนิกส์ทั้งหมดมีขนาดเกินจากขนาดที่สำนักงานกำหนดไว้

ข้อ ๑๐๕ ผู้ใช้งานต้องบริหารจัดการขนาดของจดหมายอิเล็กทรอนิกส์แต่ละฉบับของตนไม่ให้เกินมาตรฐานที่สำนักงานกำหนดไว้ เพื่อให้สามารถรับ-ส่งจดหมายอิเล็กทรอนิกส์ได้ตามปกติ

ข้อ ๑๐๖ ห้ามใช้จดหมายอิเล็กทรอนิกส์ของสำนักงานเพื่อการใด ๆ อันเป็นการขัดต่อกฎหมาย ข้อบังคับ ระเบียบ ประกาศ และคำสั่งของสำนักงาน รวมถึงการใช้งานที่มีลักษณะ ดังต่อไปนี้

(๑) กระทำการใด ๆ อันเป็นความผิดตามกฎหมาย เช่น เพื่อการค้าขาย โฆษณา แจกจ่าย เผยแพร่สิ่งเสพติดหรือสินค้าหนีภาษี หรือผลิตภัณฑ์ละเมิดลิขสิทธิ์ หรือกระทำการฉ้อโกง เป็นต้น

(๒) ส่งจดหมายอิเล็กทรอนิกส์ที่ผู้รับไม่มีความต้องการ เช่น จดหมายอิเล็กทรอนิกส์ขยะ จดหมายอิเล็กทรอนิกส์สแปม โฆษณาชวนเชื่อต่าง ๆ จดหมายลูกโซ่ หรือการหลอกลวงใด ๆ เป็นต้น

(๓) ส่งหรือส่งต่อจดหมายอิเล็กทรอนิกส์ที่มีรูปภาพหรือเนื้อหาดูหมิ่น หมิ่นประมาทหรือกล่าวร้ายทำให้บุคคลอื่นเสื่อมเสียชื่อเสียง เหยียดชนชั้น ข่มขู่ การพนัน หรือลามกอนาจาร

(๔) กระทำการใด ๆ อันเป็นความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์หรือฝ่าฝืนประกาศที่คณะกรรมการบริหารเทคโนโลยีสารสนเทศกำหนด

ข้อ ๑๐๗ ห้ามผู้ใช้งานทำสำเนาจดหมายอิเล็กทรอนิกส์ ข้อความ หรือไฟล์แนบที่เป็นข้อมูลลับจากจดหมายอิเล็กทรอนิกส์ รวมถึงห้ามส่งต่อ (Forward) จดหมายอิเล็กทรอนิกส์ที่เป็นข้อมูลลับของบุคคลอื่นโดยไม่ได้รับอนุญาตจากเจ้าของข้อมูล

การส่งข้อมูลลับผ่านระบบจดหมายอิเล็กทรอนิกส์ต้องมีการระบุชั้นความลับ และบุคคลผู้มีสิทธิเข้าถึงข้อมูลลับนั้น เพื่อให้ผู้ใช้งานหรือผู้ที่ได้รับข้อมูลทราบว่าตนมีสิทธิเข้าถึงข้อมูลนั้นหรือไม่ ในกรณีที่ผู้ได้รับข้อมูลไม่ใช่บุคคลที่มีสิทธิเข้าถึงข้อมูลลับดังกล่าว ให้ผู้รับข้อมูลลับนั้นทำลายข้อมูลที่ได้รับทันทีและแจ้งให้ผู้ส่งข้อมูลลับนั้นทราบด้วย

ข้อ ๑๐๘ ห้ามผู้ใช้งานทำการปลอมแปลงข้อความใด ๆ ในจดหมายอิเล็กทรอนิกส์ ทั้งนี้ ครอบคลุมถึงส่วนของจดหมายอิเล็กทรอนิกส์ที่ระบุผู้รับ ผู้ส่ง วันเวลา และหัวเรื่อง (E-mail Header) เนื้อความของจดหมายอิเล็กทรอนิกส์ และลายมือชื่ออิเล็กทรอนิกส์ในจดหมายอิเล็กทรอนิกส์ เพื่อให้เกิดความเข้าใจที่คลาดเคลื่อนในจดหมายอิเล็กทรอนิกส์ของบุคคลอื่น

ข้อ ๑๐๙ ผู้ใช้งานต้องตั้งค่าหรือตรวจสอบการตั้งค่าข้อมูลผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender) ให้ประกอบด้วย ชื่อ-นามสกุลของผู้ส่งเป็นภาษาอังกฤษ และจดหมายอิเล็กทรอนิกส์ของผู้ส่งเป็นอย่างน้อยและในกรณีที่ต้องการให้ผู้รับตอบกลับมาที่บัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม ให้ตั้งค่าบัญชีจดหมายอิเล็กทรอนิกส์กลุ่มนั้นที่ “Reply To” แทนการเปลี่ยนแปลงที่ข้อมูลผู้ส่งจดหมายอิเล็กทรอนิกส์ (Sender)

ข้อ ๑๑๐ ผู้ใช้งานต้องเขียนชื่อเรื่อง (Subject) ของจดหมายอิเล็กทรอนิกส์แต่ละฉบับที่กระชับแต่สามารถเข้าใจเนื้อหาของจดหมายอิเล็กทรอนิกส์ได้ง่าย มีรายละเอียดของเนื้อหามากที่สุด หรือในกรณีที่ต้องการให้สามารถเก็บจดหมายอิเล็กทรอนิกส์เป็นชุดเดียวกันได้ อาจเพิ่มคำนำหน้าของชื่อเรื่องจดหมายอิเล็กทรอนิกส์ โดยการระบุชื่อสำคัญอยู่ในวงเล็บเหลี่ยม ตัวอย่าง [NAC 2012] ขอเลื่อนการประชุมการจัดงาน NAC 2012 เป็นวันที่ ๑๑ มีนาคม ๒๕๕๕ จาก ๑๓.๐๐ น. เป็น ๑๕.๐๐ น. เป็นต้น

ข้อ ๑๑๑ ในกรณีที่ผู้ใช้งานมีเอกสารแนบที่ต้องการสื่อด้วยข้อความสั้น ๆ หรือไฟล์เอกสารที่ประกอบด้วยตัวอักษรความยาวไม่เกิน ๒๐ บรรทัด ไม่ต้องแนบไฟล์ แต่ให้นำข้อความทั้งหมดวางลงในเนื้อหาของจดหมายอิเล็กทรอนิกส์ เพื่อให้สะดวกต่อผู้อ่าน และลดเวลาในการเปิดไฟล์และการทำงานของระบบ

ข้อ ๑๑๒ ในกรณีที่ผู้ใช้งานต้องการแนบไฟล์ภาพประกอบในจดหมายอิเล็กทรอนิกส์ให้ลดขนาดของภาพเหลือไม่เกิน ๑ ล้านพิกเซล หรือไม่เกิน ๓๐๐ กิโลไบต์ เพื่อให้จดหมายอิเล็กทรอนิกส์มีขนาดเล็กลงแต่ผู้อ่านสามารถดูไฟล์ได้บนหน้าจอ

ข้อ ๑๑๓ ให้ผู้ใช้งานพึงหลีกเลี่ยงการส่งไฟล์ขนาดใหญ่ผ่านทางจดหมายอิเล็กทรอนิกส์ หรือการส่งไฟล์จำนวนหลายไฟล์ หากต้องการส่งไฟล์ขนาดใหญ่ ให้ใช้ระบบรับฝากไฟล์ขนาดใหญ่ร่วมกับการส่งจดหมายอิเล็กทรอนิกส์แจ้งแบบที่ไม่มีไฟล์แนบแทน เพื่อให้จดหมายอิเล็กทรอนิกส์มีขนาดเล็ก

ข้อ ๑๑๔ ผู้ใช้งานต้องส่งจดหมายอิเล็กทรอนิกส์ให้แก่ผู้รับที่เกี่ยวข้องและจำเป็นต้องรับทราบสารสนเทศเท่านั้น และหากได้รับจดหมายอิเล็กทรอนิกส์ที่มีผู้รับร่วมกันหลายคน ให้พึงระวังไม่ใช้คำสั่ง

"Reply All" ถ้าหากจดหมายอิเล็กทรอนิกส์ฉบับนั้นไม่ได้มีความจำเป็นต้องให้ผู้รับทุกคนตอบกลับหรือรับทราบ

ข้อ ๑๑๕ ผู้ใช้งานต้องพึงระวังในการส่งจดหมายอิเล็กทรอนิกส์ถึงกลุ่มผู้รับขนาดใหญ่โดยตรง เว้นแต่เป็นการแจ้งเวียนสารสนเทศที่จำเป็นและเป็นประโยชน์ต่อส่วนรวม และกระทำโดยพนักงานหรือพนักงานโครงการซึ่งได้รับการพิจารณาและอนุมัติจากผู้บังคับบัญชาระดับผู้อำนวยการฝ่ายขึ้นไป โดยที่การสื่อสารสารสนเทศที่มีขนาดเกินกว่า ๒๐๐ เมกะไบต์ ผ่านจดหมายอิเล็กทรอนิกส์ในแต่ละครั้ง ให้กระทำโดยการวางสารสนเทศไว้ที่ฐานข้อมูลกลางในระบบคอมพิวเตอร์หรือเว็บไซต์ที่เฉพาะพนักงาน พนักงานโครงการหรือผู้เกี่ยวข้องสามารถเข้าถึงได้

ข้อ ๑๑๖ การแจ้งข่าวสารให้กับพนักงานหรือพนักงานโครงการของสำนักงานบนระบบจดหมายอิเล็กทรอนิกส์ ให้กระทำผ่านระบบแจ้งเวียนข่าวสาร หรือระบบอื่นใดซึ่งสำนักงานกำหนดให้เป็นช่องทางสื่อสารภายในแบบเป็นทางการ

ข้อ ๑๑๗ ผู้ใช้งานที่ต้องการใช้บัญชีจดหมายอิเล็กทรอนิกส์ที่มีวัตถุประสงค์พิเศษ คือ บัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม (Groupmail Account) ซึ่งมีผู้ใช้งานร่วมกันมากกว่าหนึ่งคนขึ้นไป ต้องมอบหมายให้มีผู้ใช้งานหนึ่งคนเป็นผู้ดูแลบัญชีจดหมายอิเล็กทรอนิกส์กลุ่ม (Groupmail Moderator) ทำหน้าที่ในการดูแลบริหารจัดการสมาชิกของบัญชีจดหมายอิเล็กทรอนิกส์กลุ่มนั้น และต้องปรับปรุงข้อมูลของสมาชิกให้เป็นปัจจุบันอยู่เสมอ

ข้อ ๑๑๘ ผู้ใช้งานต้องใช้ความระมัดระวังเป็นพิเศษเมื่อจำเป็นต้องเปิดไฟล์แนบที่ได้รับจากผู้ส่งที่ตนเองไม่รู้จัก ซึ่งไฟล์แนบนั้นอาจมีชุดคำสั่งไม่พึงประสงค์ ได้แก่ Virus Trojan Worm Exploit ฯลฯ ติดมากับไฟล์แนบ

ข้อ ๑๑๙ เมื่อผู้ใช้งานได้รับข้อความเตือนจากซอฟต์แวร์ Anti-Virus ว่าเครื่องคอมพิวเตอร์ของตนถูกโจมตีโดยไวรัส ผู้ใช้งานต้องระงับการส่งจดหมายอิเล็กทรอนิกส์และหยุดการใช้งานระบบเครือข่ายของสำนักงานทันที จนกว่าเครื่องคอมพิวเตอร์จะได้รับการแก้ไขจนกลับเข้าสู่สภาพปกติ

ข้อ ๑๒๐ หากผู้ใช้งานจำเป็นต้องส่งข้อมูลลับผ่านทางจดหมายอิเล็กทรอนิกส์ ให้เข้ารหัสลับข้อมูลเพื่อป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต โดยการเข้ารหัสลับให้เป็นไปตามวิธีการที่จัดเตรียมไว้โดยหน่วยบริการเทคโนโลยีสารสนเทศ

ข้อ ๑๒๑ ในการปฏิบัติงานของสำนักงาน ให้พนักงานหรือพนักงานโครงการ ใช้ระบบจดหมายอิเล็กทรอนิกส์ของสำนักงาน หรือของผู้ให้บริการจดหมายอิเล็กทรอนิกส์ที่ได้รับอนุมัติโดยสำนักงานเท่านั้น ห้ามใช้บัญชีจดหมายอิเล็กทรอนิกส์ของผู้ให้บริการจดหมายอิเล็กทรอนิกส์รายอื่น เพื่อหลีกเลี่ยงการนำสารสนเทศที่เกี่ยวข้องกับสำนักงานไปฝากไว้กับผู้ให้บริการภายนอกที่อาจมีสิทธิในการเก็บสำเนาจดหมายอิเล็กทรอนิกส์ไว้ที่ระบบโดยไม่มีข้อจำกัด

ส่วนที่ ๔
การใช้งานอินเทอร์เน็ต

ข้อ ๑๒๒ ผู้ใช้งานต้องใช้งานอินเทอร์เน็ตด้วยความระมัดระวัง และห้ามมิให้ใช้อินเทอร์เน็ตเพื่อการใด ๆ อันเป็นการขัดต่อ กฎหมาย ข้อบังคับ ระเบียบ ประกาศ คำสั่งของสำนักงาน รวมถึงเพื่อการใช้งานที่มีลักษณะดังต่อไปนี้

(๑) กระทำการใด ๆ อันเป็นความผิดตามกฎหมาย เช่น เพื่อการค้าขาย โฆษณา แจกจ่าย เผยแพร่ สิ่งเสพติดหรือสินค้าหนีภาษี หรือผลิตภัณฑ์ละเมิดลิขสิทธิ์ เป็นต้น

(๒) เข้าชม ใช้งาน ดาวน์โหลด หรือทำซ้ำสื่อลามกอนาจารหรือสื่ออื่นใดที่ไม่เหมาะสมหรือผิดกฎหมาย

(๓) ให้ร้าย กล่าวร้าย สนับสนุน ส่งเสริม หรือกระทำการใด ๆ อันอาจก่อให้เกิดความเสื่อมเสียทั้งต่อตนเองหรือผู้อื่น หรือ

(๔) การใช้งานที่เกี่ยวพันกับการกระทำความผิดตามกฎหมายอื่น ๆ เช่น กฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เป็นต้น

ทั้งนี้ การใช้งานอินเทอร์เน็ตในทางที่ผิดอาจถือเป็นความผิดทางวินัย และอาจถูกดำเนินคดีได้ตามกฎหมายทั้งทางแพ่งและอาญา

ข้อ ๑๒๓ ให้ผู้ใช้งานเข้าใช้งานอินเทอร์เน็ตผ่านช่องทางและตามวิธีการที่สำนักงานกำหนดไว้เท่านั้น โดยสำนักงานอาจดำเนินการตรวจสอบการใช้งานอินเทอร์เน็ตของผู้ใช้งานเพื่อตรวจสอบการใช้งานที่ไม่เหมาะสมได้ โดยมิต้องแจ้งให้ผู้ใช้งานทราบก่อนล่วงหน้า

ข้อ ๑๒๔ กรณีที่มีการใช้งานระบบสารสนเทศจากเครือข่ายภายนอก ต้องใช้งานผ่านช่องทางการสื่อสารที่มีความมั่นคงปลอดภัยด้วยเทคโนโลยี Secure Sockets Layer (SSL) หรือ Transport Layer Security (TLS) เป็นอย่างน้อยทุกครั้ง เพื่อป้องกันการถูกล่วงละเมิด การดักและลักลอบนำสารสนเทศไปใช้

ข้อ ๑๒๕ ถ้าหากประสิทธิภาพการทำงานของเครื่องคอมพิวเตอร์ของผู้ใช้งานลดลงหลังจากการเข้าชมเว็บไซต์ใด ๆ ผู้ใช้งานต้องแจ้งให้หน่วยบริการเทคโนโลยีสารสนเทศทราบทันทีเพื่อดำเนินการตรวจสอบและแก้ไขปัญหา

ส่วนที่ ๕
การป้องกันชุดคำสั่งไม่พึงประสงค์

ข้อ ๑๒๖ ห้ามผู้ใช้งานสร้าง เก็บ หรือเผยแพร่ชุดคำสั่งไม่พึงประสงค์ใด ๆ ได้แก่ Virus Worm Trojan และ E-mail Bomb เข้าสู่ระบบสารสนเทศของสำนักงานหรือออกสู่ระบบสารสนเทศภายนอกสำนักงาน

ข้อ ๑๒๗ ให้ใช้ซอฟต์แวร์ Anti-Virus สแกนไวรัสในสื่อบันทึกข้อมูลพกพา ประเภท Flash Drive หรือ External Harddisk ก่อนการใช้งาน และห้ามมิให้ผู้ใช้งานขัดขวางการทำงานของซอฟต์แวร์ป้องกันไวรัสที่ติดตั้งไว้ คือ การปิดการตรวจเช็คระบบหรือการถอดซอฟต์แวร์ออกจากเครื่องคอมพิวเตอร์

ข้อ ๑๒๘ หากผู้ใช้งานสงสัยว่าเครื่องคอมพิวเตอร์ของตนมีชุดคำสั่งไม่พึงประสงค์ หรือได้รับการแจ้งเตือนจากซอฟต์แวร์ Anti-Virus ซอฟต์แวร์ Anti-Spyware หรือซอฟต์แวร์ Anti-Malware ว่าเครื่องคอมพิวเตอร์ถูกโจมตีโดยชุดคำสั่งไม่พึงประสงค์ ผู้ใช้งานต้องหยุดการทำงานทั้งหมด และแจ้งเหตุต่อหน่วยบริการเทคโนโลยีสารสนเทศทันที

ส่วนที่ ๖
การใช้งานรหัสผ่านอย่างมั่นคงปลอดภัย

ข้อ ๑๒๙ ผู้ใช้งานแต่ละคนต้องใช้บัญชีผู้ใช้งานที่ได้รับจากหน่วยบริการเทคโนโลยีสารสนเทศในการเข้าถึงระบบสารสนเทศต่าง ๆ ทั้งนี้ การมอบสิทธิของผู้ใช้งานดังกล่าวจะมอบให้เฉพาะแก่ผู้ที่จำเป็นต้องใช้งานและเฉพาะผู้ที่จำเป็นต้องทราบเกี่ยวกับสารสนเทศบนระบบนั้นเท่านั้น

ข้อ ๑๓๐ ผู้ใช้งานที่มีหน้าที่ปฏิบัติงานเกี่ยวข้องโดยตรงกับสารสนเทศ ต้องแจกแจงประเภทของข้อมูลตามลำดับชั้นความลับหรือความสำคัญของสารสนเทศ รวมถึงกำหนดผู้มีสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศระดับชั้นในการเข้าถึง เวลาและช่องทางในการเข้าถึงสารสนเทศด้วย

ข้อ ๑๓๑ ผู้ใช้งานต้องตั้งรหัสผ่านสำหรับบัญชีผู้ใช้งานของสำนักงานที่มีความมั่นคงปลอดภัยตามแนวทาง ดังต่อไปนี้

(๑) รหัสผ่านจะต้องมีความยาวไม่น้อยกว่า ๑๒ ตัวอักษร เว้นแต่รหัสผ่านระดับ BIOS (Basic Input/Output System) ให้มีความยาวไม่น้อยกว่า ๔ ตัวอักษร

(๒) ห้ามผู้ใช้งานกำหนดรหัสผ่านจากบริบทของผู้ใช้งาน ดังต่อไปนี้

(ก) ชื่อจริงภาษาอังกฤษทั้งอักษรพิมพ์เล็ก และอักษรพิมพ์ใหญ่

(ข) นามสกุลจริงภาษาอังกฤษทั้งอักษรพิมพ์เล็ก และอักษรพิมพ์ใหญ่

(ค) รหัสพนักงาน

(ง) ชื่อย่อฝ่ายที่สังกัด

(จ) ชื่อย่องานที่สังกัด

(ฉ) หมายเลขโทรศัพท์

(ช) หมายเลขบัตรประจำตัวประชาชน

(ซ) ส่วนใดส่วนหนึ่งของวันเกิด

(ฌ) ปี พ.ศ. หรือ ค.ศ. ปัจจุบัน

(ญ) ชื่อผู้ใช้งานที่ใช้เข้าสู่ระบบ

(ฎ) ชื่อเฉพาะที่เกี่ยวข้องกับสำนักงาน

(ฏ) กลุ่มคำที่สำนักงานกำหนดให้เป็นคำต้องห้ามใช้

(ฐ) การใช้งานบริการภายนอกหน่วยงาน ผู้ใช้งานไม่ควรใช้ชื่อบริการ หรือที่อยู่อีเมลเป็นรหัสผ่าน

ข้อ ๑๓๒ ผู้ใช้งานต้องเปลี่ยนรหัสผ่านสำหรับบัญชีผู้ใช้งานของสำนักงาน เมื่อเข้าใช้งานครั้งแรก และเปลี่ยนอย่างสม่ำเสมอทุก ๑ ปี

ข้อ ๑๓๓ รหัสผ่านถือเป็นข้อมูลลับและเป็นหน้าที่ของผู้ใช้งานทุกคนที่ต้องเก็บรักษารหัสผ่านให้มีความมั่นคงปลอดภัย โดยห้ามจดหรือบันทึกรหัสผ่านไว้ในที่ซึ่งง่ายต่อการสังเกตเห็นของบุคคลอื่น และห้ามมิให้มีการใช้งานบัญชีผู้ใช้งานร่วมกัน หรือให้บุคคลอื่นเข้าใช้งานบัญชีผู้ใช้งานของตน ทั้งนี้ รวมถึงสมาชิกในครอบครัวและบุคคลใกล้ชิดอื่น ๆ

ข้อ ๑๓๔ ถ้าหากผู้ใช้งานสงสัยว่าบัญชีผู้ใช้งานหรือรหัสผ่านของตนถูกล่วงละเมิด ให้ผู้ใช้งานแจ้งเหตุต่อหน่วยบริการเทคโนโลยีสารสนเทศ และทำการเปลี่ยนแปลงรหัสผ่านทั้งหมดทันที

ข้อ ๑๓๕ ผู้ใช้งานต้องรับผิดชอบต่อการกระทำใด ๆ ที่กระทำผ่านบัญชีผู้ใช้งานและรหัสผ่านของตนทั้งหมด เว้นแต่ได้แจ้งให้หน่วยบริการเทคโนโลยีสารสนเทศทราบแล้วว่าบัญชีผู้ใช้งานหรือรหัสผ่านของตนถูกล่วงละเมิด

ส่วนที่ ๗
การใช้พื้นที่สำนักงานในการปฏิบัติงานที่เกี่ยวข้องกับระบบสารสนเทศ

ข้อ ๑๓๖ ผู้ใช้งานหมั่นตรวจสอบความมั่นคงปลอดภัยของพื้นที่ทำงานของตนเป็นประจำทุกวันหลังเลิกงาน เพื่อให้มั่นใจว่าตู้เซฟ ตู้เอกสาร ลิ้นชัก และอุปกรณ์ต่าง ๆ ได้รับการปิดล็อค อย่างเหมาะสม และกุญแจถูกเก็บรักษาไว้อย่างปลอดภัย

ข้อ ๑๓๗ ผู้ใช้งานต้องไม่วางเอกสาร สื่อบันทึก วัสดุ หรืออุปกรณ์ที่จัดเก็บข้อมูลลับไว้บนโต๊ะทำงานในห้องประชุม หรือในตู้ที่ไม่ได้ล็อคกุญแจ เพื่อป้องกันการสูญหายและการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๑๓๘ ผู้ใช้งานต้องไม่ยินยอมให้ผู้ใดทำการเคลื่อนย้ายเครื่องคอมพิวเตอร์หรือสื่อบันทึกข้อมูลออกจากพื้นที่ทำงานของตน เว้นแต่บุคคลภายนอกนั้นเป็นเจ้าหน้าที่ที่มีอำนาจหน้าที่ในการดำเนินการ

ข้อ ๑๓๙ ผู้ใช้งานต้องไม่เข้าไปในสถานที่ตั้งของระบบสารสนเทศโดยไม่ได้รับอนุญาตจากหน่วยบริการเทคโนโลยีสารสนเทศ และไม่เปิดเผยสถานที่ตั้งของระบบสารสนเทศต่อบุคคลภายนอกโดยเด็ดขาด

ส่วนที่ ๘
ความมั่นคงปลอดภัยของระบบเครือข่าย

ข้อ ๑๔๐ ห้ามผู้ใช้งานทำการเชื่อมต่อเครื่องแม่ข่ายภายในหรือเครือข่ายภายใน (intranet) เข้ากับระบบเครือข่ายอินเตอร์เน็ต ด้วยวิธีการใด ๆ ที่อาจข้ามผ่าน (bypass) ระบบป้องกันของสำนักงาน เช่น การทำ tunneling, การทำ bridging ระบบเครือข่าย เว้นแต่เพื่อการทดสอบหรือพัฒนาระบบเป็นการชั่วคราวเท่านั้น

ข้อ ๑๔๑ ห้ามผู้ใช้งานติดตั้งหรือรื้อถอนฮาร์ดแวร์หรือซอฟต์แวร์ใด ๆ ที่เกี่ยวข้องกับการให้บริการระบบเครือข่าย เช่น อุปกรณ์ Router อุปกรณ์ Switch อุปกรณ์ Hub อุปกรณ์ Wireless Access Point เป็นต้น โดยไม่ได้รับอนุญาตจากผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงานกลาง

ข้อ ๑๔๒ ห้ามผู้ใช้งานพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวน หรือขัดขวางการทำงาน หรือโจมตีระบบเครือข่ายของสำนักงาน หรือพยายามเข้าถึงข้อมูลบนระบบเครือข่ายโดยไม่ปกติ เช่น การเข้าถึงสารสนเทศหรือเครื่องบริการ (Server) ที่ตนไม่ได้รับอนุญาต, การดักจับข้อมูลเครือข่าย Network Sniffing, การโจมตีระบบเครือข่ายแบบ DoS/ DDoS, การปลอมแปลงข้อมูลในระบบเครือข่าย (Packet Spoofing), การลวงเส้นทางระบบเครือข่ายด้วยวิธีการ Spoofing/ Man-in-the-middle, หรือการตรวจสอบบริการ/ช่องโหว่ของเครื่องแม่ข่ายด้วยวิธีการกราดตรวจ (Port Scanning, Security Scanning) เป็นต้น

ข้อ ๑๔๓ ห้ามผู้ใช้งานใช้ระบบเครือข่ายของสำนักงานในการทำกิจกรรมดังต่อไปนี้

(๑) ดาวน์โหลดไฟล์ขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

(๒) ใช้ application หรืออุปกรณ์ หรือ website ที่ใช้งาน internet bandwidth สูง โดยการใช้งานดังกล่าวไม่เกี่ยวข้องการปฏิบัติงาน

(๓) การใช้งานโปรแกรมประเภท P2P network, BitTorrent ที่ไม่เกี่ยวข้องกับการปฏิบัติงาน

(๔) การใช้เครือข่ายของสำนักงานในการทำ cryptocurrency mining

(๕) ใช้ระบบเครือข่ายของสำนักงานในการโจมตี หรือขัดขวางการทำงานของระบบเครือข่ายอื่น ๆ โดยตั้งใจ

(๖) ใช้ระบบเครือข่ายของสำนักงานในการกระทำที่ขัดต่อกฎหมายและศีลธรรมอันดีของประชาชน

ข้อ ๑๔๔ ห้ามผู้ใช้งานพยายามล่วงละเมิดความมั่นคงปลอดภัย หรือรบกวนการทำงานของระบบเครือข่ายของสำนักงาน

ตัวอย่างของการล่วงละเมิดความมั่นคงปลอดภัย เช่น การเข้าถึงสารสนเทศหรือเครื่องบริการ (Server) ที่ตนไม่ได้รับอนุญาต เป็นต้น และตัวอย่างของการรบกวนการทำงานของระบบเครือข่าย ได้แก่ การทำ Sniffing การทำ Pinged Floods การทำ Packet Spoofing การโจมตีแบบ Denial of Service หรือการทำ Forged Routing Information ด้วยเจตนามุ่งร้าย เป็นต้น

ข้อ ๑๔๕ ห้ามผู้ใช้งานดาวน์โหลดไฟล์ขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงานของสำนักงาน นอกจากนี้ผู้ใช้งานต้องพึงระวังการใช้ความกว้างแถบความถี่ (Bandwidth) ของระบบเครือข่ายอินเทอร์เน็ตของสำนักงานจำนวนมาก โดยเฉพาะอย่างยิ่งการใช้งานโปรแกรมประเภท P2P file sharing, BitTorrent หรือการดาวน์โหลดไฟล์ขนาดใหญ่ที่ไม่เกี่ยวข้องกับการปฏิบัติงานของสำนักงาน เช่น วีดิทัศน์ หรือ รูปภาพ เป็นต้น

ข้อ ๑๔๖ ห้ามผู้ใช้งานหลบเลี่ยงการพิสูจน์ตัวตนผู้ใช้งานหรือมาตรการด้านความมั่นคงปลอดภัยของคอมพิวเตอร์ และของระบบเครือข่ายใด ๆ รวมถึงห้ามผู้ใช้งานเปิดเผยมาตรการด้านความมั่นคงปลอดภัยของสำนักงานให้แก่ผู้ใดล่วงรู้

ส่วนที่ ๙
การใช้งานระบบเครือข่ายไร้สายของสำนักงาน

ข้อ ๑๔๗ ให้ผู้ที่ประสงค์จะใช้งานระบบเครือข่ายไร้สายของสำนักงาน ต้องขออนุมัติการใช้งานระบบเครือข่ายไร้สายที่หน่วยประสานงานเครือข่ายไร้สายที่รับผิดชอบบริหารจัดการและให้บริการระบบเครือข่ายไร้สายตามข้อ ๖๑

ข้อ ๑๔๘ ห้ามผู้ใช้งานใช้บัญชีผู้ใช้งานระบบเครือข่ายไร้สายของสำนักงาน (Wifi Account) ร่วมกันกับบุคคลอื่น หรือ WiFi Account ของตนบนเครื่องคอมพิวเตอร์ที่ไม่ใช่ของตน

ข้อ ๑๔๙ ในการขออนุมัติเพื่อติดตั้งอุปกรณ์กระจายสัญญาณไร้สาย เพื่อการวิจัยและพัฒนาให้ผู้ที่ประสงค์ขอติดตั้งแจ้งรายละเอียดต่อผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงาน ดังนี้

(๑) ชื่อเครือข่ายไร้สาย (SSID) ที่ต้องการใช้งาน โดยต้องไม่ซ้ำ เหมือนหรือคล้ายคลึงกันกับชื่อเครือข่ายไร้สายของสำนักงาน

(๒) คลื่นความถี่หรือช่องสัญญาณที่ต้องการใช้งาน

(๓) บริเวณหรือพื้นที่กระจายสัญญาณ

(๔) ระยะเวลาในการใช้งาน

และเมื่อสิ้นสุดระยะเวลาการใช้งานให้ดำเนินการถอดถอนการติดตั้งให้เรียบร้อยภายใน ๓ วันทำการ

ข้อ ๑๕๐ บุคคลใดที่ใช้อุปกรณ์ที่ทำงานในย่านความถี่ระบบเครือข่ายไร้สาย 2,401– 2,495MHz และ 4,910–5,845MHz ซึ่งรบกวนต่อระบบเครือข่ายไร้สายของสำนักงาน ให้ยกเลิกการใช้งาน เว้นแต่ได้รับอนุมัติจากผู้อำนวยการฝ่ายโครงสร้างพื้นฐานและความมั่นคงปลอดภัยดิจิทัล สำนักงานกลาง

ส่วนที่ ๑๐
การใช้สื่อสังคมออนไลน์

ข้อ ๑๕๑ ผู้ใช้งานต้องไม่ใช้บัญชีจดหมายอิเล็กทรอนิกส์ที่สำนักงานจัดให้ในการลงทะเบียนหรือประกาศข้อมูลใด ๆ ในสื่อสังคมออนไลน์ เช่น เว็บบอร์ด บล็อก และกระดานข่าว เป็นต้น เว้นแต่การลงทะเบียนหรือประกาศข้อมูลนั้นเกี่ยวข้องหรือเป็นส่วนหนึ่งของการปฏิบัติงานตามหน้าที่ที่ได้รับมอบหมายจากสำนักงาน

ข้อ ๑๕๒ ผู้ใช้งานที่ต้องสื่อสารกับบุคคลภายนอกในการปฏิบัติงานของสำนักงานผ่านสื่อสังคมออนไลน์ เช่น twitter.com หรือ facebook.com เป็นต้น ให้นำแนวปฏิบัติสภาการหนังสือพิมพ์แห่งชาติ สภาวิชาชีพข่าววิทยุและโทรทัศน์ไทย เรื่อง การใช้สื่อสังคมออนไลน์ของสื่อมวลชนมาปรับใช้ ดังนี้

(๑) การนำเสนอข่าวสารของสำนักงาน โดยการใช้สื่อสังคมออนไลน์ ต้องมีหลักในการอ้างอิงถึงสำนักงานด้วยชื่อ รายละเอียด สัญลักษณ์ หรือชื่อย่อ ที่แสดงถึงความเป็นสำนักงาน หรือด้วยมาตรการอื่นที่ยืนยันถึงสถานะและความมีตัวตนของสำนักงาน

(๒) การนำเสนอข้อมูลข่าวสารของสำนักงาน ต้องไม่เป็นการสร้างความเกลียดชังระหว่างคนในสังคมและไม่ยุยงให้เกิดความรุนแรงจนนำไปสู่ความขัดแย้งหรือความเสียหายขึ้นในสังคม

(๓) ผู้ใช้งานต้องใช้ความระมัดระวังในการเผยแพร่ข้อมูลข่าวสาร โดยไม่ละเมิดลิขสิทธิ์ของข้อมูลข่าวสาร ภาพ หรือวีดิทัศน์ที่ผลิตโดยบุคคลอื่น

(๔) การคัดลอกข้อความใด ๆ จากสื่อสังคมออนไลน์ จะทำต่อเมื่อได้รับการอนุญาตจากเจ้าของข้อความนั้น ๆ ในกรณีที่จำเป็นต้องคัดลอกข้อความจากสื่อสังคมออนไลน์เพื่อประโยชน์ในการเผยแพร่ข้อมูลข่าวสารผู้ใช้งานต้องอ้างอิงแหล่งที่มาของข้อความและข่าวสารเหล่านั้น โดยรับรู้ถึงสิทธิหรือลิขสิทธิ์ของบุคคลหรือองค์กรผู้เป็นเจ้าของข้อมูลดังกล่าวเสมอ

(๕) ให้ผู้ใช้งานใช้ความระมัดระวังในการนำเสนอข้อมูลข่าวสารของสำนักงาน โดยเน้นหลักความถูกต้องและใช้ภาษาที่เหมาะสม หลีกเลี่ยงการแสดงความคิดเห็นส่วนบุคคลในเรื่องที่เกี่ยวข้องกับการดำเนินงานของสำนักงาน ในลักษณะที่ก่อหรืออาจก่อให้เกิดความเข้าใจที่คลาดเคลื่อนไปจากความเป็นจริง

ข้อ ๑๕๓ ผู้ใช้งานไม่นำข้อมูลของสำนักงานเผยแพร่ผ่านทางสื่อสังคมออนไลน์แบบสาธารณะ เพื่อไม่ให้สำนักงานตกอยู่ในภาวะเสี่ยงหรือเกิดความเสียหาย

ส่วนที่ ๑๑
การจัดการสารสนเทศตามชั้นความลับ

ข้อ ๑๕๔ สำนักงานกำหนดให้ข้อมูลลับ แบ่งออกเป็น ๔ ชั้น คือ

(๑) ลับที่สุด

(๒) ลับมาก

(๓) ลับ

(๔) ใช้ภายใน

ให้เจ้าของข้อมูลหรือผู้ที่มีหน้าที่ปฏิบัติงานเกี่ยวข้องโดยตรงกับสารสนเทศนั้น กำหนดลำดับชั้นความลับของสารสนเทศตามความสำคัญของสารสนเทศ รวมถึงกำหนดสิทธิในการเข้าถึงหรือควบคุมการใช้งานสารสนเทศ ระดับชั้นในการเข้าถึง เวลาและช่องทางในการเข้าถึงด้วย และในกรณีจำเป็นที่ต้องมีการจำกัดการเข้าถึงสารสนเทศให้แก่บุคคลผู้ที่มีหน้าที่เกี่ยวข้องเท่านั้น ให้จัดทำรายชื่อผู้ได้รับอนุญาตให้เข้าถึงดังกล่าวอย่างรอบคอบ

ข้อ ๑๕๕ การบริหารจัดการและการเข้าถึงข้อมูลลับที่กำหนดชั้นความลับ แบ่งออกเป็น ดังนี้

(๑) ข้อมูลลับรูปแบบเอกสารตีพิมพ์ ให้ผู้ใช้ข้อมูลปฏิบัติดังนี้

ลับที่สุด	**ลับมาก**	**ลับ**	**ใช้ภายใน**
การระบุชั้นความลับของสารสนเทศ			
ระบุคำว่า “ลับที่สุด” และชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่น และระบุบนปกหรือหน้าแรกของเอกสารหากเอกสารได้รับการเข้าเล่ม	ระบุคำว่า “ลับมาก” และชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่น และระบุบนปกหรือหน้าแรกของเอกสารหากเอกสารได้รับการเข้าเล่ม	ระบุคำว่า “ลับ” และชื่อผู้เป็นเจ้าของข้อมูลทุกหน้าเอกสารสำหรับเอกสารแยกแผ่น และระบุบนปกหรือหน้าแรกของเอกสารหากเอกสารได้รับการเข้าเล่ม	ระบุคำว่า “เอกสารปกปิด สำหรับเผยแพร่ใน สวทช. เท่านั้น”
การเข้าถึงเอกสาร			
บุคคลที่มีหน้าที่เกี่ยวข้อง	บุคคลที่มีหน้าที่เกี่ยวข้องและ	บุคคลที่มีหน้าที่เกี่ยวข้อง	ใช้งานได้ภายใน

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
ตามรายชื่อผู้ได้รับอนุญาตให้เข้าถึงสารสนเทศ	ได้รับอนุญาตจากผู้บังคับบัญชาตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	และเป็นไปตามหลักการ Need-to-know	ศูนย์ข้อมูล สำนักงาน หรือภายในฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การเก็บรักษาเอกสาร			
เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เก็บรักษาในตู้เอกสารที่ปิดล็อคเมื่อไม่ได้ใช้งาน	เอกสารต้นฉบับต้องได้รับการเก็บรักษาอย่างดีไม่ให้เกิดความเสียหาย
การทำสำเนาเอกสาร			
ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอ และสำเนาต้องได้รับการระบุชื่อผู้ที่ได้รับอนุญาตให้ใช้งาน	ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอ และสำเนาต้องได้รับการระบุชื่อผู้ที่ได้รับอนุญาตให้ใช้งาน	ต้องขออนุญาตจากเจ้าของข้อมูลก่อนเสมอ และสำเนาต้องได้รับการระบุชื่อผู้ที่ได้รับอนุญาตให้ใช้งาน	อนุญาตให้ทำสำเนาได้เพื่อใช้ในการปฏิบัติงานเท่านั้น
การส่งเอกสารภายในสำนักงาน			
สอดในซองปิดผนึกและระบุคำว่า “ลับที่สุด” และชื่อ-ที่อยู่ผู้รับบนหน้าซอง	สอดในซองปิดผนึกและระบุคำว่า “ลับมาก” และชื่อ-ที่อยู่ผู้รับ บนหน้าซอง	สอดในซองปิดผนึก และระบุคำว่า “ลับ” และชื่อ-ที่อยู่ผู้รับ บนหน้าซอง	มีปกเอกสารเพื่อปกปิดข้อมูลอย่างมิดชิด
การส่งเอกสารภายนอกสำนักงาน			
สอดในซอง ๒ ชั้น ปิดผนึกชั้นนอกและชั้นในด้วยวัสดุที่ป้องกันการลักลอบเปิดอ่านได้ ซองชั้นใน ระบุคำว่า “ลับที่สุด” และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้ ระบุชื่อ-ที่อยู่ของผู้รับ	สอดในซอง ๒ ชั้น ปิดผนึกชั้นนอกและชั้นในด้วยวัสดุที่ป้องกันการลักลอบเปิดอ่านได้ ซองชั้นใน ระบุคำว่า “ลับมาก” และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้ ระบุชื่อ-ที่อยู่ของผู้รับและผู้ส่ง	สอดในซอง ๒ ชั้น ปิดผนึกชั้นนอกและชั้นในด้วยวัสดุที่ป้องกันการลักลอบเปิดอ่านได้ ซองชั้นใน ระบุคำว่า “ลับ” และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้ ระบุชื่อ-ที่อยู่ของผู้รับ	สอดซองปิดผนึกและระบุชื่อ-ที่อยู่ของผู้รับและผู้ส่ง และใช้บริการไปรษณีย์ลงทะเบียน หรือบริษัทขนส่งที่เชื่อถือได้

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
และผู้ส่ง		และผู้ส่ง	
การส่งโทรสาร			
ตรวจสอบเลขหมายปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	ตรวจสอบเลขหมายปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	ตรวจสอบเลขหมายปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว	ตรวจสอบเลขหมายปลายทางให้ถูกต้อง โทรศัพท์แจ้งให้ผู้รับทราบถึงการส่งเอกสาร และขอให้ผู้รับแจ้งยืนยันเมื่อได้รับเอกสารแล้ว
การรับโทรสาร			
รอรับเอกสารที่ครื่องโทรสารทุกครั้ง	รอรับเอกสารที่เครื่องโทรสารทุกครั้ง	รอรับเอกสารที่เครื่องโทรสารทุกครั้ง	รอรับเอกสารที่เครื่องโทรสารทุกครั้ง
การทำลายเอกสาร			
ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร	ใช้เครื่องทำลายเอกสาร
การนำกระดาษกลับมาใช้ซ้ำ			
ห้ามนำกระดาษกลับมาใช้ซ้ำ	ห้ามนำกระดาษกลับมาใช้ซ้ำ	ห้ามนำกระดาษกลับมาใช้ซ้ำ	สามารถนำกระดาษกลับมาใช้ซ้ำได้ โดยหากมีการนำกลับมาใช้ซ้ำให้ใช้เฉพาะเอกสารที่ใช้ภายใน สวทช. เท่านั้น

(๒) ข้อมูลลับในรูปแบบอิเล็กทรอนิกส์ ให้ผู้ใช้ข้อมูลปฏิบัติดังนี้

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
การระบุชั้นความลับของข้อมูลบนจอแสดงผล			
ต้องระบุคำว่า “ลับที่สุด” บนหน้าจอ และระบุชื่อผู้เป็นเจ้าของข้อมูล	ต้องระบุคำว่า “ลับมาก” บนหน้าจอ และระบุชื่อผู้เป็นเจ้าของข้อมูล	ระบุคำว่า “ลับ” บนหน้าจอ	ไม่จำเป็นต้องระบุ
การเข้าถึงและการทำสำเนาสารสนเทศ			

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
บุคคลที่มีหน้าที่เกี่ยวข้องตามรายชื่อผู้ได้รับอนุญาตให้เข้าถึงข้อมูล	บุคคลที่มีหน้าที่เกี่ยวข้องและได้รับอนุญาตจากผู้บังคับบัญชาตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	บุคคลที่มีหน้าที่เกี่ยวข้องและเป็นไปตามหลักการ Need-to-know	ใช้งานได้ภายในศูนย์ข้อมูล สำนักงานหรือภายในฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ได้ควบคุมการเข้าถึง)			
ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล	ไม่ต้องเข้ารหัสข้อมูล
การเก็บรักษาบนสื่อที่ไม่สามารถเคลื่อนย้ายได้ (ที่ไม่ได้ควบคุมการเข้าถึง)			
เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	เข้ารหัสข้อมูล	ไม่มีข้อจำกัด
การสั่งพิมพ์สารสนเทศ			
ต้องมีผู้รอรับเอกสารที่เครื่องทุกครั้ง	ต้องมีผู้รอรับเอกสารที่เครื่องทุกครั้ง	ต้องมีผู้รอรับเอกสารที่เครื่อง	มีผู้รอรับเอกสารที่เครื่อง
การส่งสารสนเทศผ่านเครือข่ายสาธารณะ			
ต้องเข้ารหัสข้อมูล	ต้องเข้ารหัสข้อมูล	ต้องเข้ารหัสข้อมูล	เข้ารหัสข้อมูล
การทำลายสารสนเทศ			
ต้องทำลายด้วยวิธี Secure Delete	ต้องทำลายด้วยวิธี Secure Delete	ต้องทำลายด้วยวิธี Secure Delete	ลบไฟล์ด้วยวิธีปกติโดยการกดแป้นDelete หรือ Shift+Delete
การทำลายสื่อบันทึกข้อมูล			
เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่า สื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	เจ้าของข้อมูลต้องเลือกใช้วิธีทำลายที่มั่นใจว่าสื่อบันทึกข้อมูลถูกทำลายจนไม่สามารถกู้ข้อมูลกลับคืนมาได้ ไม่ว่าจะด้วยวิธีการใด ๆ ก็ตาม	ทำลายด้วยวิธีปกติโดยการกดแป้นDelete หรือ Shift+Delete

(๓) ข้อมูลลับที่ส่งผ่านทางวาจา ให้ผู้ใช้ข้อมูลปฏิบัติดังนี้

ลับที่สุด	ลับมาก	ลับ	ใช้ภายใน
การเข้าถึงสารสนเทศ			
บุคคลที่มีหน้าที่เกี่ยวข้องตามรายชื่อผู้ได้รับอนุญาตให้เข้าถึงข้อมูล	บุคคลที่มีหน้าที่เกี่ยวข้องและได้รับอนุญาตจากผู้บังคับบัญชาตั้งแต่ระดับผู้อำนวยการฝ่ายขึ้นไปที่เป็นเจ้าของข้อมูล	บุคคลที่มีหน้าที่เกี่ยวข้องและเป็นไปตามหลักการ Need-to-Know	ใช้งานได้ภายในศูนย์ข้อมูล สำนักงาน หรือฝ่ายงานที่เป็นเจ้าของข้อมูลเท่านั้น
การสนทนาทางโทรศัพท์			
ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้งว่าเป็นผู้ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้งว่าเป็นผู้ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ทุกครั้งว่าเป็นผู้ที่ต้องการสนทนาด้วย	ตรวจสอบคู่สนทนาทางโทรศัพท์ว่าเป็นผู้ที่ต้องการสนทนาด้วย
การฝากข้อความทางโทรศัพท์			
ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติหรือระบบวอยซ์เมล์	ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติ หรือระบบวอยซ์เมล์	ห้ามฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติหรือระบบวอยซ์เมล์	หลีกเลี่ยงการฝากข้อความที่มีเนื้อหาข้อมูลไว้ในเครื่องตอบรับอัตโนมัติ หรือระบบวอยซ์เมล์

ส่วนที่ ๑๒
การป้องกันสารสนเทศรั่วไหล

ข้อ ๑๕๖ ผู้ใช้งานมีหน้าที่ดูแลรักษาสารสนเทศของสำนักงานให้มีความมั่นคงปลอดภัยอย่างเหมาะสม โดยเก็บในระบบสารสนเทศที่มีการตรวจพิสูจน์ผู้ใช้งานก่อนการเข้าถึงสารสนเทศ

ข้อ ๑๕๗ การเก็บรวบรวม ใช้หรือเปิดเผยข้อมูลส่วนบุคคล ให้ปฏิบัติตามนโยบายหรือแนวปฏิบัติของสำนักงาน รวมไปถึงกฎหมายที่เกี่ยวข้อง

ข้อ ๑๕๘ ผู้ใช้งานต้องเข้ารหัสลับข้อมูลที่มีลำดับชั้นความลับเมื่อจำเป็นต้องถูกส่งผ่านทางจดหมายอิเล็กทรอนิกส์เพื่อป้องกันการเข้าถึงโดยบุคคลที่ไม่ได้รับอนุญาต โดยการเข้ารหัสลับให้เป็นไปตามวิธีการที่จัดเตรียมไว้โดยหน่วยบริการเทคโนโลยีสารสนเทศ

ข้อ ๑๕๙ ผู้ใช้งานที่ใช้เครื่องคอมพิวเตอร์แบบพกพาและสื่อบันทึกข้อมูลพกพาประเภท Flash Drive หรือ External Harddisk ต้องเข้ารหัสลับอุปกรณ์ที่ใช้เก็บรักษาข้อมูลของสำนักงาน ตามวิธีการที่จัดเตรียมไว้โดยหน่วยบริการเทคโนโลยีสารสนเทศ และไม่วางเครื่องคอมพิวเตอร์แบบพกพาหรือสื่อบันทึกข้อมูลพกพาไว้ในที่สาธารณะโดยไม่มีผู้ดูแลรับผิดชอบ ทั้งนี้ เพื่อป้องกันการสูญหายและการเข้าถึงสารสนเทศโดยไม่ได้รับอนุญาต

ข้อ ๑๖๐ ผู้ใช้งานมีหน้าที่ต้องลบทำลายข้อมูลอย่างมั่นคงปลอดภัย หรือมั่นใจได้ว่า สารสนเทศที่ตนดูแลรักษาอยู่นั้น ได้ถูกลบทำลายอย่างมั่นคงปลอดภัย เพื่อป้องกันข้อมูลรั่วไหลจากการลักลอบกู้คืนข้อมูล

การลบทำลายข้อมูลอย่างมั่นคงปลอดภัย ให้ดำเนินการด้วยวิธีการใดวิธีการหนึ่งดังต่อไปนี้

(๑) ลบทำลายข้อมูลในระดับไฟล์ด้วยวิธีการ Secure delete

(๒) ลบทำลายคีย์ไฟล์สำหรับสารสนเทศที่มีการเข้ารหัสลับ (Encrypted data)

(๓) ทำลายข้อมูลแบบ Secure delete/ Secure erase ด้วยวิธีการที่ผู้ผลิตกำหนด

(๔) ใช้ซอฟต์แวร์ หรือฮาร์ดแวร์สำหรับการลบข้อมูลโดยเฉพาะ (Sanitization)

(๕) กรณีครุภัณฑ์ หรือส่วนใดส่วนหนึ่งของครุภัณฑ์ของสำนักงานให้ทำลายทิ้งในเชิงกายภาพ เช่น การทำให้เสื่อมภาพของจานแม่เหล็ก (Degauss) บดทำลาย เผาทำลาย โดยต้องผ่านกระบวนการทางพัสดุก่อน

(๖) วิธีการอื่นใดที่คณะกรรมการบริหารเทคโนโลยีสารสนเทศกำหนด

ทั้งนี้ ให้หน่วยบริการเทคโนโลยีสารสนเทศมีหน้าที่ให้การสนับสนุนผู้ใช้งานตามความเหมาะสม

ข้อ ๑๖๑ ผู้ใช้งานที่ได้รับสารสนเทศจากการส่งโทรสารหรือการส่งจดหมายอิเล็กทรอนิกส์ที่ผิดพลาดซึ่งอาจเกิดจากการส่งโทรสารผิดหมายเลข ผิดกิจกรรมหรือหน่วยงาน หรือส่งจดหมายอิเล็กทรอนิกส์ผิดบัญชี เป็นต้น ต้องแจ้งให้ผู้ส่งข้อมูลนั้นรับทราบ และทำลายเอกสารนั้นทันที

ข้อ ๑๖๒ ห้ามมิให้สนทนาเกี่ยวกับข้อมูลลับผ่านระบบการสื่อสารใด ๆ เว้นแต่ผู้เข้าร่วมการสื่อสารหรือประชุมทุกฝ่ายได้รับการพิสูจน์ตัวตนแล้วว่าเป็นผู้ที่มีหน้าที่เกี่ยวข้องและมีสิทธิรับทราบข้อมูล และไม่มีบุคคลที่ไม่ได้รับอนุญาตอยู่ในบริเวณใกล้เคียงที่อาจได้ยินข้อมูลลับที่สนทนาอยู่ และการประชุม

ผ่านระบบสื่อสารนั้นจะต้องจัดขึ้นในบริเวณที่มีความมั่นคงปลอดภัย ได้แก่ ห้องประชุมที่มีผนังและประตูที่เหมาะสมสามารถป้องกันเสียงลอดออกมาได้

ข้อ ๑๖๓ ผู้ใช้งานต้องใช้ความระมัดระวังในการสนทนาทางโทรศัพท์ เพื่อป้องกันมิให้ผู้ที่มิได้รับอนุญาตแอบฟังหรือได้ยินการสนทนา

ข้อ ๑๖๔ ผู้ใช้งานต้องมีหลักฐานการได้รับอนุญาตจากเจ้าของข้อมูลลับก่อนทำสำเนาหรือสแกนเอกสารที่มีข้อมูลลับทุกครั้ง โดยการสำเนาเอกสารดังกล่าวต้องได้รับการปกป้องดูแลด้วยวิธีการและขั้นตอนในระดับเดียวกันกับเอกสารต้นฉบับ

ส่วนที่ ๑๓
การรายงานเหตุการณ์ด้านความมั่นคงปลอดภัย

ข้อ ๑๖๕ ผู้ใช้งานมีหน้าที่รายงานเหตุการณ์ด้านความมั่นคงปลอดภัย จุดอ่อน หรือการกระทำที่ไม่เหมาะสมใด ๆ ที่เกิดขึ้น หรือต้องสงสัยว่าเกิดขึ้นภายในสำนักงาน ต่อหน่วยบริการเทคโนโลยีสารสนเทศทันทีที่พบเหตุ เพื่อดำเนินการแก้ไขปัญหาอย่างทันท่วงที

ตัวอย่างของเหตุการณ์ด้านความมั่นคงปลอดภัย เช่น เหตุการณ์บัญชีผู้ใช้งานหรือรหัสผ่านของผู้ใช้งานถูกล่วงละเมิดโดยบุคคลอื่น เครื่องคอมพิวเตอร์ติดไวรัสหรือชุดคำสั่งไม่พึงประสงค์ เป็นต้น

ข้อ ๑๖๖ ผู้ใช้งานผู้ใดพบหรือทราบถึงการทำงานที่ผิดปกติ ข้อผิดพลาดหรือข้อบกพร่องของซอฟต์แวร์ที่พัฒนาหรือใช้งานภายในสำนักงาน ให้ผู้ใช้งานนั้นรายงานต่อหน่วยบริการเทคโนโลยีสารสนเทศทันที

ข้อ ๑๖๗ ผู้ใช้งานผู้ใดพบว่าฮาร์ดแวร์หรืออุปกรณ์ภายในระบบสารสนเทศเกิดความเสียหายหรือทำงานผิดปกติ ให้ผู้ใช้งานนั้นรายงานต่อหน่วยบริการเทคโนโลยีสารสนเทศทันที

ข้อ ๑๖๘ ผู้ใช้งานผู้ใดพบว่าเครื่องคอมพิวเตอร์ที่ใช้ในกิจการของสำนักงาน สูญหายหรือถูกขโมยให้รายงานต่อหน่วยบริการเทคโนโลยีสารสนเทศทันที เพื่อดำเนินการในส่วนที่เกี่ยวข้อง คือ การเปลี่ยนรหัสผ่านระบบสารสนเทศของสำนักงาน จากนั้นให้แจ้งความกับเจ้าหน้าที่ตำรวจและรายงานให้ผู้บังคับบัญชาชั้นต้นทราบ

ข้อ ๑๖๙ ผู้ใช้งานผู้ใดพบเหตุการณ์ด้านความมั่นคงปลอดภัยหรือข้อบกพร่องอื่นใดของระบบสารสนเทศ ต้องไม่เปิดเผยเหตุละเมิด ข้อผิดพลาด หรือข้อบกพร่องนั้นต่อผู้อื่น เว้นแต่เป็นผู้ที่ได้รับมอบหมายให้รับผิดชอบดำเนินการอย่างเป็นทางการ และห้ามมิให้ทำการพิสูจน์ข้อสงสัยเกี่ยวกับเหตุละเมิด ข้อผิดพลาด หรือข้อบกพร่องด้านความมั่นคงปลอดภัยนั้นด้วยตนเอง

หมวด ๖
การกำหนดความรับผิดชอบในการปฏิบัติตามแนวปฏิบัติ

ข้อ ๑๗๐ ผู้ดูแลระบบหรือผู้ใช้งานผู้ใด ละเลยหรือฝ่าฝืนไม่ปฏิบัติ หรือปฏิบัติไม่ถูกต้องตามระเบียบนี้ สำนักงานอาจพิจารณาดำเนินการทางวินัย หรือดำเนินคดีทางกฎหมายได้

ข้อ ๑๗๑ ผู้บังคับบัญชามีหน้าที่กำกับดูแลการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่สำนักงานประกาศกำหนด และแนวปฏิบัติตามที่กำหนดไว้ในระเบียบนี้ โดยให้มีอำนาจตักเตือนผู้ใต้บังคับบัญชา เมื่อพบว่ามีการละเลยหรือฝ่าฝืนไม่ปฏิบัติ หรือปฏิบัติไม่ถูกต้องตามระเบียบนี้

ผู้บังคับบัญชาผู้ใดละเว้นการกำกับดูแลการปฏิบัติตามระเบียบนี้ จนเป็นเหตุให้ผู้ใต้บังคับบัญชาของตนละเลยหรือฝ่าฝืนนโยบายและแนวปฏิบัติตามวรรคหนึ่งจนก่อให้เกิดความเสียหายแก่สำนักงานหรือบุคคลอื่น สำนักงานอาจพิจารณาดำเนินการทางวินัยกับผู้บังคับบัญชาผู้นั้นได้

ข้อ ๑๗๒ ให้สำนักงานเป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้นจากความบกพร่อง ละเลย หรือฝ่าฝืนการปฏิบัติตามนโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่สำนักงานประกาศกำหนด และแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศตามที่กำหนดไว้ในระเบียบนี้

ข้อ ๑๗๓ ให้ผู้อำนวยการ ผู้อำนวยการหน่วยงานเฉพาะทาง คณะกรรมการบริหารเทคโนโลยีสารสนเทศ และผู้บริหารเทคโนโลยีสารสนเทศระดับสูงของสำนักงานทบทวนนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ รวมทั้งติดตามผลการปฏิบัติตามระเบียบนี้อย่างน้อยปีละ ๑ ครั้ง

ประกาศ ณ วันที่ ๒ กันยายน พ.ศ. ๒๕๖๓

(นายณรงค์ ศิริเลิศวรกุล)
ผู้อำนวยการ
สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ