ประกาศสำนักเลขาธิการคณะรัฐมนตรี
เรื่อง นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
ของสำนักเลขาธิการคณะรัฐมนตรี
พ.ศ. ๒๕๖๐ – ๒๕๖๑

โดยที่พระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙ มาตรา ๕ และมาตรา ๗ กำหนดให้หน่วยงานของรัฐต้องจัดทำแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์กับหน่วยงานของรัฐ หรือโดยหน่วยงานของรัฐมีความมั่นคงปลอดภัยและเชื่อถือได้ เลขาธิการคณะรัฐมนตรีโดยความเห็นชอบของคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ออกประกาศไว้ดังต่อไปนี้

ข้อ ๑ ในประกาศนี้

"แนวนโยบาย" หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งสำนักเลขาธิการคณะรัฐมนตรีประกาศไว้เพื่อเจ้าหน้าที่และผู้ปฏิบัติงานของสำนักเลขาธิการคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน และเพื่อให้มีการรักษาความมั่นคงปลอดภัยด้านสารสนเทศที่สอดคล้องกับประกาศแนบท้ายพระราชกฤษฎีกากำหนดหลักเกณฑ์และวิธีการในการทำธุรกรรมทางอิเล็กทรอนิกส์ภาครัฐ พ.ศ. ๒๕๔๙

"แนวปฏิบัติ" หมายถึง ขั้นตอนวิธีการที่สำนักเลขาธิการคณะรัฐมนตรีได้กำหนดไว้โดยภาพรวมสำหรับการปฏิบัติงานของเจ้าหน้าที่และผู้ปฏิบัติงาน โดยมีจุดมุ่งหมายเพื่อให้การดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์นั้น มีวิธีการที่มั่นคงปลอดภัย

"ผู้ใช้งาน" หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป

"สิทธิของผู้ใช้งาน" หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี

"สินทรัพย์" (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิ หรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

"เหตุการณ์ด้านความมั่นคงปลอดภัย" (information security event) หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

/ตัวอย่าง....

ตัวอย่างเหตุการณ์ด้านความมั่นคงปลอดภัยและผลกระทบจากเหตุการณ์ ได้แก่

๑. การไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส ส่งผลให้ข้อมูลขององค์กรเกิดความเสียหาย

๒. มีข้อถกเถียงเกิดขึ้นเกี่ยวกับผู้รับผิดชอบในส่วนประกอบต่าง ๆ ของระบบงาน อาจส่งผลให้การแก้ปัญหาของระบบงานเกิดความล่าช้า

๓. ประตูของศูนย์คอมพิวเตอร์ไม่สามารถล็อคได้ หรือเจ้าหน้าที่รักษาความปลอดภัยนั่งหลับยาม อาจส่งผลให้ระบบ อุปกรณ์ หรือทรัพย์สินสารสนเทศถูกขโมย

๔. การใช้เครือข่ายขององค์กรเพื่อกระทำการใด ๆ ที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ ๒) พ.ศ. ๒๕๖๐ อาจส่งผลให้เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร

๕. การเกิดเหตุการณ์โจมตีเว็บไซต์ขององค์กร ซึ่งอาจทำให้เว็บไซต์ของสำนักเลขาธิการคณะรัฐมนตรีไม่สามารถใช้งานได้

๖. การเกิดเหตุการณ์ปัญหาเว็บไซต์ไม่สามารถแสดงผลได้ อันเนื่องมาจากสาเหตุไฟล์สำคัญเกี่ยวกับการควบคุมการแสดงผลทางเว็บไซต์สูญหายและเสียหาย ส่งผลให้ประชาชนผู้ใช้บริการไม่สามารถสืบค้นข้อมูลสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีได้

เหตุการณ์ดังกล่าวจำเป็นต้องได้รับการรายงานจากผู้ใช้งานที่พบเหตุหรือผู้ที่เกี่ยวข้องโดยเร็ว เพื่อให้มีการจัดการกับเหตุการณ์เหล่านั้นได้อย่างถูกต้อง เหมาะสม และทันการณ์

"สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด" (information security incident) หมายความว่า สถานการณ์ด้านความมั่นคงปลอดภัยที่ไม่พึงประสงค์หรือไม่อาจคาดคิด (unwanted of unexpected) ซึ่งอาจทำให้ระบบขององค์กรถูกบุกรุกหรือโจมตี และความมั่นคงปลอดภัยถูกคุกคาม

"ผู้ดูแลระบบ" (System Administrator) หมายความว่า เจ้าหน้าที่ที่ได้รับมอบหมายจากผู้บังคับบัญชาให้มีหน้าที่รับผิดชอบในการดูแลรักษาระบบสารสนเทศ หรือระบบคอมพิวเตอร์ หรือระบบเครือข่าย

"ระบบสารสนเทศ" (Information System) หมายความว่า ระบบที่ประกอบด้วยส่วนต่าง ๆ ได้แก่ Hardware, Software, User, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์ และติดตามผลการดำเนินงานขององค์กร

"ระบบสารสนเทศการประชุมคณะรัฐมนตรีแบบอิเล็กทรอนิกส์" (CABNET) หมายความว่า ระบบเครือข่ายสารสนเทศแบบปลอดภัยเพื่อสนับสนุนการปฏิบัติภารกิจที่เกี่ยวข้องกับคณะรัฐมนตรี โดยการนำเทคโนโลยีสารสนเทศและการสื่อสารมาปรับใช้การประสานงานและรับส่งข้อมูลในการเสนอเรื่องและการประชุมคณะรัฐมนตรี โดยผู้ใช้งานระบบประกอบด้วย รัฐมนตรีและเลขานุการรัฐมนตรี ผู้ประสานงานคณะรัฐมนตรีและรัฐสภา (ปคร.) และผู้ช่วย ปคร. ตลอดจนบุคลากรของสำนักเลขาธิการคณะรัฐมนตรี

ข้อ ๒ นโยบายในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี แบ่งเป็น ๒ ส่วน ได้แก่

ส่วนที่ ๑ แนวนโยบาย

ส่วนที่ ๒ แนวปฏิบัติ

/รายละเอียด...

รายละเอียดภายในทั้งสองส่วน ประกอบด้วย เนื้อหาสาระสำคัญในประเด็นต่อไปนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน ในกรณีที่ไม่สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ข้อ ๓ ข้อปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ให้เป็นไปตามที่กำหนดไว้ใน แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการคณะรัฐมนตรี พ.ศ. ๒๕๖๐-๒๕๖๑

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบเทคโนโลยีสารสนเทศ ตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและประเมินทบทวนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของสำนักเลขาธิการคณะรัฐมนตรี เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้ระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักเลขาธิการคณะรัฐมนตรีและสื่อต่าง ๆ ให้แก่ผู้ใช้งานและบุคคลทั่วไปสามารถเข้าถึงได้

(๒) จัดอบรมให้ความรู้ความเข้าใจแก่ผู้ใช้งานในเรื่องการรักษาความมั่นคงปลอดภัยสารสนเทศ (information security awareness training) และจัดทำคู่มือการใช้งานระบบสารสนเทศเป็นประจำทุกปี

ข้อ ๖ ในการกำหนดชั้นความลับของสารสนเทศให้เป็นไปตามพระราชบัญญัติข้อมูลข่าวสารของราชการ พ.ศ. ๒๕๔๐ และระเบียบว่าด้วยการรักษาความลับของทางราชการ พ.ศ. ๒๕๔๔ หรือข้อกำหนดอื่น ๆ ที่ได้ประกาศใช้ทดแทน

ข้อ ๗ กรณีระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักเลขาธิการคณะรัฐมนตรี หน่วยงาน หรือบุคคลใดอันเนื่องมาจากการละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น

ข้อ ๘ ให้ผู้ใช้งานสำนักเลขาธิการคณะรัฐมนตรีปฏิบัติตามแนวทางและขั้นตอนการปฏิบัติงานของมาตรการทำลายข้อมูลอิเล็กทรอนิกส์และสื่อบันทึกข้อมูล (Disposal of Media Procedure)

ข้อ ๙ ให้กองบริหารงานสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันและสอดคล้อง ครบถ้วน ตามที่กฎหมายกำหนดไว้

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๒๖ พฤษภาคม พ.ศ. ๒๕๖๐

(นายธีระพงษ์ วงศ์ศิวะวิลาส)
เลขาธิการคณะรัฐมนตรี

แนวปฏิบัติของผู้ใช้งาน (user) ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการคณะรัฐมนตรี พ.ศ. ๒๕๖๐

๑. การบริหารจัดการการเข้าถึงระบบและอุปกรณ์ของผู้ใช้งาน มีแนวทางปฏิบัติ ดังนี้

๑.๑ การเก็บรักษาบัญชีผู้ใช้และการใช้งานรหัสผ่าน

- ผู้ใช้งานจะต้องเก็บรักษาบัญชีผู้ใช้ไว้เป็นความลับห้ามเปิดเผยหรือแจกจ่ายต่อบุคคลอื่น โดยไม่ได้รับอนุญาตจากผู้บังคับบัญชาระดับผู้อำนวยการสำนัก/กอง
- ผู้ใช้งานจะต้องลงบันทึกเข้า (Login) โดยใช้บัญชีผู้ใช้ของตนเอง และทำการลงบันทึกออก (Logout) ทุกครั้งเมื่อหยุดการใช้งานชั่วคราวหรือสิ้นสุดการใช้งาน
- กำหนดให้ผู้ใช้งานเปลี่ยนรหัสผ่านโดยทันที ภายหลังจากที่ได้รับรหัสผ่านชั่วคราว
- ผู้ใช้งานต้องเปลี่ยนรหัสผ่านโดยทันทีที่ทราบว่ารหัสผ่านของตนเองอาจถูกเปิดเผยหรือล่วงรู้โดยผู้อื่น

๑.๒ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน (Clear Desk)

- ผู้ใช้งานต้องออกจากระบบสารสนเทศทันที เมื่อว่างเว้นจากการใช้งานหรือเสร็จสิ้นการใช้งาน

๑.๓ การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Server Policy)

- กำหนดให้เจ้าหน้าที่จัดเก็บข้อมูลสำคัญ และข้อมูลที่มีชั้นความลับไว้ในตู้หรือลิ้นชักที่ล็อกกุญแจหรือที่ที่ปลอดภัยภายหลังจากใช้งานเสร็จ
- ผู้ใช้งานต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงของผู้ไม่มีสิทธิ และต้องจัดเก็บไว้ในที่ที่ปลอดภัยในเวลาที่ไม่มีผู้ดูแล

๑.๔ การใช้งานเครื่องคอมพิวเตอร์

- เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในราชการ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน
- การเคลื่อนย้ายหรือส่งคืนคอมพิวเตอร์เพื่อตรวจซ่อมจะต้องแจ้งให้กองบริหารงานสารสนเทศทราบเพื่อดำเนินการซ่อมบำรุงหรือจัดหาอุปกรณ์มาทดแทน รวมทั้ง บันทึกการรับคืนและส่งมอบให้กับบุคคลที่ได้รับอุปกรณ์ไว้ใช้งานให้เป็นปัจจุบัน

๑.๕ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

- ผู้ใช้งานต้องตระหนักและระมัดระวังต่อการใช้งานข้อมูล ไม่ว่าข้อมูลจะเป็นของสำนักเลขาธิการคณะรัฐมนตรี หรือเป็นข้อมูลบุคคลภายนอก
- ข้อมูลที่เป็นความลับหรือมีระดับความสำคัญ ที่อยู่ในการครอบครอง/ดูแลของหน่วยงาน ห้ามไม่ให้ทำการเผยแพร่ เปลี่ยนแปลง ทำซ้ำ หรือทำลาย โดยไม่ได้รับอนุญาตจากหัวหน้าส่วนราชการ
- การนำการเข้ารหัสมาใช้กับข้อมูลที่เป็นความลับ ผู้ใช้งานต้องปฏิบัติตามระเบียบการรักษาความลับทางราชการ พ.ศ. ๒๕๔๔ และจะต้องใช้วิธีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

๑.๖ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property)

- ให้มีการขออนุญาต ก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน
- ให้ผู้อำนวยการสำนัก/กอง กำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงานและตรวจสอบสภาพอุปกรณ์เมื่อมีการส่งคืน
- บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงาน เพื่อเป็นหลักฐานป้องกันการสูญหายรวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์กลับสู่หน่วยงาน

๒. การควบคุมการเข้าถึงระบบปฏิบัติการ มีแนวทางปฏิบัติ ดังนี้

๒.๑ กำหนดให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ - ๖ เดือน

๒.๒ เมื่อผู้ใช้งานเปลี่ยนรหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกัน ระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่าง ๆ

๒.๓ ผู้ใช้งานไม่ควรอนุญาตให้ผู้อื่นใช้ชื่อผู้ใช้ (User name) และรหัสผ่านของตน ในการเข้าใช้งานเครื่องคอมพิวเตอร์ของหน่วยงานร่วมกัน เมื่อไม่มีการใช้งานต้องทำการล็อกหน้าจอภาพ หลังจากนั้นเมื่อต้องการใช้งานผู้ใช้งานต้องใส่รหัสผ่าน (Password) เพื่อเข้าใช้งานใหม่

๒.๔ ผู้ใช้งานจะต้องลงบันทึกเข้า (Log in) โดยใช้บัญชีผู้ใช้งาน (Account) ของตนเอง และทำการลงบันทึกออก (Log out) ทุกครั้งเมื่อสิ้นสุดการใช้งานหรือหมดการใช้งานชั่วคราว

๒.๕ ผู้ใช้งานจะต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคลและจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๒.๖ กรณีจำเป็นต้องนำข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายออกไปทดสอบหรือดำเนินการใด ๆ ภายนอกหน่วยงาน ผู้ร้องขอจะต้องมีหนังสือรับรองจากผู้บังคับบัญชาระดับผู้บริหารองค์กร เพื่อรับรองการรักษาความลับข้อมูลของทางราชการต่อสำนักเลขาธิการคณะรัฐมนตรีทุกครั้ง

๒.๗ กำหนดให้มีการควบคุมการติดตั้งการใช้งานโปรแกรมอรรถประโยชน์ที่เกี่ยวข้องต่อการปฏิบัติงาน โดยผู้ใช้งานจะต้องอยู่ในระบบ Active Directory และได้รับมอบหมายจากผู้บังคับบัญชา โดยมีหนังสือขอใช้โปรแกรมมายังผู้ดูแลระบบเพื่อเปิดสิทธิในการติดตั้งโปรแกรมอรรถประโยชน์โดยเฉพาะ กำหนดให้มีการบันทึกรายละเอียดการใช้งานโปรแกรมอรรถประโยชน์ของผู้ใช้งานทุกคน

๓. การควบคุมการเข้าถึงโปรแกรมประยุกต์ มีแนวทางปฏิบัติ ดังนี้

๓.๑ กำหนดให้สำนัก/กอง แจ้งรายชื่อผู้ใช้งานระบบสารสนเทศให้กับผู้ดูแลระบบ เพื่อดำเนินการติดตั้งโปรแกรมและกำหนดกลุ่ม/สิทธิในการเข้าถึงระบบสารสนเทศ

๓.๒ กำหนดให้สำนัก/กอง แจ้งยกเลิกรายชื่อผู้ใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานมีการลาออก หรือโอนไปยังหน่วยงานอื่น

๓.๓ กำหนดให้มีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานของสำนัก/กอง ทุก ๆ ปี

การใช้งานอินเทอร์เน็ต (Use of the Internet)

มีแนวทางปฏิบัติ ดังนี้

๑. การเชื่อมต่อคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สำนักเลขาธิการคณะรัฐมนตรีจัดสรรไว้เท่านั้น

๒. เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีการ update pattern ไวรัสคอมพิวเตอร์ให้ทันสมัยอยู่ตลอดเวลา หากตรวจสอบพบว่ายังไม่ได้ติดตั้งให้แจ้งกองบริหารงานสารสนเทศเพื่อทำการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนทำการเชื่อมต่ออินเทอร์เน็ต

๓. ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสำนักเลขาธิการคณะรัฐมนตรี ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ดังต่อไปนี้

๓.๑ เพื่อก่อให้เกิดความเสียหายแก่สำนักเลขาธิการคณะรัฐมนตรีและบุคคลอื่น หรือละเมิดสิทธิ หรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลของบุคคลอื่นการแสดงความคิดเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

๓.๒ เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์

๓.๓ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่มีเนื้อหาขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๔ เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาตซึ่งได้มาจากองค์กรหรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

๔. ผู้ใช้ไม่ควรทำการดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดียที่ไม่เกี่ยวข้องกับการปฏิบัติราชการที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูล (Bandwidth) ตลอดเวลา ผ่านอินเทอร์เน็ตในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวีดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น

๕. ผู้ใช้ไม่ควรดาวน์โหลดไฟล์ข้อมูลหรือโปรแกรมจากเว็บไซต์ที่ไม่น่าเชื่อถือหรือไม่มั่นใจว่าปลอดภัยหรือไม่ เช่น Freeware โปรแกรมรักษาจอภาพ เกม และโปรแกรมที่ลงท้ายด้วย .exe หรือ .com ตลอดจนต้องระมัดระวังการดาวน์โหลดโปรแกรมโดยไม่ละเมิดทรัพย์สินทางปัญญา

๖. ผู้ใช้ต้องระมัดระวัง ไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น อาทิ เลขที่บัตรต่าง ๆ ได้แก่ บัตรประชาชน บัตรเครดิต วันเดือนปีเกิด หรือ หมายเลขโทรศัพท์ ไม่ควรเผยแพร่ลงบนสื่อออนไลน์

๗. ผู้ใช้ไม่ควรเปิดหรือส่งต่อ E-mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ เช่น E-mail โฆษณาขายสินค้า E-mail ให้สินเชื่อ E-mail เสนอให้รางวัล เป็นต้น

๘. ผู้ใช้ต้องตรวจสอบไวรัสคอมพิวเตอร์กับไฟล์ที่แนบมาพร้อม E-mail ทุกครั้งเสมอ ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก

๙. หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นติดไวรัสคอมพิวเตอร์ ผู้ใช้จะต้องไม่ใช้บริการเชื่อมต่อระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่น ๆ

การใช้งานจดหมายอิเล็กทรอนิกส์ (Use of Electronic Mail/@soc.go.th)

มีแนวทางปฏิบัติ ดังนี้

๑. ผู้ใช้ที่ต้องการขอลงทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ต้องทำหนังสือจากผู้อำนวยการสำนัก/กอง ถึงผู้อำนวยการกองบริหารงานสารสนเทศเพื่อดำเนินการกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

๒. ผู้ใช้งาน เมื่อได้รับรหัสผ่านเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ครั้งแรก จะต้องเปลี่ยนรหัสผ่านใหม่ทันที

๓. ผู้ใช้งาน ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือรูปแบบที่ไม่ได้ป้องกันการเข้าถึงข้อมูล และไม่ควรตั้งค่าการช่วยจำรหัสผ่านอัตโนมัติ (Save Password)

๔. ผู้ใช้งาน ควรเปลี่ยนรหัสผ่าน ทุก ๓ - ๖ เดือน

๕. ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับ - ส่งข้อความ ยกเว้นแต่จะได้รับความยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่าง ๆ

๖. หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๗. ผู้ใช้งาน มีหน้าที่ต้องรักษาชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ไว้เป็นความลับ

๘. ผู้ใช้งาน ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงานหรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์

๙. ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์เป็นประจำ และควรจัดเก็บแฟ้มข้อมูล เพื่อให้จดหมายอิเล็กทรอนิกส์เหลือน้อยที่สุด ตลอดจนควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

Do & Don't

แนวปฏิบัติของผู้ใช้งาน ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการคณะรัฐมนตรี

Vol. 1

Cyber Security Tips

ช่วยกันปฏิบัติตามหลัก Do & Don't เพื่อความปลอดภัยของหน่วยงานเรานะครับ

Do:1

Log in เข้าระบบ
ด้วยบัญชีของตนเอง
และ Log out ทุกครั้ง
ที่ท่านใช้งานเสร็จสิ้น

Do:2

การตั้งรหัสผ่าน
ห้ามต่ำกว่า 8 ตัว
ควรมีตัวเลข ตัวอักษร
และอักขระพิเศษ ปนกัน

Do:3

ผู้ใช้งานควรทำการ
เปลี่ยนรหัสผ่าน
ทุกๆ 3-6 เดือน
เพื่อความปลอดภัย

Do:4

ตั้งระบบล็อกหน้าจอ
กำหนดรหัสผ่าน
ป้องกันผู้อื่นเข้ามา
ใช้ระบบงานของท่าน

Don't 1

ไม่เก็บข้อมูลส่วนตัว
ไว้ในคอมพิวเตอร์
เช่น รหัสบัตรประชาชน
และรหัสบัตรเครดิต

Don't 2

ไม่แปะรหัสผ่านสำคัญ
ไว้ที่จอคอมพิวเตอร์ และ
โต๊ะทำงาน เพราะผู้อื่น
จะเข้าถึงข้อมูลได้ง่าย

Don't 3

ไม่เปิดหรือส่งต่อ
E-Mail ที่ไม่รู้จัก
และไม่ทราบแหล่งที่มา
เพื่อป้องกันไวรัส

Don't 4

ไม่เปิดเผยรหัสสำคัญ
หรือแจกจ่ายรหัสผ่าน
ของท่านให้บุคคลอื่น
ที่ไม่มีความน่าเชื่อถือ

ติดต่อ: กองบริหารงานสารสนเทศ (กบส.) หมายเลขภายใน 568

Do & Don't

แนวปฏิบัติของผู้ใช้งาน ตามแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการคณะรัฐมนตรี

Vol. 2

➤ Cyber Security Tips

ช่วยกันปฏิบัติตามหลัก Do & Don't
เพื่อความปลอดภัยของหน่วยงานเรานะครับ

Do:1

ติดตั้งโปรแกรม Anti-Virus และ Update อย่างสม่ำเสมอ

Don't 1

ไม่ใช้อินเทอร์เน็ตของหน่วยงาน Download ไฟล์มัลติมีเดีย ที่มีขนาดไฟล์ใหญ่เกินไป

Do:2

เก็บทรัพย์สินหรือข้อมูลสารสนเทศไว้ในจุดที่ปลอดภัย ให้ยากต่อการเข้าถึง

Don't 2

ไม่ใช้อินเทอร์เน็ตของหน่วยงานทำเรื่องเสื่อมเสีย ผิดศีลธรรม

Do:3

หากสงสัยว่าคอมพิวเตอร์ติดไวรัส ให้ติดต่อเจ้าหน้าที่ และหยุดการแชร์ไฟล์

Don't 3

ไม่ Download ไฟล์จากเว็บไซต์ที่ไม่มีความน่าเชื่อถือ

ติดต่อ: กองบริหารงานสารสนเทศ (กบส.) หมายเลขภายใน 568