ประกาศสำนักเลขาธิการคณะรัฐมนตรี
เรื่อง แนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ
พ.ศ. ๒๕๕๗

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

ข้อ ๑ ในประกาศนี้

"แนวนโยบาย" หมายถึง หลักการรักษาความมั่นคงปลอดภัยด้านสารสนเทศในการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ ซึ่งสำนักเลขาธิการคณะรัฐมนตรีประกาศไว้เพื่อให้เจ้าหน้าที่และผู้ปฏิบัติงานของสำนักเลขาธิการคณะรัฐมนตรีที่เกี่ยวข้องกับการดำเนินงานดังกล่าวได้ถือปฏิบัติให้เป็นไปในแนวทางเดียวกัน 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 สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี

"สินทรัพย์" (asset) หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร

"การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ" หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้

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

/เหตุการณ์ ...

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

ตัวอย่างเหตุการณ์ด้านความมั่นคงปลอดภัยและผลกระทบจากเหตุการณ์ ได้แก่

๑. การไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส ส่งผลให้ข้อมูลขององค์กรเกิดความเสียหาย

๒. มีข้อถกเถียงเกิดขึ้นเกี่ยวกับผู้รับผิดชอบในส่วนประกอบต่าง ๆ ของระบบงาน อาจส่งผลให้การแก้ปัญหาของระบบงานเกิดความล่าช้า

๓. ประตูของศูนย์คอมพิวเตอร์ไม่สามารถล็อคได้ หรือเจ้าหน้าที่รักษาความปลอดภัยนั่งหลับยาม อาจส่งผลให้ระบบ อุปกรณ์ หรือทรัพย์สินสารสนเทศถูกขโมย

๔. การใช้เครือข่ายขององค์กรเพื่อกระทำการใด ๆ ที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อาจส่งผลให้เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร

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 โดยการนำเทคโนโลยีสารสนเทศและการสื่อสารมาปรับใช้ในการประสานงานและรับส่งข้อมูลในการเสนอเรื่องและการประชุมคณะรัฐมนตรี 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. ๒๕๕๗**

ข้อ ๔ ตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ โดยกำหนดให้มีการตรวจสอบและควบคุมคุณภาพระบบเทคโนโลยีสารสนเทศ ตรวจประเมินระบบรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศและประเมินทบทวนความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

ข้อ ๕ สร้างความรู้ความเข้าใจให้กับผู้ใช้งานของสำนักเลขาธิการคณะรัฐมนตรี เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศโดยไม่ระมัดระวังหรือรู้เท่าไม่ถึงการณ์ด้วยวิธีการ

(๑) เผยแพร่นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านเทคโนโลยีสารสนเทศทางเว็บไซต์สำนักเลขาธิการคณะรัฐมนตรี และสื่อต่าง 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 ให้สำนักบริหารงานสารสนเทศเป็นผู้รับผิดชอบดำเนินการให้เป็นไปตามประกาศนี้ และให้มีการทบทวนนโยบายและแนวปฏิบัติให้เป็นปัจจุบันอย่างน้อยปีละ ๑ ครั้ง

ทั้งนี้ ตั้งแต่บัดนี้เป็นต้นไป

ประกาศ ณ วันที่ ๗ กรกฎาคม พ.ศ. ๒๕๕๗

(นายอำพน กิตติอำพน)
เลขาธิการคณะรัฐมนตรี

แนวนโยบาย
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักเลขาธิการคณะรัฐมนตรี

พ.ศ. ๒๕๕๗

แนวนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักเลขาธิการคณะรัฐมนตรี พ.ศ. ๒๕๕๗

๑. วัตถุประสงค์และขอบเขต

เพื่อให้การพัฒนาระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีเป็นไปอย่างเหมาะสม มีประสิทธิภาพ และการดำเนินการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ โดยสำนักเลขาธิการคณะรัฐมนตรีมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้อง และการถูกคุกคามจากภัยต่าง ๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักเลขาธิการคณะรัฐมนตรี จึงเห็นสมควรกำหนดนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีให้ครอบคลุมการดำเนินการ ดังนี้

๑.๑ การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

๑.๒ จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งาน และจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์ เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

๑.๓ การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

โดยจะต้องมีการดำเนินการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันตามระยะเวลา ๑ ครั้งต่อปี และจะต้องมีการสร้างความรู้ความเข้าใจให้กับผู้ใช้งานเพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานสารสนเทศ

๒. องค์ประกอบของนโยบาย

๒.๑ นโยบายการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

กำหนดพื้นที่ที่ต้องมีการรักษาความมั่นคงปลอดภัย กระบวนการควบคุมการเข้าออกเฉพาะบุคคลที่ได้รับการอนุญาตเพื่อปฏิบัติงานในพื้นที่ควบคุม และการป้องกันระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายที่ติดตั้งในพื้นที่ควบคุมจากภาวะเสี่ยงต่อการสูญหายจากอัคคีภัย หรือความเสียหายจากการเข้าถึงโดยผู้ไม่มีสิทธิ

๒.๒ นโยบายการควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

กำหนดกระบวนการควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่าย และระบบเครือข่ายเฉพาะบุคคลที่ได้รับการอนุญาตเพื่อปฏิบัติงาน และการป้องกันระบบคอมพิวเตอร์ ระบบสารสนเทศ และระบบเครือข่ายที่ติดตั้งในห้องควบคุมจากภาวะเสี่ยงต่อการสูญหาย จากอัคคีภัย หรือความเสียหายจากการเข้าถึงโดยผู้ไม่มีสิทธิ

๒.๓ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศภายในสำนักเลขาธิการคณะรัฐมนตรี

๒.๓.๑ มีการบริหารจัดการการเข้าถึงระบบและอุปกรณ์ของผู้ใช้งาน เพื่อควบคุมการเข้าถึงอุปกรณ์ในการประมวลผลข้อมูลเฉพาะผู้ที่ได้รับอนุญาตและลงทะเบียนแล้ว และควบคุมการเข้าถึงระบบสารสนเทศแต่ละระบบตามความเหมาะสม มีการทบทวนสิทธิการเข้าถึงของผู้ใช้งานตามระยะเวลาที่กำหนด และมีการบริหารจัดการรหัสผ่านสำหรับผู้ใช้งานที่รัดกุม

๒.๓.๒ มีการกำหนดหน้าที่ความรับผิดชอบของผู้ใช้งาน เพื่อป้องกันการเข้าถึงระบบและอุปกรณ์โดยไม่ได้รับอนุญาต ป้องกันการเปิดเผยหรือการลักลอบทำสำเนาข้อมูลสารสนเทศและการลักขโมยอุปกรณ์ประมวลผลข้อมูล

๒.๓.๓ มีการควบคุมการเข้าถึงระบบเครือข่าย เพื่อป้องกันการเข้าถึงระบบและอุปกรณ์ โดยไม่ได้รับอนุญาต โดยผู้ดูแลระบบต้องควบคุมการจัดเส้นทางเชื่อมต่อเครือข่าย แบ่งแยกเครือข่ายตามกลุ่มผู้ใช้งานที่เหมาะสม โดยเฉพาะการกำหนดเส้นทางการเชื่อมต่อระบบคอมพิวเตอร์เพื่อใช้งานอินเทอร์เน็ต ต้องผ่านอุปกรณ์รักษาความปลอดภัยที่สำนักเลขาธิการคณะรัฐมนตรีจัดหาไว้ป้องกันภัยคุกคามอย่างเป็นระบบ

๒.๓.๔ มีการควบคุมการเข้าถึงระบบปฏิบัติการและโปรแกรมประยุกต์ โดยมีการควบคุมการเข้าใช้งานฟังก์ชั่นต่าง ๆ ของโปรแกรมตามนโยบายที่กำหนดไว้ มีการบริหารจัดการรหัสผ่านที่มีการทำงานในลักษณะอัตโนมัติ และมีการยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นการใช้งานในระยะเวลาที่กำหนด

๒.๔ นโยบายการควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

๒.๔.๑ มีการบริหารจัดการการเข้าถึงของผู้ใช้งาน เพื่อควบคุมการเข้าถึงระบบสารสนเทศเฉพาะผู้ที่ได้รับอนุญาตและลงทะเบียนแล้ว และสำหรับระบบ CABNET ผู้ใช้งานทุกคนต้องผ่านการพิสูจน์ตัวตน (Authentication) โดยการสแกนลายนิ้วมือที่จัดเก็บ จึงสามารถเข้าใช้งานเครือข่ายและระบบสารสนเทศ CABNET ตามสิทธิที่ได้รับอนุญาตไว้เท่านั้น

๒.๔.๒ มีการควบคุมการเข้าถึงระบบปฏิบัติการและโปรแกรมประยุกต์ โดยมีการควบคุมการเข้าใช้งานฟังก์ชั่นต่าง ๆ ของโปรแกรมตามนโยบายที่กำหนดไว้ มีการบริหารจัดการรหัสผ่านที่มีการทำงานในลักษณะอัตโนมัติ และมีการยุติการใช้งานระบบสารสนเทศเมื่อว่างเว้นจากการใช้งานในระยะเวลาที่กำหนด

๒.๕ นโยบายการใช้งานอินเทอร์เน็ต และจดหมายอิเล็กทรอนิกส์

๒.๕.๑ มีระบบรักษาความปลอดภัยเพื่อตรวจสอบการใช้งานและภัยคุกคาม

๒.๕.๒ มีข้อกำหนดสำหรับผู้ใช้งานที่ถูกต้องโดยไม่ผิดกฎหมาย ไม่ละเมิดสิทธิ หรือไม่กระทำการใด ๆ ที่สร้างปัญหาให้แก่ระบบหรือบุคคลอื่น และต้องใช้จดหมายอิเล็กทรอนิกส์ที่สำนักเลขาธิการคณะรัฐมนตรีจัดให้เท่านั้น

๒.๖ นโยบายการจัดทำระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน

มีแนวทางปฏิบัติหรือมาตรการในการจัดทำระบบคอมพิวเตอร์สำรองนอกสถานที่ (Offsite Backup) และระบบสำรองข้อมูล (Backup System) เพื่อป้องกันข้อมูลสูญหาย เพิ่มความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ในกรณีฉุกเฉินหรือสถานการณ์ไม่ปกติหรือมีภัยพิบัติเกิดขึ้น ให้สามารถใช้ระบบสารสนเทศที่สำคัญได้อย่างต่อเนื่องด้วยระบบ Offsite Backup ที่สามารถทำงานแทนระบบหลักได้ทันทีหรือในเวลาอันสั้น และสามารถกู้คืนระบบสารสนเทศที่มีความสำคัญระดับรองจาก Backup System ภายในระยะเวลาที่เหมาะสม

๒.๗ นโยบายการตรวจสอบและประเมินความเสี่ยง

มีการตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศปีละ ๑ ครั้ง ทั้งนี้ การตรวจสอบและประเมินความเสี่ยงจะดำเนินการโดยผู้ตรวจสอบภายในของสำนักเลขาธิการคณะรัฐมนตรี เพื่อให้สำนักเลขาธิการคณะรัฐมนตรีทราบถึงระดับความเสี่ยงและความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี

๒.๘ นโยบายการสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศ

มีการฝึกอบรมจัดทำคู่มือการใช้งานระบบสารสนเทศเป็นประจำทุก ๆ ปี ตลอดจนเผยแพร่ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความตระหนักถึงความสำคัญของการปฏิบัติงานของผู้ใช้งาน

๒.๙ นโยบายการบริหารจัดการซอฟต์แวร์และลิขสิทธิ์

การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsourced Software development) จะต้องพิจารณาระบุว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ด ในการพัฒนาซอฟต์แวร์

นโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีนี้จัดเป็นมาตรฐานด้านความปลอดภัยในการใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารของสำนักเลขาธิการคณะรัฐมนตรี ซึ่งเจ้าหน้าที่ของสำนักเลขาธิการคณะรัฐมนตรีและผู้ที่เกี่ยวข้องจะต้องทราบและปฏิบัติตามอย่างเคร่งครัด โดยให้ผู้บริหารระดับสูงสุดของหน่วยงาน (Chief Executive Officer : CEO) เป็นผู้รับผิดชอบต่อความเสี่ยง ความเสียหาย หรืออันตรายที่เกิดขึ้น ทั้งนี้ กรณีที่ระบบคอมพิวเตอร์หรือข้อมูลสารสนเทศเกิดความเสียหายหรืออันตรายใด ๆ แก่สำนักเลขาธิการคณะรัฐมนตรี หน่วยงาน หรือบุคคลใด อันเนื่องมาจากการละเลยหรือฝ่าฝืนการปฏิบัติตามนโยบายการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ สำนักเลขาธิการคณะรัฐมนตรีจะทำการตรวจสอบและดำเนินการตามสมควรแก่เหตุและผลที่เกิดขึ้นจากการละเมิดนโยบายดังกล่าวนี้

แนวปฏิบัติ
ในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักเลขาธิการคณะรัฐมนตรี

พ.ศ. ๒๕๕๗

แนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ

สำนักเลขาธิการคณะรัฐมนตรี พ.ศ. ๒๕๕๗

๑. วัตถุประสงค์และขอบเขต

เพื่อให้การพัฒนาระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีเป็นไปอย่างเหมาะสม มีประสิทธิภาพ และการดำเนินการใดๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ โดยสำนักเลขาธิการคณะรัฐมนตรีมีความมั่นคงปลอดภัยและเชื่อถือได้ ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล รวมทั้งเพื่อป้องกันปัญหาที่อาจจะเกิดขึ้นจากการใช้ระบบเทคโนโลยีสารสนเทศในลักษณะที่ไม่ถูกต้องและการถูกคุกคามจากภัยต่างๆ ซึ่งอาจก่อให้เกิดความเสียหายแก่สำนักเลขาธิการคณะรัฐมนตรี สำนักเลขาธิการคณะรัฐมนตรีจึงเห็นสมควรกำหนดแนวนโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีให้ครอบคลุมการดำเนินการ ดังนี้

(๑) การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ

(๒) จัดให้มีระบบสารสนเทศและระบบสำรองของสารสนเทศซึ่งอยู่ในสภาพพร้อมใช้งานและจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉินในกรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์เพื่อให้สามารถใช้งานสารสนเทศได้ตามปกติอย่างต่อเนื่อง

(๓) การตรวจสอบและประเมินความเสี่ยงด้านสารสนเทศอย่างสม่ำเสมอ

ทั้งนี้ สำนักเลขาธิการคณะรัฐมนตรีจะต้องทำการเผยแพร่นโยบายและแนวปฏิบัตินี้ให้เจ้าหน้าที่ทุกระดับในสำนักเลขาธิการคณะรัฐมนตรีและผู้เกี่ยวข้อง ที่จะเข้าใช้งานระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ได้รับทราบและถือปฏิบัติโดยเคร่งครัด และจะต้องมีการดำเนินการทบทวนปรับปรุงนโยบายและข้อปฏิบัติให้เป็นปัจจุบันตามระยะเวลา ๑ ครั้งต่อปี ซึ่งสำนักเลขาธิการคณะรัฐมนตรีได้จัดทำ “นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี” ขึ้นเมื่อเดือนกันยายน ๒๕๕๓ และมีการแจ้งเวียนให้ข้าราชการ พนักงานราชการ และลูกจ้างประจำของหน่วยงานถือปฏิบัติตลอดระยะเวลาที่ผ่านมา

๒. องค์ประกอบของแนวปฏิบัติ

๒.๑ คำนิยาม

๒.๒ การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม

๒.๓ การควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๒.๔ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศภายในสำนักเลขาธิการคณะรัฐมนตรี

๒.๕ การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

๒.๖ การใช้งานอินเทอร์เน็ต

๒.๗ การใช้งานจดหมายอิเล็กทรอนิกส์
๒.๘ การจัดทำระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน
๒.๙ การตรวจสอบและประเมินความเสี่ยง
๒.๑๐ การสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ
๒.๑๑ การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์

องค์ประกอบของแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยด้านสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรีแต่ละส่วนดังกล่าวจะประกอบด้วย วัตถุประสงค์ รายละเอียดของข้อกำหนด แนวทางปฏิบัติ และขั้นตอนวิธีการปฏิบัติในการรักษาความมั่นคงปลอดภัยในระบบเทคโนโลยีสารสนเทศ รวมทั้งการกำหนดผู้รับผิดชอบตามนโยบายและข้อปฏิบัติแต่ละส่วน เพื่อให้สำนักเลขาธิการคณะรัฐมนตรีสามารถใช้ระบบเทคโนโลยีสารสนเทศประกอบการปฏิบัติงานและการให้บริการหน่วยงานและประชาชนได้อย่างมีประสิทธิภาพ ตลอดจนเป็นการสร้างความเชื่อมั่นของหน่วยงานและประชาชนต่อการดำเนินการของสำนักเลขาธิการคณะรัฐมนตรีด้วยวิธีการทางอิเล็กทรอนิกส์ด้วย

ส่วนที่ ๑
คำนิยาม

คำนิยามที่ใช้ในแนวปฏิบัตินี้ ประกอบด้วย

- **หน่วยงาน** หมายความว่า สำนักเลขาธิการคณะรัฐมนตรี
- **ผู้ใช้งาน** หมายความว่า ข้าราชการ เจ้าหน้าที่ พนักงานของรัฐ ลูกจ้าง ผู้ดูแลระบบ ผู้บริหารขององค์กร ผู้รับบริการ ผู้ใช้งานทั่วไป
- **สิทธิของผู้ใช้งาน** หมายความว่า สิทธิทั่วไป สิทธิจำเพาะ สิทธิพิเศษ และสิทธิอื่นใดที่เกี่ยวข้องกับระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี
- **สินทรัพย์ (asset)** หมายความว่า สิ่งใดก็ตามที่มีคุณค่าสำหรับองค์กร
- **การเข้าถึงหรือควบคุมการใช้งานสารสนเทศ** หมายความว่า การอนุญาต การกำหนดสิทธิหรือการมอบอำนาจให้ผู้ใช้งาน เข้าถึงหรือใช้งานเครือข่ายหรือระบบสารสนเทศ ทั้งทางอิเล็กทรอนิกส์และทางกายภาพ รวมทั้งการอนุญาตเช่นว่านั้นสำหรับบุคคลภายนอก ตลอดจนอาจกำหนดข้อปฏิบัติเกี่ยวกับการเข้าถึงโดยมิชอบเอาไว้ด้วยก็ได้
- **ความมั่นคงปลอดภัยด้านสารสนเทศ (information security)** หมายความว่า การธำรงไว้ซึ่งความลับ (confidentiality) ความถูกต้องครบถ้วน (integrity) และสภาพพร้อมใช้งาน (availability) ของสารสนเทศ รวมทั้งคุณสมบัติอื่น ได้แก่ความถูกต้องแท้จริง (authenticity) ความรับผิด (accountability) การห้ามปฏิเสธความรับผิด (non-repudiation) และความน่าเชื่อถือ (reliability)
- **เหตุการณ์ด้านความมั่นคงปลอดภัย (information security event)** หมายความว่า กรณีที่ระบุการเกิดเหตุการณ์ สภาพของบริการหรือเครือข่ายที่แสดงให้เห็นความเป็นไปได้ที่จะเกิดการฝ่าฝืนนโยบายด้านความมั่นคงปลอดภัยหรือมาตรการป้องกันที่ล้มเหลว หรือเหตุการณ์อันไม่อาจรู้ได้ว่าอาจเกี่ยวข้องกับความมั่นคงปลอดภัย

ตัวอย่างเหตุการณ์ด้านความมั่นคงปลอดภัยและผลกระทบจากเหตุการณ์ ได้แก่

๑. การไม่ได้ติดตั้งโปรแกรมป้องกันไวรัส ส่งผลให้ข้อมูลขององค์กรเกิดความเสียหาย

๒. มีข้อถกเถียงเกิดขึ้นเกี่ยวกับผู้รับผิดชอบในส่วนประกอบต่าง ๆ ของระบบงาน อาจส่งผลให้การแก้ปัญหาของระบบงานเกิดความล่าช้า

๓. ประตูของศูนย์คอมพิวเตอร์ไม่สามารถล็อคได้ หรือเจ้าหน้าที่รักษาความปลอดภัยนั่งหลับยาม อาจส่งผลให้ระบบ อุปกรณ์ หรือทรัพย์สินสารสนเทศถูกขโมย

๔. การใช้เครือข่ายขององค์กรเพื่อกระทำการใด ๆ ที่ขัดต่อพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ อาจส่งผลให้เกิดภาพลักษณ์ที่ไม่ดีต่อองค์กร

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 ระบบที่ประกอบด้วยส่วนต่างๆ ได้แก่ Hardware, Software, User, Data และ Procedure ซึ่งทุกองค์ประกอบนี้ทำงานร่วมกันเพื่อกำหนด รวบรวม จัดเก็บข้อมูล ประมวลผลข้อมูลเพื่อสร้างสารสนเทศ และส่งผลลัพธ์หรือสารสนเทศที่ได้ให้ผู้ใช้งานเพื่อช่วยสนับสนุนการทำงาน การตัดสินใจ การวางแผน การบริหาร การควบคุม การวิเคราะห์และติดตามผลการดำเนินงานขององค์กร
- **ระบบสารสนเทศการประชุมคณะรัฐมนตรีแบบอิเล็กทรอนิกส์ (CABNET)** หมายความว่า ระบบเครือข่ายสารสนเทศแบบปลอดภัยเพื่อสนับสนุนการปฏิบัติภารกิจที่เกี่ยวข้องกับคณะรัฐมนตรี โดยการนำเทคโนโลยีสารสนเทศและการสื่อสารมาปรับใช้ในการประสานงานและรับส่งข้อมูลในการเสนอเรื่องและการประชุมคณะรัฐมนตรี โดยผู้ใช้งานระบบประกอบด้วย รัฐมนตรีและเลขานุการรัฐมนตรี ผู้ประสานงานคณะรัฐมนตรีและรัฐสภา (ปคร.) และผู้ช่วย ปคร. ตลอดจนบุคลากรของสำนักเลขาธิการคณะรัฐมนตรี (สลค.)

ส่วนที่ ๒
การรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม
(Physical and Environment Security)

๑. วัตถุประสงค์

เพื่อให้การบริหารจัดการด้านอาคาร สถานที่ และพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศมีมาตรการควบคุมและป้องกันเพื่อการรักษาความมั่นคงปลอดภัยทางด้านกายภาพและสิ่งแวดล้อม โดยการกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัยโดยพิจารณาตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและระบบข้อมูล การควบคุมการเข้าออกอาคารสถานที่ รวมทั้งการจัดทำแผนและมาตรการการป้องกันอัคคีภัยในบริเวณพื้นที่ดังกล่าว โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานที่มีส่วนเกี่ยวข้องกับการใช้ระบบเทคโนโลยีสารสนเทศและการสื่อสารของ สำนักเลขาธิการคณะรัฐมนตรี

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศ
- เห็นชอบการกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบเทคโนโลยีสารสนเทศ
- เห็นชอบการกำหนดผู้มีสิทธิ์เข้าออกพื้นที่

๒.๒ ผู้ดูแลระบบการรักษาความมั่นคงปลอดภัยในพื้นที่ที่กำหนด
- ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ ดูแลในภาพรวมของพื้นที่ที่กำหนด
- นายพนมกาญ สุขขุนทด ดูแลห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย
- นายพนมกาญ สุขขุนทด ดูแลห้องระบบไฟฟ้าสำรอง
- นายพนมกาญ สุขขุนทด ดูแลห้องฝึกอบรมคอมพิวเตอร์
- นายอัฐพงษ์ โสภา ดูแลห้องปฏิบัติงาน Help Desk
- นายอุดมรัตน์ สุวรรณราช ดูแลห้องเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ โซน A
- นางสาวนวสรณ์ สร้อยโพธิ์พันธุ์ ดูแลห้องเจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศ โซน B

๓. การกำหนดบริเวณที่ต้องมีการรักษาความมั่นคงปลอดภัย

๓.๑ สำนักบริหารงานสารสนเทศ ทำหน้าที่กำหนดพื้นที่ของระบบเทคโนโลยีสารสนเทศต่างๆ ตามความสำคัญของอุปกรณ์ระบบเทคโนโลยีสารสนเทศและระบบข้อมูลตามเอกสาร *“การกำหนดพื้นที่เพื่อการรักษาความมั่นคงปลอดภัยของระบบสารสนเทศ”* เพื่อจุดประสงค์ในการเฝ้าระวัง ควบคุม การรักษาความมั่นคงปลอดภัย จากผู้ที่ไม่ได้รับอนุญาต รวมทั้งป้องกันความเสียหายอื่นๆ ที่อาจเกิดขึ้นได้

๓.๒ การกำหนดและจำแนกบริเวณพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารประกอบด้วยพื้นที่ส่วนต่างๆ ตามแผนผังแสดงตำแหน่งของพื้นที่ใช้งาน แบ่งออกเป็นพื้นที่ทำงานทั่วไปของ

เจ้าหน้าที่ด้านเทคโนโลยีสารสนเทศและผู้ดูแลระบบ พื้นที่ติดตั้งเครื่องคอมพิวเตอร์แม่ข่าย (Server) และจัดเก็บข้อมูลคอมพิวเตอร์ พื้นที่ติดตั้งอุปกรณ์ระบบเครือข่าย (Network Equipment area) พื้นที่ห้องควบคุมระบบไฟฟ้าสำรอง พื้นที่ห้องปฏิบัติงาน Help Desk และพื้นที่ห้องฝึกอบรมคอมพิวเตอร์

๓.๓ การกำหนดสิทธิให้กับเจ้าหน้าที่ ให้สามารถมีสิทธิในการเข้าถึงพื้นที่ใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสารเพื่อปฏิบัติหน้าที่ตามที่ได้รับมอบหมาย ประกอบด้วย

๓.๓.๑ การจัดทำ “ทะเบียนผู้มีสิทธิเข้าออกพื้นที่” เพื่อใช้งานระบบเทคโนโลยีสารสนเทศและการสื่อสาร

๓.๓.๒ การจัดให้มีเจ้าหน้าที่ทำหน้าที่ปรับปรุงรายการผู้มีสิทธิเข้าออกพื้นที่ใช้งานระบบสารสนเทศและการสื่อสารทันทีที่มีการโอนย้าย ลาออก และทบทวนรายการอย่างน้อยปีละ ๑ ครั้ง

๓.๔ กำหนดให้เครื่องคอมพิวเตอร์แม่ข่ายของระบบงานที่สำคัญของสำนักเลขาธิการคณะรัฐมนตรี รวมทั้งระบบที่ไวต่อการรบกวน (ถ้ามี) ติดตั้งอยู่ในบริเวณห้องควบคุมเครื่องแม่ข่ายและอุปกรณ์เครือข่าย เนื่องจากเป็นพื้นที่ที่มีการรักษาความมั่นคงปลอดภัยมากที่สุด

๔. การควบคุมการเข้าออกอาคารสถานที่

๔.๑ การควบคุมการเข้าออกสำหรับผู้ใช้งานและบุคคลภายนอก ในการเข้าถึงสถานที่ มีดังนี้

๔.๑.๑ สำนักเลขาธิการคณะรัฐมนตรีกำหนดสิทธิผู้ใช้งานที่มีสิทธิผ่านเข้าออก และช่วงเวลาที่มีสิทธิในการผ่านเข้าออกในแต่ละพื้นที่ใช้งานระบบอย่างชัดเจน

๔.๑.๒ การเข้าถึงอาคารของสำนักเลขาธิการคณะรัฐมนตรี ของบุคคลภายนอก หรือผู้มาติดต่อเจ้าหน้าที่รักษาความปลอดภัย จะต้องให้มีการแลกบัตรที่ใช้ระบุตัวตนของบุคคลนั้นๆ เช่น บัตรประชาชน ใบอนุญาตขับขี่ เป็นต้น แล้วทำการลงบันทึกข้อมูลบัตรในสมุดบันทึกและรับแบบฟอร์มการเข้าออกพร้อมกับบัตรผู้ติดต่อ (Visitor)

๔.๑.๓ บุคคลที่มาติดต่อต้องติดบัตรผู้ติดต่อ (Visitor) ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ในสำนักเลขาธิการคณะรัฐมนตรี

๔.๑.๔ เจ้าหน้าที่ที่บุคคลภายนอกเข้ามาติดต่อ จะต้องลงชื่ออนุญาตการเข้าออกในแบบฟอร์มการเข้าออกให้ถูกต้อง และจะต้องอยู่กับบุคคลที่มาติดต่อตลอดเวลา

๔.๑.๕ บุคคลภายนอกหรือผู้ติดต่อ ต้องคืนบัตรผู้ติดต่อ (Visitor) กับเจ้าหน้าที่รักษาความปลอดภัยก่อนออกจากอาคาร และเจ้าหน้าที่รักษาความปลอดภัยต้องตรวจสอบผู้ติดต่อ อุปกรณ์ที่ติดตัว พร้อมลงเวลาออกที่สมุดบันทึกให้ถูกต้อง

๔.๒ ผู้ใช้งาน จะได้รับสิทธิให้เข้าออกสถานที่ทำงานได้เฉพาะบริเวณพื้นที่ที่ถูกกำหนดเพื่อใช้ในการทำงานเท่านั้น

๔.๓ หากมีบุคคลอื่นที่ไม่ใช้ผู้ใช้งานขอเข้าพื้นที่ ผู้ดูแลพื้นที่นั้นต้องตรวจสอบเหตุผลและความจำเป็นก่อนที่จะอนุญาต และจดบันทึกบุคคลและการเข้าออกไว้เป็นหลักฐานการอนุญาตให้เข้าใช้พื้นที่

เอกสารประกอบปรากฏตามภาคผนวก ๓(๓) แผนผังพื้นที่รักษาความมั่นคงปลอดภัยอาคารสำนักงานเลขาธิการคณะรัฐมนตรี และทะเบียนผู้มีสิทธิเข้าออกพื้นที่

ส่วนที่ ๓

การควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

(Server and Network System Control Room)

๑. วัตถุประสงค์

เพื่อให้การบริหารจัดการการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่าย (Server) และระบบเครือข่ายมีมาตรการควบคุมการเข้าถึงอุปกรณ์ระบบสารสนเทศและระบบเครือข่าย โดยมาตรการนี้จะมีผลบังคับใช้กับผู้ใช้งานและบุคคลภายนอกที่มีส่วนเกี่ยวข้องกับอุปกรณ์ระบบสารสนเทศ และระบบเครือข่าย

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศ เป็นผู้เห็นชอบการกำหนดสิทธิเข้าออกพื้นที่ใช้งานห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย และเห็นชอบกระบวนการควบคุมการเข้าออกห้องควบคุมฯ

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี เป็นผู้กำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมฯ โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในสำนักเลขาธิการคณะรัฐมนตรี

๒.๓ นางสาวปาจรีย์ แจ่มจักษุ เป็นผู้ดูแลห้องควบคุมฯ ทำหน้าที่ตรวจดูแลผู้มีสิทธิเข้าออกพื้นที่และบุคคลที่ขออนุญาตเข้าถึงห้องควบคุมฯ ให้มีการปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมฯ อย่างเคร่งครัด

๒.๔ นางฉันทนา อ้นมี เป็นผู้ตรวจสอบการเข้าห้องควบคุมฯ ทำหน้าที่ สังเกต และตักเตือนให้บุคคลที่ขออนุญาตเข้าถึงห้องควบคุมฯ ให้มีการปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๓. กระบวนการควบคุมการเข้าออกห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๓.๑ ผู้ดูแลห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย และเจ้าหน้าที่ IT มีแนวทางปฏิบัติดังนี้

๓.๑.๑ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรีต้องทำการกำหนดสิทธิบุคคลในการเข้าออกห้องควบคุมฯ โดยเฉพาะบุคคลที่ปฏิบัติหน้าที่เกี่ยวข้องภายในสำนักเลขาธิการคณะรัฐมนตรี

๓.๑.๒ ผู้ดูแลห้องควบคุมฯ ต้องจัดทำบันทึกทะเบียนผู้มีสิทธิเข้าออกพื้นที่ต่างๆ ในห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๓.๑.๓ สิทธิในการเข้าออกพื้นที่ต่างๆในห้องควบคุมฯ ของเจ้าหน้าที่แต่ละคนต้องได้รับความเห็นชอบจากผู้อำนวยการสำนักบริหารงานสารสนเทศเป็นลายลักษณ์อักษร โดยสิทธิของเจ้าหน้าที่แต่ละคนขึ้นอยู่กับหน้าที่การปฏิบัติงานภายในห้องควบคุมฯ

๓.๑.๔ เจ้าหน้าที่ทุกคนจะต้องสแกนลายนิ้วมือเพื่อการเข้าออกห้องควบคุมฯ

๓.๑.๕ การเข้าออกห้องควบคุมฯ ต้องมีการลงบันทึกเวลาเข้าออก เหตุผลในการเข้าห้องควบคุมฯ ในสมุดบัญชีควบคุมการเข้าใช้งานห้องควบคุมเครื่องคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๓.๑.๖ เจ้าหน้าที่ทุกคนจะต้องติดบัตรแสดงตนตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ภายในอาคารสถานที่

๓.๑.๗ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบเจ้าหน้าที่ IT

๓.๑.๘ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๓.๒ เจ้าหน้าที่ IT ผู้ใช้งาน และบุคคลภายนอก มีแนวทางปฏิบัติ ดังนี้

๓.๒.๑ เจ้าหน้าที่ IT ผู้ใช้งาน และบุคคลภายนอก จะต้องติดบัตรแสดงตน/บัตรผู้ติดต่อ ตรงจุดที่สามารถเห็นได้ชัดเจนตลอดเวลาที่อยู่ภายในอาคารสถานที่

๓.๒.๒ เจ้าหน้าที่ IT ผู้ใช้งาน และบุคคลภายนอก ที่ประสงค์จะเข้ามาปฏิบัติงานที่ห้องควบคุมฯ ได้นั้น จะต้องมีเจ้าหน้าที่ตามข้อ ๓.๑ คนใดคนหนึ่งเป็นผู้พาเข้าห้องควบคุมฯ และต้องมีการลงบันทึกเวลาเข้าออก เหตุผลในการเข้าห้องควบคุมฯ ในสมุดบัญชีควบคุมการเข้าใช้งานห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๓.๒.๓ ในกรณีที่มีความจำเป็นเร่งด่วนหรือเหตุการณ์ฉุกเฉินอันอาจเป็นผลทำให้เกิดความเสียหายต่อทรัพย์สินของหน่วยงานจะอนุญาตให้เข้าไปในพื้นที่ควบคุมได้โดยได้รับความเห็นชอบจากฝ่าย IT

๓.๒.๔ ไม่อนุญาตให้นำอาหารหรือเครื่องดื่มเข้าไปในเขตพื้นที่ควบคุม

๓.๓ ผู้ตรวจสอบการเข้าห้องควบคุมฯ มีแนวทางปฏิบัติ ดังนี้

๓.๓.๑ สังเกตพฤติกรรมการเข้าห้องควบคุมฯ ของ เจ้าหน้าที่ IT ผู้ใช้งาน และบุคคลภายนอก

๓.๓.๒ มีการตักเตือนเจ้าหน้าที่เมื่อไม่ปฏิบัติตามระเบียบและกฎเกณฑ์ของห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่าย

๓.๓.๓ รายงานต่อผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศเมื่อเจ้าหน้าที่คนใดคนหนึ่งทำผิดระเบียบและกฎเกณฑ์ของห้องควบคุมคอมพิวเตอร์แม่ข่ายและระบบเครือข่ายเป็นประจำเพื่อการตัดสิทธิในการเข้าห้องควบคุม

ส่วนที่ ๔

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศภายในสำนักเลขาธิการคณะรัฐมนตรี

(Access Control)

๑. วัตถุประสงค์

เพื่อให้สำนักเลขาธิการคณะรัฐมนตรีมีแนวทางปฏิบัติหรือมาตรการในการควบคุมการเข้าถึงระบบสารสนเทศ ระบบคอมพิวเตอร์ และระบบเครือข่ายของสำนักเลขาธิการคณะรัฐมนตรี ให้บุคคลที่ได้รับอนุญาตเข้าถึงระบบและอุปกรณ์เพื่อใช้งานได้อย่างมั่นคงปลอดภัยตามสิทธิที่ได้รับ และควบคุมบุคคลที่ไม่ได้รับอนุญาตหรือผู้บุกรุกมิให้สร้างความเสียหายแก่ข้อมูล หรือการทำงานของระบบเทคโนโลยีสารสนเทศและการสื่อสารให้หยุดชะงัก และสามารถตรวจสอบติดตามพิสูจน์ตัวบุคคลที่เข้าใช้งานระบบและอุปกรณ์ของสำนักเลขาธิการคณะรัฐมนตรีได้อย่างถูกต้อง

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ เป็นผู้ดูแลระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ยกเว้นระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๒ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี เป็นผู้ดูแลระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๓ นางสาวปาจรีย์ แจ่มจักษุ เป็นผู้ดูแลระบบคอมพิวเตอร์แม่ข่าย

๒.๔ นางสาวนงนุช จงเจริญสมบัติ เป็นผู้ดูแลระบบเครือข่าย

๒.๕ นางสาวชุลีกร สุขโทน เป็นผู้ดูแลระบบป้องกันไวรัสคอมพิวเตอร์

๓. การบริหารจัดการการเข้าถึงระบบและอุปกรณ์ของผู้ใช้งาน มีแนวทางปฏิบัติ ดังนี้

๓.๑ การลงทะเบียนผู้ใช้งาน (User Registration) ของสำนักเลขาธิการคณะรัฐมนตรี มีขั้นตอนการปฏิบัติสำหรับลงทะเบียนผู้ใช้งาน ดังนี้

- ผู้ดูแลระบบสารสนเทศจะกำหนดบัญชีผู้ใช้งานเป็นรายบุคคลและจำแนกตามสำนัก/กองของสำนักเลขาธิการคณะรัฐมนตรี และกำหนดสิทธิสำหรับเจ้าหน้าที่ใหม่ตามความจำเป็นใช้งาน ได้แก่ ระบบอินทราเน็ต ชุดโปรแกรมสำนักงาน และการใช้งานระบบจดหมายอิเล็กทรอนิกส์ (E-mail)
- การเพิ่มบัญชีผู้ใช้งาน จะกระทำได้เมื่อได้รับแจ้งขอบัญชีผู้ใช้งานจากผู้อำนวยการสำนัก/กอง และการแจ้งชื่อผู้ใช้งานและรหัสผ่านจะต้องกระทำด้วยความระมัดระวัง โดยส่งเป็นจดหมายปิดผนึกถึงผู้ใช้งานโดยตรง
- การยกเลิกสิทธิการใช้งานเมื่อมีการลาออก โอนย้ายงาน และกรณีอื่นๆ จะต้องดำเนินการยกเลิกสิทธิออกจากทะเบียนให้แล้วเสร็จภายใน ๓ วันทำการ

๓.๒ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) มีแนวทางปฏิบัติ ดังนี้

- ผู้ดูแลระบบสารสนเทศจะกำหนดสิทธิของเจ้าหน้าที่ในการเข้าถึงระบบสารสนเทศแต่ละระบบ โดยกำหนดบัญชีผู้ใช้เป็นรายบุคคล และจำแนกตามสำนัก/กอง ของสำนักเลขาธิการคณะรัฐมนตรี

และกำหนดสิทธิแยกตามหน้าที่ความรับผิดชอบที่ได้รับมอบหมายจากผู้อำนวยการสำนัก/กอง ตามที่กำหนดไว้ในเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบและรหัสผ่าน”*

- กำหนดให้มีการเก็บบันทึกรายละเอียดการสืบค้น/แก้ไขข้อมูลของผู้ใช้งานทุกคนที่มีการใช้งานระบบงานที่สำคัญ โดยรายละเอียดที่จัดเก็บ ได้แก่ ชื่อผู้ใช้งาน วันเวลาที่เข้าใช้งาน ผลการใช้งาน
- มีการทบทวนสิทธิการเข้าถึงระบบงานของผู้ใช้งานตามรอบระยะเวลา ๑ ปี ผู้ดูแลระบบต้องทบทวนบัญชีผู้ใช้งานและสิทธิ์การใช้งานอย่างสม่ำเสมออย่างน้อยปีละ ๑ ครั้ง เพื่อป้องกันการเข้าถึงระบบโดยไม่ได้รับอนุญาต โดยพิมพ์รายชื่อของผู้ที่ยังมีสิทธิ์ในระบบแยกตามหน่วยงานเพื่อจัดส่งรายชื่อนั้นให้กับผู้บังคับบัญชาของหน่วยงานพิจารณาทบทวนรายชื่อและสิทธิ์การเข้าใช้งานที่ถูกต้อง และส่งให้สำนักบริหารงานสารสนเทศดำเนินการแก้ไขข้อมูลสิทธิ์ต่าง ๆ ให้ถูกต้องตามที่ได้รับแจ้งจากหน่วยงาน
- มีการจำกัดจำนวนครั้งในการพยายามเข้าสู่ระบบงานไม่เกิน ๓ ครั้ง
- มีการยกเลิกบัญชีผู้ใช้งานของผู้ไม่ระบุนาม เช่น Guest เว้นแต่กรณีมีความจำเป็นต้องมีบัญชีผู้ใช้งานของผู้ไม่ระบุนาม จึงจะกำหนดสิทธิเท่าที่จำเป็นต่อการใช้งาน

๓.๓ การบริหารจัดการรหัสผ่านสำหรับผู้ใช้งาน มีแนวทางปฏิบัติ ดังนี้

- ผู้ดูแลระบบสารสนเทศต้องตั้งรหัสผ่านอย่างรัดกุมให้แก่ผู้ใช้งาน (รหัสผ่านชั่วคราว)
- ผู้ดูแลระบบสารสนเทศต้องแจ้งให้ผู้ใช้งานทราบถึงความสำคัญของการเปลี่ยนรหัสผ่านและทราบถึงวิธีการตั้งรหัสผ่านที่รัดกุม ดังนี้
    - การตั้งรหัสผ่าน ต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร มีการผสมกันระหว่างตัวอักษรตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวเลข และตัวอักขระพิเศษ และเป็นรหัสผ่านที่ยากต่อการเดาของผู้อื่น ไม่ควรตั้งรหัสผ่านให้เหมือนชื่อผู้ใช้งานหรือนามสกุล หรือข้อมูลอื่นที่เกี่ยวข้องกับผู้ใช้งาน เช่น วันเกิด หมายเลขโทรศัพท์ เป็นต้น และไม่ควรตั้งรหัสผ่านโดยใช้คำที่อยู่ในพจนานุกรม
    - ให้ผู้ดูแลระบบเปลี่ยนรหัสผ่านทุกๆ ๓ เดือน และให้ผู้ใช้งานทั่วไปเปลี่ยนรหัสผ่านทุก ๖ เดือน

๓.๔ การเก็บรักษาบัญชีผู้ใช้และการใช้งานรหัสผ่าน

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

๓.๕ การป้องกันอุปกรณ์ในขณะที่ไม่มีผู้ใช้งาน (Clear Desk) มีแนวทางปฏิบัติ ดังนี้

- ผู้ใช้งานต้องออกจากระบบสารสนเทศทันที เมื่อว่างเว้นจากการใช้งานหรือเสร็จสิ้นการใช้งาน

- สำหรับระบบงานที่สำคัญผู้ดูแลระบบสารสนเทศต้องป้องกันผู้อื่นเข้าใช้งานระบบงานที่สำคัญ โดยตั้งระบบให้ล็อกหน้าจอซึ่งผู้อื่นต้องกำหนดรหัสผ่านให้ถูกต้องจึงจะสามารถเปิดหน้าจอนั้นได้

๓.๖ การควบคุมการไม่ทิ้งทรัพย์สินสารสนเทศสำคัญไว้ในที่ที่ไม่ปลอดภัย (Clear Server Policy) มีแนวทางปฏิบัติ ดังนี้

- สำนักเลขาธิการคณะรัฐมนตรีกำหนดนโยบายให้ทุกหน่วยงานขององค์กรปฏิบัติตามนโยบาย ๕ ส.
- กำหนดให้เจ้าหน้าที่จัดเก็บข้อมูลสำคัญ และข้อมูลที่มีชั้นความลับไว้ในตู้หรือลิ้นชักที่ล็อกกุญแจหรือที่ที่ปลอดภัยภายหลังจากใช้งานเสร็จ
- ผู้ใช้งานต้องควบคุมไม่ให้ทรัพย์สินสารสนเทศ เช่น เอกสาร สื่อคอมพิวเตอร์ อุปกรณ์คอมพิวเตอร์ หรือสารสนเทศ อยู่ในภาวะเสี่ยงต่อการเข้าถึงของผู้ไม่มีสิทธิ และต้องจัดเก็บไว้ในที่ที่ปลอดภัยในเวลาที่ไม่มีผู้ดูแล

๓.๗ การใช้งานเครื่องคอมพิวเตอร์ เครื่องคอมพิวเตอร์ที่หน่วยงานอนุญาตให้ใช้งานเป็นสินทรัพย์ของหน่วยงานเพื่อใช้ในราชการ ไม่อนุญาตให้ผู้ใช้งานทำการติดตั้งและแก้ไขเปลี่ยนแปลงโปรแกรมในเครื่องคอมพิวเตอร์ส่วนบุคคลของหน่วยงาน การเคลื่อนย้ายหรือส่งคืนคอมพิวเตอร์เพื่อตรวจซ่อมจะต้องแจ้งให้สำนักบริหารงานสารสนเทศทราบเพื่อดำเนินการซ่อมบำรุงหรือจัดหาอุปกรณ์มาทดแทน รวมทั้ง บันทึกการรับคืนและส่งมอบให้กับบุคคลที่ได้รับอุปกรณ์ไว้ใช้งานให้เป็นปัจจุบัน

๓.๘ หน้าที่ความรับผิดชอบของผู้ใช้งาน (User Responsibilities)

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

๓.๙ การนำสินทรัพย์ของหน่วยงานออกนอกหน่วยงาน (Removal of Property) ให้มีการขออนุญาตก่อนนำอุปกรณ์หรือทรัพย์สินนั้นออกไปใช้งานนอกหน่วยงาน ให้ผู้อำนวยการสำนัก/กองกำหนดผู้รับผิดชอบในการเคลื่อนย้ายหรือนำอุปกรณ์ออกนอกหน่วยงาน และตรวจสอบสภาพอุปกรณ์เมื่อมีการส่งคืน บันทึกข้อมูลการนำอุปกรณ์ของหน่วยงานออกไปใช้งานนอกหน่วยงานเพื่อเป็นหลักฐานป้องกันการสูญหาย รวมทั้งบันทึกข้อมูลเพิ่มเติมเมื่อนำอุปกรณ์กลับสู่หน่วยงาน

เจ้าหน้าที่ผู้ใช้งานอุปกรณ์ทุกคนมีความรับผิดชอบดูแลอุปกรณ์หรือทรัพย์สินเสมือนเป็นทรัพย์สินของตน

๓.๑๐ การกำจัดอุปกรณ์หรือนำอุปกรณ์กลับไปใช้งานอีกครั้ง (Secure Disposal or re-use of Equipment) ให้ทำลายข้อมูลสำคัญในอุปกรณ์ก่อนที่จะกำจัดอุปกรณ์ดังกล่าวมีวิธีการชำระล้างข้อมูลที่มีความสำคัญตามมาตรฐานสากลในอุปกรณ์สำหรับจัดเก็บข้อมูลก่อนที่จะอนุญาตให้ผู้อื่นนำอุปกรณ์ไปใช้งานต่อ เพื่อป้องกันไม่ให้เข้าถึงข้อมูลสำคัญนั้นได้

เอกสารประกอบปรากฏตามภาคผนวก ๓(๕) การอนุญาต – การกำหนดสิทธิและการบริหารจัดการการเข้าถึงสารสนเทศ

๔. การบริหารจัดการการเข้าถึงข้อมูลตามระดับชั้นความลับ มีแนวทางปฏิบัติ ดังนี้

๔.๑ ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อการเข้าถึงระบบงานและใช้ในการพิสูจน์ตัวตน (Authentication) ของผู้ใช้ข้อมูลในแต่ละระบบข้อมูล (หรือประเภทข้อมูล) และแต่ละชั้นความลับของข้อมูล มีการใช้เมนูเพื่อควบคุมการเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ ของระบบงานที่สอดคล้องกับนโยบายควบคุมการเข้าถึงของสำนักเลขาธิการคณะรัฐมนตรี

๔.๒ มีการลงทะเบียนผู้ใช้งานเพื่อควบคุมสิทธิการเข้าถึงข้อมูลและฟังก์ชั่นต่างๆ ของระบบงาน ได้แก่ สิทธิที่สามารถอ่านข้อมูล แก้ไขข้อมูล ลบข้อมูล หรือสั่งให้โปรแกรมประมวลผลข้อมูล

๔.๓ มีการจำกัดข้อมูลที่มีความสำคัญ เพื่อให้มีเฉพาะข้อมูลที่เกี่ยวข้อง และจำเป็นสำหรับนำไปใช้งาน

๔.๔ มีการติดตั้งระบบงานที่มีความสำคัญสูงแยกไว้ในเครื่องคอมพิวเตอร์ต่างหาก และติดตั้งบนเครือข่ายที่แยกต่างหากจากเครือข่ายอื่น

๔.๕ มีการกำหนดช่องทางการเข้าถึงข้อมูลที่มีชั้นความลับผ่านระบบอินทราเน็ตที่เป็นระบบปิดของสำนักเลขาธิการคณะรัฐมนตรีตลอดเวลา ๒๔ ชั่วโมง และกำหนดช่องทางการเข้าถึงข้อมูลที่ไม่มีชั้นความลับผ่านระบบอินเทอร์เน็ตไว้ตลอดเวลา ๒๔ ชั่วโมง

๔.๖ มีระบบการเข้ารหัสข้อมูลที่มีความสำคัญหรือมีชั้นความลับโดยอัตโนมัติหรือการกำหนดสิทธิการเข้าถึงข้อมูลของผู้ใช้ในการรับส่งข้อมูลระหว่างใช้งานกับเครื่องแม่ข่ายระบบฐานข้อมูล

เอกสารประกอบปรากฏตามภาคผนวก ๓(๕) การอนุญาต – การกำหนดสิทธิและการบริหารจัดการการเข้าถึงสารสนเทศ และ ๓(๖) คู่มือปฏิบัติงานการจัดเก็บข้อมูลมติคณะรัฐมนตรีที่มีชั้นความลับ

๕. การบริหารจัดการการเข้าถึงระบบเครือข่ายและระบบเครือข่ายไร้สาย มีแนวทางปฏิบัติ ดังนี้

๕.๑ มีการออกแบบระบบเครือข่ายโดยจำแนกตามกลุ่มของบริการระบบเทคโนโลยีสารสนเทศ กลุ่มของผู้ใช้งาน และกลุ่มของระบบสารสนเทศ ด้วยการกำหนด VLAN (Virtual LAN) เช่น โซนคอมพิวเตอร์ลูกข่าย โซนคอมพิวเตอร์แม่ข่าย โซนระบบสารสนเทศต่างๆ โซนระบบเครือข่ายไร้สาย (Wireless LAN) และโซนภายนอกหน่วยงาน เป็นต้น เพื่อให้การควบคุมหรือบริหารจัดการระบบ และการป้องกันการบุกรุกทำได้อย่างเป็นระบบและมีประสิทธิภาพ

ตลอดจนเพื่อให้เกิดความปลอดภัย และเป็นการจำกัดการเข้าใช้ทรัพยากรของคอมพิวเตอร์ในเครือข่ายที่อยู่ต่างกลุ่มกัน

๕.๒ มีการระบุอุปกรณ์บนเครือข่ายด้วยการกำหนด IP Address และการติดป้าย label ที่อุปกรณ์เครือข่าย อาทิ สายสัญญาณเครือข่าย (สาย LAN) ภายในตู้ RACK, สาย LAN จากตู้ RACK ไปยังเครื่องคอมพิวเตอร์ลูกข่าย (Client) ปลายทาง และติดที่กล่อง Outlet เป็นต้น ให้กับอุปกรณ์คอมพิวเตอร์ทุกชนิดที่อยู่ในเครือข่าย เพื่อใช้ในการบริหารจัดการเครือข่ายให้เป็นระบบ

๕.๓ มีการควบคุมการจัดเส้นทางบนเครือข่ายผ่านอุปกรณ์เราท์เตอร์ (Router) เพื่อให้การเชื่อมต่อเครื่องคอมพิวเตอร์และอุปกรณ์ ตลอดจนการไหลเวียนของข้อมูลและระบบสารสนเทศเป็นไปด้วยความถูกต้องและเป็นระบบ

๕.๔ มีการควบคุมการเข้าถึงระบบเครือข่ายที่มีการใช้งานร่วมกันภายในหน่วยงาน หรือการเชื่อมต่อระหว่างระบบเครือข่ายไร้สายกับระบบเครือข่ายภายในหน่วยงาน หรือการเชื่อมต่อเครือข่ายระหว่างหน่วยงาน โดยการควบคุมการเข้าถึงเครือข่ายผ่านระบบหรืออุปกรณ์ป้องกันการบุกรุกด้วยการใช้ไฟร์วอล (Firewall) หรือฮาร์ดแวร์อื่นๆ

๕.๕ มีการดูแลตรวจสอบช่องทางการสื่อสารของระบบเครือข่ายอยู่เสมอ และปิดช่องทางการสื่อสารของระบบเครือข่ายที่ไม่มีความจำเป็นในการใช้งาน

๕.๖ มีการควบคุมการเข้าถึงพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม และเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น บริการ telnet, ftp และ ping เป็นต้น

๕.๗ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายในลักษณะที่ผิดปกติ

๕.๘ มีการควบคุมการเข้าถึงระบบสารสนเทศด้วยการพิสูจน์ตัวตน (Authentication) ผ่านโดเมนคอนโทรลเลอร์ (AD : Active Directory) โดยเครื่องคอมพิวเตอร์ของผู้ใช้งานจะต้องมีการกำหนดชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) สำหรับเข้าใช้งานระบบสารสนเทศ และมีการพิสูจน์ตัวตนสำหรับผู้ใช้งานที่อยู่ภายนอกองค์กร ก่อนที่อนุญาตให้ผู้ใช้งานที่อยู่ภายนอกองค์กรสามารถเข้าใช้งานระบบเครือข่ายและระบบสารสนเทศขององค์กรได้

๕.๙ มีการจำกัดสิทธิ์การใช้งานเพื่อควบคุมผู้ใช้งานให้สามารถใช้ได้เฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๑๐ มีการติดตั้งระบบเครือข่ายไร้สาย (Wireless LAN) เพื่อให้บริการกับผู้ใช้งานที่นำเครื่องคอมพิวเตอร์แบบพกพา (Notebook) มาใช้ในการปฏิบัติงาน โดยผู้ที่มีความประสงค์ใช้งานระบบเครือข่ายไร้สายจะต้องประสานกับผู้ดูแลระบบเพื่อกำหนดค่า Parameter ที่เครื่องคอมพิวเตอร์ Notebook ให้สามารถเข้าใช้งานระบบเครือข่ายไร้สายได้

๕.๑๑ มีการควบคุมสัญญาณของอุปกรณ์กระจายสัญญาณ (Access Point) บริเวณโดยรอบห้องประชุมคณะรัฐมนตรีให้มีการกระจายสัญญาณออกนอกพื้นที่ใช้งานระบบเครือข่ายไร้สายน้อยที่สุด เพื่อป้องกันผู้ไม่ประสงค์ดีทำการลักลอบดักจับข้อมูลเกี่ยวกับการประชุมคณะรัฐมนตรี ตลอดจนมีการกำหนดช่วงเวลาในการให้บริการเครือข่ายไร้สายตามที่หน่วยงานกำหนด

๕.๑๒ มีการเปลี่ยนค่า SSID (Service Set Identifier) ที่ถูกกำหนดเป็นค่าโดยปริยาย (Default) มาจากผู้ผลิตทันทีที่นำอุปกรณ์กระจายสัญญาณ (Access Point) มาใช้งาน

๕.๑๓ มีการกำหนดค่า WEP (Wired Equivalent Privacy) หรือ WPA (Wi-Fi Protected Access) ในการเข้ารหัสข้อมูลระหว่าง Wireless LAN Client และอุปกรณ์กระจายสัญญาณ (Access Point)

๕.๑๔ มีการควบคุมการใช้งานเครือข่ายไร้สายด้วยการใช้ MAC Address (Media Access Control Address) ตลอดจนการ Login เข้าใช้งานด้วยชื่อผู้ใช้ (Username) และรหัสผ่าน (Password) ตามที่กำหนดไว้เท่านั้นจึงจะสามารถเข้าใช้ระบบเครือข่ายไร้สายได้

๕.๑๕ มีการควบคุมดูแลไม่ให้บุคคลหรือหน่วยงานภายนอกที่ไม่ได้รับอนุญาตเข้าใช้งานระบบเครือข่ายไร้สายในการเข้าสู่ระบบอินทราเน็ต (Intranet) และฐานข้อมูลภายในต่างๆ ของหน่วยงาน

๕.๑๖ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่าย และอุปกรณ์ต่างๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑๗ มีการกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่างๆ ของระบบเครือข่ายและอุปกรณ์ต่างๆ ที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และมีการทบทวนการกำหนดค่า Parameter ต่างๆ อย่างน้อยปีละครั้ง ทั้งนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๑๘ ไม่ใช้อำนาจหน้าที่ของผู้ดูแลระบบ (System Administrator) ในการเข้าถึงข้อมูลของผู้ใช้งานในระบบเครือข่าย ตลอดจนไม่กระทำการอื่นใดที่มีลักษณะเป็นการละเมิดสิทธิ์หรือข้อมูลส่วนบุคคลของผู้ใช้งาน โดยไม่มีเหตุผลอันสมควร

๕.๑๙ ห้ามเปิดเผยข้อมูลที่ได้มาจากการปฏิบัติหน้าที่ ซึ่งข้อมูลดังกล่าวเป็นข้อมูลที่ไม่พึงเปิดเผยให้บุคคลหนึ่งบุคคลใดทราบ โดยไม่มีเหตุอันสมควร

เอกสารประกอบปรากฏตามภาคผนวก ๓(๗) การควบคุมการเข้าถึงเครือข่าย

๖. การควบคุมการเข้าถึงระบบปฏิบัติการ มีแนวทางปฏิบัติ ดังนี้

๖.๑ กำหนดให้การเข้าสู่ระบบปฏิบัติการต้องมีการพิสูจน์ตัวตนของผู้ใช้งาน (Active Directory)

๖.๒ กำหนดให้มีการระบุและยืนยันตัวตนของผู้ใช้งาน โดยผู้ใช้งานต้องแสดงตัวตนด้วยชื่อผู้ใช้งาน (User name) และพิสูจน์ยืนยันตัวตนด้วยการใช้รหัสผ่าน (Password)

๖.๓ กำหนดให้มีการยุติการใช้งานระบบสารสนเทศ เมื่อว่างเว้นจากการใช้งานเป็นเวลา ๒๐ นาที

๖.๔ กำหนดให้ผู้ใช้งานทำการเปลี่ยนรหัสผ่านทุก ๆ ๓ เดือน

๖.๕ เมื่อผู้ใช้งานเปลี่ยนรหัสผ่านต้องมีความยาวไม่น้อยกว่า ๘ ตัวอักษร โดยอาจจะมีการผสมกันระหว่างตัวเลข ตัวอักษรที่เป็นตัวพิมพ์เล็กหรือตัวพิมพ์ใหญ่ ตัวอักขระพิเศษและสัญลักษณ์ต่างๆ

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

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

๖.๘ ผู้ใช้งานจะต้องเก็บรักษารหัสผ่าน (Password) สำหรับการใช้งานเครื่องคอมพิวเตอร์สำหรับการใช้งานเครื่องคอมพิวเตอร์และระบบเครือข่ายที่ได้มาโดยถือว่าเป็นความลับเฉพาะบุคคล และจะต้องไม่เปิดเผยหรือกระทำการใดให้ผู้อื่นทราบโดยไม่ได้รับอนุญาตจากผู้บังคับบัญชา

๖.๙ กรณีจำเป็นต้องนำข้อมูลจากเครื่องคอมพิวเตอร์แม่ข่ายออกไปทดสอบหรือดำเนินการใด ๆ ภายนอกหน่วยงาน ผู้ร้องขอจะต้องมีหนังสือรับรองจากผู้บังคับบัญชาระดับผู้บริหารองค์กร เพื่อรับรองการรักษาความลับข้อมูลของทางราชการต่อสำนักเลขาธิการคณะรัฐมนตรีทุกครั้ง

๖.๑๐ กำหนดให้มีการควบคุมการติดตั้งการใช้งานโปรแกรมอรรถประโยชน์ที่เกี่ยวข้องต่อการปฏิบัติงาน โดยผู้ใช้งานจะต้องอยู่ในระบบ Active Directory และได้รับมอบหมายจากผู้บังคับบัญชา โดยมีหนังสือขอใช้โปรแกรมมายังผู้ดูแลระบบเพื่อเปิดสิทธิในการติดตั้งโปรแกรมอรรถประโยชน์โดยเฉพาะ

๖.๑๑ กำหนดให้มีการบันทึกรายละเอียดการใช้งานโปรแกรมอรรถประโยชน์ของผู้ใช้งานทุกคน

๗. การควบคุมการเข้าถึงโปรแกรมประยุกต์ มีแนวทางปฏิบัติ ดังนี้

๗.๑ กำหนดให้สำนัก/กอง แจ้งรายชื่อผู้ใช้งานระบบสารสนเทศให้กับผู้ดูแลระบบ เพื่อดำเนินการติดตั้งโปรแกรมและกำหนดกลุ่ม/สิทธิในการเข้าถึงระบบสารสนเทศ

๗.๒ กำหนดให้สำนัก/กอง แจ้งยกเลิกรายชื่อผู้ใช้งานระบบสารสนเทศ เมื่อผู้ใช้งานมีการลาออกหรือโอนไปยังหน่วยงานอื่น

๗.๓ กำหนดให้มีการทบทวนสิทธิการเข้าถึงระบบสารสนเทศของผู้ใช้งานของสำนัก/กอง ทุก ๆ ปี

๗.๔ กำหนดให้มีการจัดเก็บซอร์สโค้ด ไลบรารี่ และเอกสารสำหรับซอร์ฟแวร์ของระบบงานไว้ในสถานที่ที่มีความมั่นคงปลอดภัย

๘. การบริหารจัดการการบันทึกและตรวจสอบ มีแนวทางปฏิบัติ ดังนี้

๘.๑ กำหนดให้มีการบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่าย บันทึกการปฏิบัติงานของผู้ใช้งาน (Application logs) และบันทึกรายละเอียดของระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบ บันทึกการพยายามเข้าสู่ระบบ บันทึกการใช้งาน Command line และ Firewall log เป็นต้น เพื่อประโยชน์ในการใช้ตรวจสอบและต้องเก็บบันทึกดังกล่าวไว้อย่างน้อย ๓ เดือน

๘.๒ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๘.๓ มีวิธีการป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่างๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘.๔ การเก็บรักษาข้อมูลจราจรทางคอมพิวเตอร์ (Log) ไว้ไม่น้อยกว่าเก้าสิบวันนับแต่วันที่ข้อมูลนั้นเข้าสู่ระบบคอมพิวเตอร์ ตาม พ.ร.บ. ว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. ๒๕๕๐ ข้อ ๒๖

๙. **การสร้างความมั่นคงปลอดภัยของระบบสารสนเทศด้านบุคลากรกรณีที่หน่วยงานจ้างบริษัท หรือบุคคลภายนอก** เข้ามาทำงานหรือให้บริการ หน่วยงานควรมีการตรวจสอบประวัติหรือคุณสมบัติให้เป็นไปตามกฎหมายระเบียบที่เกี่ยวข้อง และในข้อตกลงการว่าจ้างต้องครอบคลุมถึงการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ โดยให้ลงนามรับทราบนโยบายและขั้นตอนการปฏิบัติสำหรับการรักษาความมั่นคงปลอดภัยขององค์กร **และเมื่อสิ้นสุดการจ้างงาน ต้องให้คืนทรัพย์สินขององค์กรและถอดถอนสิทธิในการเข้าถึงสารสนเทศ**

ส่วนที่ ๕

การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก

(Third Party Access Control)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการควบคุมบุคคลในการเข้าถึงระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี การป้องกันการบุกรุกผ่านระบบเครือข่ายจากผู้บุกรุกหรือโปรแกรมระบบ (System Software) ชุดคำสั่งไม่พึงประสงค์ที่อาจจะสร้างความเสียหายแก่ระบบข้อมูลหรือการทำงานของระบบเทคโนโลยีสารสนเทศไม่สามารถทำงานได้ รวมถึงการตรวจสอบและพิสูจน์ตัวตนที่เข้าใช้งานระบบเทคโนโลยีสารสนเทศได้อย่างถูกต้อง

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี เป็นผู้ดูแลระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ เป็นผู้ดูแลระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ยกเว้นระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๓ นายประวิทย์ อมรฤทธิ์ และนางจินตนา งามภูมิ เป็นผู้ดูแลระบบคอมพิวเตอร์แม่ข่ายของระบบ CABNET

๒.๔ นางสาวนงนุช จงเจริญสมบัติ และนางจินตนา งามภูมิ เป็นผู้ดูแลระบบเครือข่ายของระบบ CABNET

๒.๕ นางจินตนา งามภูมิ และนายอุดมรัตน์ สุวรรณราช เป็นผู้ดูแลระบบคอมพิวเตอร์ของระบบ CABNET

๒.๖ นางจินตนา งามภูมิ และนางสาวนงนุช จงเจริญสมบัติ เป็นผู้ดูแลระบบป้องกันไวรัสคอมพิวเตอร์ของระบบ CABNET

๓. การควบคุมการเข้าถึงระบบเทคโนโลยีสารสนเทศ

๓.๑ สำนักเลขาธิการคณะรัฐมนตรีจะอนุญาตให้ผู้ใช้งานเข้าสู่ระบบเฉพาะในส่วนที่เกี่ยวข้อง เนื่องจากการให้สิทธิเกินความจำเป็นในการใช้งานจะนำไปสู่ความเสี่ยงในการใช้งานเกินอำนาจหน้าที่และความรับผิดชอบ ดังนั้น การกำหนดสิทธิในการเข้าถึงระบบงานจะต้องกำหนดตามความจำเป็นเท่านั้น

๓.๒ ผู้ที่จะเข้าใช้งานได้จะต้องมีเอกสารรับรองสิทธิการเข้าใช้งานระบบที่เกี่ยวข้องจากผู้บังคับบัญชาของหน่วยงานของผู้ใช้งานเท่านั้น

ทั้งนี้ สำนักเลขาธิการคณะรัฐมนตรีได้กำหนดแนวทางการเข้าถึงข้อมูลระเบียบวาระการประชุมคณะรัฐมนตรีในระบบ CABNET ซึ่งเป็นระบบที่เชื่อมต่อกับหน่วยงานต่างๆ ที่อยู่ภายนอกสำนักเลขาธิการคณะรัฐมนตรี

เอกสารประกอบปรากฏตามภาคผนวก ๓(๕) การอนุญาต – การกำหนดสิทธิและการบริหารจัดการการเข้าถึงสารสนเทศ

๔. การบริหารจัดการการเข้าถึงของผู้ใช้ มีแนวปฏิบัติ ดังนี้

๔.๑ สำนักเลขาธิการคณะรัฐมนตรีกำหนดให้มีการประเมินความเสี่ยงจากการเข้าถึงระบบเทคโนโลยีสารสนเทศจากหน่วยงานภายนอก และกำหนดมาตรการรองรับหรือแก้ไขที่เหมาะสมก่อนที่จะอนุญาตให้เข้าถึงระบบเทคโนโลยีสารสนเทศได้

๔.๒ การควบคุมการเข้าถึงของผู้ใช้งาน มีแนวทางปฏิบัติ ดังนี้

๔.๒.๑ การลงทะเบียนผู้ใช้งาน โดยกำหนดให้มีขั้นตอนปฏิบัติอย่างเป็นทางการ สำหรับการลงทะเบียนผู้ใช้งานเพื่อให้มีสิทธิต่าง ๆ ในการใช้งานตามสิทธิการเข้าใช้งานระบบ รวมทั้ง ขั้นตอนปฏิบัติสำหรับการยกเลิกสิทธิการใช้งาน เช่น การลาออกหรือไม่มีสิทธิของผู้ใช้งานต้องดำเนินการภายในระยะเวลาที่กำหนด การยืนยันสิทธิผู้ใช้งานของหน่วยงานต่าง ๆ เป็นระยะเพื่อการตรวจสอบสิทธิของผู้ใช้งาน เป็นต้น

๔.๒.๒ กำหนดสิทธิการใช้ระบบเทคโนโลยีสารสนเทศที่สำคัญ เช่น ระบบงาน (Application) การพิมพ์ข้อมูลจดหมายอิเล็กทรอนิกส์ (E-mail) เป็นต้น โดยต้องให้สิทธิเฉพาะการปฏิบัติงานเท่านั้น

๔.๒.๓ การบริหารจัดการบัญชีรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) ของผู้ใช้งาน

(๑) ผู้ดูแลระบบจะต้องมีการจัดเก็บลายนิ้วมือผู้ใช้งานแต่ละคน หรือกำหนดรายชื่อผู้ใช้งานและรหัสผ่านของผู้ใช้งานทั้งหมด ทั้งนี้เพื่อการกำหนดสิทธิการใช้งานซึ่งมีแนวทางปฏิบัติตามที่กำหนดไว้ในเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบ”*

(๒) การกำหนดการเปลี่ยนแปลงและการยกเลิกรหัสผ่านต้องปฏิบัติตามเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบ”*

(๓) กรณีมีความจำเป็นต้องให้สิทธิพิเศษกับผู้ใช้งาน ต้องมีการพิจารณาการควบคุมผู้ใช้ที่มีสิทธิพิเศษนั้นอย่างรัดกุมเพียงพอ โดยใช้ปัจจัยต่อไปนี้ประกอบการพิจารณา

(๓.๑) กำหนดหลักเกณฑ์การให้สิทธิพิเศษกับผู้ใช้งาน

(๓.๒) ต้องได้รับความเห็นชอบและอนุมัติจากผู้ดูแลระบบ

(๓.๓) มีการควบคุมการใช้งานหรือการตรวจสอบการใช้งาน

(๓.๔) มีการกำหนดระยะเวลาการใช้งานและพิจารณาระงับการใช้งาน เมื่อพ้นระยะเวลาดังกล่าว

(๓.๕) ควรมีการเปลี่ยนรหัสผ่าน เช่น ในกรณีที่มีความจำเป็นต้องใช้งานเป็นระยะเวลานานก็ควรเปลี่ยนรหัสผ่านทุก ๓ เดือน เป็นต้น

๔.๒.๔ การบริหารจัดการการเข้าถึงข้อมูลตามประเภทข้อมูล ระดับชั้นความลับ เวลาที่เข้าถึง และช่องทางการเข้าถึง

(๑) ผู้ดูแลระบบต้องกำหนดชั้นความลับของข้อมูล วิธีปฏิบัติในการจัดเก็บข้อมูลและวิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภท ชั้นความลับทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน รวมถึงวิธีการทำลายข้อมูลแต่ละประเภทชั้นความลับ

(๒) สำนักเลขาธิการคณะรัฐมนตรีกำหนดให้มีการสอบทานหรือทบทวนความเหมาะสมของสิทธิในการเข้าถึงข้อมูลของผู้ใช้งาน (Review of User Access Rights) อย่างน้อยปีละ ๑ ครั้ง เพื่อให้มั่นใจได้ว่าสิทธิต่าง ๆ ที่ให้ไว้ยังคงมีความเหมาะสม

(๓) วิธีปฏิบัติในการควบคุมการเข้าถึงข้อมูลแต่ละประเภทชั้นความลับ ทั้งการเข้าถึงโดยตรงและการเข้าถึงผ่านระบบงาน ผู้ดูแลระบบต้องกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อใช้ในการพิสูจน์ตัวตน (Authentication) ของผู้ใช้ข้อมูลในแต่ละชั้นความลับของข้อมูล

(๔) การรับส่งข้อมูลสำคัญผ่านเครือข่ายสาธารณะ จะมีการเข้ารหัส (Encryption) ที่เป็นมาตรฐานสากล

(๕) มีการกำหนดให้เปลี่ยนรหัสผ่านตามระยะเวลาที่กำหนดของระดับความสำคัญของข้อมูลตามที่ระบุไว้ในเอกสาร *“การบริหารจัดการสิทธิการใช้งานระบบ”*

(๖) มีมาตรการรักษาความมั่นคงปลอดภัยของข้อมูลในกรณีที่นำเครื่องคอมพิวเตอร์ของสำนักเลขาธิการคณะรัฐมนตรีใช้ในกิจการอื่น ๆ เช่น ส่งเครื่องคอมพิวเตอร์ไปตรวจซ่อม ควรสำรองและลบข้อมูลที่เก็บอยู่ในสื่อบันทึกก่อน เป็นต้น

เอกสารประกอบปรากฏตามภาคผนวก ๓(๕) การอนุญาต – การกำหนดสิทธิและการบริหารจัดการการเข้าถึงสารสนเทศ

๕. การบริหารจัดการการเข้าถึงระบบเครือข่าย มีแนวทางปฏิบัติ ดังนี้

๕.๑ ผู้ดูแลระบบต้องมีการออกแบบระบบเครือข่ายตามกลุ่มผู้ใช้งานระบบเทคโนโลยีสารสนเทศ ทั้งนี้ เพื่อทำให้การควบคุมและป้องกันการบุกรุกได้อย่างเป็นระบบ

๕.๒ ผู้ดูแลระบบต้องมีวิธีการจำกัดสิทธิการใช้งานเพื่อควบคุมผู้ใช้ให้สามารถใช้งานเฉพาะเครือข่ายที่ได้รับอนุญาตเท่านั้น

๕.๓ ผู้ดูแลระบบควรมีวิธีการจำกัดเส้นทางการเข้าถึงเครือข่ายที่มีการใช้งานร่วมกัน

๕.๔ ผู้ดูแลระบบควรจัดให้มีวิธีเพื่อจำกัดการใช้เส้นทางบนเครือข่าย (Enforced Path) จากเครื่องคอมพิวเตอร์ลูกข่ายไปยังเครื่องคอมพิวเตอร์แม่ข่าย เพื่อการจำกัดเส้นทางการใช้งานของผู้ใช้

๕.๕ มีการกำหนดบุคคลที่รับผิดชอบในการกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ต่าง ๆ ของระบบเครือข่ายที่เชื่อมต่อกับระบบเครือข่ายอย่างชัดเจน และควรมีการทบทวนการกำหนดค่า Parameter ต่าง ๆ อย่างน้อยปีละ ๑ ครั้ง นอกจากนี้ การกำหนด แก้ไข หรือเปลี่ยนแปลงค่า Parameter ควรแจ้งบุคคลที่เกี่ยวข้องให้รับทราบทุกครั้ง

๕.๖ ระบบเครือข่ายทั้งหมดที่มีการเชื่อมต่อไปยังระบบเครือข่ายอื่น ๆ ต้องเชื่อมต่อผ่านอุปกรณ์ป้องกันการบุกรุก หรือโปรแกรมในการทำ Packet filtering เช่น การใช้ไฟร์วอลล์ (Firewall) หรือฮาร์ดแวร์อื่น ๆ รวมทั้ง ต้องมีความสามารถในการตรวจจับมัลแวร์ (Malware) ได้

๕.๗ มีการติดตั้งระบบตรวจจับการบุกรุก (IPS/IDS) เพื่อตรวจสอบการใช้งานของบุคคลที่เข้าใช้งานระบบเครือข่ายของสำนักเลขาธิการคณะรัฐมนตรีในลักษณะที่ผิดปกติผ่านระบบเครือข่าย โดยมีการตรวจสอบการบุกรุกผ่านระบบเครือข่าย การใช้งานในลักษณะที่ผิดปกติ และการแก้ไขเปลี่ยนแปลงระบบเครือข่ายโดยบุคคลที่ไม่มีอำนาจหน้าที่ที่เกี่ยวข้อง

๕.๘ มีระบบอุปกรณ์จัดการ Network Policy ที่สามารถควบคุมการเชื่อมต่อระหว่างเครื่องลูกข่ายของแต่ละหน่วยงานและเครื่องแม่ข่ายในระบบของสำนักเลขาธิการคณะรัฐมนตรีให้เป็นไปตามข้อกำหนด และการเข้าสู่ระบบงานผ่านระบบเครือข่ายจะต้องมีการพิสูจน์ตัวตน (Authentication) เพื่อตรวจสอบผู้ใช้งานที่ถูกต้อง

๕.๙ IP Address ภายในของระบบเครือข่ายสำนักเลขาธิการคณะรัฐมนตรีต้องมีการป้องกันไม่ให้หน่วยงานภายนอกที่เชื่อมต่อสามารถมองเห็นได้ รวมทั้งมีการจัดการเพื่อเป็นการป้องกันไม่ให้บุคคลภายนอกสามารถรู้ข้อมูลเกี่ยวกับโครงสร้างของระบบเครือข่ายและส่วนประกอบได้โดยง่าย

๕.๑๐ ต้องจัดทำแผนผังระบบเครือข่าย (Network Diagram) ซึ่งมีรายละเอียดเกี่ยวกับขอบเขตของเครือข่าย และอุปกรณ์ต่าง ๆ พร้อมทั้งปรับปรุงให้เป็นปัจจุบันอยู่เสมอ

๕.๑๑ การใช้เครื่องมือต่าง ๆ (Tools) เพื่อการตรวจสอบระบบเครือข่ายควรได้รับการอนุมัติจากผู้ดูแลระบบและจำกัดการใช้งานเฉพาะเท่าที่จำเป็น

๕.๑๒ การติดตั้งและการเชื่อมต่ออุปกรณ์เครือข่ายจะต้องดำเนินการโดยเจ้าหน้าที่ของสำนักเลขาธิการคณะรัฐมนตรีเท่านั้น

๖. การบริหารจัดการระบบคอมพิวเตอร์แม่ข่าย มีแนวทางปฏิบัติ ดังนี้

๖.๑ มีระบบคอมพิวเตอร์แม่ข่าย เพื่อกรณีฉุกเฉินไม่สามารถใช้งานเครื่องคอมพิวเตอร์แม่ข่ายหลักได้ โดยกำหนดแนวทางหรือวิธีการอัพเดทระบบข้อมูลของระบบให้มีความถูกต้อง ทันสมัยเหมือนกัน และการทดสอบระบบในกรณีฉุกเฉินอย่างน้อยปีละ ๑ ครั้ง

๖.๒ มีขั้นตอนหรือวิธีปฏิบัติในการตรวจสอบระบบคอมพิวเตอร์แม่ข่ายและในกรณีที่พบว่า มีการใช้งานหรือเปลี่ยนแปลงค่าในลักษณะผิดปกติจะต้องดำเนินการแก้ไข รวมทั้งจัดทำรายงานด้วย

๖.๓ เปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น เช่น Telnet, Ftp และ ping เป็นต้น ทั้งนี้ หากบริการที่จำเป็นต้องใช้มีความเสี่ยงต่อระบบรักษาความปลอดภัยแล้วต้องมีมาตรการเพิ่มเติมด้วย

๖.๔ มีการติดตั้งอัพเดทระบบซอฟต์แวร์ให้เป็นปัจจุบัน เพื่ออุดช่องโหว่ต่าง ๆ ของโปรแกรมระบบอย่างสม่ำเสมอ

๖.๕ มีการจำกัดระยะเวลาเชื่อมต่อระบบสารสนเทศที่มีความสำคัญสูงเพื่อให้มีความมั่นคงปลอดภัยยิ่งขึ้น

๖.๖ มีการทดสอบโปรแกรมระบบเกี่ยวกับการรักษาความปลอดภัย และประสิทธิภาพการใช้งานโดยทั่วไป ก่อนติดตั้งและหลังจากการแก้ไข หรือบำรุงรักษา

๖.๗ การติดตั้งและการเชื่อมต่อระบบคอมพิวเตอร์แม่ข่ายจะดำเนินการโดยเจ้าหน้าที่ของสำนักเลขาธิการคณะรัฐมนตรีเท่านั้น

๗. การบริหารจัดการการบันทึกและการตรวจสอบ มีแนวทางปฏิบัติ ดังนี้

๗.๑ ต้องกำหนดให้การบันทึกการทำงานของระบบคอมพิวเตอร์แม่ข่ายและเครือข่าย บันทึกการปฏิบัติงานของผู้ใช้ระบบงาน (Application log) และบันทึกระบบป้องกันการบุกรุก เช่น บันทึกการเข้าออกระบบของผู้ใช้งาน (Users Access Log) และ Firewall Log เป็นต้น ทั้งนี้ เพื่อประโยชน์ในการใช้ตรวจสอบ และต้องเก็บบันทึกดังกล่าวไว้ระยะหนึ่ง

๗.๒ มีการตรวจสอบบันทึกการปฏิบัติงานของผู้ใช้งานอย่างสม่ำเสมอ

๗.๓ ต้องมีวิธีป้องกันการแก้ไขเปลี่ยนแปลงบันทึกต่าง ๆ และจำกัดสิทธิการเข้าถึงบันทึกเหล่านั้นให้เฉพาะบุคคลที่เกี่ยวข้องเท่านั้น

๘. การควบคุมการเข้าใช้งานระบบจากภายนอกสำนักเลขาธิการคณะรัฐมนตรี มีแนวทางปฏิบัติ ดังนี้

๘.๑ การเข้าสู่ระบบระยะไกล (Remote Access) สู่ระบบเครือข่ายของสำนักเลขาธิการคณะรัฐมนตรี มีการควบคุมบุคคลที่จะเข้าสู่ระบบขององค์กรจากระยะไกลโดยผู้ที่มีความประสงค์จะใช้งานต้องขออนุมัติจาก ผอ.สบส. ก่อน จากนั้นผู้ดูแลระบบสารสนเทศจะกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ให้กับผู้ใช้งานที่ขออนุมัติเท่านั้น โดยจะกำหนดสิทธิให้ใช้งานในกรณีที่ไม่สามารถปฏิบัติงานเร่งด่วนและมีความสำคัญที่ต้องรีบดำเนินการและจะยกเลิกสิทธิการใช้งานทันทีเมื่อการปฏิบัติงานดังกล่าวแล้วเสร็จ

๘.๒ การเข้าใช้งานระบบงานจากภายนอกสำนักเลขาธิการคณะรัฐมนตรี ในกรณีต้องปฏิบัติงานจากภายนอก เช่น การประชุมคณะรัฐมนตรีนอกสถานที่ มีการเข้าสู่ระบบด้วยเทคโนโลยี VPN โดยมีการกำหนดชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ให้กับผู้ใช้งานที่มีหน้าที่เกี่ยวข้องเท่านั้น

๘.๓ การให้สิทธิในการเข้าสู่ระบบจากระยะไกล ผู้ใช้ต้องแสดงหลักฐานระบุเหตุผลหรือความจำเป็นในการดำเนินงานอย่างเพียงพอ และต้องได้รับอนุมัติจากผู้อำนวยการสำนักบริหารงานสารสนเทศอย่างเป็นทางการ

๘.๔ มีการควบคุมพอร์ตที่ใช้ในการเข้าสู่ระบบอย่างรัดกุม โดยการใช้ Firewall หรือฮาร์ดแวร์อื่น และเปิดใช้บริการ (Service) เท่าที่จำเป็นเท่านั้น

๘.๕ การอนุญาตให้ผู้ใช้เข้าสู่ระบบข้อมูลจากระยะไกลต้องอยู่บนพื้นฐานของความจำเป็นเท่านั้น ช่องทางดังกล่าวจะถูกตัดการเชื่อมต่อเมื่อไม่ได้ใช้งานแล้วทันที

๙. การพิสูจน์ตัวตนผู้ใช้งานจากภายนอก มีแนวทางปฏิบัติ ดังนี้

๙.๑ มีการกำหนดรายชื่อผู้ใช้งาน (User Account) และรหัสผ่าน (Password) เพื่อการเข้าถึงระบบงานและใช้ในการพิสูจน์ตัวตน (Authentication) ของผู้ใช้ข้อมูลในแต่ละระบบข้อมูล (หรือประเภทข้อมูล) และแต่ละชั้นความลับของข้อมูล

๙.๒ ผู้ใช้งานระบบทุกคนจะต้องผ่านการตรวจสอบเอกลักษณ์บุคคลทุกครั้ง

(๑) ผู้ใช้งานระบบทุกคนทั้งที่อยู่ภายในและภายนอกหน่วยงาน จะได้รับการจัดเก็บลายนิ้วมือเพื่อใช้แทนการพิสูจน์ตัวตนด้วยชื่อผู้ใช้งานก่อนการเข้าใช้งานระบบ

(๒) ผู้ใช้งานระบบทุกคนเมื่อจะเข้าใช้งานระบบต้องผ่านการพิสูจน์ตัวตนจากระบบโดยการสแกนลายนิ้วมือผ่านอุปกรณ์สแกนลายนิ้วมือ (finger print reader) โดยระบบจะตรวจสอบกับลายนิ้วมือที่ได้จัดเก็บไว้ในเครื่องแม่ข่ายเพื่อการเข้าถึงข้อมูลต่างๆ

เอกสารประกอบปรากฏตามภาคผนวก ๓(๘) การยืนยันตัวบุคคลสำหรับผู้ใช้ที่อยู่ภายนอกองค์กร

ส่วนที่ ๖
การใช้งานอินเทอร์เน็ต
(Use of the Internet)

๑. วัตถุประสงค์

เพื่อให้ผู้ใช้รับทราบกฎเกณฑ์ แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ตอย่างปลอดภัย และเป็นการป้องกันไม่ให้ละเมิดพระราชบัญญัติว่าด้วยการกระทำผิดเกี่ยวกับคอมพิวเตอร์ เช่น การส่งข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดที่อยู่ในระบบคอมพิวเตอร์แก่บุคคลอื่นอันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข ทำให้ระบบคอมพิวเตอร์ของสำนักเลขาธิการคณะรัฐมนตรีถูกระงับ ชะลอ ขัดขวางหรือถูกรบกวนจนไม่สามารถทำงานได้ตามปกติ

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศเห็นชอบการเปิด-ปิดการให้บริการอินเทอร์เน็ตบนเครือข่ายของสำนักเลขาธิการคณะรัฐมนตรี ตลอดจนการจำแนกโซนเครือข่ายของกลุ่มผู้มีสิทธิและไม่มีสิทธิใช้งานอินเทอร์เน็ต

๒.๒	นางสาวปาจรีย์ แจ่มจักษุ	เป็นผู้ดูแลระบบรักษาความปลอดภัย
๒.๓	นางสาวชุลีกร สุขโทน	เป็นผู้ดูแลระบบป้องกันไวรัสคอมพิวเตอร์
๒.๔	นางสาวนงนุช จงเจริญสมบัติ	เป็นผู้ดูแลระบบเครือข่าย
๒.๕	นางสาวชุลีกร สุขโทน	เป็นผู้ดูแลระบบจดหมายอิเล็กทรอนิกส์

๓. แนวทางปฏิบัติในการใช้งานอินเทอร์เน็ต

๓.๑ การเชื่อมต่อคอมพิวเตอร์เพื่อเข้าใช้งานอินเทอร์เน็ต ต้องเชื่อมต่อผ่านระบบรักษาความปลอดภัยที่สำนักเลขาธิการคณะรัฐมนตรีจัดสรรไว้เท่านั้น

๓.๒ เครื่องคอมพิวเตอร์ส่วนบุคคลและเครื่องคอมพิวเตอร์แบบพกพา ต้องมีการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ที่มีการ update pattern ไวรัสคอมพิวเตอร์ให้ทันสมัยอยู่ตลอดเวลา หากตรวจสอบพบว่ายังไม่ได้ติดตั้งให้แจ้งสำนักบริหารงานสารสนเทศเพื่อทำการติดตั้งโปรแกรมป้องกันไวรัสคอมพิวเตอร์ก่อนทำการเชื่อมต่ออินเทอร์เน็ต

๓.๓ ผู้ใช้ต้องไม่ใช้เครือข่ายอินเทอร์เน็ตของสำนักเลขาธิการคณะรัฐมนตรี ในการเผยแพร่หรือใช้งานโดยมีวัตถุประสงค์ดังต่อไปนี้

๓.๓.๑ เพื่อก่อให้เกิดความเสียหายแก่สำนักเลขาธิการคณะรัฐมนตรีและบุคคลอื่น หรือละเมิดสิทธิหรือสร้างความรำคาญต่อผู้อื่น เช่น การตัดต่อภาพของผู้อื่นแล้วนำมาเผยแพร่ทำให้เกิดความอับอาย ลักลอบแก้ไขข้อมูลของบุคคลอื่น การแสดงความคิดเห็นดูหมิ่นผู้อื่นบนเว็บไซต์ เป็นต้น

๓.๓.๒ เพื่อหาประโยชน์ในเชิงธุรกิจเป็นการส่วนตัวหรือการพาณิชย์

๓.๓.๓ เพื่อการกระทำที่ขัดต่อความสงบเรียบร้อย หรือศีลธรรมอันดีของประชาชน เช่น การเข้าสู่เว็บไซต์ที่ไม่เหมาะสม เว็บไซต์ที่มีเนื้อหาขัดต่อชาติ ศาสนา พระมหากษัตริย์ หรือเว็บไซต์ที่เป็นภัยต่อสังคม เป็นต้น

๓.๓.๔ เพื่อการเปิดเผยข้อมูลที่เป็นความลับหรือข้อมูลที่ไม่ได้รับอนุญาตซึ่งได้มาจากองค์กร หรือผู้ที่มีสิทธิในข้อมูลดังกล่าว

๓.๔ ผู้ใช้ไม่ควรทำการดาวน์โหลดหรือใช้งานข้อมูลมัลติมีเดีย ที่มีลักษณะยึดครองช่องสัญญาณการสื่อสารข้อมูล (Bandwidth) ตลอดเวลา ผ่านอินเทอร์เน็ตในเวลาราชการ เช่น เล่นเกม/ดูหนัง/ฟังเพลงออนไลน์ ดูคลิปวีดีโอผ่านเว็บไซต์ ดาวน์โหลดซอฟต์แวร์ที่มีขนาดใหญ่ผ่านเว็บไซต์ เป็นต้น

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

๓.๖ ผู้ใช้ต้องระมัดระวัง ไม่เปิดเผยข้อมูลส่วนตัวเกินความจำเป็น เช่น เลขที่บัตรต่าง ๆ ได้แก่ บัตรประชาชน บัตรเครดิต บัตรประจำตัวผู้เสียภาษีอากร

๓.๗ ผู้ใช้ไม่ควรเปิดหรือส่งต่อ E-mail ที่ไม่ทราบแหล่งที่มาหรือไม่น่าเชื่อถือ เช่น E-mail โฆษณาขายสินค้า E-mail ให้สินเชื่อ E-mail เสนอให้รางวัล เป็นต้น

๓.๘ ผู้ใช้ต้องตรวจสอบไวรัสคอมพิวเตอร์กับไฟล์ที่แนบมาพร้อม E-mail ทุกครั้งเสมอ ถึงแม้ว่าจะมาจากผู้ส่งที่รู้จัก

๓.๙ หากผู้ใช้พบหรือสงสัยว่าเครื่องคอมพิวเตอร์ที่ใช้งานอยู่นั้นติดไวรัสคอมพิวเตอร์ ผู้ใช้จะต้องไม่ใช้บริการเชื่อมต่อระบบเครือข่ายเพื่อป้องกันการแพร่กระจายของไวรัสไปยังเครื่องคอมพิวเตอร์อื่นๆ

เอกสารประกอบปรากฏตามภาคผนวก ๓(๑) นโยบายและแนวปฏิบัติในการรักษาความมั่นคงปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี (ปี ๒๕๕๓) และ ๓(๒) มาตรการและแผนปฏิบัติการป้องกัน/แก้ไขไวรัสคอมพิวเตอร์สำนักเลขาธิการคณะรัฐมนตรี

ส่วนที่ ๗

การใช้งานจดหมายอิเล็กทรอนิกส์

(Use of Electronic Mail)

๑. วัตถุประสงค์

เพื่อกำหนดมาตรการการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail) ของผู้ใช้ของสำนักเลขาธิการคณะรัฐมนตรี โดยผู้ใช้จะต้องให้ความสำคัญและตระหนักถึงปัญหาที่เกิดขึ้นจากการใช้บริการจดหมายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต ตลอดจนการประสานงานและรับ-ส่งข้อมูลข่าวสารด้วยจดหมายอิเล็กทรอนิกส์เพื่อสนับสนุนงานตามภารกิจของสำนักเลขาธิการคณะรัฐมนตรีเป็นไปอย่างถูกต้อง สะดวก รวดเร็ว ทันสถานการณ์ มีประสิทธิภาพ และประสิทธิผล ทั้งนี้ ผู้ใช้ต้องปฏิบัติตามกฎเกณฑ์และคำแนะนำของผู้ดูแลระบบฯ ที่กำหนดไว้อย่างเคร่งครัด จะทำให้การใช้งานจดหมายอิเล็กทรอนิกส์เป็นไปอย่างปลอดภัยและมีประสิทธิภาพ

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศ เห็นชอบให้เพิ่มบัญชีรายชื่อ (User Account) ของผู้ใช้รายใหม่ เพื่อจัดเก็บลงสู่ฐานข้อมูลและใช้ในการพิสูจน์ตัวตน (Authentication) ของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ เห็นชอบให้ดำเนินการกำหนดสิทธิบัญชีรายชื่อผู้ใช้และรหัสผ่านของผู้ใช้รายใหม่ เพื่อใช้งานระบบจดหมายอิเล็กทรอนิกส์

๒.๓ นางสาวชุลีกร สุขโทน เป็นผู้ดูแลระบบฯ ทำหน้าที่ตรวจสอบและกำหนดสิทธิการเข้าถึงระบบจดหมายอิเล็กทรอนิกส์โดยกำหนดบัญชีรายชื่อผู้ใช้และรหัสผ่านให้กับผู้ใช้งาน

๓. แนวทางปฏิบัติและการควบคุมการใช้งานจดหมายอิเล็กทรอนิกส์ (E-mail)

๓.๑ แนวทางปฏิบัติการใช้งานสำหรับผู้ใช้งาน

๓.๑.๑ ผู้ใช้งานที่ต้องการขอลงทะเบียนบัญชีผู้ใช้จดหมายอิเล็กทรอนิกส์ ต้องทำหนังสือจากผู้อำนวยการสำนัก/กอง ถึงผู้อำนวยการสำนักบริหารงานสารสนเทศเพื่อดำเนินการกำหนดสิทธิบัญชีรายชื่อผู้ใช้งานรายใหม่และรหัสผ่าน

๓.๑.๒ ผู้ใช้งาน เมื่อได้รับรหัสผ่านเข้าใช้งานระบบจดหมายอิเล็กทรอนิกส์ครั้งแรก จะต้องเปลี่ยนรหัสผ่านใหม่ทันที

๓.๑.๓ ผู้ใช้งาน ไม่ควรบันทึกหรือเก็บรหัสผ่านไว้ในระบบคอมพิวเตอร์หรือรูปแบบที่ไม่ได้ป้องกันการเข้าถึงข้อมูล และไม่ควรตั้งค่าการช่วยจำรหัสผ่านอัตโนมัติ (Save Password)

๓.๑.๔ ผู้ใช้งาน ควรเปลี่ยนรหัสผ่าน ทุก ๓-๖ เดือน

๓.๑.๕ ผู้ใช้งาน ไม่ควรใช้ที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) ของผู้อื่นเพื่ออ่านหรือรับ-ส่งข้อความ ยกเว้นแต่จะได้รับความยินยอมจากเจ้าของผู้ใช้และให้ถือว่าเจ้าของจดหมายอิเล็กทรอนิกส์เป็นผู้รับผิดชอบต่อการใช้งานต่างๆ

๓.๑.๖ หลังจากการใช้งานระบบจดหมายอิเล็กทรอนิกส์เสร็จสิ้น ผู้ใช้ควรทำการบันทึกออก (Logout) ทุกครั้ง เพื่อป้องกันบุคคลอื่นเข้าใช้งานจดหมายอิเล็กทรอนิกส์

๓.๑.๗ ผู้ใช้งาน มีหน้าที่ต้องรักษาชื่อผู้ใช้ (User name) และรหัสผ่าน (Password) ไว้เป็นความลับ

๓.๑.๘ ผู้ใช้งาน ต้องระมัดระวังในการใช้จดหมายอิเล็กทรอนิกส์เพื่อไม่ให้เกิดความเสียหายต่อหน่วยงาน หรือละเมิดสิทธิ สร้างความรำคาญต่อผู้อื่น หรือผิดกฎหมาย หรือละเมิดศีลธรรมและไม่แสวงหาประโยชน์

๓.๑.๙ ผู้ใช้งาน ควรตรวจสอบตู้เก็บจดหมายอิเล็กทรอนิกส์ประจำ และควรจัดเก็บแฟ้มข้อมูลเพื่อให้จดหมายอิเล็กทรอนิกส์เหลือน้อยที่สุด ตลอดจนควรลบจดหมายอิเล็กทรอนิกส์ที่ไม่ต้องการออกจากระบบ เพื่อลดปริมาณการใช้เนื้อที่ของระบบจดหมายอิเล็กทรอนิกส์

๓.๒ แนวทางการควบคุมการใช้งานสำหรับผู้ดูแลระบบ

๓.๒.๑ ผู้ดูแลระบบ (System Administrator) ต้องกำหนดสิทธิการเข้าถึงจดหมายอิเล็กทรอนิกส์ของหน่วยงานให้เหมาะสมกับการเข้าใช้บริการและหน้าที่ความรับผิดชอบของผู้ใช้งาน รวมทั้งมีการทบทวนสิทธิการเข้าใช้งานอย่างสม่ำเสมอ เช่น การลาออก การเกษียณอายุราชการ การโอนย้าย เป็นต้น

๓.๒.๒ ผู้ดูแลระบบ ต้องกำหนดสิทธิบัญชีรายชื่อผู้ใช้รายใหม่และรหัสผ่าน สำหรับการใช้งานครั้งแรก เพื่อใช้ในการตรวจสอบตัวตนจริงของผู้ใช้ระบบจดหมายอิเล็กทรอนิกส์ของหน่วยงาน

๓..๒.๓ ผู้ดูแลระบบจะทำหนังสือแจ้งผู้ใช้งานรายใหม่ที่ขอลงทะเบียนใช้จดหมายอิเล็กทรอนิกส์ของหน่วยงานทราบถึงวิธีการเข้าใช้งานจดหมายอิเล็กทรอนิกส์ โดยมีรายละเอียด เช่น ที่อยู่ของเอกสารบนเว็บ (URL) ชื่อ-นามสกุล ชื่อผู้ใช้ (Username) รหัสผ่าน (Password) และที่อยู่จดหมายอิเล็กทรอนิกส์ (E-mail address) เป็นต้น

ส่วนที่ ๘
การจัดทำระบบสำรองและแผนเตรียมพร้อมกรณีฉุกเฉิน
(Backup System and Emergency Plan)

๑. วัตถุประสงค์

เพื่อให้สำนักเลขาธิการคณะรัฐมนตรี มีแนวทางปฏิบัติหรือมาตรการในการจัดทำระบบคอมพิวเตอร์สำรองนอกสถานที่ (Offsite Backup) และระบบสำรองข้อมูล (Backup System) เพื่อป้องกันข้อมูลสูญหาย เพิ่มความมั่นคงปลอดภัยให้แก่ระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ในกรณีฉุกเฉินหรือสถานการณ์ไม่ปกติหรือมีภัยพิบัติเกิดขึ้น สำนักเลขาธิการคณะรัฐมนตรีจะยังคงให้บริการระบบสารสนเทศที่สำคัญได้อย่างต่อเนื่องด้วยระบบ Offsite Backup ที่สามารถทำงานแทนระบบหลักได้ทันทีหรือในเวลาอันสั้น และสามารถกู้คืนระบบสารสนเทศที่มีความสำคัญระดับรองจาก Backup System ภายในระยะเวลาที่เหมาะสม

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ เป็นผู้ดูแลระบบการสำรองระบบสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี ยกเว้นระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๒ ผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี เป็นผู้ดูแลระบบการสำรองระบบสารสนเทศตามภารกิจด้านคณะรัฐมนตรี

๒.๓ เจ้าหน้าที่ผู้ทำการสำรองข้อมูลระบบสารสนเทศแต่ละระบบ ปรากฏตามเอกสารแผนเตรียมพร้อมกรณีฉุกเฉิน

๓. การบริหารจัดการสำรองข้อมูลมีแนวทางปฏิบัติ ดังนี้

๓.๑ มีการคัดเลือกและกำหนดประเภทของข้อมูลเพื่อจัดทำระบบสำรองที่เหมาะสมและอยู่ในสภาพพร้อมใช้งาน ทั้งนี้ สำหรับระบบข้อมูลที่มีความสำคัญให้มีระบบสำรองที่สามารถทำงานแทนระบบหลักได้ทันที ส่วนระบบข้อมูลที่มีความสำคัญระดับรองให้กำหนดความถี่ในการสำรองข้อมูลไว้สัปดาห์ละครั้ง

๓.๒ มีการบันทึกข้อมูลที่เกี่ยวข้องกับกิจกรรมการสำรองข้อมูล ได้แก่ ผู้ดำเนินการ วัน/เวลา ชื่อข้อมูลที่สำรอง สำเร็จ/ไม่สำเร็จ เป็นต้น

๓.๓ ชนิดและความถี่ในการสำรองข้อมูลต้องสอดคล้องกับความสำคัญของข้อมูล เช่น ถ้าปริมาณข้อมูลที่สำนักเลขาธิการคณะรัฐมนตรีสามารถสูญเสียได้มากที่สุดไม่เกิน ๑ วัน ก็จะทำการสำรองข้อมูลอย่างน้อยวันละ ๑ ครั้ง เป็นต้น

๓.๔ สำนักเลขาธิการคณะรัฐมนตรีจัดเก็บข้อมูลที่สำรองไว้นอกสถานที่ ระยะทางระหว่างสถานที่ที่จัดเก็บข้อมูลสำรองกับสำนักเลขาธิการคณะรัฐมนตรีห่างกันเพียงพอเพื่อไม่ให้ส่งผลกระทบต่อ

ข้อมูลที่จัดเก็บไว้นอกสถานที่นั้นในกรณีที่เกิดภัยพิบัติ หรือกรณีสถานการณ์บ้านเมืองไม่ปกติ เช่น มีการชุมนุมทางการเมืองที่ปิดล้อมสถานที่ทำงาน เป็นต้น

๓.๕ มีการป้องกันทางกายภาพอย่างเพียงพอต่อสถานที่สำรอง (Backup site) ที่ใช้จัดเก็บข้อมูลนอกสถานที่ และสำหรับระบบสารสนเทศที่มีความสำคัญยิ่งจะมีมาตรการป้องกันสถานที่ที่ใช้จัดเก็บข้อมูลนอกสถานที่ที่เข็มแข็งเหมือนกับมาตรการที่ใช้กับสำนักงานหลัก (Main site)

๓.๖ มีการทดสอบความเชื่อถือได้ของสื่อบันทึกข้อมูลสำรองอย่างสม่ำเสมอ (ทุก ๆ ครั้งที่มีการสำรองข้อมูล) เพื่อตรวจสอบว่ายังคงสามารถเข้าถึงข้อมูลได้ตามปกติหรือไม่

๓.๗ มีการจัดทำขั้นตอนปฏิบัติสำหรับการกู้คืนข้อมูลที่เสียหายจากข้อมูลที่ได้สำรองเก็บไว้

๓.๘ มีการตรวจสอบและทดสอบประสิทธิภาพและประสิทธิผลของขั้นตอนปฏิบัติในการกู้คืนข้อมูลอย่างน้อยปีละสี่ครั้ง

๓.๙ มีการทดสอบข้อมูลที่ได้สำรองเก็บไว้เพื่อดูว่าข้อมูลเหล่านั้นยังสามารถใช้งานได้อย่างน้อยปีละสี่ครั้ง

๓.๑๐ มีการตรวจสอบว่าข้อมูลทั้งหมดของระบบงานสำคัญได้รับการสำรองไว้อย่างครบถ้วน เช่น ซอฟต์แวร์ระบบ ซอฟต์แวร์สำหรับระบบงาน ข้อมูลคอนฟิกกูเรชั่น ฐานข้อมูล เป็นต้น

๓.๑๑ มีการกำหนดระยะเวลาสำหรับการจัดเก็บข้อมูลสำคัญแต่ละประเภท กล่าวคือ ต้องจัดเก็บข้อมูลไว้ให้ถึงตามระยะเวลาที่กำหนดไว้นั้น

๓.๑๒ มีการจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน กรณีที่ไม่สามารถดำเนินการด้วยวิธีการทางอิเล็กทรอนิกส์

เอกสารประกอบปรากฏตามภาคผนวก ๓(๙) แผนปฏิบัติการรักษาความปลอดภัยระบบเทคโนโลยีสารสนเทศของสำนักเลขาธิการคณะรัฐมนตรี และรายละเอียดขั้นตอนการสำรองและกู้คืนระบบสารสนเทศ

ส่วนที่ ๙

การตรวจสอบและประเมินความเสี่ยง

(Checking and Risk Assessment)

๑. วัตถุประสงค์

เพื่อให้การบริหารจัดการการตรวจสอบและประเมินความเสี่ยงและป้องกันผลกระทบที่มีต่อความมั่นคงปลอดภัยด้านระบบสารสนเทศเป็นไปอย่างมีประสิทธิภาพ สามารถควบคุมความเสี่ยงด้านระบบสารสนเทศได้อย่างดี

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศ เห็นชอบการควบคุมความเสี่ยงด้านระบบสารสนเทศและตรวจข้อมูลการรายงานความเสี่ยง ประจำปีของสำนักบริหารงานสารสนเทศ

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี ควบคุมให้ปฏิบัติตามการควบคุมความเสี่ยง และเป็นผู้รายงานความเสี่ยงประจำปีของสำนักบริหารงานสารสนเทศ

๒.๓ ผู้อำนวยการกลุ่มตรวจสอบภายใน เป็นผู้ตรวจสอบภายในของสำนักเลขาธิการคณะรัฐมนตรี

๒.๔ เจ้าหน้าที่ของกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศและกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี เป็นตัวแทนของสำนักบริหารงานสารสนเทศในคณะทำงานบริหารความเสี่ยงและควบคุมภายในของสำนักเลขาธิการคณะรัฐมนตรี

๓. การบริหารการตรวจสอบและประเมินความเสี่ยง มีแนวทางการปฏิบัติ ดังนี้

๓.๑ สำนักเลขาธิการคณะรัฐมนตรีจัดให้มีการตรวจสอบและประเมินความเสี่ยงที่อาจเกิดขึ้นกับระบบเทคโนโลยีสารสนเทศปีละ ๑ ครั้ง โดยให้สำนักบริหารงานสารสนเทศระบุความเสี่ยง สาเหตุของความเสี่ยงและผลกระทบที่เกิดขึ้นจากความเสี่ยง ให้สอดคล้องตามแผนบริหารความเสี่ยงของสำนักเลขาธิการคณะรัฐมนตรี

๓.๒ จัดทำมาตรการในการควบคุมความเสี่ยงที่มีอยู่ในปัจจุบัน และมาตรการในภาวะฉุกเฉิน

๓.๓ ให้จัดทำรายงานการควบคุมความเสี่ยงประจำปี

๓.๔ หากมีความเสี่ยงที่เกิดขึ้นใหม่ ให้มีการจัดทำรายงานและวิเคราะห์การแก้ไขความเสี่ยง เพื่อไม่ให้เกิดขึ้นซ้ำอีก

๓.๕ ให้มีการทบทวนประเมินความเสี่ยงอย่างน้อยปีละ ๑ ครั้ง

๓.๖ ให้มีการประเมินการควบคุมด้านระบบสารสนเทศโดยผู้ตรวจสอบภายในของสำนักเลขาธิการคณะรัฐมนตรีเป็นประจำทุกปี

เอกสารประกอบปรากฏตามภาคผนวก ๓(๑๐) แบบรายงานการบริหารความเสี่ยง

ส่วนที่ ๑๐

การสร้างความรู้ความเข้าใจในการใช้งานระบบสารสนเทศ

๑. วัตถุประสงค์

เพื่อสร้างความรู้ ความเข้าใจในการใช้งานระบบสารสนเทศให้กับผู้ใช้งานของสำนักเลขาธิการคณะรัฐมนตรี เพื่อให้เกิดความตระหนัก ความเข้าใจถึงภัยและผลกระทบที่เกิดจากการใช้งานระบบสารสนเทศ

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศเห็นชอบหลักสูตรการจัดฝึกอบรม และเอกสารเผยแพร่ความรู้

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศเป็นผู้ควบคุมการจัดฝึกอบรม/คู่มือการอบรม/เอกสารเผยแพร่ความรู้

๒.๓ เจ้าหน้าที่ที่เกี่ยวข้องจัดทำคู่มือการอบรม เอกสารเผยแพร่ความรู้และเป็นวิทยากร

๓. การบริหารการสร้างความรู้ความเข้าใจในการใช้ระบบสารสนเทศ

๓.๑ จัดให้มีการฝึกอบรมการใช้งานระบบสารสนเทศของหน่วยงานทุก ๆ ปี

๓.๒ จัดให้มีการทำคู่มือการใช้งานระบบสารสนเทศ เอกสารเผยแพร่ความรู้ที่เกี่ยวข้อง และเผยแพร่ทางอินทราเน็ตของสำนักเลขาธิการคณะรัฐมนตรี

๓.๓ จัดให้มีการฝึกอบรม/เผยแพร่ความรู้ความเข้าใจเกี่ยวกับการรักษาความมั่นคงปลอดภัยด้านสารสนเทศ เพื่อสร้างความตระหนักถึงความสำคัญของการปฏิบัติงานของผู้ใช้งาน

ส่วนที่ ๑๑
การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์

๑. วัตถุประสงค์

เพื่อให้ความสำคัญต่อทรัพย์สินทางปัญญาของซอฟต์แวร์ต่าง ๆ รวมทั้งการพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอก (Outsource Software development)

๒. บทบาทและความรับผิดชอบ

๒.๑ ผู้อำนวยการสำนักบริหารงานสารสนเทศเห็นชอบการใช้งานและการจัดเก็บซอฟต์แวร์ รวมทั้งการพิจารณาอนุญาตการนำซอฟต์แวร์ไปใช้ที่อื่น

๒.๒ ผู้อำนวยการกลุ่มพัฒนาระบบเทคโนโลยีสารสนเทศ และผู้อำนวยการกลุ่มเทคโนโลยีสารสนเทศคณะรัฐมนตรี ควบคุมการติดตั้งใช้งาน และจัดเก็บซอฟต์แวร์ รวมทั้งซอร์สโค้ดที่หน่วยงานจ้างหน่วยงานภายนอกพัฒนา

๒.๓ เจ้าหน้าที่ที่เกี่ยวข้องติดตั้งการใช้งานซอฟต์แวร์ที่มีลิขสิทธิ์

๓. การบริหารจัดการซอฟต์แวร์และลิขสิทธิ์

๓.๑ ให้ติดตั้งซอฟต์แวร์ที่มีลิขสิทธิ์ถูกต้องกับผู้ใช้งาน ห้ามมิให้ผู้ใช้งานทำสำเนา เปลี่ยนแปลง แก้ไขเพื่อนำไปใช้งานที่อื่นยกเว้นมีความจำเป็นจะต้องนำไปใช้งานจะได้รับอนุญาตจากผู้อำนวยการสำนักบริหารงานสารสนเทศ

๓.๒ ห้ามมิให้ผู้ใช้งานติดตั้งหรือใช้งานซอฟต์แวร์ที่ไม่มีลิขสิทธิ์ หากมีการตรวจสอบพบความผิดฐานละเมิดลิขสิทธิ์ให้ถือว่าเป็นความผิดส่วนบุคคล ผู้ใช้งานจะต้องรับผิดชอบแต่เพียงผู้เดียว

๓.๓ การพัฒนาซอฟต์แวร์โดยหน่วยงานภายนอกนั้น จะต้องจัดให้มีการควบคุมการพัฒนาซอฟต์แวร์และพิจารณาว่าใครจะเป็นผู้มีสิทธิ์ในทรัพย์สินทางปัญญาสำหรับซอร์สโค้ดที่ได้จากการพัฒนาซอฟต์แวร์โดยผู้รับจ้างจากภายนอกหน่วยงาน